

Міністерство освіти і науки України
Хмельницький національний університет



ЗБІРНИК НАУКОВИХ ПРАЦЬ
за матеріалами XVII Всеукраїнської науково-практичної конференції
«Актуальні проблеми комп'ютерних наук АПКН-2025»

14-15 листопада 2025

Хмельницький 2025

УДК 004:37:001:62

Збірник наукових праць за матеріалами XVII Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2025». Хмельницький. 2025. 500с.

У збірнику наукових праць подані перспективні практичні розробки аспірантів, студентів та здобувачів в області сучасних інформаційних технологій. Розглянуто актуальні проблеми комп'ютерних наук, комп'ютерної інженерії, прикладної математики й інженерії програмного забезпечення, приведено ряд робіт по впровадженню інформаційних технологій у виробництво та управління. Висвітлено перспективні розробки сучасних систем пошуку, обробки й захисту інформації, медійних та комунікаційних системи.

УДК 004:37:001:62

Матеріали конференції відтворені з авторських оригіналів, друкуються в авторській редакції та наведені в алфавітному порядку прізвищ авторів. При макетуванні можливі незначні зміни компоновки контенту авторських оригіналів. Відповідальність за якість та зміст публікацій несе автор.

Участь у конференції та складові всіх її етапів (розгляд праць, перевірка на плагіат, макетування, публікація збірника наукових праць та видача сертифікатів) є безкоштовними для всіх учасників. Оргкомітет конференції висловлює подяку учасникам конференції та сподівається на подальшу співпрацю.

З питань проведення конференції та подальшого обміну інформацією звертатись на e-mail конференції: apkt.khnu@gmail.com

АКТУАЛЬНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК - 2025

XVII Всеукраїнська науково-практична конференція

Метою конференції є висвітлення актуальних проблем комп'ютерних наук, інформатики та інформаційних технологій.

Робочі мови конференції:

українська, англійська

СЕКЦІЇ КОНФЕРЕНЦІЇ:

1. Комп'ютерні науки, штучний інтелект та прикладні інформаційні технології.
2. Комп'ютерна інженерія та системи захисту інформації.
3. Математичне моделювання та інженерія програмного забезпечення
4. Телерадіокомунікації, медійні та комунікаційні системи.
5. Проблеми впровадження інформаційних технологій у виробництво та управління.

СПИСОК ОРГАНІЗАЦІЙ,

ПРЕДСТАВНИКИ ЯКИХ БРАЛИ УЧАСТЬ У РОБОТІ

КОНФЕРЕНЦІЇ:

Донбаська державна машинобудівна академія

Інститут кібернетики імені В. М. Глушкова НАН України

Кам'янський енергетичний фаховий коледж

Київський національний університет імені Т. Г. Шевченка

Національного аерокосмічного університету імені М. Є. Жуковського

«Харківський авіаційний інститут»

Національний технічний університет «Харківський політехнічний інститут»

Сумський державний університет

Харківський національний університет радіоелектроніки

Хмельницький національний університет

Хмельницький фаховий економіко-технологічний коледж УЕП

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ:

СИНЮК О. М. – голова оргкомітету, проректор Хмельницького національного університету з наукової роботи, доктор технічних наук, професор.

ГОВОРУЩЕНКО Т. О. – заступник голови оргкомітету, декан факультету інформаційних технологій Хмельницького національного університету, доктор технічних наук, професор.

БАРМАК О. В. – заступник голови оргкомітету, завідувач кафедри комп'ютерних наук Хмельницького національного університету, доктор технічних наук, професор.

САВЕНКО О. С. – професор кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету, доктор технічних наук, професор.

ВИСОЦЬКА О. В. – завідувач кафедри радіоелектронних та біомедичних комп'ютеризованих засобів і технологій Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», доктор технічних наук, професор.

ЛАВРОВ Є. А. – доктор технічних наук, професор (Сумський державний університет).

ТІМОФЄЄВА Л. В. – відповідальна за студентську науково-дослідну роботу ХНУ.

МАЗУРЕЦЬ О. В. – секретар конференції, доцент кафедри комп'ютерних наук Хмельницького національного університету, кандидат технічних наук, доцент.

МОЛЧАНОВА М. О. – секретар конференції, старший викладач кафедри комп'ютерних наук Хмельницького національного університету, доктор філософії з комп'ютерних наук.

КОНТАКТНА ІНФОРМАЦІЯ:

e-mail для листування: apkt.khnu@gmail.com

ЗМІСТ

Андрощук В.І., Молчанова М.О.

Трансформерне виявлення суб'єктів кібербулінгу за текстовими повідомленнями 15

Бабасєвський В.М., Дика В.В., Муляр І.В.

Метод захисту вебзастосунків на основі інтелектуального аналізу трафіку 20

Басистий В.А., Городецька А.О., Чешун В.М., Чешун О.В.

Фізичні топології розгортання агентної системи моніторингу мережевого трафіку IoT 23

Безprozвана Ю.Г., Шурина М.О., Мазурець О.В.

Нейромережева оцінка стану будівель за візуальними даними..... 28

Бербец Д.В., Петляк Н.С.

Аналіз застосування технологій штучного інтелекту в системах моніторингу кіберзагроз 33

Благодир І.А., Гнатчук Є.Г.

Інформаційна система підтримки управління державними інфраструктурними проектами на основі хмарних технологій 36

Бондар О.А., Пасічник О.А., Скрипник Т.К.

Метод діагностики захворювань за описом симптомів на основі рекурентних нейронних мереж 39

Бондар О.П., Пасічник О.А., Скрипник Т.К., Петровський С.С.

Метод виявлення шахрайських транзакцій у фінансових операціях з застосуванням згорткових нейронних мереж..... 42

Боярчук І.О., Молчанова М.О.

Підхід до нейромережевого виявлення мови ворожнечі у зашумлених текстових повідомленнях 46

Ваховська В.М., Праворська Н.І.

СКЕМА: скетч-орієнтований адаптер для параметроефективного тонкого налаштування великих мовних моделей..... 52

Відельський Я.В., Кльоц Ю.П., Піснячевський Я.В., Рудий Р.С.

Виявлення прихованих каналів передачі у вихідному трафіку публічних мереж 57

Вім Р.В.

Практична реалізація методу виявлення цифрового виснаження за аналізом цільових об'єктів множини повідомлень людини 61

Вовк С.В., Радюк П.М., Скрипник Т.К.

Метод інтерпретування результатів виявлення фейкових новин за великою мовною моделлю..... 68

Волколуп Б.А., Пасічник О.А., Скрипник Т.К.

Метод класифікації настроїв у текстах соціальних мереж на основі рекурентних нейронних мереж..... 72

Вонсович Б.А., Багрій Р.О., Пасічник О.А., Скрипник Т.К.

Метод виявлення неоднозначностей у вимогах до програмного забезпечення з використанням великих мовних моделей..... 75

Гнатюк П.В., Залуцька О.О.

Підхід до визначення психоемоційної тональності україномовних повідомлень у соціально-орієнтованих сервісах..... 79

Горбатюк І.В., Форкун Ю.В.

Метод проектування програмного забезпечення на основі агентно-орієнтованої архітектури для багатокomпонентних програмних систем 87

Гордієнко Є.О.

Аналіз інструментів та засобів формалізації вимог при проектуванні та розробці програмного забезпечення 89

Грінчук М.О., Залуцька О.О.

Інтелектуальна система діагностування хвороб листя томата за нейромережевим аналізом фотозображень 92

Гуляєв Н.Ю.

Методи криптографічного захисту інформації в сучасних комп'ютерних системах..... 98

Держак В.В., Мазурець О.В.

Проектування інтелектуальної системи класифікації побутового сміття за візуальними даними 101

Дидо Р.А., Собко О.В.

Метод побудови аудіопотоку доповненої реальності для покращення орієнтації та безпеки людей із проблемами зору 106

Добрицький І.Д., Юрейко К.Ю., Міліція Б.М., Дзюлій В.М.

Модель інформаційного забезпечення подання предметної області 111

Жураковська Д.О.

Застосування алгоритму Isolation Forest для побудови системи виявлення вторгнень в IoT-мережі 116

Загурський Б.З., Манзюк Е.А., Скрипник Т.К.

Метод аналізу тональності відгуків клієнтів з використанням гібридної моделі машинного навчання 118

Задорожний М.О., Крак Ю.В.

Підвищення генералізації моделі розпізнавання дактилем української жестової мови в умовах обмежених даних 124

Залуцька О.О., Скрипльонов С.Д.

Проектування інформаційної системи семантичної обробки текстів для визначення тональності 127

Зарицька О.А., Лада М.Р., Чешун В.М., Чешун Д.В.

Перехід від комплексних систем захисту інформації до авторизації з безпеки інформаційних систем 137

Ісаєв Т.С., Лисенко С.М., Лисенко Н.С.

Інтелектуальна адаптивна інформаційна технологія автоматичного оновлення моделей виявлення загроз в комп'ютерних системах 141

Ільчишин В.В., Манзюк Е.А., Скрипник Т.К.

Метод виявлення шахрайських банківських операцій з використанням машинного навчання 145

Ішук-Яшурина С.Я., Кліменко В.І., Мазурець О.В.

Пояснений підхід до нейромережевої класифікації діабетичної ретинопатії за зображеннями очного дна 151

Кадинська В.Д., Молчанова М.О.

Адаптований нейромережевий підхід до виявлення фрагментів будівельних відходів на зображеннях реальних сцен 155

Казмірчук Я.М., Микитюк М.О., Мазурець О.В.

Алгоритм масштабування зображень принтів нейромережевими засобами для трафаретного друку 163

Канішев В.О., Мельников О.Ю.

Вдосконалення об'єктно-орієнтованої моделі програмного забезпечення для оцінки якості фонового оформлення сайтів для людей із дальтонізмом 168

Коржан М.М., Підченко С.К.

Інфокомунікаційна система екзаменаційно-тренінгового центру іноземних мов .. 176

Катревич О.Б.

Метод інтеграції RAG-компонентів у мультиагентні системи 181

Кашиперук Т.Р., Мазурець О.В.

Метод визначення мовно-детермінованого індексу суб'єктивного благополуччя з використанням NLP 184

Кириченко О.М.

Інтерпретована нейронна мережа для класифікації МРТ-зображень з генерацією клінічно релевантних пояснень 195

Коваль М.О., Підченко С.К.

Антенна решітка GPS-сигналу на базі спіральних антен 199

Коваль О.В., Олексюк Д.А., Чешун Д.В., Чешун В.М.

Застосування технологій DevSecOps для зменшення вразливостей програмного забезпечення 203

Кок І.А., Поліщук Д.С., Кліменко В.І., Бармак О.В.

Нейромережева система автоматизованого контролю за тютюнопалінням у публічних місцях..... 208

Колесніков В.Р., Капустян М.В.

Порівняльний аналіз рівнів обфускації .NET-коду 217

Коркунда Н.С., Манзюк Е.А., Скрипник Т.К.

Метод класифікації резюме за професійними категоріями з використанням машинного навчання 222

Красникова Д.П.

Захист даних у хмарних обчисленнях 225

Красюк В.К., Резнікова М.А., Бойцун Д.О., Тимош В.Л.

Формалізація структури ZigBee-мереж та атак графовими множинами 228

Крива Д.О., Кліменко В.І.

Методологія створення набору тегів для формалізованого опису моделей формування тестових завдань 232

Кузь М.М.

Аналіз існуючих рішень захисту користувачів Wi-Fi-мереж від підроблених точок доступу 241

Кутній М.С., Литвинова Є.І.

Шумочутливий Adam для гібридних квантових моделей 244

Кухар Т.Г., Собко О.В.

Розробка чатботу для самооцінки соціальної тривожності з використанням засобів машинного навчання 247

Куцький А.С., Павлова О.О.

Аналіз сучасних напрямків досліджень у сфері периферійних обчислень 251

Левченко А.С., Кліменко В.І.

Метод формування GIFT-файлів для середовища Moodle для автоматизованого формування тестових завдань 255

Лисенко С.М., Качур А.В.

Метод синтезу резильєнтних архітектур систем віртуальної та доданої реальності 263

Лісовий В.В., Мішан В.В.

Мережева архітектура розумного міста з використанням IoT-рішень 267

Лянськорунський К.О., Молчанова М.О.

Алгоритм сегментації принтів засобами штучного інтелекту для шовкографії 269

Мазурець О.В., Віт Р.В.

Модель виявлення цифрової втоми у текстовому контенті засобами штучного інтелекту 274

Малярчук Н.В., Молчанова М.О.

Підхід до нейромережевого виявлення ознак насильства гендерного спрямування за повідомленнями соціально-орієнтованих сервісів 277

Мараховський Р.К., Дарачюс Є.Є, Джулій В.М.

Алгоритм виявлення атак в бездротових мережах передачі даних 280

Масловська В.В., Залуцька О.О.

Особливості розробки та тестування інтелектуальної системи визначення тональності в україномовних повідомленнях 284

Мацюк Д.В., Кустовський Р.С.

Метод оцінювання якості програмного забезпечення на основі диференціального тестування функціональної поведінки 293

Мельник М.М., Дзіблюк К.С., Навроцька К.В., Чешун В.М.

Аналіз існуючих рішень для розслідування кіберінцидентів критичної інфраструктури України..... 297

Мізін Д.В., Мазурець О.В.

Нейромережевий підхід до раннього виявлення ознак аутизму за фотозображенням..... 302

Молчанова М.О., Мурава В.В.

Виявлення шаблонів веб-пропаганди нейромережевими методами 307

Морозов А.В.

Використання штучного інтелекту у системах кібербезпеки 314

Москальчук С.О., Яшина О.М.

Удосконалення метрик якості програмного забезпечення шляхом врахування історії змін коду та дефектів у системах контролю версій 317

Назарчук В.С., Лавренюк О.В., Якушевський Р.В., Стецюк М.В.

Метод виявлення аномалій на основі статистичних медіаних значень 321

Нич А.А., Бедратюк Л.П.

Методика автоматизації виробничих процесів з використанням сучасних інструментів на базі штучного інтелекту 326

Овчарук О.М.

Модель аналізу психічного стану громадян із посттравматичним стресовим розладом за повідомленнями 330

Павлова О.О., Погорєлов Д.В.

Інтелектуальна інформаційна система рекомендацій у середовищі
онлайн-навчання 335

Павлова О.О., Слободзян Р.О.

Порівняльний аналіз AWS, Microsoft Azure та Google Cloud для роботи
Docker-оркестрованих Node.js API у регіонах, найближчих до України..... 337

Папка С.Ф., Праворська Н.І.

Веб-застосунок для персонального обліку фінансів..... 339

Повстенко Р.О.

Технології розробки інформаційних систем 343

Приймак М.О., Праворська Н.І.

Інтерактивна веб-система для підбору кінотворів на основі стану
користувача «MOVI.FLOW ER»..... 346

П'явкін В.О., Лисенко С.М.

Метод та інформаційна система виявлення підозрілих об'єктів у громадських
місцях 350

Разовий О.О., Пивовар О.С., Голевич О.Б.

Модель системної завади для багатоканальних хаотичних систем
передачі даних..... 354

Ратушняк М.В., Рябчук І.С, Муляр І.В.

Аналіз управління ресурсами кіберзахисту в умовах невизначеності та
асиметрії інформації шляхом адаптивної пріоритезації заходів захисту 358

Рибак А.М., Лисенко С.М, Лисенко Н.С.

Абстрактна модель віртуальної реальності 361

Рисований О.М.

Розробка алгоритму отримання псевдовипадкової послідовності на основі
реєстру зузуу 365

Романов Б.А., Бармак О.В., Багрій Р.О., Скрипник Т.К.

Метод класифікації програмних вимог з використанням великих мовних
моделей (LLM) 368

Савчук В.В., Гартрамф М.С., Шкребета В.С., Муляр І.В.

Метод захисту вебзастосунків на основі інтелектуального аналізу трафіку..... 373

Сиротенко Д.А., Троц В.В., Анікін В.А.

Ризики використання штучного інтелекту з перспективи кібербезпеки та захисту інформації 377

Скрипнюк О.Ю., Манзюк Е.А., Багрій Р.О., Петровський С.С.

Метод виявлення трасувальних зв'язків між вимогами та програмним кодом із використанням великих мовних моделей 380

Соколовський В.С., Манзюк Е.А.

Метод класифікації патологій листя рослин на основі згорткових нейронних мереж 385

Старостенко К.В.

Аналіз ефективності методів машинного навчання для виявлення мережових атак типу DDoS 390

Стецюк П.П., Форкун Ю.В.

Метод удосконаленого модульного проєктування агентно-орієнтованих програмних систем з підтримкою розширюваності та повторного використання . 393

Тимофієв І.А., Мазурець О.В.

Нейромережевий підхід до виявлення депресивних патернів за аналізом текстового контенту цифрових сервісів у закладах освіти 395

Тростянецький Н.О., Кльоц Ю.П., Калій К.В. Откидач В.В.

Виявлення атак типу «блокування IP через NAT» в публічних мережах 405

Трохимчук О.В., Пасічник О.А., Поплавська О.А., Міхалевський В.Ц.

Підхід до оцінювання відповідності хештегів коротким текстам засобами NLP ... 409

Філюк Є.В., Джулій В.М.

Метод безпеки криптоактивів на основі технології багатосторонніх обчислень ... 413

Футорний Р.В., Медведчук Н.К.

Дослідження виявлення кібератак в Агро-ІОТ з використанням аналізу енергоспоживання 417

Ціцьвіра І.О., Радюк П.М., Скрипник Т. К.

Метод агентно-орієнтованого аналізу ринку криптовалют з використанням великих мовних моделей 421

Червончук І.С.

Аналіз методів та засобів виявлення логів у програмному забезпеченні 425

Чешун В.М.

Світові практики регулювання та стандартизації кібербезпеки інтернету речей..... 428

Чорненко С.В., Джулій В.М.

Метод взаємодії квантової апаратури з користувальницькими системами захисту 433

Чумак М.В., Мазурець О.В.

Пояснення виявлення фішингових повідомлень нейромережевими засобами в системах кіберзахисту 437

Шаповалов О.О., Петренко Ю.О.

Архітектура безпечних комп'ютерних мереж..... 441

Шашок Д.А., Микитюк М.О., Кліменко В.І.

Інтелектуальна система для нейромережевого виявлення гендерної дискримінації у соціально-орієнтованих сервісах 444

Швець Б.А., Праворська Н.І.

Онлайн сервіс для редагування документів з можливістю командної роботи у реальному часі..... 453

Шиманська С.А., Мельников О.Ю.

Порівняльний аналіз математичних методів для розрахунку передбачення обірання освітніх дисциплін здобувачами освіти 457

Шимко А.С., Зваричук М.Д., Собко О.В.

Дослідження ефективності методу виявлення стресу на основі аналізу візуальних характеристик обличчя за фото нейромережевими засобами 462

Шуневич В.І., Павлова О.О.

Сучасні тенденції розвитку апаратного забезпечення персональних комп'ютерів 473

Шурина М.О., Мазурець О.В.

Нейромережеве короткострокове прогнозування траєкторій БПЛА у відеопотоці на основі трансформерної архітектури 475

Юрченко Д.Ю., Мазурець О.В.

Метод інтерпретації результатів нейромережевого виявлення ознак маніпулятивних технік за емоційною тональністю текстів 485

Юрчук Р.В., Праворська Н.І.

Інструмент візуального створення та редагування користувацьких редакторів
для ігрового рушія Unity 494

Яшина В.А.

Проектування програмних систем для інтернету речей..... 498

УДК 004.8

Андрощук В.І., Молчанова М.О.

Хмельницький національний університет

ТРАНСФОРМЕРНЕ ВИЯВЛЕННЯ СУБ'ЄКТІВ КІБЕРБУЛІНГУ ЗА ТЕКСТОВИМИ ПОВІДОМЛЕННЯМИ

Розглянуто підхід до трансформерного виявлення кібербулінгу, орієнтований на інтерпретоване визначення не лише факту агресивної комунікації, а й суб'єктів впливу та спрямованості взаємодії. На першому рівні трансформерна модель класифікує повідомлення щодо наявності ознак кібербулінгу, після чого за пороговим значенням активується модуль залежнісного синтаксичного аналізу та семантико-рольової інтерпретації. Для навчання використано спеціалізовані корпуси кібербулінгу зі збалансованим розподілом класів і стилістичною різноманітністю даних. Реалізований прототип інтелектуальної системи забезпечує автоматизоване виявлення кібербулінгу та візуалізацію рольових зв'язків, що підвищує пояснюваність результатів і придатність рішення до інтеграції в системи цифрової безпеки.

The paper presents the transformer-based approach to cyberbullying detection focused on interpretable identification of both aggressive communication and its underlying actors and targets. At the first level, a transformer model classifies messages for the presence of cyberbullying indicators; once a probability threshold is exceeded, a dependency-based syntactic and semantic role analysis. The neural component is trained on specialized cyberbullying corpora combining balanced class distributions with stylistically diverse data. The implemented prototype of an intelligent system provides automated cyberbullying detection and visualization of role relations, improving the explainability of results and supporting integration into digital safety and social media monitoring systems.

Агресивна взаємодія в цифрових комунікаціях дедалі частіше набуває непрямих форм, у яких кібербулінг проявляється не стільки через відверто образливу лексику, скільки через серії натяків, приниження, остракізм і рольові «підсилювачі» конфлікту [1, 2]. Більшість наявних систем обмежуються бінарною класифікацією «токсично / не токсично» на рівні окремих повідомлень і не відтворюють суб'єктну структуру дискурсу: хто ініціює агресію, на кого вона спрямована, хто її підтримує або транслює далі [3]. Це знижує інтерпретованість результатів автоматизованого моніторингу та ускладнює практичне використання моделей у модераторських і превентивних системах [4].

Отож, зростання обсягів цифрової комунікації та перенесення значної частини соціальної взаємодії у мережеві середовища зумовлює необхідність автоматизованого моніторингу проявів кібербулінгу [5, 6]. У соціально-орієнтованих сервісах агресивні повідомлення поширюються з високою швидкістю,

формуючи середовище підвищеного ризику для вразливих груп, особливо підлітків [7]. Традиційні методи модерації виявляються недостатньо ефективними через масштабність потоків даних [8], багатомовність [9], контекстуальну мінливість [10] і постійну еволюцію мовних патернів [11], у яких агресія може маскуватися під сарказм, іронію чи непрямі форми впливу [12]. Тому сучасні дослідження у сфері Natural Language Processing орієнтовані на побудову більш гнучких і семантично чутливих моделей [13], здатних виявляти не лише факт вербальної агресії [14, 15], а й структуру комунікативної взаємодії [16].

У цьому контексті трансформерні моделі демонструють суттєві переваги завдяки механізму уваги, що дає змогу моделі фокусуватися на ключових словах і міжсловних залежностях, релевантних для інтерпретації агресивної поведінки [17]. На відміну від класичних підходів, що ґрунтувалися на частотних ознаках або поверхневій лінгвістичній структурі, трансформери здатні враховувати широкий контекст висловлювання й моделювати латентні семантичні зв'язки, характерні для складних соціально-комунікативних патернів [18]. Це забезпечує підвищену точність розпізнавання прихованих або непрямих форм кібербулінгу, а також сприяє кращій генералізації на даних з різних платформ [19].

Актуальною науковою задачею є також ідентифікація суб'єктів кібербулінгу – визначення того, хто є ініціатором агресивної дії і хто зазнає її впливу [20]. Таке завдання виходить за межі класичної бінарної класифікації й потребує глибшого аналізу синтаксичних та семантичних структур тексту. Сучасні NLP-підходи інтегрують трансформери з методами залежнісного аналізу, семантико-рольового розподілу та векторизації іменованих сутностей, що уможливорює побудову пояснюваних структур взаємодії. Виявлення ролей учасників є критичним для застосування в освітніх або соціальних системах, де реакція на інцидент має базуватися не лише на самому факті агресії, а й на коректному визначенні її джерела та адресата [21].

Суттєвий потенціал для розвитку мають і мультимодальні підходи, які поєднують текстовий аналіз з метаданими, реакціями користувачів, часовими патернами та специфікою платформи. Такі системи дозволяють враховувати ширший контекст комунікації, що часто є ключовим для точного розрізнення конфлікту, іронії та кібербулінгу [22]. Додатково, перспективним є застосування моделей із вбудованими пояснювальними механізмами, здатних генерувати прозорі аргументи щодо виявленої агресії, що є необхідною умовою інтеграції таких систем у регуляторні та безпекові платформи.

Загалом, розвиток NLP у сфері виявлення кібербулінгу визначається потребою у моделях, що поєднують високу точність, контекстну чутливість та пояснюваність. Трансформерні архітектури відкривають можливість створення комплексних систем, здатних аналізувати не лише зміст повідомлення, а й структуру комунікативної взаємодії між користувачами. Такі підходи формують потенційну основу для інтегрованих систем цифрової безпеки, орієнтованих на

раннє виявлення, превенцію та аналіз ризикової комунікації у масштабних онлайн-платформах.

Метою роботи є підвищення інтерпретованості автоматизованого виявлення кібербулінгу шляхом переходу від виявлення самого факту агресивної комунікації до ідентифікації суб'єктів впливу та спрямованості взаємодії на основі трансформерних моделей. Об'єктом дослідження є процес автоматизованого виявлення кібербулінгу та його суб'єктів у текстових комунікаціях, предметом – моделі, методи та програмні засоби обробки природної мови для інтерпретованого аналізу агресивних висловлювань.

Запропонований метод реалізує багаторівневу обробку тексту. На першому рівні трансформерна модель виконує класифікацію повідомлень щодо наявності ознак кібербулінгу, формуючи ймовірнісну оцінку належності висловлювання до агресивного контенту. Після перевищення заданого порогу текст переходить до другого рівня аналізу, де поєднуються залежні синтаксичний розбір і семантико-рольова інтерпретація. Для кожного речення відновлюється предикативна структура, виділяються предикати та їх актанти, на основі чого текстове повідомлення відображається у множину семантичних трійок виду «суб'єкт – дія – об'єкт». У результаті для кожного фрагмента формується пара $\langle u, R \rangle$, де u – індикатор наявності кібербулінгу, а R – структура рольових зв'язків між учасниками комунікації.

Методологічно це дозволяє відокремити два логічні шари: детекцію агресії як такої та інтерпретацію комунікативних ролей у межах виявлених токсичних висловлювань. Використання *dependency-parsing* і механізмів відновлення актантних ролей забезпечує автоматизоване виокремлення потенційних кривдників і жертв, а також проміжних суб'єктів, які підсилюють або транслюють агресію, включно з випадками, коли вплив реалізується через конструкції з копулою чи непрямі характеристики, а не через явно образливі дієслова. Це особливо важливо для соціальних платформ, де значна частина кібербулінгу має завуальований характер.

Для навчання та валідації нейромережевої компоненти використано спеціалізовані корпуси кібербулінгу з відкритих джерел, що містять марковані приклади агресивних і нейтральних повідомлень, а також підмножини з деталізацією типів ворожих висловлювань. Один із застосованих корпусів характеризується збалансованим розподілом класів за основними категоріями кібербулінгу, інший – стилістичною й тематичною різноманітністю, оскільки агрегує дані з різних платформ. Комбіноване використання цих наборів даних дозволяє одночасно забезпечити стабільність базової класифікації та підвищити здатність моделі узагальнюватися на різні типи дискурсу.

На основі запропонованого методу спроектовано та реалізовано прототип інтелектуальної системи, що поєднує трансформерний класифікатор, синтаксико-семантичний аналізатор та веб-інтерфейс для інтерактивного аналізу текстів. Система забезпечує введення довільних повідомлень, автоматичне визначення

наявності кібербулінгу, формування відсоткової оцінки ризику і візуалізацію виявлених суб'єктно-об'єктних зв'язків у вигляді таблиці семантичних трійок. Це створює передумови для інтеграції рішення в інформаційні системи цифрової безпеки, освітні платформи та аналітичні модулі моніторингу соціальних мереж.

Узагальнюючи, розроблений підхід демонструє можливість переходу від плоскої детекції токсичності до структурованого опису кібербулінгових ситуацій з урахуванням ролей учасників і спрямованості впливу. Багаторівневе поєднання трансформерних моделей і синтаксико-семантичного аналізу підвищує пояснюваність результатів і придатність системи до практичного використання. Подальші дослідження доцільно спрямувати на розширення рольової таксономії, адаптацію методу до україномовних і багатомовних корпусів та інтеграцію часово-графових моделей, що дозволить аналізувати динаміку кібербулінгу на рівні довготривалих комунікативних сценаріїв.

Перелік посилань

1. Civila S. Cyberbullying. Comprehensive Sexuality Education for Gender-Based Violence Prevention. 2024. P. 229–245.
2. Casas F. Age Discrimination. Encyclopedia of Quality of Life and Well-Being Research. Cham, 2023. P. 118–121.
3. Lee H. Lived Religion in Religious Vaccine Exemptions. Perspectives in Biology and Medicine. 2024. Vol. 67, no. 1. P. 96–113.
4. Протидія булінгу. МОН. URL: <https://mon.gov.ua/tag/protidiya-bulingu?&type=all&tag=protidiya-bulingu>
5. Антибулінг. AIKOM. URL: <https://aikom.ica.gov.ua/bullying/help>
6. Unnava S., Parasana S. R. A Study of Cyberbullying Detection and Classification Techniques: A Machine Learning Approach. Engineering, Technology & Applied Science Research. 2024. Vol. 14, no. 4. P. 15607–15613.
7. Mazurets O., Vit R. Practical Application of Method of Thematic Classification of Text Information Using LDA. Information Technology and Implementation (Satellite). Proceedings 11th International Conference. November 21, 2024. Kyiv, Ukraine. 2024. Pp. 151–152.
8. Віт Р.В., Мазурець О.В. Тематична класифікація текстової інформації засобами обробки природної мови. Збірник наукових праць XXIII Міжнародної наукової конференції «Нейромережні технології та їх застосування НМТіЗ-2024». 11-12 грудня 2024. Краматорськ-Тернопіль, ДДМА. 2024. с. 63-66.
9. Овчарук О.М., Мазурець О.В. Нейромережеве діагностування проявів ПТСР у текстовому контенті з використанням помилко-орієнтованого навчального набору даних. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2024. №6, Т.1 (343). С. 195-200.
10. Крак Ю.В., Дідур В.О., Молчанова М.О., Мазурець О.В., Собко О.В., Залуцька О.О., Бармак О.В. Метод виявлення політичної пропаганди в інтернет-контенті нейромережевими засобами обробки природної мови. Науковий журнал «Проблеми програмування». Київ, 2024, №2-3. с. 288-295.
11. Овчарук О.М., Мазурець О.В. Нейромережева архітектура з квантовим шаром для аналізу текстових повідомлень на прояви посттравматичного стресового розладу. Науковий журнал «Наука і техніка сьогодні». Київ, 2024. №13 (41). С. 1192-1204.

12. Мазурець О.В., Тимофієв І.А., Кліменко В.І., Тищенко О.О. Метод виявлення депресивного стану пов'язаного із навчанням у закладах освіти із використанням нейромережі дуальної архітектури. Науковий журнал «Вісник Херсонського національного технічного університету». 2024. №4 (91). С. 311-318.
13. Віт Р.В., Мазурець О.В. Підхід до тематичної класифікації текстової інформації засобами обробки природної мови. Науковий журнал «Наукові праці Донецького національного технічного університету», серія «Проблеми моделювання та автоматизації проектування». 2025. №1 (21). С. 94-99.
14. Овчарук О.М., Мазурець О.В. Нейромережевий метод діагностування психологічних розладів за аналізом повідомлень на основі роздільного підходу до класифікації. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». № 1, 2025. с. 210-216.
15. Murava V., Zalutska O., Didur V., Mazurets O. Software architecture of information system for exchanging LLM thematic prompts. Global Trends in the Development of Information Technology and Science. Proceedings IV International Scientific and Practical Conference. June 25-27, 2025. Stockholm, Sweden. Pp. 121-127.
16. Юрченко Д.Ю., Овчарук О.М., Мазурець О.В., Шевчук П.О. Метод використання нейромережі гібридної архітектури для визначення емоційної тональності текстових повідомлень. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». № 2, 2025. с. 136-141.
17. Віт Р.В., Мазурець О.В. Метод виявлення психологічного цифрового перевантаження за аналізом текстових даних нейромережевими моделями глибокого навчання. Науковий журнал «Вісник Херсонського національного технічного університету». 2025. №2 (93). Т. 2. С. 107-114.
18. Віт Р.В., Мазурець О.В. Метод виявлення комунікаційних об'єктів як індикаторів цифрової втоми. Інтелектуальний метод виявлення цільових об'єктів предметної області для класифікації текстової інформації. Матеріали XIII Міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології ІУСТ-ОДЕСА-2025». 24-26.09.2025. Одеса. 2025. С.119-121.
19. Собко О.В. Метод нейромережевого формування репрезентативних недискримінаційних текстових датасетів згідно FATE-принципу справедливості. Вісник Херсонського національного технічного університету. 2024. № 4 (91). С. 342–348.
20. Krak, I., Sobko, O., Mazurets, O., Tymofiiiev, I., Molchanova, M., Barmak, O. Method for Detecting and Classifying Cyberbullying in Text Content Using Neural Networks. Lecture Notes in Networks and Systems. Springer, Cham, 2025, vol. 1473, pp. 486–498.
21. Krak I., Sobko O., Molchanova M., Tymofiiiev I., Mazurets O., Barmak O. Method for neural network cyberbullying detection in text content with visual analytic. CEUR Workshop Proceedings, 2025, vol. 3917, pp. 298-309.
22. Молчанова М.О., Мазурець О.В., Собко О.В., Кліменко В.І., Андрощук В.І. Метод нейромережевого виявлення кібербулінгу з використанням хмарних сервісів та об'єктно-орієнтованої моделі. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2024. №2 (333). С. 200-206.

УДК 004.6

Бабаєвський В.М., Дика В.В., Муляр І.В.

Хмельницький національний університет

МЕТОД ЗАХИСТУ ВЕБЗАСТОСУНКІВ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ТРАФІКУ

У роботі розглянуто практичні аспекти створення інтелектуальної системи виявлення атак на вебзастосунки на основі аналізу HTTP-трафіку. Запропоновано архітектуру, яка поєднує збір запитів, виділення ознак, машинне навчання та інтеграцію з інструментами безпеки, зокрема OWASP ZAP. Продемонстровано можливість виявлення атак типу SQL-ін'єкція, XSS, brute-force та інших завдяки оцінці ризику на основі поведінкових та контекстних ознак. Показано методи візуалізації результатів для подальшого аналізу ефективності моделі.

The paper examines practical aspects of developing an intelligent system for detecting attacks on web applications using HTTP traffic analysis. The proposed architecture combines request logging, feature extraction, machine learning, and integration with security tools such as OWASP ZAP. The system demonstrates the capability to detect SQL injection, XSS, brute-force, and other attacks by evaluating risk based on behavioral and contextual features. Methods for visualizing the results are also presented to support further analysis of model effectiveness.

З розвитком цифрових технологій зростає і рівень загроз у сфері веббезпеки. Атаки на вебзастосунки залишаються одними з найпоширеніших — згідно з OWASP Top-10, серед найбільш небезпечних вразливостей фігурують SQL-ін'єкції, міжсайтове скриптування (XSS), зловживання правами доступу тощо. Традиційні методи захисту — такі як фільтрація запитів на рівні WAF (Web Application Firewall) — часто виявляються недостатніми в умовах складних і постійно змінюваних атак.

Метою цієї роботи є розробка інтелектуальної системи аналізу HTTP-трафіку, яка здатна автоматично виявляти підозрілі запити на основі поведінкових ознак із застосуванням методів машинного навчання, та інтегруватися з існуючими інструментами тестування безпеки, зокрема OWASP ZAP.

Штучний інтелект (ШІ) дедалі активніше застосовується для виявлення атак на вебсервери та захисту вебзастосунків. Завдяки здатності обробляти великі обсяги даних і виявляти складні закономірності в мережевому трафіку, ШІ-системи можуть автоматично ідентифікувати аномальні та потенційно шкідливі дії, що традиційними методами часто залишаються непоміченими. Особливо це важливо для серверів, які обслуговують велику кількість користувачьких запитів та мають різноманітні типи атак, включно з DDoS, brute-force, SQL-ін'єкціями та іншими.

Інтелектуальні системи виявлення атак на вебсервери базуються на використанні машинного навчання та алгоритмів глибокого аналізу, які аналізують поведінкові та структурні характеристики HTTP-запитів, а також метадані трафіку. Вони здатні адаптуватися до нових загроз завдяки безперервному навчанню на основі актуальних даних. Це підвищує якість виявлення і зменшує кількість помилкових тривог, що дозволяє оперативно реагувати на атаки і мінімізувати можливі збитки.

Обчислення частоти згадувань окремих ознак, наприклад, символів ' чи script у запитах виконується аналогічно до термінів у текстах за формулою TF:

$$TF_i = \frac{n(i)}{N}, \quad (1)$$

де $n(i)$ – кількість появ ознаки i у запиті, N – загальна кількість ознак у запиті.

Виділення категорій за допомогою кривої з прямих ліній виконується аналогічно (рисунок 1).

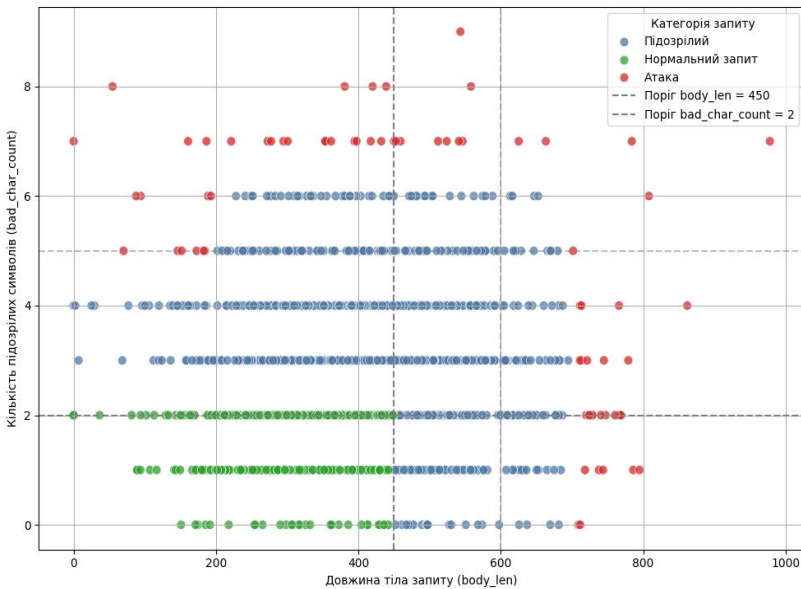


Рисунок 1 – Виділення категорій та формування правил

Впровадження ШІ в інфраструктуру серверів дозволяє створити проактивні системи безпеки, які не лише виявляють атаки в реальному часі, але й передбачають потенційні загрози, що дає змогу ефективно запобігати інцидентам. Такі підходи особливо важливі в умовах постійного зростання складності та масштабів кіберзагроз, забезпечуючи захист критично важливих систем і даних.

Індикаторами потенційно небезпечних або аномальних HTTP-запитів можуть виступати як окремі ключові слова, так і шаблони, структурні характеристики запиту чи поведінкові ознаки. Їх формалізація дозволяє системі аналізу трафіку автоматично класифікувати запити за рівнем підозри (таблиця 1).

Таблиця 1 – Підходи до пошуку ознак атак у HTTP-запитах

Тип терміну	Підхід до формалізації
Ключові слова	Визначаються за частотою появи в тілі запиті.
Підозрілі шаблони	Регулярні вирази, що вказують на можливі ін'єкції або спроби обходу безпеки.
Аномальна довжина	Визначається як значення, що перевищує статистичні межі.
Кількість спецсимволів	Велика кількість символів, характерних для атак.
Поведінкові ознаки	Незвична частота запитів, аномальні User-Agent або IP, що не властиві типовій поведінці

Отже, запропонована інтелектуальна система аналізу трафіку забезпечує ефективне виявлення та класифікацію аномальних та потенційно шкідливих HTTP-запитів за допомогою комплексного набору ознак та правил. Використання автоматизованого аналізу трафіку сприяє підвищенню безпеки вебзастосунків за рахунок своєчасного виявлення атак та зменшення кількості помилкових спрацьовувань. Подальші дослідження будуть спрямовані на вдосконалення методів машинного навчання для більш гнучкого та адаптивного виявлення нових типів атак, а також на інтеграцію системи у реальні програмні комплекси для забезпечення їх захищеності в умовах постійно зростаючих кіберзагроз.

Перелік посилань

1. SQLMap Community. "Enhancing SQL Injection Detection Using LLM". [Електронний ресурс]. Режим доступу: <https://sqlmap.org/resources/llm-integration> (Дата звернення: 15.10.2025).
2. Ленков С., Джулій В., Муляр І., Димбовський М. Модель визначення актуальних загроз безпеки конфіденційних даних в розподіленій інформаційній системі. Underwater Technologies: Industrial and Civil Engineering. 2023. Issue 13. С. 45–59.
3. WhiteHat Security's Approach to Detecting Cross-Site Request Forgery (CSRF). URL: <https://www.whitehatsec.com/> (Дата звернення: 22.10.2025).
4. Джулій В. М., Кльоц Ю. П., Муляр І. В., Жилевич М. Л., Джулій А. В. Контроль додатків інтернет-трафіка комп'ютерних мереж методами машинного навчання. Вісник Хмельницького національного університету. Серія: Технічні науки. 2021. № 5. С. 22–36. DOI: 10.31891/2307-5732-2021-301-5-22-26

УДК 004.056.5

Басистий В.А., Городецька А.О., Чешун В.М., Чешун О.В.

Хмельницький національний університет

ФІЗИЧНІ ТОПОЛОГІЇ РОЗГОРТАННЯ АГЕНТНОЇ СИСТЕМИ МОНІТОРИНГУ МЕРЕЖЕВОГО ТРАФІКУ ІОТ

Розглядається мультиагентний підхід до моніторингу мережевого трафіку ІоТ, що базується на принципах розподілених систем. Запропоновано три фізичні топології розгортання агентної системи – безпроводну, провідну та комбіновану, які забезпечують гнучкість, масштабованість і надійність аналізу. Моделювання в Cisco Packet Tracer підтвердило ефективність архітектури та її придатність для виявлення кіберзагроз у реальному часі.

A multi-agent approach to monitoring IoT network traffic based on distributed systems principles is considered. Three physical topologies for deploying the agent system are proposed - wireless, wired, and combined, which provide flexibility, scalability, and reliability of analysis. Simulation in Cisco Packet Tracer confirmed the effectiveness of the architecture and its suitability for real-time detection of cyber threats.

Проектування архітектури будь-якої технічної системи є визначальним етапом, оскільки саме архітектурна невідповідність досить часто стає ключем проблеми її застосування. Замість спроб адаптувати централізовану модель, пропонується підхід, що базується на парадигмі розподілених систем – мультиагентних систем (MAS - Multi-agent system) [1].

Проектована мультиагентна система являє собою сукупність автономних програмних сутностей (агентів), які взаємодіють між собою для вирішення складної задачі, що не може бути вирішена одним агентом. Можна ідентифікувати наступні ключові властивості програмних агентів, що роблять цей підхід ідеальним для цілей забезпечення кібербезпеки в ІоТ:

- автономність – здатність діяти без прямого втручання людини;
- реактивність – здатність своєчасно реагувати на зміни в оточенні;
- проактивність – здатність діяти за власною ініціативою;
- соціальність – здатність взаємодіяти з іншими агентами для досягнення спільної мети.

Головна перевага MAS полягає в архітектурному ізоморфізмі. Замість збору трафіку в єдину точку, MAS "приносить" аналітичні обчислення безпосередньо до джерел трафіку. Пропонована агентна система може бути розгорнута у трьох основних фізичних топологіях, що ілюструють її гнучкість. Моделювання цих

топологій було виконано за допомогою програмного симулятора Cisco Packet Tracer, який дозволяє віртуально створювати та тестувати мережеві інфраструктури.

На всіх трьох схемах, компоненти системи мають наступне призначення:

- вузли (PC-PT) – одноплатні комп'ютери (ОПК), на яких розгорнуто програмний комплекс агентів моніторингу;

- центральний вузол (Server-PT) – внутрішній сервер. Він ідеально підходить для розгортання MQTT-брокера (для координації агентів) та сервера SIEM (для прийому фінальних звітів);

- мережеве обладнання (HomeRouter, Switch) забезпечує зв'язність мережі. Маршрутизатор також виступає як шлюз до інтернету;

- інтернет (Ethernet (Cloud)) – зовнішня, неконтрольована мережа, що є основним джерелом зовнішніх загроз;

- пристрій адміністратора (Laptop-PT Admin) – робоча станція адміністратора. У провідних сценаріях він підключений через консольний кабель для прямого налаштування комутатора.

На рисунку 1 представлено схематичне зображення безпроводної топології мережі.

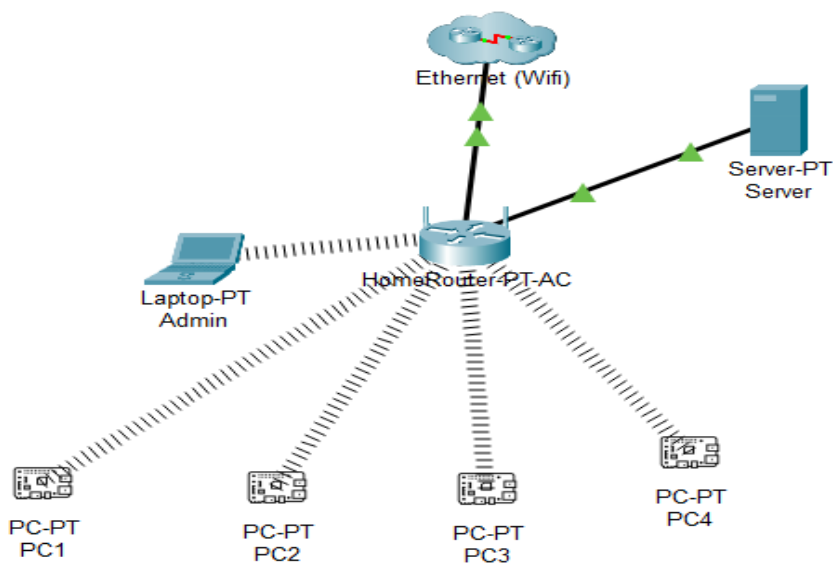


Рисунок 1 – Безпроводна (Wi-Fi) топологія розгортання системи

У даній топології всі пристрої (PC-PT PC1-PC4, Laptop-PT Admin та Server-PT Server) підключені до мережі через безпроводний маршрутизатор HomeRouter-PT-AC.

Захоплення відбувається в наступний спосіб. Вузли ОПК переводяться в режим моніторингу. Це дозволяє кожному агенту пасивно моніторити та захоплювати весь Wi-Fi трафік у своєму радіусі дії, використовуючи системні бібліотеки, такі як libpcap [2]. Таким чином досягається гнучкість, мобільність, легкість масштабування та виявлення специфічних Wi-Fi атак.

На рисунку 2 представлено схематичне зображення провідної топології мережі.

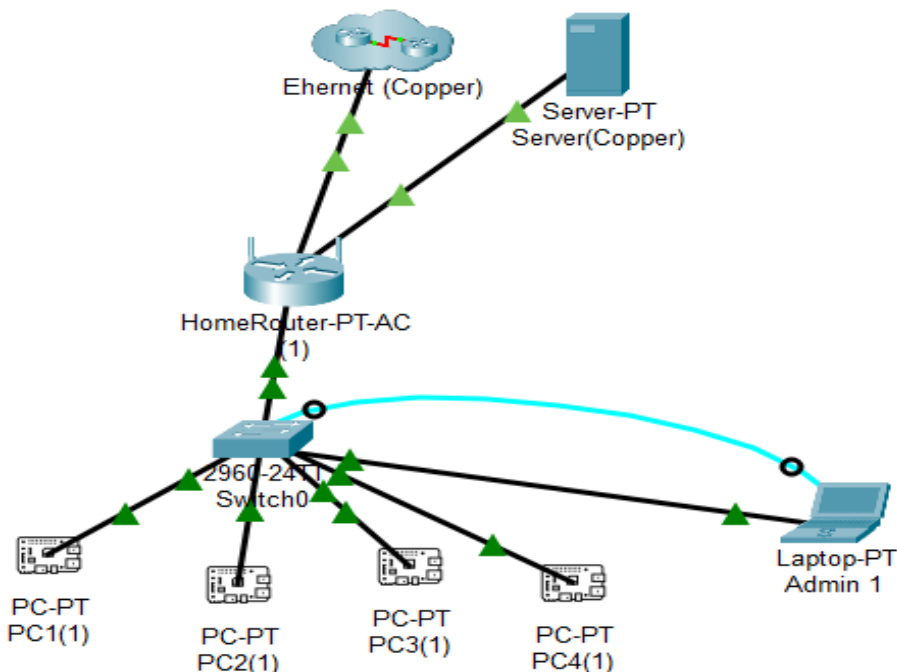


Рисунок 2 – Провідна (Ethernet) топологія розгортання системи

У провідній конфігурації пристрої (PC-PT PC1(1)-PC4(1)) підключені до центрального керованого комутатора (Switch0). Комутатор підключений до маршрутизатора HomeRouter-PT-AC(1), який також обслуговує Server-PT Server(Copper) та має вихід в Інтернет.

Спосіб захоплення полягає в наступному. Використовується технологія SPAN (Switched Port Analyzer) на керованому комутаторі Switch0. Технологія SPAN є функцією мережевих комутаторів, що дозволяє дзеркалізувати (копіювати) мережевий трафік з одного або кількох портів на інший порт для моніторингу безпеки або аналізу продуктивності. Комутатор Switch0 налаштовується на

копіювання всього трафіку (наприклад, з порту, що веде до маршрутизатора) на один з портів, до якого підключений наш ОПК-агент (наприклад, PC-PT PC1(1)) [3].

Таким чином досягається повна видимість та висока надійність захоплення всього провідного трафіку без втрат, що є критичним для точного аналізу.

На рисунку 3 представлено схематичне зображення комбінованої топології мережі. Мережа складається з двох сегментів: провідного (PC-PT PC1-Combo...) та безпроводного (PC-PT PC1 Wifi-Combo...). Маршрутизатор HomeRouter-PT-PC Combo об'єднує ці сегменти, обслуговує сервер Server-PT Server-Combo та має вихід в Інтернет. У даній конфігурації, топологія є найбільш ефективною і поєднує обидва підходи.

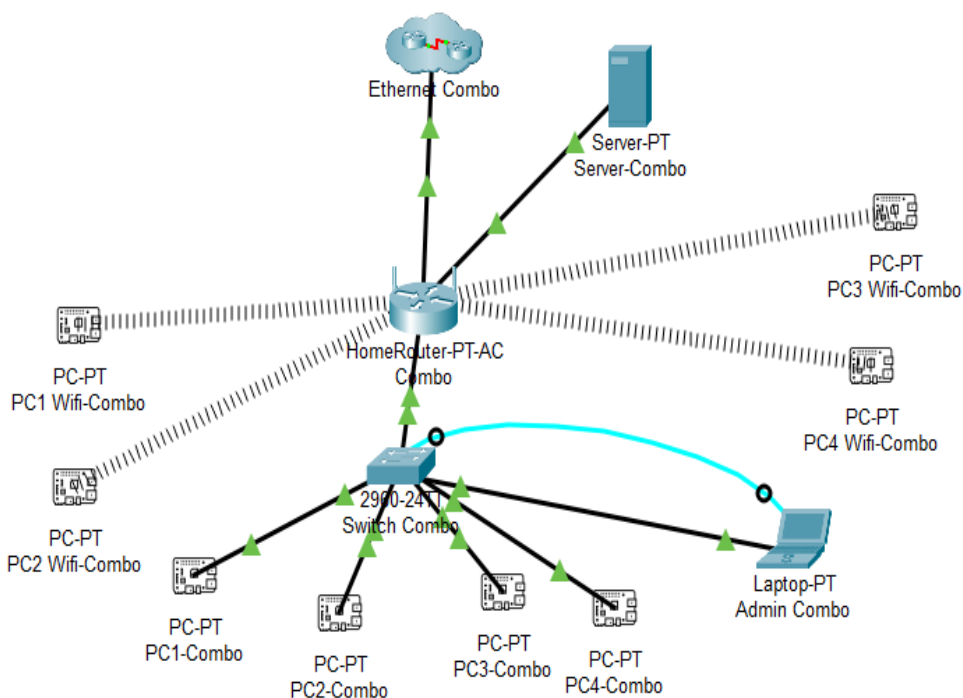


Рисунок 3 – Комбінована (гібридна) топологія системи

Для забезпечення повного моніторингу трафіку необхідна комбінація агентів:

моніторинг провідного сегмента – один з ОПК (наприклад, PC1-Combo) підключається до SPAN-порту комутатора Switch Combo;

моніторинг безпроводного сегмента – один з ОПК (наприклад, PC1 Wifi-Combo) налаштовується на режим моніторингу (Monitor Mode).

Ключова перевага гібридної топології – хоча фізично трафік збирається різними агентами з різних середовищ, логічно вони становлять єдину систему. Так досягається вся потужність агентного підходу.

Використовуючи агентів-координаторів та спільний MQTT-брокер (на Server-Combo), система може виявляти складні атаки, що перетинають сегменти. Наприклад, якщо злоумисник з *інтернету* починає одночасно сканувати Wi-Fi та провідні пристрої, агент-координатор скорелює алерти від *обох* агентів в єдиний, більш серйозний "інцидент" безпеки [4].

Висновки. Запропонована мультиагентна архітектура доводить переваги розподіленого підходу для моніторингу IoT-трафіку, дозволяючи «приносити аналітику» до джерел замість централізованого збору. Агентна модель забезпечує автономність, реактивність, проактивність і соціальність – властивості, критичні для виявлення та локалізації атак у реальному часі. Три фізичні топології (безпроводна, провідна, комбінована) демонструють гнучкість розгортання: Wi-Fi – мобільність і масштабованість; Ethernet – надійність захоплення через SPAN; гібридний варіант – комплексний моніторинг мережі. Моделювання в Cisco Packet Tracer підтвердило практичну застосовність схем і дозволило відпрацювати сценарії захоплення та кореляції подій.

Перелік посилань

1. The confluence of evolutionary computation and multi-agent systems: A survey / T.Y. Chen et al. IEEE/CAA J. Autom. Sinica. 2025. P. 1-20. DOI: 10.1109/JAS.2025.125246 (date of access: 23.10.2025).
2. Cheng C., Ren S., Wang J. Implementation of Wireless Network Quality Evaluation Method for Agent Twins Based on Active Passive Dual Periodic Collaborative Measurement. 5th International Conference on Neural Networks, Information and Communication Engineering (NNICE), Guangzhou, China, 2025, P. 937-944. DOI: 10.1109/NNICE64954.2025.11064354 (date of access: 23.10.2025).
3. Saad R. A., Alkekli F. B., Gshera H. B. Network Monitoring Using Port-Mirroring Technology (SPAN and RSPAN). SUCP. 2025. Vol. 4, № 1. P. 84-89.
4. Resilient topology optimization on cyber-physical system of distribution networks under FDIA-Worm hybrid attacks / Li Huifeng et al. Journal of Electric Power Science and Technology. 2024. Vol. 39: Iss. 4. Article 3. P. 20-32. DOI: 10.19781/j.issn.1673-9140.2024.04.003 (date of access: 25.10.2025).

УДК 004.8

Безпрозвана Ю.Г., Шурипа М.О., Мазурець О.В.

Хмельницький національний університет

НЕЙРОМЕРЕЖЕВА ОЦІНКА СТАНУ БУДІВЕЛЬ ЗА ВІЗУАЛЬНИМИ ДАНИМИ

Розглянуто нейромережевий підхід до оцінки стану будівель за ортофотопланами та аерофотознімками, актуальний для післявоєнної відбудови та зношеного житлового фонду. Використано одностадійні сегментаційні детектори YOLOv8/YOLOv11/YOLOv12 у легких модифікаціях з тайлуванням зображень, балансуванням класів та аугментаціями. Розмітка поєднує маски «будівля/фон» і три рівні пошкодження, що дає змогу спільно навчати сегментацію та класифікацію. Найкращий результат показали конфігурації buildings-seg-8s-new та buildings-seg-11n-new: mAP50 до 0,35 для масок, 0,39 для рамок і макро- $F_1 \approx 0,78$ для трьох класів стану. Запропоноване рішення дозволяє автоматично будувати карти пошкодження і формувати пріоритети для інженерних обстежень.

The paper presents a neural-network approach to building condition assessment from orthophotos and aerial imagery, motivated by post-war reconstruction and aging urban stock. Lightweight one-stage segmentation detectors of the YOLOv8/YOLOv11/YOLOv12 families are trained on tiled images with class balancing and augmentations using combined "building/background" masks and three damage levels. This enables joint learning of segmentation and condition classification. The best configurations, buildings-seg-8s-new and buildings-seg-11n-new, achieve mAP50 up to 0.35 for masks, 0.39 for boxes and a macro F_1 score of about 0.78 across three condition classes. The approach supports automatic damage mapping and prioritisation of engineering inspections.

Післявоєнна відбудова та старіння житлового фонду вимагають оперативного контролю стану будівель без повсюдних виїзних обстежень [1]. Класичні методи технічної діагностики опираються на візити експертів і точкові вимірювання, що є дорогим, повільним і складно масштабованим для цілих кварталів чи міст [2]. Натомість супутникові знімки, аерофото з БПЛА та наземні зображення вже масово накопичуються, однак без автоматизованої обробки не перетворюються на придатні для прийняття рішень показники [3, 4]. Тому актуальною є розробка нейромережевих методів, здатних за візуальними даними виділяти контури будівель та оцінювати їхній стан як основу для пріоритизації детального обстеження й планування ремонтів.

Нейромережеві методи аналізу візуальних даних [5, 6] набувають особливої актуальності у сфері оцінки технічного стану будівель, що пов'язано з необхідністю підвищення ефективності моніторингу, своєчасного виявлення дефектів та запобігання аварійним ситуаціям. Традиційні підходи, які ґрунтуються на ручному

огляді або класичних алгоритмах обробки зображень [7], є трудомісткими, суб'єктивними та малоефективними при опрацюванні великих обсягів даних [8, 9]. Розвиток глибинного навчання, зокрема архітектур згорткових нейронних мереж [10], відкриває можливість автоматизованого виявлення тріщин, корозії, деформацій та інших структурних порушень із високим рівнем точності.

Сучасні CNN-моделі демонструють здатність до ефективного вилучення просторово-структурних ознак з фотозображень, відеопотоків, даних дронів та лазерного сканування [11, 12]. Досягнення комп'ютерного зору у сегментації [13], класифікації [14] та детекції об'єктів [15] дозволяють формувати багаторівневі карти пошкоджень, визначати ступінь деградації матеріалів і оцінювати потенційні ризики руйнування. Особливо перспективними є підходи, що інтегрують CNN з трансформерними архітектурами та методами мультимодального аналізу, що дає змогу поєднувати зображення з текстовими описами дефектів, показниками сенсорів чи геометричними моделями [16].

У контексті оцінки стану будівель важливим напрямком є розвиток алгоритмів, здатних працювати в умовах шуму, різної освітленості, варіативності кутів зйомки та складного фону, що характерно для реальних інженерних споруд [17].

Мета роботи – сформувати та експериментально обґрунтувати нейромережевий підхід до оцінки стану будівель за візуальними даними, який поєднує автоматичну сегментацію будівельних об'єктів на зображеннях та подальшу інтерпретацію їхніх візуальних ознак для визначення ступеня ушкоджень.

Об'єкт дослідження – процес моніторингу технічного стану будівель у міській забудові.

Предмет дослідження – методи й моделі нейромережевої сегментації та класифікації будівель за візуальними ознаками ушкоджень (деформації покрівлі, обвалені перекриття, руйнування фасадів тощо).

Методологія. Для виділення будівель у сцені застосовано одностадійні сегментаційні детектори сімейств YOLOv8/YOLOv11/YOLOv12 у легких модифікаціях (8s, 11n, 11s, 11m, 12n). Вихідні ортофотоплани та аерофотознімки були нарізані у тайли з нормалізованою роздільністю; виконано балансування класів та розширення вибірки через геометричні та фотометричні перетворення [18]. Розмітка містила маски «будівля/фон» та категорії стану будівлі («задовільний», «пошкоджений», «значно пошкоджений/зруйнований»). Навчання здійснювалось у режимі багатозадачної оптимізації: перша голова моделі виконувала детекцію та сегментацію будівель, друга – класифікацію стану об'єкта на основі ознак, агрегованих у межах відповідної маски [19]. Якість сегментації оцінювали за показниками mAP50(B) для рамок та mAP50(M) для масок, а точність оцінки стану – за макро-усередненими Precision, Recall та F_1 [20].

Отримані результати. Порівняння конфігурацій показало, що попередньо налаштовані компактні моделі демонструють кращий баланс точності та обчислювальної складності, ніж глибші варіанти (рисунок 1). Модель buildings-seg-

8s-new, навчена з доопрацьованим набором аугментацій, досягла найкращих результатів за сегментаційними метриками: на валідаційній вибірці mAP50(M) для масок становив близько 0,35, а mAP50(B) для рамок – близько 0,39. Конфігурація buildings-seg-11n-new продемонструвала близькі значення ($\approx 0,34$ та $\approx 0,37$ відповідно), забезпечуючи невеликий програш у точності при кращій швидкодії на GPU та можливості роботи на ресурсно-обмежених вузлах. Базові варіанти моделей без вдосконалених аугментацій (buildings-seg-8s, buildings-seg-11n, buildings-seg-11s) забезпечили mAP50 у межах 0,24–0,30, що вказує на внесок додаткової обробки даних у зменшення кількості пропусків дрібних чи частково перекритих будівель. Найгірші результати показали більш громіздкі моделі buildings-seg-11m та buildings-seg-12n, для яких наявний обсяг вибірки виявився недостатнім: їхні криві навчання характеризуються повільним зростанням і насиченням на рівнях mAP50(M) < 0,15.

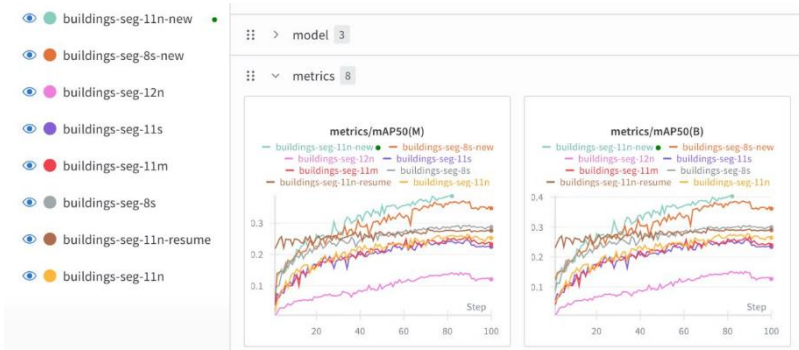


Рисунок 1 – Графіки навчання YOLO різних версій

На другому етапі, після фіксації найкращої сегментаційної архітектури, було проведено навчання класифікаційної голови для оцінки стану будівель. Для конфігурації на основі buildings-seg-8s-new макро-усереднений показник F_1 для трьох класів стану склав близько 0,78, при цьому найвищу точність досягнуто для класу «зруйнований», а найбільша кількість помилок спостерігалась у межах переходу між «пошкодженим» та «значно пошкодженим» станами [21]. Аналіз помилок виявив чутливість моделі до сильних тіней, сезонних відмінностей та маскуванню фасадів рослинністю, що вказує на доцільність додавання мультиспектральних каналів та текстурних ознак.

Практичне значення. Запропонований підхід дозволяє на основі серій аерофотознімків автоматично будувати карти пошкоджень, на яких виділяються контури будівель та їхній орієнтовний стан. Це забезпечує формування списків пріоритетних об'єктів для інженерного обстеження, підтримує прийняття рішень щодо планування відновлювальних робіт та може інтегруватися у наявні геоінформаційні системи органів місцевого самоврядування.

Висновки та перспективи. Проведене дослідження показало, що легкі сегментаційні моделі типу YOLO-seg за умови правильно організованої підготовки даних здатні забезпечити прийнятну якість автоматичного виділення будівель та первинної оцінки їхнього стану на візуальних даних. Найкраще співвідношення точності та швидкодії продемонстрували конфігурації buildings-seg-8s-new та buildings-seg-11n-new. Подальший розвиток роботи передбачає розширення датасету за рахунок знімків різних сенсорів і сезонів, використання багатоспектральної інформації, уточнення шкали станів з урахуванням будівельних норм, а також впровадження модулів пояснюваності, що дозволять інженерам інтерпретувати рішення нейромережевої системи при плануванні відбудови.

Перелік посилань

1. Demian, P., Hassan, T. M., Kalmykov, O., Demianenko, I., & Makarov, R. (2024). BIM implementation in post-war reconstruction of Ukraine. *Buildings*, 14(11), 3495.
2. Chashyn, D., Khurudzhi, Y., & Daukšys, M. (2024). Directions for the formation of «City Intelligent models» using artificial intelligence for the post-war reconstruction of historical buildings. *Budownictwo i architektura.*, 23(1), 73-86.
3. Zalizko, V. D., Cherniak, A. M., Nowak, D., & Artemov, V. Y. (2024). Assessing Ukrainian education security in the context of artificial intelligence integration for accelerated post-war recovery. *Scientific Bulletin of National Mining University*, (6).
4. Alshafei, I. A., & Almashhour, R. T. N. (2025). Integrating Artificial Intelligence in urban re-design: A collaborative approach to post-war design phases. *International Journal of Human Capital in Urban Management*, 10(2).
5. Собко О.В., Кліменко В.І., Мазурець О.В., Залуцька О.О., Гладун О.В. Особливості програмної інженерії та тестування програмного забезпечення для нейромережевого аналізу фотоданих залишків зруйнованих будівель із роботизованої техніки. *Науковий журнал «Наука і техніка сьогодні»*. Київ, 2025. №4 (45). С. 1566-1581.
6. Дідур В.О., Молчанова М.О., Мазурець О.В. Спосіб виявлення та класифікації залишків зруйнованих будівель та будівельного сміття за фотографіями з використанням моделей CNN. *Науковий журнал «Наука і техніка сьогодні»*. Київ, 2025. №1 (42). С. 1162-1175.
7. Zharnovskyi O., Mazurets O., Sobko O. Approach to Identification of Artificial Intelligence-Generated People Images by Means of Machine Learning. *Key Aspects of the Development of Scientific Research in Modern Conditions. Proceedings of the XLV International scientific and practical conference. October 30 – November 1, 2024. Constanta, Romania. 2024.* Pp. 69-73.
8. Pokhytun A., Mazurets O., Molchanova M., Tyschenko O. Method for Neural Network Detecting Changed Images of People's Faces Using CNN. *New Horizons in Scientific Research: Challenges and Solutions. Proceedings of the 1st International scientific and practical conference. October 21-23, 2024. Marseille, France. 2024.* Pp. 35-40.
9. Kharysh I., Sobko O., Mazurets O. Designing CNN Neural Network Model for Detecting Fractures of Lower Extremities by X-ray Images. *The Impact of Scientific Research on the Development of the Modern World. Proceedings of the XLIV International scientific and practical conference. October 23-25, 2024. Dubrovnik, Croatia. 2024.* Pp. 91-96.
10. Bas I.S., Kadynska V.D., Klimenko V.I., Mazurets O.V. Convolutional Neural Network Transfer Learning Method for Aircraft Image Classification. *Scientific method: reality and future*

trends of researching. Proceedings of VI International Scientific and Theoretical Conference. June 6, 2025. Montreal, Canada. Pp. 147-155.

11. Mushtyn O., Sobko O., Molchanova M., Mazurets O. Convolutional Neural Network Architecture for Image-Based Architectural Style Recognition. *Evolving Science: Theories, Discoveries and Practical Outcomes. Proceedings of 4th International Scientific and Practical Conference.* June 9-11, 2025. Zurich, Switzerland. Pp. 130-143.

12. Malaydakh V., Molchanova M., Shevchuk P., Mazurets O. Deep learning neural network architecture for determining sunflower growth stage from visual data. *Modern Scientific Research: Theoretical and Practical Aspects. Proceedings II International Scientific and Practical Conference.* May 26-28, 2025. Riga, Latvia. Pp. 143-148.

13. Mazurets O. V., Klimenko V. I., Molchanova M. O., Sultanov A. V. Object-Oriented Intelligent System for Neural Network Detection of Sugar Crystallization Zones. *Global Science: Prospects and Innovations. Proceedings of the 10th International scientific and practical conference.* Cognum Publishing House. Liverpool, United Kingdom. 2024. Pp. 198-207.

14. Mazurets O., Uspenska K., Vit R., Tyschenko O. Intelligent System for Determining the Object Attributes Values by Neural Networks Means by Graphic Images in Databases. *Current Trends in the Development of Scientific Research in Today's Conditions. Proceedings of XXV International scientific and practical conference.* May 29-31, 2024. International Scientific Unity. Florence, Italy. 2024. Pp. 86-91.

15. Ostapchenko N., Tyschenko O., Denysenko B., Mazurets O. Semantic search of relevant images using vector databases. *Modern Scientific Research: Theoretical and Practical Aspects. Proceedings II International Scientific and Practical Conference.* May 26-28, 2025. Riga, Latvia. Pp. 161-165. URL: https://www.eoss-conf.com/wp-content/uploads/2025/05/Riga_Latvia_26.05.25.pdf

16. Kok I.A., Kadynska V.D., Zalutska O.O., Mazurets O.V. Object-Oriented Intelligent System for Automated Control of Smoking by Video Data. *Current scientific goals, approaches and challenges. Proceedings of IV International Scientific and Theoretical Conference.* June 13, 2025. Dresden, Federal Republic of Germany. Pp. 156-164.

17. Hladun O., Zalutska O., Klimenko V., Mazurets O. Research on the effectiveness of classifying the remains of destroyed buildings using MobileNetV3 neural network architecture. *Innovations in Science: From Theoretical Foundations to Practical Impact. Proceedings 1st International Scientific and Practical Conference.* May 12-14, 2025. Antwerp, Belgium. Pp. 158-162.

18. Hladun O.V., Molchanova M.O., Zalutska O.O., Mazurets O.V. Effectiveness research of using ViT neural network architecture for classifying the destroyed buildings remains. *Achievements of Science and Applied Research. Proceedings of 2nd International Scientific and Theoretical Conference.* May 19-21, 2025. Dublin, Ireland. Pp. 96-100.

19. Didur V., Molchanova M., Mazurets O. Research on the effectiveness of neural network detection of plots with the destroyed buildings remains. *Modern technologies and science: problems, new and relevant developments. Proceedings XXI International Scientific and Practical Conference.* May 26, 2025. Zaragoza, Spain. Pp. 245-251.

20. Dydo R., Sobko O., Klimenko V., Mazurets O. Datalogic structure for intelligent system for areas localization in photos with the remains of buildings using neural network. *Modern Scientific Research: Theoretical and Practical Aspects. Proceedings II International Scientific and Practical Conference.* May 26-28, 2025. Riga, Latvia. Pp. 123-127.

21. Molchanova M., Didur V., Mazurets O., Sobko O., Zakharkevich O. Method for Construction and Demolition Waste Classification Using Two-Factor Neural Network Image Analysis. *CEUR Workshop Proceedings, 2025, vol. 3970, pp. 168-182.*

УДК 004.8

Бербец Д.В., Петляк Н.С.

Хмельницький національний університет

АНАЛІЗ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ МОНІТОРИНГУ КІБЕРЗАГРОЗ

У роботі досліджено особливості впровадження технологій ШІ в системи кіберзахисту. Проаналізовано сучасні підходи до використання методів МН для моніторингу загроз, OSINT-розвідки та систем запобігання витокам даних. Показано, що застосування ШІ підвищує ефективність виявлення кіберзагроз, однак існує проблема захисту моделей МН.

The study examines the peculiarities of implementing AI technologies in cybersecurity systems. Modern approaches to the use of ML methods for threat monitoring, OSINT intelligence, and data loss prevention systems are analyzed. It is shown that the application of AI increases the efficiency of cyber threat detection; however, the problem of protecting ML models remains relevant.

В умовах цифрової трансформації суспільства та зростання залежності всіх секторів економіки від інформаційних технологій проблема забезпечення кібербезпеки набуває стратегічного значення. Стрімке збільшення кількості кібератак, їхня технічна складність і динамічна змінність методів зловмисників призводять до того, що традиційні сигнатурні підходи до моніторингу загроз демонструють низьку результативність. Такі методи не можуть ефективно аналізувати потоки великих даних, що постійно оновлюються, і виявляти нові, раніше невідомі вектори атак. Саме тому зростає актуальність застосування технологій штучного інтелекту (ШІ), зокрема методів машинного (МН) і глибокого навчання (ГН), які дозволяють створювати адаптивні та самонавчальні системи виявлення загроз.

Використання ШІ у сфері кібербезпеки сприяє формуванню гнучких механізмів захисту інформаційних систем. Завдяки здатності алгоритмів ШІ виконувати безперервний аналіз поведінкових шаблонів користувачів, мережевого трафіку й взаємодії між компонентами інфраструктури, з'являється можливість ідентифікувати аномалії на ранніх етапах, ще до того, як вони призведуть до інцидентів. Автоматизація процесів реагування, заснована на інтелектуальних моделях ухвалення рішень, істотно скорочує час ліквідації наслідків атак і підвищує стійкість інформаційних систем до зовнішніх впливів.

Проблема впровадження ШІ у сферу кіберзахисту активно досліджується як на міжнародному рівні, так і в Україні. Вітчизняні науковці О. М. Євтушенко, С. В.

Синьогуб, О. В. Лисенко, І. В. Примуженко та інші зосереджують увагу на розробці моделей МН для детектування кібератак, створенні систем адаптивного реагування та дослідженні методів інтелектуальної обробки великих даних. Їхні роботи формують основу сучасних науково-практичних підходів до побудови ефективних систем інформаційної безпеки. Водночас залишаються невирішеними питання забезпечення надійності моделей ШІ в умовах adversarial-атак, обмеженості доступу до якісно розмічених даних, а також труднощів інтеграції інтелектуальних рішень у наявні технологічні екосистеми підприємств і державних структур.

Метою дослідження є поглиблений аналіз сучасних концепцій і практик використання технологій ШІ в системах кіберзахисту, визначення їхніх переваг, обмежень і перспектив розвитку. У центрі уваги перебуває оцінка ефективності використання ШІ для інтелектуального моніторингу, OSINT-розвідки та систем запобігання витокам даних (DLP).

Розвідка на основі відкритих джерел (OSINT), що історично спиралася на ручний аналіз публічної інформації, у сучасних умовах зазнала глибокої технологічної трансформації. Завдяки впровадженню алгоритмів ШІ та МН, OSINT перетворюється на комплексну методологічну систему, яка охоплює весь життєвий цикл роботи з даними від збору та фільтрації інформації до її інтерпретації та формування аналітичних висновків. Такі інструменти, як Maltego, SpiderFoot, Social Links, Skopenios, дозволяють проводити масштабне картографування цифрових слідів, виявляючи взаємозв'язки між доменами, IP-адресами, сертифікатами, профілями користувачів і метаданими. Їх використання підвищує ефективність реагування на інциденти, дає змогу своєчасно виявляти спроби фішингових атак, реєстрацію підроблених доменів або створення шкідливих інфраструктур.

Крім того, важливу роль у системі кіберзахисту відіграють DLP-системи (Data Loss Prevention), що забезпечують запобігання витокам конфіденційної інформації. Інтелектуальні компоненти таких систем базуються на методах контентного аналізу, МН, пошуку за ключовими ознаками та цифрових відбитках. Алгоритми ШІ в DLP дають змогу ідентифікувати приховані витоки, аналізувати контекст даних і відрізнати легітимні дії користувачів від потенційно небезпечних. Це значно підвищує рівень захищеності інформаційних ресурсів та мінімізує ризик людського фактору.

Особливу увагу слід приділити аспектам безпеки самих систем ШІ, які стають потенційними цілями для атак. Серед найвідоміших міжнародних ініціатив у цій сфері можна виокремити проєкти MITRE, DARPA, а також стандарти, що розробляються Національним інститутом стандартів і технологій США (NIST). Ці ініціативи спрямовані на створення відкритих платформ для тестування безпеки моделей МН, розробку таксономій ризиків і механізмів їхнього зниження. Наприклад, Microsoft пропонує інструмент Counterfit для оцінки стійкості моделей ШІ, а Міністерство оборони США включило безпеку інтелектуальних систем до переліку базових принципів побудови алгоритмічних рішень.

Проведений аналіз свідчить, що впровадження технологій штучного інтелекту радикально змінює підходи до забезпечення кібербезпеки. Сучасні системи переходять від фіксації вже скоєних інцидентів до передбачення потенційних загроз через постійне навчання на основі накопичених даних. Це створює умови для формування нової парадигми безпеки, орієнтованої на випереджувальне виявлення ризиків, підвищення гнучкості систем захисту та їх здатності до самоадаптації в умовах невизначеності.

Водночас розширення можливостей ШІ породжує і нові виклики від необхідності захисту самих моделей до забезпечення етичності їх використання. Ризики, пов'язані з автоматизацією прийняття рішень, потребують створення комплексних систем аудиту, сертифікації та стандартизації алгоритмів. Особливе значення мають питання прозорості роботи моделей, верифікації вхідних даних і запобігання алгоритмічним упередженням.

Отже, технології ШІ не лише підвищують ефективність сучасних систем кіберзахисту, а й створюють передумови для розвитку нового покоління інформаційної безпеки, заснованої на аналітичному передбаченні, самонавчанні та інтеграції з глобальними базами даних про загрози. Подальші наукові дослідження мають бути спрямовані на вдосконалення алгоритмів детектування, створення методів захисту моделей МН від зовнішнього втручання, розробку національних стандартів безпеки ШІ та формування єдиного нормативного поля для їх практичного застосування у сфері кіберзахисту.

Перелік посилань

1. Катков Ю.І., Березовська Ю.В., Ключова В.В., Вишнівський О.В., Заднепрянець О.Ю., Ришиковець І.О. Аналіз способів застосування штучного інтелекту для покращення моніторингу захищеної ІТ-інфраструктури. Наукові записки ДУІКТ. 2025. №1(7). С.203-212. DOI: 10.31673/2786-8362.2025.016252
2. Антоненко А. В., Бенедіко І. В., Вічкарук А. І., Лисенко К. В., Сижко О. Ю. Класифікації моделей застосування машинного навчання у кібербезпеці. Таврійський науковий вісник. 2023. № 4. С. 11-22. DOI: 10.32782/tnv-tech.2023.4.2
3. Лозовський Р. Мороз А. Вплив штучного інтелекту на стратегії захисту інформаційних систем від нових типів кіберзагроз. Вісник Хмельницького національного університету. 2024. №3 (337), Т.2. С. 366-372. DOI: 10.31891/2307-5732-2024-337-3-55.

УДК 004.738.5

Благодир І.А., Гнатчук Є.Г.

Хмельницький національний університет

ІНФОРМАЦІЙНА СИСТЕМА ПІДТРИМКИ УПРАВЛІННЯ ДЕРЖАВНИМИ ІНФРАСТРУКТУРНИМИ ПРОЕКТАМИ НА ОСНОВІ ХМАРНИХ ТЕХНОЛОГІЙ

Розглянуто концептуальні підходи до проектування інформаційної системи підтримки управління державними інфраструктурними проектами, її структурну організацію та інтеграцію користувацьких інтерфейсів із базою даних у хмарному середовищі.

The conceptual approaches to designing an information system for supporting the management of state infrastructure projects, its structural organization, and the integration of user interfaces with the database in a cloud environment are considered.

Сучасний розвиток державного управління характеризується активним впровадженням цифрових інструментів, які сприяють підвищенню ефективності планування, реалізації та моніторингу інфраструктурних проектів [1]. З огляду на масштабність, багаторівневість та високу вартість таких проектів, виникає потреба у створенні єдиної інформаційної системи підтримки управління, що базується на хмарних технологіях. Хмарні сервіси дозволяють державним органам забезпечити централізоване управління даними, віддалений доступ до інформації, гнучкість масштабування, а також прозорість взаємодії між усіма учасниками проектного процесу від замовників і підрядників до контролюючих структур.

Метою роботи є розроблення концепції та визначення підходів до створення інформаційної системи підтримки управління державними інфраструктурними проектами на основі хмарних технологій, яка забезпечить підвищення ефективності планування, моніторингу, координації та контролю реалізації інфраструктурних ініціатив.

Концепція побудови сучасної інформаційної системи підтримки управління державними інфраструктурними проектами на основі хмарних технологій ґрунтується на інтеграції цифрових технологій обробки та аналізу даних, хмарних сервісів і аналітичних платформ, що забезпечує безперервну взаємодію всіх учасників життєвого циклу проекту, починаючи від його ініціації та завершуючи експлуатацією.

Основна ідея полягає у створенні єдиного цифрового простору, де всі дані щодо стану реалізації проєктів, фінансування, строків виконання, діяльності підрядників, ризиків та ефективності доступні в режимі реального часу, що значно підвищує прозорість та контрольованість процесів. Інформаційна система має модульну архітектуру, яка дозволяє адаптувати її до різних типів державних інфраструктурних проєктів, таких як транспортні, будівельні, енергетичні або соціальні об'єкти. Кожен модуль відповідає за окремі аспекти управління, включаючи планування ресурсів та графіків робіт, моніторинг виконання завдань і ключових показників ефективності, оцінку ризиків та розробку заходів реагування, а також забезпечує комунікацію між державними органами, підрядниками та громадськістю і створює умови для аналітики і формування звітів на основі даних.

Особливістю інфраструктурних проєктів державного рівня (будівництво доріг, мостів, лікарень, шкіл, систем водопостачання, енергетичних об'єктів тощо) є те, що вони вимагають координації великої кількості учасників, таких як міністерства, підрядні організації, банки, органи місцевого самоврядування та громадськість. Проблеми традиційних методів управління з використанням локальних баз даних або паперових звітів мають ряд недоліків, що в свою чергу призводять до затримок у реалізації проєктів, перевитрат коштів та ризику корупційних зловживань [2].

Хмарні технології можуть вирішити ряд цих проблем або зменшити їх вплив. Для державних потреб оптимальним є поєднання гібридної хмарної моделі, що поєднує безпечне зберігання критичних даних у державному дата-центрі з можливістю використання публічних сервісів (Microsoft Azure, Amazon Web Services, Google Cloud тощо) для аналітики, візуалізації та управління [3].

Отже, інформаційна система управління державними інфраструктурними проєктами має модульну структуру, що включає такі основні компоненти:

1. Модуль реєстрації та моніторингу проєктів для зберігання основних параметрів (бюджет, етапи, терміни, відповідальні); автоматичного відстеження статусів виконання та візуалізації прогресу у вигляді дашбордів.
2. Модуль управління документами для створення, погодження та версійний контролю документів з інтеграцією з електронним документообігом державних структур.
3. Фінансово-аналітичний модуль для контролю бюджетного фінансування, аналітики витрат за статтями та прогнозуванням ризиків перевищення кошторисів.
4. Модуль взаємодії з підрядниками та громадськістю для електронних тендерів та звітності підрядників.

5. Аналітичний модуль для візуалізації ключових показників та прогнозової аналітики.

Впровадження такої системи у хмарному середовищі забезпечує низку важливих переваг. Зокрема, масштабованість і гнучкість, доступність для всіх учасників, безпека, оскільки сучасні хмарні платформи підтримують шифрування, резервне копіювання та контроль доступу та відсутність потреби у локальному серверному обладнанні та скорочення витрат на адміністрування.

Отже, запропонована інформаційна система підтримки управління державними інфраструктурними проектами на основі хмарних технологій дозволяє підвищити ефективність планування, координації та контролю реалізації проектів завдяки централізованому зберіганню даних, інтеграції користувацьких інтерфейсів із базою даних та модульній архітектурі системи

Перелік посилань

1. Tsyfrovi transformatsii v Ukraini: chy vidpovidaiut vitchyzniani instytutsiini umovy zovnishnim vykykam ta yevropeiskomu poriadku dennomu? [Elektronnyi resurs]. URL: http://eap-csf.org.ua/wp-content/uploads/2021/04/Research_DT_PF_WG2_ua-1.pdf.
2. Jajac N. Decision Support for Infrastructure Management of Public Institutions. Sustainability. 2025. 17(5). p.2096.
3. Wang D., Zhong D., Li L. A comprehensive study of the role of cloud computing on the information technology infrastructure library (ITIL) processes. Library Hi Tech, 2022. Vol. 40 №6. pp. 1954–1975

УДК 004.8

Бондар О.А., Пасічник О.А., Скрипник Т.К.

Хмельницький національний університет

МЕТОД ДІАГНОСТИКИ ЗАХВОРЮВАНЬ ЗА ОПИСОМ СИМПТОМІВ НА ОСНОВІ РЕКУРЕНТНИХ НЕЙРОННИХ МЕРЕЖ

Розглянуто метод автоматичної діагностики захворювань за текстовими описами симптомів з використанням рекурентних нейронних мереж типу LSTM з механізмом уваги. Запропонована архітектура включає двонаправлений LSTM шар для захоплення контекстних залежностей, шар уваги для фокусування на важливих симптомах та повнозв'язні шари для класифікації. Розроблено модифікацію з додатковим навчанням ембедінгів на медичних текстах та механізмом max pooling.

A method for automatic disease diagnosis from textual symptom descriptions using LSTM recurrent neural networks with attention mechanism is considered. The proposed architecture includes a bidirectional LSTM layer for capturing contextual dependencies, an attention layer for focusing on important symptoms, and fully connected layers for classification. A modification with additional training of embeddings on medical texts and max pooling mechanism has been developed.

Автоматична діагностика захворювань за описом симптомів є важливою задачею для телемедицини та систем підтримки медичних рішень. Традиційні підходи базуються на правилах та експертних системах, які потребують ручного формування бази знань. Використання технологій обробки природної мови та глибокого навчання дозволяє автоматично витягувати залежності між симптомами та захворюваннями з текстових описів без необхідності експліцитного програмування правил діагностики [1-3].

Метою роботи є розробка методу автоматичної діагностики захворювань за текстовими описами симптомів на основі рекурентних нейронних мереж типу LSTM з механізмом уваги, який забезпечує високу точність класифікації та можливість інтерпретації результатів для медичного персоналу.

Запропонований метод базується на використанні рекурентних нейронних мереж для послідовної обробки текстових описів симптомів українською мовою. Вхідними даними є текстовий опис симптомів довжиною від 20 до 150 слів, а вихідними – розподіл ймовірностей по 23 можливих захворювань. Метод складається з чотирьох послідовних етапів (рисунок 1): попередня обробка тексту (токенізація, лематизація, видалення стоп-слів), векторизація токенів з використанням попередньо навчених ембедінгів розмірністю 300, обробка послідовності двонаправленим LSTM шаром з механізмом уваги для виявлення важливих симптомів, класифікація повнозв'язними шарами з функцією активації softmax.

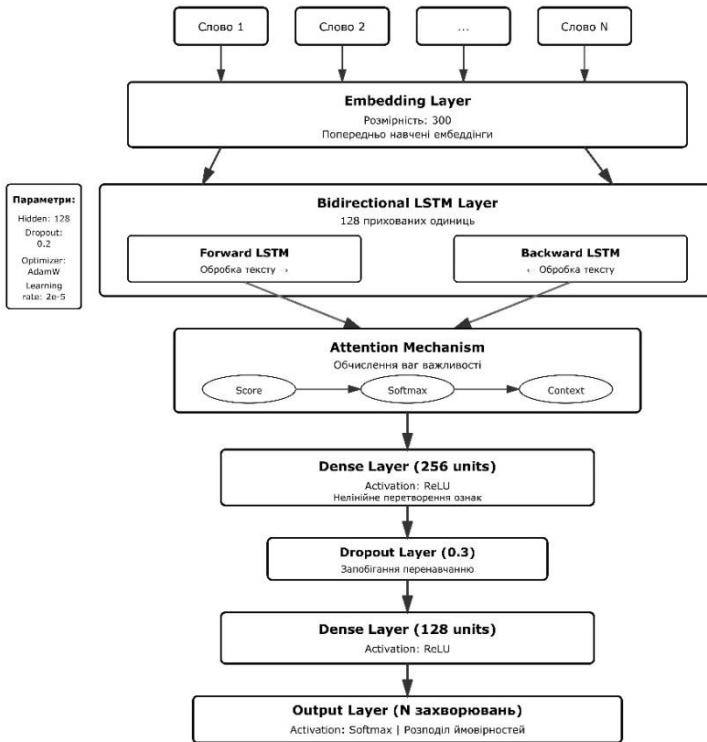


Рисунок 1 – Загальна схема методу діагностики захворювань

Етап попередньої обробки включає токенизацію тексту з використанням спеціалізованого токенизатора для української мови, очищення від непотрібних символів та приведення до нижнього регістру, лематизацію з використанням бібліотеки `ru morphology2` для приведення слів до базової словникової форми (наприклад, "болить", "боліло" → "боліти"), видалення стоп-слів. Особливістю попередньої обробки є збереження медичної термінології та її контекстного використання.

Архітектура нейронної мережі. Базова архітектура включає шар ембедінгів розмірністю 300, ініціалізований попередньо навченими векторними представленнями слів. Використовується двонаправлений LSTM шар з 128 прихованими одиницями, який обробляє послідовність слів у прямому та зворотному напрямках для врахування контексту з обох сторін. Шар LSTM використовує три вентиля для контролю потоку інформації: вектор вентиля забування, сигмоїдна функція, матриця ваг.

Механізм уваги обчислює ваги важливості для кожної позиції в послідовності. Для кожного виходу LSTM обчислюється скалярна оцінка

важливості, яка нормалізується функцією softmax. Зважена сума виходів LSTM формує фінальне представлення тексту, що дозволяє автоматично виявляти найбільш важливі симптоми для діагностики. Після шару уваги розташовані два шари з 256 та 128 нейронами відповідно з активацією ReLU та дропаут 0.3 для запобігання перенаванчання. Вихідний шар має 45 нейронів з функцією softmax.

Для покращення якості класифікації розроблено модифікацію базової архітектури з чотирма ключовими змінами. Перша модифікація – додаткове навчання ембедінгів на корпусі медичних статей та документації, що дозволяє векторним представленням краще відображати медичну термінологію (наприклад, "лихоманка" та "підвищена температура" отримують схожі вектори). Друга модифікація – додавання механізму max pooling паралельно до шару уваги, що дозволяє захопити найбільш виражені ознаки, після чого результати уваги та max pooling об'єднуються операцією конкатенації.

Третя модифікація – техніка поступового розморожування шарів під час навчання, коли спочатку заморожуються всі шари крім вихідного, а потім поступово розморожуються верхні шари, що знижує ризик перенаванчання. Додатково застосовується аугментація даних через випадкову заміну слів синонімами з медичного тезаурусу (наприклад, "головний біль" → "цефалгія").

Модифікована модель демонструє покращення точності на 5.2% порівняно з базовою версією при незначному збільшенні часу обробки (на 0.01 секунди). Особливо значне покращення спостерігається для рідкісних захворювань, де F1-score зріс на 7.8%. Аналіз матриці помилок показав, що найскладнішими для класифікації є захворювання зі схожими симптомами (грип та ГРВІ, різні типи інфекцій). Механізм уваги дозволяє визначити ключові симптоми: для діагнозу "грип" найбільшу вагу мають слова "лихоманка", "біль у м'язах", "слабкість". Порівняння з базовими методами показало перевагу: наївний баєсівський класифікатор – 68.4%, логістична регресія – 74.2%, LSTM без уваги – 82.1%.

Отже, модифікація з додатковим навчанням ембедінгів на медичних текстах та механізмом max pooling покращує точність на 5.2% порівняно з базовою архітектурою, особливо для рідкісних захворювань. Двонаправлений LSTM шар з 128 одиницями ефективно захоплює контекстні залежності між симптомами. Механізм уваги забезпечує інтерпретованість результатів через визначення найбільш важливих симптомів. Метод є придатним для практичного застосування в телемедичних системах та системах підтримки медичних рішень.

Перелік посилань

1. Balasubramanian N. S. P., Dakshit S. Can Public LLMs be used for Self-Diagnosis of Medical Conditions ? arXiv, 2024. URL: <https://doi.org/10.48550/arXiv.2405.11407>.
2. Raza S., Schwartz B. Constructing a disease database and using natural language processing to capture and standardize free text clinical information. Scientific Reports. 2023. Vol. 13, No. 1. Pp. 8591. URL: <https://doi.org/10.1038/s41598-023-35482-0>.
3. Wang Z., Wen R., Chen X., Cao S., Huang S.-L., Qian B., Zheng Y. Online Disease Self-diagnosis with Inductive Heterogeneous Graph Convolutional Networks / Proceedings of the Web Conference 2021, April 19, 2021. Pp. 3349–3358. URL: <https://doi.org/10.1145/3442381.3449795>.

УДК 004

Бондар О.П., Пасічник О.А., Скрипник Т.К., Петровський С.С.

Хмельницький національний університет

МЕТОД ВИЯВЛЕННЯ ШАХРАЙСЬКИХ ТРАНЗАКЦІЙ У ФІНАНСОВИХ ОПЕРАЦІЯХ З ЗАСТОСУВАННЯМ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ

Розглянуто прикладні аспекти розробки інформаційної системи для виявлення шахрайських транзакцій у фінансових операціях із використанням згорткових нейронних мереж. Запропонована система забезпечує ефективну обробку та аналіз великих обсягів транзакційних даних, виявляючи приховані закономірності, характерні для шахрайської поведінки.

The applied aspects of developing an information system for detecting fraudulent transactions in financial operations using convolutional neural networks are considered. The proposed system provides effective processing and analysis of large volumes of transaction data, revealing hidden patterns characteristic of fraudulent behavior.

Поява шахрайських транзакцій з банківськими картками збгається з розвитком електронних та безготівкових способів оплати. Шахрайські дії полягають у незаконному виведенні коштів з користувачів шляхом підробки даних картки або отримання несанкціонованого доступу до рахунків. Збільшення кількості випадків таких дій підштовхнуло фінансові організації до впровадження механізмів підвищеної безпеки, в даному випадку систем спостереження та виявлення сумнівних транзакцій.

Кредитні картки можуть бути фізично викрадені з гаманця або отримані віртуально з незахищених веб-сайтів, через витік даних або схеми крадіжки особистих даних. Наприклад, у 2019 році хакери зламали бази даних Capital One та оприлюднили інформацію про кредитні картки понад 100 мільйонів людей [1].

Захист фінансової інформації є важливим але, попри захист, який вони пропонується банками, кредитні картки не є захищеними від шахрайства. Навпаки, вони постійно є головною мішенню для злодіїв особистих даних, причому у 2024 році до Федеральної торгової комісії було подано майже 450 000 повідомлень про крадіжку особистих даних з кредитних карток [2].

Роль ШІ у виявленні фінансового шахрайства суттєво змінилася, перейшовши від статичних систем, заснованих на правилах, до динамічних, адаптивних алгоритмів. Структури раннього виявлення в основному залежали від заздалегідь визначених правил та ручного перегляду транзакцій, де сповіщення запускалися фіксованими параметрами, такими як сума транзакцій, частота або

географічне розташування. Хоча ці методи пропонували базовий рівень захисту, їм бракувало можливості адаптуватися до нових та складних шахрайських схем. Як наслідок, такі системи часто видавали високий рівень хибнопозитивних результатів, що призводило до неефективних розслідувань та погіршення обслуговування клієнтів.

Досягнення в машинному навчанні змінили цей процес, дозволивши системам аналізувати величезні набори даних та виявляти поведінкові моделі, що свідчать про шахрайську діяльність. Завдяки впровадженню таких методів, як поведінкова аналітика, глибоке навчання та нейронні мережі, сучасні моделі виявлення шахрайства тепер оцінюють численні точки даних у режимі реального часу. Ці системи на основі ІІ не лише оцінюють особу та наміри користувача, але й постійно адаптуються до нових та мінливих загроз. В результаті фінансові установи можуть досягти швидшого, точнішого та адаптивнішого виявлення шахрайства, значно підвищуючи як безпеку, так і операційну ефективність [3].

Розглянемо метод виявлення шахрайства з кредитними картками за допомогою перетворення зображень [4]

Автори розглядають зростаючу складність даних про транзакції з кредитними картками, що характеризуються високою швидкістю, серйозним дисбалансом класів та зміною моделей шахрайства, та пропонують нову структуру під назвою «Виявлення шахрайства за допомогою перетворення зображень» (FDIC) для покращення ефективності виявлення. У FDIC транзакції обробляються як часові ряди та перетворюються на двовимірні зображення за допомогою таких методів, як кутові поля Грама (GAF), поля переходів Маркова (MTF) та діаграми повторення (RP). Ці зображення потім класифікуються за допомогою згорткової нейронної мережі (CNN), тим самим фіксуючи часові та двосторонні зв'язки між характеристиками транзакцій, які може бути важко фіксувати за допомогою звичайних табличних або послідовних моделей. Для підвищення прозорості та інтерпретованості автори застосовують підхід штучного інтелекту (XAI) на основі теплових карт (через Grad-CAM та «сфокусований» варіант), щоб візуалізувати, які області перетворених зображень впливають на прийняття рішень моделлю.

Хоча запропонований підхід FDIC демонструє інновації у представленні даних про транзакції для виявлення шахрайства, певні обмеження та наслідки заслуговують на розгляд. Авторі повідомляють про F1-бал 85,49% та повноту 80,35% для класу шахрайства, що демонструє конкурентоспроможну продуктивність порівняно з попередніми дослідженнями.

Мета: розробка та програмна реалізація методу виявлення шахрайських транзакцій у фінансових операціях із використанням згорткових нейронних мереж.

На етапі попередньої обробки даних ознака Amount масштабована за допомогою RobustScaler. Цей метод базується не на мінімальних та максимальних значеннях, а на медіані та інтерквартильному розмаху, що робить його стійким до

наявності викидів у даних – поширеного явища у фінансових транзакціях, де окремі операції можуть мати надзвичайно великі суми. Формула перетворення має вигляд:

$$x' = \frac{x - \text{median}(x)}{\text{IQR}(x)} \quad (1)$$

У результаті більшість значень суми зосереджуються поблизу нуля, тоді як екстремальні транзакції не мають надмірного впливу на навчання моделі. Такий підхід забезпечує стабільнішу збіжність нейронної мережі та підвищує її стійкість до нетипових значень у даних.

Ознаку Time було нормалізовано до інтервалу $[-1,1]$ за допомогою лінійного перетворення:

$$x' = \frac{x - \min(x)}{\max(x) - \min(x)} \quad (2)$$

Таким чином, найменше значення часу отримує -1, найбільше +1, а всі проміжні значення рівномірно розподіляються між ними.

Після масштабування ознак було виконано балансування вибірки, оскільки у вихідних даних спостерігався суттєвий дисбаланс між кількістю шахрайських та не шахрайських транзакцій. У більшості реальних фінансових наборів даних кількість легітимних операцій значно перевищує кількість шахрайських, що може призвести до переважного навчання моделі на більший клас і, відповідно, погіршення здатності виявляти шахрайство.

Після тренування моделі було проведено оцінювання роботи моделі та отримано основні показники оцінювання роботи моделі (Риснок 1).

```
Epoch 1/5
3110/3110 ————— 19s 6ms/step - accuracy: 0.9817 - loss: 0.0502 - precision: 0.9831 - re
call: 0.9802 - val_accuracy: 0.9957 - val_loss: 0.0144 - val_precision: 0.9916 - val_recall: 0.9998
Epoch 2/5
3110/3110 ————— 18s 6ms/step - accuracy: 0.9960 - loss: 0.0145 - precision: 0.9944 - re
call: 0.9975 - val_accuracy: 0.9989 - val_loss: 0.0074 - val_precision: 0.9981 - val_recall: 0.9996
Epoch 3/5
3110/3110 ————— 18s 6ms/step - accuracy: 0.9974 - loss: 0.0097 - precision: 0.9964 - re
call: 0.9985 - val_accuracy: 0.9979 - val_loss: 0.0077 - val_precision: 0.9958 - val_recall: 0.9999
Epoch 4/5
3110/3110 ————— 18s 6ms/step - accuracy: 0.9982 - loss: 0.0071 - precision: 0.9974 - re
call: 0.9990 - val_accuracy: 0.9983 - val_loss: 0.0052 - val_precision: 0.9975 - val_recall: 0.9992
Epoch 5/5
3110/3110 ————— 17s 6ms/step - accuracy: 0.9984 - loss: 0.0061 - precision: 0.9978 - re
call: 0.9991 - val_accuracy: 0.9985 - val_loss: 0.0072 - val_precision: 0.9975 - val_recall: 0.9996
2666/2666 ————— 4s 1ms/step - accuracy: 0.9981 - loss: 0.0057 - precision: 0.9971 - re
call: 0.9992

Model Evaluation:
Accuracy: 1.00
Precision: 1.00
Recall: 1.00
F1: 1.00
```

Рисунок 1 – Процес та результати тренування моделі

На основі отриманих результатів навчання розроблена згорткова нейронна мережа (ЗНМ) продемонструвала винятково високу продуктивність у завданні

виявлення шахрайських транзакцій. Протягом п'яти епох навчання точність як навчання, так і валідації постійно зростала, досягнувши приблизно 99,8–99,9% з дуже низьким значенням втрат (близько 0,005–0,007). Значення точності та повноти як на навчальному, так і на валідаційному наборі також були надзвичайно високими (близько 0,998–0,999), що свідчить про те, що модель успішно ідентифікує майже всі шахрайські транзакції, практично не даючи хибнопозитивних результатів.

Під час остаточної тестової оцінки модель досягла 100% точності, прецизійності, повноти та F1-балу, що підтверджує її хороше узагальнення та високу надійність у розрізненні шахрайських та легітимних операцій. Такі результати показують, що кроки попередньої обробки, обрана архітектура ЗНМ та стратегія оптимізації були ефективними. Однак, незважаючи на ці ідеальні показники, важливо зазначити, що така висока продуктивність може також свідчити про незначне перенавчання через синтетичне балансування та відносно просту структуру даних про транзакції. Тому для розгортання в реальних фінансових системах рекомендується додаткова валідація на реальних, невидимих потоках транзакцій, щоб забезпечити стійкість моделі та стабільну продуктивність у динамічних реальних умовах.

Перелік посилань

1. Credit Card Fraud Detection: How To Spot & Avoid Fraud URL: <https://www.identityguard.com/news/credit-card-fraud-detection>
2. credit card scams to watch out for in 2025 URL: <https://lifelock.norton.com/learn/fraud/credit-card-scams>
3. Financial Fraud Detection in the AI Era: Best Practices for Compliance and Risk Management – Avahi URL: <https://avahi.ai/blog/financial-fraud-detection-in-the-ai-era/>
4. Explainable Credit Card Fraud Detection with Image Conversion — d9ffa86ca415aeefcbcd3703ed6d602598db.pdf URL: <https://pdfs.semanticscholar.org/e437/d9ffa86ca415aeefcbcd3703ed6d602598db.pdf>

УДК 004.8

Боярчук І.О., Молчанова М.О.

Хмельницький національний університет

ПІДХІД ДО НЕЙРОМЕРЕЖЕВОГО ВИЯВЛЕННЯ МОВИ ВОРОЖНЕЧІ У ЗАШУМЛЕНИХ ТЕКСОВИХ ПОВІДОМЛЕННЯХ

У роботі розглянуто нейромережевий підхід до виявлення мови ворожнечі у зашумлених текстових повідомленнях соціальних мереж і месенджерів, де широко присутні орфографічні відхилення, суржик, емодзі, транслітерація та змішані мовні коди. Метою є підвищення точності та стійкості класифікації за рахунок адаптації моделі до спотворених і навмисно маскованих мовних конструкцій. Запропоновано двоетапний конвеєр: на першому етапі формується контрольовано зашумлений корпус на основі анотованого набору «Hate Speech Detection curated Dataset» з побудовою чистої та зашумленої підвипірок; на другому – здійснюється поетапне донавчання трансформерної моделі типу BERT/RoBERTa з мінімальною нормалізацією тексту. Результати підтверджують доцільність включення параметризованих шумових операторів у навчальний цикл та окреслюють перспективи використання підходу у сервісах модерації контенту й моніторингу інформаційної безпеки.

The paper presents a neural network-based approach to hate speech detection in noisy short texts from social media and messaging platforms, which are characterised by spelling deviations, code-mixing, emojis, transliteration and intentionally distorted tokens. The aim is to improve the accuracy and robustness of hate speech classification by adapting the model to corrupted and masked linguistic patterns. A two-stage pipeline is proposed. First, a controllably noised training corpus is constructed on top of the annotated “Hate Speech Detection curated Dataset” by generating clean and noisy subsets. Second, a transformer model of the BERT/RoBERTa family is progressively fine-tuned on these data under conditions of minimal text normalisation. The proposed approach can serve as a foundation for content moderation services, information security monitoring systems and analytical tools for public online communication.

Підхід до нейромережового виявлення мови ворожнечі у зашумлених повідомленнях ґрунтується на усвідомленні того, що сучасні цифрові комунікації формуються не в умовах «лабораторної» мови, а в середовищі постійних викривлень [1]. Соціальні мережі, месенджери та коментарні платформи насичені суржигом [2], орфографічними девіаціями [3], емодзі, навмисними замінами символів, транслітерацією та змішаністю мовних кодів [4]. У такому контексті навіть потужні трансформерні моделі [5, 6], навчені на відносно чистих корпусах [7], втрачають чутливість до завуальованої агресії, оскільки ключові лексичні маркери мови ворожнечі маскуються або систематично спотворюються [8]. Це зумовлює потребу не лише у більш складних архітектурах, а насамперед у методах,

які прямо враховують шумовий характер вхідних даних [9] і відтворюють його на етапі навчання [10].

Актуальність дослідження виявлення мови ворожнечі у зашумлених повідомленнях зумовлена стрімким зростанням обсягів неформального, спонтанного та навмисно модифікованого текстового контенту в соціальних мережах і месенджерах [11]. У середовищах, де користувачі активно застосовують нестандартні правописні форми, жаргон, суржик, коди-міксинг, емодзі та символи, що виконують семантичні функції, традиційні методи автоматичної модерації втрачають ефективність [12]. Мова ворожнечі дедалі частіше маскується шляхом орфографічних викривлень [13], введенням латинізмів, навмисним «каламутінням» токсичних слів або їхнім креативним поділом [14], що ускладнює роботу як класичних алгоритмів, так і сучасних моделей без додаткової адаптації [15]. У контексті посилення інформаційної безпеки та необхідності швидкого реагування на токсичний контент, що може сприяти ескалації конфліктів, радикалізації або порушенню прав користувачів, розроблення методів стійкого до шумів розпізнавання мови ворожнечі постає як критично важливе завдання.

Сучасні підходи NLP відкривають широкі можливості для роботи з такими ускладненими, гетерогенними текстовими потоками, оскільки моделі глибинного навчання здатні оперувати контекстуальними представленнями, враховувати багатозначність та латентні структури, притаманні неформальному онлайн-дискурсу [16]. Трансформерні архітектури [17], зокрема BERT-подібні моделі [18], демонструють здатність інтерпретувати послідовності зі змішаними кодами, відносно стійко працювати з неповними або деформованими токенами [19] та вловлювати семантичну подібність [20] навіть у разі суттєвих орфографічних модифікацій. Додатковий потенціал криється у можливості навчання на спеціально створених зашумлених корпусах [21], де моделі поступово формують інваріантні до шумів представлення й набувають здатності узагальнювати токсичні патерни у значно ширшому діапазоні їхніх проявів, ніж той, який міститься у вихідних «чистих» даних.

Розвиток напрямку також пов'язаний із дедалі активнішим впровадженням методів робастного навчання, спрямованих на забезпечення стабільної роботи моделей у реалістичних умовах. Параметризовані оператори шуму, регуляризаційні техніки та доменно-орієнтоване донавчання дозволяють наближати тренувальні дані до фактичної комунікації користувачів, де помилки, жаргонізми та креативні викривлення є нормою. У поєднанні з методами тонкого донавчання та динамічного машинного розуміння контексту це дає змогу суттєво підвищити якість і надійність класифікації мови ворожнечі, забезпечуючи адаптивність моделей до різноманітних типів спотворених вхідних сигналів [22].

З огляду на те, що токсичний контент часто виникає саме в умовах підвищеної емоційності та неструктурованого письма, NLP-підходи, орієнтовані на

роботу з шумами, стають ключовим інструментом для побудови ефективних систем модерації, моніторингу та аналізу інформаційних загроз. Дослідження у цьому напрямку не лише підвищують точність автоматичного виявлення небезпечних повідомлень, а й сприяють формуванню більш стійких, адаптивних та етично орієнтованих технологій аналізу онлайн-комунікацій.

Метою запропонованого підходу є підвищення точності та стійкості виявлення мови ворожнечі у зашумлених соціальних текстових даних шляхом розроблення нейромережевого методу, адаптованого до спотворених, змішаномовних і навмисно маскованих мовних конструкцій. На відміну від традиційних рішень, що припускають попереднє очищення текстів або їхню максимальну нормалізацію, у роботі реалізовано концепцію контрольованого зашумлення корпусу з подальшим донавчанням моделі у «реалістичних» умовах цифрового мовлення. Об'єктом дослідження виступає процес автоматизованого виявлення мови ворожнечі у соціальних текстах із нестабільною мовною структурою та наявністю шумових викривлень, а предметом – моделі, методи та засоби обробки природної мови, здатні інтерпретувати такі тексти без істотної втрати класифікаційної якості.

Ключова ідея методу полягає у побудові двоетапного конвеєра. На першому етапі формується контрольовано зашумлений навчальний корпус на основі початкового датасету виявлення мови ворожнечі, до якого застосовуються спеціально спроектовані оператори лінгвістичних викривлень. Вони імітують типові для соціальних мереж практики модифікації тексту: випадкові та систематичні орфографічні помилки, заміна літер схожими символами, часткова або повна транслітерація, домішування елементів іншої мови, вставка емодзі та графічних маркерів, що виконують семантичну або маскувальну функцію. Введення таких спотворень дає змогу сфокусувати навчання моделі не на поверхневій формі токенів, а на стійкіших контекстуальних патернах агресивної комунікації.

Для валідації методу використано анотований набір даних «Hate Speech Detection curated Dataset» з платформи Kaggle, що містить бінарну розмітку повідомлень за класами «мова ворожнечі» / «нейтральний текст» та відображає сучасні практики онлайн-комунікації із включенням сленгу, скорочень і емодзі. На основі цього корпусу побудовано чисту та зашумлену підвибірки, які застосовано для поетапного донавчання трансформерної моделі типу BERT/RoBERTa. Така організація даних дозволяє порівнювати поведінку класифікатора на стандартизованих і спотворених текстах та оцінювати внесок шумового донавчання у підвищення стійкості до реальних цифрових викривлень.

На другому етапі реалізується власне нейромережевий аналіз. Попередню донавчена модель приймає на вхід текстові фрагменти, які проходять мінімальну попередню обробку (токенізація, приведення до формату, сумісного з архітектурою трансформера) без агресивної нормалізації, що могла б знищити інформативні

шумові патерни. Мережа видає як категоріальну оцінку наявності мови ворожнечі, так і числовий бал впевненості, який може бути використаний у політиках модерації та для побудови людиноорієнтованих інтерфейсів пояснення. Оцінювання якості здійснюється за класичними для задач бінарної класифікації метриками – точністю, повнотою, F_1 -мірою, а також за допомогою аналізу помилок на підмножинах із різними типами шуму. Особлива увага приділяється збереженню повноти виявлення ворожих висловлювань, оскільки асиметрія класів робить просту точність ненадійним показником.

Експериментальні дослідження засвідчили, що попереднє формування контрольовано зашумлених корпусів у поєднанні з цілеспрямованим донавчанням трансформерної моделі підвищує стійкість класифікації до орфографічних, графічних і змішаномовних викривлень. У порівнянні з базовою моделлю, навченою на «очищений» вибірці, запропонований підхід забезпечує вищі значення F_1 -міри для класу мови ворожнечі саме на повідомленнях зі штучно змодельованим шумом, зменшуючи кількість пропущених агресивних випадків за незначного зростання кількості хибних спрацьовувань. Отримані результати свідчать, що параметризація шумових операторів та їх включення у навчальний цикл є ефективним способом адаптації нейромережових моделей до реальних умов функціонування в соціальних мережах.

Запропонований підхід може бути використаний як основа для побудови сервісних модулів модерації контенту в соціально-орієнтованих платформах, системах моніторингу інформаційної безпеки та інструментах аналітики публічних комунікацій. Подальші дослідження доцільно спрямувати на розширення номенклатури шумових трансформацій із урахуванням специфіки україномовних і змішаномовних онлайн-спільнот, експерименти з гібридними архітектурами та інтеграцію інтерпретованих методів аналізу (LIME, SHAP) для підвищення пояснюваності рішень нейромережі у чутливих з етичної та правової точки зору сценаріях використання.

Перелік посилань

1. Unnava S., Parasana S. R. A Study of Cyberbullying Detection and Classification Techniques: A Machine Learning Approach. Engineering, Technology & Applied Science Research. 2024. Vol. 14, no. 4. P. 15607–15613.
2. Hladun O., Mazurets O., Molchanova M., Sobko O. Real Time Detection the Person Emotion State Using Neural Network. Scientific Research: Modern Innovations and Future Perspectives. Proceedings of the 2 International scientific and practical conference. November 25-27, 2024. Montreal, Canada. 2024. Pp. 119-123.
3. Mazurets O., Molchanova M., Klimenko V., Prosvitliuk M Practice Implementation of Neural Network Model BART-Large-CNN for Text Annotation. Prospects of Scientific Research in the Conditions of the Modern World. Proceedings of XXVII International scientific and practical conference. June 12-14, 2024. Rotterdam, Netherlands. 2024. Pp. 97-102.

4. Віт Р.В., Мазурець О.В. Тематична класифікація текстової інформації засобами обробки природної мови. Збірник наукових праць XXIII Міжнародної наукової конференції «Нейромережні технології та їх застосування НМТіЗ-2024». 11-12 грудня 2024. Краматорськ-Тернопіль, ДДМА. 2024. с. 63-66.
5. Овчарук О.М., Мазурець О.В. Нейромережеве діагностування проявів ПТСР у текстовому контенті з використанням помилко-орієнтованого навчального набору даних. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2024. №6, Т.1 (343). С. 195-200.
6. Civila S. Cyberbullying. Comprehensive Sexuality Education for Gender-Based Violence Prevention. 2024. P. 229–245.
7. Овчарук О.М., Мазурець О.В. Нейромережева архітектура з квантовим шаром для аналізу текстових повідомлень на прояви посттравматичного стресового розладу. Науковий журнал «Наука і техніка сьогодні». Київ, 2024. №13 (41). С. 1192-1204.
8. Мазурець О.В., Тимофієв І.А., Кліменко В.І., Тищенко О.О. Метод виявлення депресивного стану пов'язаного із навчанням у закладах освіти із використанням нейромережі дуальної архітектури. Науковий журнал «Вісник Херсонського національного технічного університету». 2024. №4 (91). С. 311-318.
9. Віт Р.В., Мазурець О.В. Підхід до тематичної класифікації текстової інформації засобами обробки природної мови. Науковий журнал «Наукові праці Донецького національного технічного університету», серія «Проблеми моделювання та автоматизації проектування». 2025. №1 (21). С. 94-99.
10. Овчарук О.М., Мазурець О.В. Нейромережевий метод діагностування психологічних розладів за аналізом повідомлень на основі роздільного підходу до класифікації. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». № 1, 2025. с. 210-216.
11. Blazhuk V., Mazurets O., Zalutska O. An Approach to Using the mBERT Deep Learning Neural Network Model for Identifying Emotional Components and Communication Intentions. The Impact of Scientific Research on the Development of the Modern World. Proceedings of the XLIV International scientific and practical conference. October 23-25, 2024. Dubrovnik, Croatia. 2024. Pp. 79-84.
12. Tymofiiiev I., Mazurets O., Hardysh D., Molchanova M. Neural Network Dual Architecture for Depression Detection Using Cloud Services. Scientific Research in the Era of Digital Technologies: Challenges and Opportunities. Proceedings of the XLVI International scientific and practical conference. November 6-8, 2024. Barcelona, Spain. 2024. Pp. 84-88.
13. Юрченко Д.Ю., Овчарук О.М., Мазурець О.В., Шевчук П.О. Метод використання нейромережі гібридної архітектури для визначення емоційної тональності текстових повідомлень. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». № 2, 2025. с. 136-141.
14. Mazurets O., Tymofiiiev I., Dydo R. Approach for Using Neural Network BERT-GPT2 Dual Transformer Architecture for Detecting Persons Depressive State. Ricerche scientifiche e metodi della loro realizzazione: esperienza mondiale e realtà domestiche. Raccolta di articoli scientifici con gli atti della VI Conferenza scientifica e pratica internazionale. 15 novembre, 2024. Bologna, Repubblica Italiana. 2024. Pp. 147-151.
15. Віт Р.В., Мазурець О.В. Метод виявлення психологічного цифрового перевантаження за аналізом текстових даних нейромережевими моделями глибокого навчання. Науковий

журнал «Вісник Херсонського національного технічного університету». 2025. №2 (93). Т. 2. С. 107-114.

16. Mazurets O., Sobko O., Vit R., Pasternak V. Practical Approach for Detection by Deep Learning of Target Objects of Subject Area Based on Semantic Connectivity Indicators in Audio Database. Proceedings of XXIV International Scientific and Practical Conference «Modern Scientific Challenges are the Driving Force of the Development of Scientific Research». May 22-24, 2024. Bruges, Belgium. International Scientific Unity. 2024. Pp. 91-96.

17. Біт Р.В., Мазурець О.В. Метод виявлення комунікаційних об'єктів як індикаторів цифрової втоми. Інтелектуальний метод виявлення цільових об'єктів предметної області для класифікації текстової інформації. Матеріали XIII Міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології ІУСТ-ОДЕСА-2025». 24-26.09.2025. Одеса. 2025. С.119-121.

18. Yurchenko D., Mazurets O., Didur V., Molchanova M. Approach to Using Cloud Services for Visual Analytics of Neural Network Analysis of Texts Emotional Tonality. The Future of Scientific Discoveries: New Trends and Technologies. Proceedings of the XLVII International scientific and practical conference. November 13-15, 2024. Marseille, France. 2024. Pp. 108-113.

19. Mazurets O.V., Sobko O.V., Molchanova M.O., Zalutska O.O., Yurchak A.V. Practical Implementation of Neural Network Method for Stress Features Detection by Social Internet Networks Posts. Global Science: Prospects and Innovations. Proceedings of the II International Scientific and Theoretical Conference «Scientific Review of the Actual Events, Achievements and Problems». May 31, 2024. Berlin, Federal Republic of Germany: International Center of Scientific Research. 2024. Pp. 160-167.

20. Molchanova M., Mazurets O., Sobko O., Boiarchuk I. Object-Oriented Approach for Ethnic Enmity Detection in Text Messages by NLP. Proceedings of XXI International Scientific and Practical Conference «Scientific Achievements and Innovations as a Way to Success». May 1-3, 2024. Vilnius, Lithuania. 2024. Pp. 73-77.

21. Casas F. Age Discrimination. Encyclopedia of Quality of Life and Well-Being Research. Cham, 2023. P. 118–121.

22. Lee H. Lived Religion in Religious Vaccine Exemptions. Perspectives in Biology and Medicine. 2024. Vol. 67, no. 1. P. 96–113.

УДК 004.4

Ваховська В.М., Праворська Н.І.

Хмельницький національний університет

СКЕМА: СКЕТЧ-ОРІЄНТОВАНИЙ АДАПТЕР ДЛЯ ПАРАМЕТРОЕФЕКТИВНОГО ТОНКОГО НАЛАШТУВАННЯ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ

Запропоновано SkeMA – нову архітектуру адаптера для параметроефективного тонкого налаштування LLM в обмежених середовищах. Метод поєднує нульовий інференс-оверхед (завдяки повному злиттю) з потенційно вищою виразністю за сталого бюджету параметрів шляхом навчання компактного блоку у стислому підпросторі з фіксованими проєкціями.

Proposed SkeMA – a new adapter architecture for parameter-efficient fine-tuning of LLM in resource-constrained environments. The method combines zero inference overhead (due to full merge) with potentially higher expressivity at a fixed parameter budget by training a compact block in a compressed subspace with fixed projections.

Інтеграція великих мовних моделей (LLM) у продукти обмежується трьома факторами: високою вартістю донавчання на обмежених ресурсах, затримками на інференсі та потребою підтримувати багато доменних варіантів однієї базової моделі [1]. Парадигма параметрично ефективного донавчання (PEFT) зменшує кількість навчуваних параметрів, однак зберігає компроміси, що впливають на продуктивність і розгортання [2]. Зокрема, адитивні методи (класичні адаптери, підказки) додають обчислення на етапі інференсу, тоді як підходи зі злиттям результатів навчання з базовими вагами усувають інференс-накладні витрати, але обмежують виразність оновлень через низькорангову природу змін. Це формує практичний запит на метод, який поєднує відсутність інференс-накладних витрат після злиття та вищу ефективну розмірність оновлень за сталого параметричного бюджету [3].

Класичні адаптери Houlsby [4] вставляються в кожен блок трансформера двічі, утворюють вузький «bottleneck» і навчаються за фіксованих базових ваг (рис. 1). Вони економічні за параметрами, але створюють додаткову гілку обчислень на інференсі.

LoRA описує оновлення ваг як низькорангове наближення і після навчання зливає адаптер у базові ваги. Це повертає вихідну архітектуру без додаткових обчислень, однак виразність модифікацій визначається вибраним рангом. На

складних задачах для збереження якості часто доводиться підвищувати ранг і, відповідно, параметричний бюджет.

BitFit навчає лише bias-параметри у шарах трансформера та класифікаторі. Підхід дуже простий, не додає оверхеду на інференсі і різко зменшує кількість навчуваних ваг, але за максимальною якістю зазвичай поступається гнучкішим методам.

IA³ мінімізує кількість параметрів завдяки множникам, що масштабують внутрішні активації. Ці множники можна «влити» у ваги перед розгортанням, тому інференс не сповільнюється. Водночас гнучкість таких змін нижча, ніж у низькорангових оновлень, і на частині задач IA³ поступається LoRA.

Prompt- і prefix-tuning зменшують навчувані параметри до підказок, не змінюючи архітектуру. Це зручно і швидко, але потенційно обмежує глибину адаптації, тому в практиці ці підходи часто поєднують з адаптерами.

QLoRA квантує базову модель до 4 біт і навчає адаптери у 16 біт. Поєднання NF4 і подвійного квантування дозволяє тонувати моделі з десятками мільярдів параметрів на одній GPU, зберігаючи якість близьку до 16-бітного режиму. Водночас QLoRA успадковує архітектурне обмеження LoRA, пов'язане з фіксованим рангом.

AdaLoRA вирішує проблему фіксованого рангу шляхом адаптивного розподілу параметричного бюджету. Метод динамічно перерозподіляє ресурси між шарами та матрицями, відсікаючи менш важливі компоненти оновлення, при цьому повністю зберігаючи можливість злиття з базовою моделлю.

DoRA, у свою чергу, пропонує декомпозицію ваг на компоненти напрямку та величини. Низькорангове оновлення застосовується лише до компоненти напрямку, тоді як величина оптимізується окремо. Такий підхід підвищує здатність моделі до навчання, не порушуючи параметричної ефективності та можливості злиття.

Узагальнюючи, у сучасній літературі фіксуються дві ключові прогалини [5]. По-перше, обмежена виразність низькорангових оновлень без збільшення параметричного бюджету. По-друге, наявність інференс-накладних витрат у класичних адаптерів, які доводиться враховувати у продакшені. Додатково важливими залишаються коректна взаємодія з агресивним квантуванням і стабільність навчання при стисканні представлень.

Мета роботи полягає у створенні та обґрунтуванні адаптера SkeMA, який переносить навчання у стислий підпростір із фіксованими проєкціями, навчає лише компактне «ядро» та повністю зливається з базовими вагами після навчання. Очікуваний результат полягає у поєднанні відсутності накладних витрат на інференсі зі зростанням ефективної розмірності оновлень за сталого параметричного бюджету, що підсилює практичну придатність підходу в умовах обмежених ресурсів.

Концепція методу SkeMA (Sketched Matrix Adapter) полягає у формуванні параметроефективного адитивного оновлення (ΔW) до базової матриці ваг (W) лінійного шару (рис. 1). Архітектура підходу розроблена для забезпечення повного злиття з базовими вагами після завершення процесу тонкого налаштування.

Під час фази навчання обчислювальний шлях адаптера складається з трьох послідовних етапів:

- вхідний вектор активацій стискається у підпростір меншої розмірності за допомогою фіксованої лінійної проєкції (S_{in});

- у цьому стислому підпросторі до вектора застосовується компактний параметричний блок (M), який є єдиним компонентом, параметри якого навчаються;

- отриманий вектор розгортається назад у вихідний простір через другу фіксовану лінійну проєкцію (S_{out}^T) і додається до виходу основного шару.

Таким чином, повне адитивне оновлення ваг, що генерується адаптером, ΔW_{SkeMA} (1), може бути виражене як добуток трьох матриць:

$$\Delta W_{SkeMA} = S_{out}^T M S_{in} \quad 1)$$

де S_{in} , S_{out} – фіксовані (нетреновані) проєкції, M – єдиний тренований блок.

Після завершення навчання виконується одноразова операція злиття (2), яка модифікує базові ваги моделі:

$$W \leftarrow W + \alpha \Delta W_{SkeMA} \quad 2)$$

де α – коефіцієнт масштабування.

В результаті, граф обчислень моделі повертається до своєї вихідної архітектури. Це повністю усуває будь-яке додаткове обчислювальне навантаження (inference overhead) під час експлуатації та забезпечує нульову затримку.

Для емпіричної валідації та коректного зіставлення методу SkeMA з еталонними низькоранговими підходами, як-от LoRA, було визначено протокол оцінювання. Ключовим гіперпараметром методу є розмірність стислого простору k . Цей параметр визначає як ефективну розмірність оновлення (верхня межа рангу $\leq k$), так і кількість параметрів, що навчаються, яка складає k^2 . Це дозволяє чітко співставляти SkeMA з низькоранговими підходами за однакового параметричного бюджету.

Протокол передбачає два сценарії порівняння, засновані на паритеті, для коректного зіставлення SkeMA з LoRA. Перший сценарій, паритет параметрів, передбачає фіксацію однакової кількості тренованих параметрів для обох методів (наприклад, $k^2 \approx 16384$, що відповідає $k = 128$ для SkeMA та $r = 8$ для LoRA). У

цьому випадку SkeMA демонструє значно вищу потенційну виразність, оскільки верхня межа рангу оновлення визначається розміром k , який суттєво перевищує r (ранг ≤ 128 проти ≤ 8). Другий сценарій, паритет обчислень, забезпечує співмірну обчислювальну вартість кроку навчання, що відповідає умові $k \approx r$ (наприклад, $k = r = 8$). За таких умов SkeMA має кардинально менший параметричний слід ($k^2 = 64$ параметри) порівняно з LoRA ($\approx 16\,384$ параметри) при однаковій межі виразності (ранг ≤ 8).

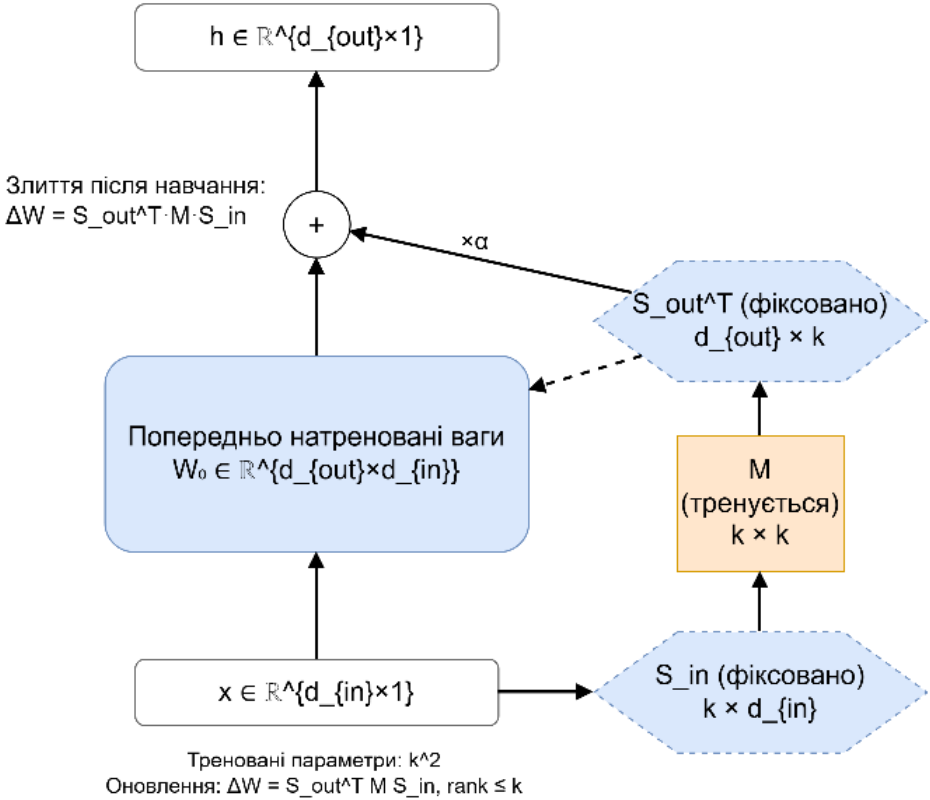


Рисунок 1 – Схема роботи адаптера SkeMA

Попередня валідація реалізації була проведена на задачі мовного моделювання (модель Pythia-160M, корпус WikiText-2). Обидві схеми продемонстрували стабільну збіжність, а отримані валідаційні показники перплексії є близькими (SkeMA ≈ 40.5 , LoRA ≈ 39.3).

Отже, запропонований метод SkeMA надає архітектурне рішення для підвищення гнучкості параметроефективних оновлень за сталого бюджету параметрів, концентруючи треновані параметри у компактному блоці, що діє у стислому підпросторі, та забезпечуючи нульове навантаження на інференсі шляхом повного злиття. Початкові експерименти підтверджують стабільність та якість методу, що обґрунтовує доцільність подальших досліджень щодо оптимізації гіперпараметрів, вивчення різних типів проєкцій та розширення на інші завдання й техніки.

Перелік посилань

1. Zhang S., Roller S., Goyal N., та ін. OPT: Open Pre-trained Transformer Language Models. arXiv preprint arXiv:2205.01068. 2022. URL: <https://arxiv.org/abs/2205.01068> (дата звернення: 22.10.2025).
2. Ouyang L., Wu J., Jiang X., та ін. Training language models to follow instructions with human feedback. arXiv preprint arXiv:2203.02155. 2022. 68 p. URL: <https://arxiv.org/pdf/2203.02155> (дата звернення: 22.10.2025)
3. Pfeiffer J., Vulić I., Gurevych I., Ruder S. Modular Deep Learning. Transactions of the Association for Computational Linguistics. 2023. Vol. 11. P. 187–204.
4. Tunstall L., von Werra L., Wolf T. Natural Language Processing with Transformers. Sebastopol, CA: O'Reilly Media, 2022. 408 p.
5. Zhao W. X., Zhou K., Li J., Tang T., Wang X., та ін. A Survey of Large Language Models. arXiv preprint arXiv:2303.18223. 2023. URL: <https://arxiv.org/abs/2303.18223> (дата звернення: 22.10.2025).

УДК 004.4

Відельський Я.В., Кльоц Ю.П., Піснячевський Я.В., Рудий Р.С.

Хмельницький національний університет

ВИЯВЛЕННЯ ПРИХОВАНИХ КАНАЛІВ ПЕРЕДАЧІ У ВИХІДНОМУ ТРАФІКУ ПУБЛІЧНИХ МЕРЕЖ

Робота присвячена виявленню прихованих каналів передачі у вихідному трафіку публічних мереж. Запропоновано методiku аналізу з використанням Wireshark, Suricata, Zeek та NetFlow, що поєднує сигнатурні, статистичні й поведінкові підходи. Експерименти в середовищі NAT підтвердили ефективність методу: точність виявлення DNS- та ICMP-каналів перевищила 90%. Отримані результати свідчать про можливість інтеграції системи у сучасні засоби мережевого моніторингу для підвищення безпеки публічних мереж.

The study focuses on detecting covert communication channels in outbound traffic of public networks. A comprehensive analysis methodology using Wireshark, Suricata, Zeek, and NetFlow is proposed, combining signature-based, statistical, and behavioral approaches. Experiments conducted in a NAT environment confirmed the method's efficiency, achieving over 90% accuracy in detecting DNS and ICMP channels. The obtained results demonstrate the feasibility of integrating the developed system into modern network monitoring solutions to enhance public network security.

Зростання обсягів трафіку в публічних мережах, особливо у середовищах із динамічними IP-адресами та NAT-трансляцією, ускладнює контроль вихідних потоків даних. Приховані канали передачі (covert channels) використовуються для непомітного виведення інформації за межі корпоративних і публічних мереж, що становить загрозу конфіденційності й цілісності систем. Найчастіше зловмисники застосовують техніки DNS- або HTTP-стеганографії, ICMP-тунелювання чи часові маніпуляції між пакетами [1].

Актуальність теми зумовлена тим, що традиційні сигнатурні системи виявлення не завжди фіксують аномалії в шифрованому трафіку, тоді як поведінкові ознаки прихованих каналів часто залишаються поза увагою. Мета роботи – розробити та експериментально перевірити методiku виявлення прихованих каналів передачі у вихідному трафіку публічних мереж на основі аналізу часових і структурних характеристик.

Сучасні дослідження поділяють методи виявлення прихованих каналів на три групи: сигнатурні, статистичні та гібридні [2]. Сигнатурні орієнтуються на відомі шаблони пакетів і заголовків, але малоефективні при шифруванні даних.

Статистичні методи аналізують розподіл інтервалів між пакетами (Inter-Packet Delay – IPD) і розмірів сегментів, виявляючи приховану кореляцію, тоді як гібридні поєднують сигнатури та часові метрики.

Для публічних мереж характерна мультиарендність, що ускладнює ідентифікацію джерела передачі. Більшість IDS/IPS, таких як Suricata або Snort, не забезпечують повної кореляції між вихідним трафіком різних користувачів за спільною IP-адресою, тому потрібні поведінкові підходи [3]. Порівняння основних підходів до виявлення прихованих каналів представлено в табл. 1.

Таблиця 1 – Порівняння основних підходів до виявлення прихованих каналів

Тип методу	Основна ознака	Переваги	Недоліки
Сигнатурний	Відомі шаблони заголовків	Висока швидкість	Не працює зі шифруванням
Статистичний	Аналіз IPD, розмірів пакетів	Виявляє нові типи каналів	Вимагає великих обсягів даних
Гібридний	Комбінація сигнатур і статистики	Краща точність	Складна реалізація
Поведінковий (запропонований)	Динаміка відхилень у часі та структурі	Виявляє приховані канали у реальному трафіку	Потребує навчання моделей

Для перевірки методики було побудовано експериментальне середовище (рис. 1), що імітує публічну Wi-Fi-мережу з NAT-шлюзом і групою клієнтів, які генерують типовий веб-трафік. У контрольних умовах створювалися моделі прихованих каналів: DNS-стегаграфія, ICMP-тунель і часовий канал із регульованими інтервалами між пакетами [4].

Моніторинг трафіку здійснювався комплексно з використанням набору спеціалізованих інструментів Wireshark, Suricata, Zeek та NetFlow, які забезпечували як глибокий пакетний аналіз, так і узагальнену статистику потоків. Wireshark застосовувався для низькорівневої інспекції заголовків TCP, UDP та ICMP-пакетів, що дозволяло виявляти відхилення у порядку слідування пакетів, довжині полів і частоті службових повідомлень. Suricata функціонувала як IDS-платформа реального часу, здатна виконувати сигнатурний і поведінковий аналіз на основі наборів правил Emerging Threats. Zeek, у свою чергу, використовувався для семантичного розбору протоколів і логування сесій на рівні застосунків (HTTP, DNS, SSL), що створювало умови для кореляції з іншими джерелами подій. NetFlow-збірники забезпечували побудову агрегованої статистики потоків, у тому числі облік кількості байтів, пакетів, часу початку і завершення сеансів, що дозволяло ідентифікувати аномалії у вихідному трафіку великих сегментів публічних мереж.

Зібрані дані конвертувалися у формат CSV і зберігалися у централізованому сховищі для подальшої обробки Python-скриптами. На етапі попередньої обробки виконувалося очищення записів від неповних і дубльованих рядків, нормалізація часових міток та обчислення похідних метрик, таких як середній час між послідовними пакетами (Δt), коефіцієнт варіації інтервалів, щільність пакетів у вікні часу та ентропія розподілу розмірів пакетів. Особлива увага приділялася виявленню «зворотних запитів» – повторних звернень до одного вузла через однакові порти, що могло свідчити про активний прихований канал. Крім того, додатково аналізувалася частка нетипових розмірів пакетів, які відхилялися від стандартних фреймів Ethernet, оскільки саме в них часто вбудовуються стеганографічні фрагменти даних.

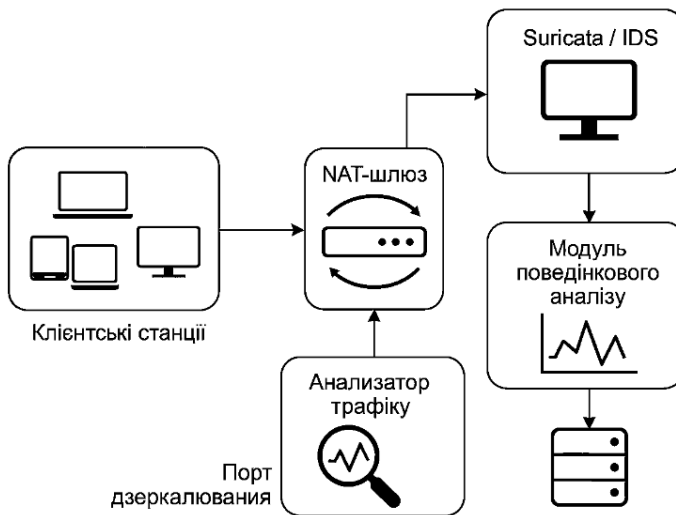


Рисунок 1 – Схема архітектури системи виявлення прихованих каналів

Виявлення прихованих каналів здійснювалося шляхом обчислення статистичних аномалій і їх подальшої перевірки за допомогою адаптивних порогових значень. Якщо середній час між пакетами Δt перевищував еталонне значення більше ніж на 2σ або відхилення у структурі заголовків досягало 15 %, трафік позначався як потенційно прихований і передавався до модуля поведінкового аналізу. Для підвищення точності результати зіставлялися з логами DNS-запитів, журналами фаєрвола та даними Zeek, що дозволяло перевіряти консистентність між рівнями транспортного й прикладного протоколів. Кореляція

подій у часі забезпечила можливість відокремлення технічних збоїв і природних пікових навантажень від справжніх ознак прихованої передачі даних. У підсумку система формувала звіти з ранжуванням аномалій за рівнем критичності, що дало змогу створити основу для автоматизованої детекції прихованих каналів у публічних мережах.

У результаті тестування модель змогла виявляти DNS- та ICMP-канали зі середньою точністю 94 %, а часові канали – до 89 %. Найвищу ефективність показали сценарії з комбінованим використанням Suricata і Zeek, де поведінковий аналіз доповнював сигнатурний.

Отримані результати свідчать, що поєднання часових метрик і структурної кореляції дозволяє своєчасно виявляти приховані передачі у вихідному трафіку навіть у середовищах із NAT і високим рівнем зашумлення. Запропонований підхід може бути інтегрований у системи мережевого моніторингу для підвищення рівня інформаційної безпеки публічних мереж. Подальші дослідження передбачають автоматизацію процесу класифікації прихованих каналів із використанням методів машинного навчання.

Перелік посилань

1. A Comprehensive Review of Tunnel Detection on Multilayer Protocols: From Traditional to Machine Learning Approaches / Z. Sui et al. Applied Sciences. 2023. Vol. 13, no. 3. P. 1974. URL: <https://doi.org/10.3390/app13031974>.
2. ReDAN: An Empirical Study on Remote DoS Attacks against NAT Networks / X. Feng et al. Network and Distributed System Security Symposium, San Diego, CA, USA. Reston, VA, 2025. URL: <https://doi.org/10.14722/ndss.2025.230972>.
3. A Comparative Analysis of Snort 3 and Suricata / A. A. E. Boukebous et al. 2023 IEEE IAS Global Conference on Emerging Technologies (GlobConET), London, United Kingdom, 19–21 May 2023. 2023. URL: <https://doi.org/10.1109/globconet56651.2023.10150141>.
4. Walter M., Keller J. Design and Evaluation of Steganographic Channels in Fifth-Generation New Radio. Future Internet. 2024. Vol. 16, no. 11. P. 410. URL: <https://doi.org/10.3390/fi16110410>.

УДК 004.8

Віт Р.В.

Хмельницький національний університет

ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДУ ВИЯВЛЕННЯ ЦИФРОВОГО ВИСНАЖЕННЯ ЗА АНАЛІЗОМ ЦІЛЮВИХ ОБ'ЄКТІВ МНОЖИНИ ПОВІДОМЛЕНЬ ЛЮДИНИ

У роботі розглянуто поточний стан наукового напрямку виявлення цифрового виснаження за аналізом цільових об'єктів множини повідомлень людини у контексті пошуку іменованих сутностей та пошуку ключових слів, та на основі опрацьованого матеріалу запропоновано власний метод виявлення цифрового виснаження за аналізом цільових об'єктів множини повідомлень людини. Цей метод використовує алгоритми машинного навчання для адаптивного розпізнавання об'єктів, враховуючи специфіку предметної області, що дозволяє значно скоротити час обробки даних і знизити ризик втрати важливої інформації. Розроблений метод виявлення цифрового виснаження за аналізом цільових об'єктів множини повідомлень людини призначений для автоматизації процесу ідентифікації ключових елементів у великих масивах текстових даних, й спрямований на підвищення точності та ефективності аналізу текстової інформації.

The paper reviews the current state of the scientific direction of digital exhaustion detection by analyzing target objects of a set of human messages in the context of named entity search and keyword search, and based on the developed material, proposes its own method of digital exhaustion detection by analyzing target objects of a set of human messages. This method uses machine learning algorithms for adaptive object recognition, taking into account the specifics of the subject area, which allows significantly reducing data processing time and reducing the risk of losing important information. The developed method of digital exhaustion detection by analyzing target objects of a set of human messages is designed to automate the process of identifying key elements in large arrays of text data, and is aimed at increasing the accuracy and efficiency of text information analysis.

Методи виявлення цільових об'єктів у предметній області є критично важливими для ефективного аналізу та обробки великих обсягів інформації. В умовах зростаючої складності даних, які охоплюють різноманітні предметні області, необхідність розробки та вдосконалення методів автоматизованого виявлення цільових об'єктів стає все більш актуальною [1]. Це особливо важливо в таких сферах, як штучний інтелект, а саме системи обробки природної мови та інформаційний пошук. Відсутність надійних та ефективних методів виявлення цільових об'єктів може призвести до втрати важливої інформації, зниження точності прийняття рішень та збільшення витрат на аналіз даних. Враховуючи

швидкий розвиток технологій та постійне зростання обсягів інформації, дослідження методів виявлення цільових об'єктів набуває особливої ваги.

Виявлення цільових об'єктів у заданій предметній області передбачає застосування спеціальних алгоритмів та методів, спрямованих на ідентифікацію та класифікацію елементів, які мають ключове значення для аналізу конкретної задачі. У роботі цільові об'єкти будуть шукатись у текстових даних, а під терміном «цільові об'єкти» буде матись на увазі сукупність множини ключових слів та множини NER з групуванням шляхом лематизації.

Виявлення цільових об'єктів у системах NLP, зокрема розпізнавання іменованих сутностей, відіграє важливу роль у багатьох завданнях аналізу тексту та обробки інформації. Основна мета NER полягає в ідентифікації і класифікації значущих елементів тексту, таких як імена людей, назви організацій, географічні назви, дати та інші сутності, які мають специфічне значення для конкретного контексту. Це завдання є ключовим для ряду практичних задач, таких як інформаційний пошук, машинний переклад, обробка юридичних документів та аналіз даних у соціальних медіа.

Одним із перспективних напрямків для задачі виявлення цільових об'єктів є використання методів машинного навчання, які дозволяють автоматично адаптуватися до особливостей даних та поліпшувати точність виявлення об'єктів з часом [2].

З проведеного аналізу, запропоновано автоматизувати виявлення цільових об'єктів предметної області з використанням підходів машинного навчання. Автоматизація виявлення цільових об'єктів предметної області сприятиме значному підвищенню ефективності та точності ідентифікації релевантних об'єктів у великих обсягах даних.

Проблему виявлення цільових об'єктів предметної області варто розглядати у контексті пошуку іменованих сутностей та пошуку ключових слів [2]. Даними задачами широко займаються науковці як по всьому світу, так і в Україні [3, 4].

Стрімке зростання обсягів цифрової комунікації та постійна взаємодія з інформаційними системами формують нові виклики для психоемоційного стану користувачів [5]. Одним із таких викликів є феномен цифрового виснаження – стану, що характеризується перевантаженням інформацією, зниженням мотивації, когнітивною втомою та зменшенням залученості у цифрові взаємодії [6]. На відміну від класичних проявів стресу, цифрове виснаження формується у контексті щоденного використання гаджетів і цифрових сервісів, що ускладнює його своєчасне та об'єктивне виявлення традиційними методами психологічної діагностики.

Текстові дані, які продукує користувач – повідомлення у месенджерах [7], коментарі на платформах, електронні листи, внутрішні освітні та корпоративні комунікації – відображають його когнітивні та емоційні стани [8]. Саме тому аналіз множини повідомлень людини, зокрема цільових об'єктів (тематичних доменів, адресатів, намірів, інформаційних фокусів), відкриває можливість раннього

виявлення цифрового виснаження шляхом виявлення змін у структурі, частотності та семантиці цифрової взаємодії [9].

Метою роботи є практична реалізація та дослідження методу виявлення цифрового виснаження за аналізом цільових об'єктів множини повідомлень людини.

Метод виявлення цифрового виснаження за аналізом цільових об'єктів множини повідомлень людини призначений для автоматизації процесу ідентифікації ключових елементів у великих масивах текстових даних, спрямований на підвищення точності та ефективності аналізу текстової інформації. Схема та кроки методу виявлення цифрового виснаження за аналізом цільових об'єктів множини повідомлень людини наведені на рис. 1.

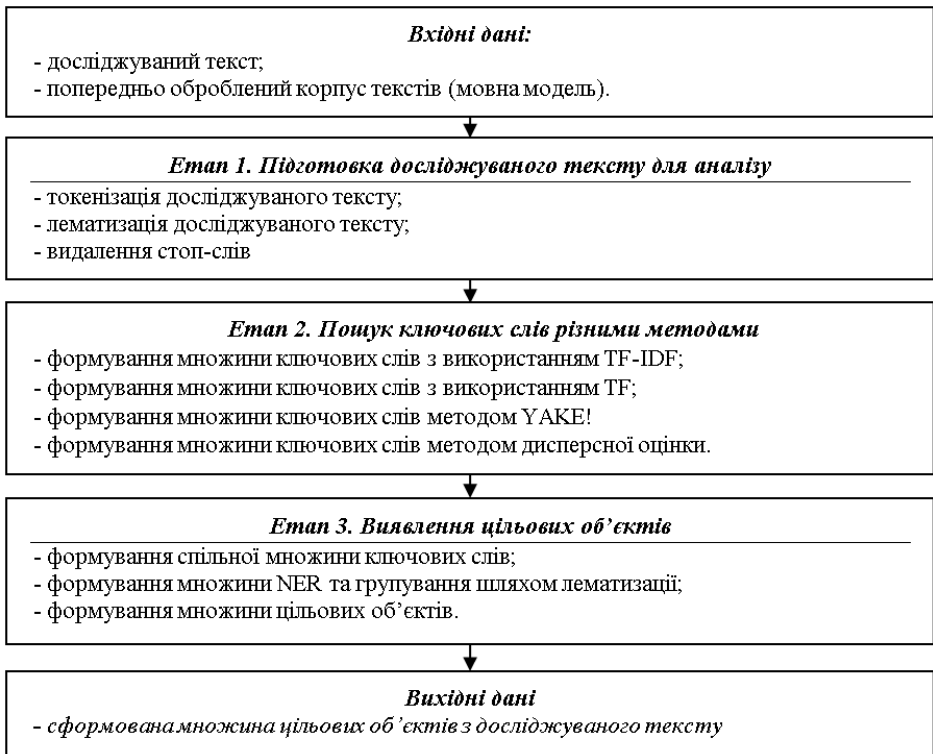


Рисунок 1 – Етапи роботи методу виявлення цифрового виснаження за аналізом цільових об'єктів множини повідомлень людини

Запропонований підхід ґрунтується на використанні алгоритмів машинного навчання, які забезпечують адаптивне розпізнавання релевантних об'єктів із

урахуванням специфіки предметної області та особливостей множини повідомлень користувача. Такий підхід дає змогу істотно прискорити обробку текстових даних і зменшити ймовірність втрати змістовно значущої інформації [10]. Розроблений метод цифрової діагностики, побудований на аналізі цільових об'єктів у масиві повідомлень людини, здійснює перетворення вхідних даних – досліджуваного тексту та збалансованого корпусу відповідної предметної області – у вихідний набір цільових об'єктів. Цей набір формується шляхом об'єднання ключових слів, отриманих різними підходами без дублювання, і NER-сутностей, що пройшли лематизацію.

Метод оперує двома типами вхідних даних:

- 1) текстом, що підлягає аналізу;
- 2) попередньо підготовленим корпусом текстів певної предметної області.

Перший етап передбачає лінгвістичну нормалізацію вхідного тексту, що включає токенізацію, лематизацію та усунення стоп-слів. На другому етапі виконується виявлення ключових слів за допомогою кількох незалежних методів, таких як TF-IDF, TF, YAKE! та дисперсійний підхід [11], після чого для кожного методу формується відповідна множина ключових термінів.

Третій етап спрямований на побудову остаточного набору цільових об'єктів. Він включає об'єднання всіх отриманих множин ключових слів без повторів та інтеграцію NER-сутностей, нормалізованих шляхом лематизації. Результатом є структурований набір цільових елементів, який відображає предметно-орієнтовані характеристики досліджуваного тексту.

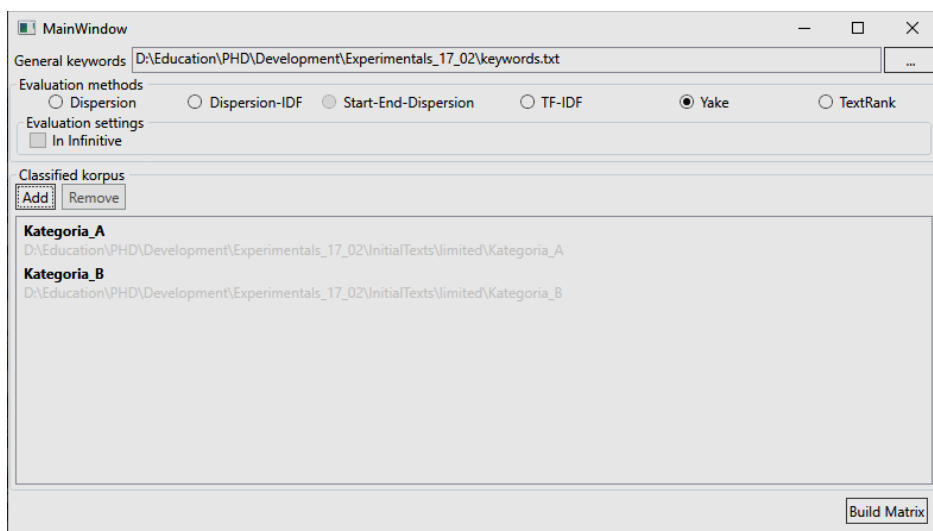


Рисунок 2 – Експериментальний застосунок для пошуку цільових об'єктів множини повідомлень людини досліджуваними методами

Для перевірки працездатності та валідності запропонованого методу було створено програмний застосунок мовою C#, призначений для автоматичного перетворення текстових файлів тестового набору у відповідні множини цільових об'єктів предметної області. Інтерфейс головного вікна розробленого застосунку наведено на рис. 2.

Оскільки українська мова повсякденного спілкування значно відрізняється від літературної через велику кількість діалектів, слів-запозичень та слів-покручів, наявні частотні словники не здатні охопити всю множину української мови [12]. Для створення вектора значущих слів українською мовою було вирішено об'єднати кілька частотних словників, з відсіканням стоп-слів. Після об'єднання та фільтрації довжина вектора значущих слів склала 1500 елементів.

Для дослідження ефективності запропонованого підходу було створено окреме консольне програмне забезпечення мовою Python, яке передбачає використання отриманого списку цільових об'єктів для досліджуваних текстів, та словників для окреслених тем. Відповідно, знайдені цільові об'єкти були переведені у векторне представлення розміром 1500 (як розмір словника) методом One-Hot Encoding. Надалі було перевірено Евклідові відстані між текстами одного спрямування, а також були обраховані Евклідові відстані між векторами протилежних категорій.

Матриця відстаней рис. 3 демонструють чітке розділення текстів на дві основні групи з різним змістом [8]. Перша група текстів (1–5) має тісніші зв'язки між собою, аналогічно як друга група (6–10) також має менші внутрішні відстані, але водночас має великі відстані до текстів з першої групи, що свідчить про те, що ці групи належать до різних тематик. Тексти всередині кожної групи мають невеликі відстані, що свідчить про їхню тематичну схожість.

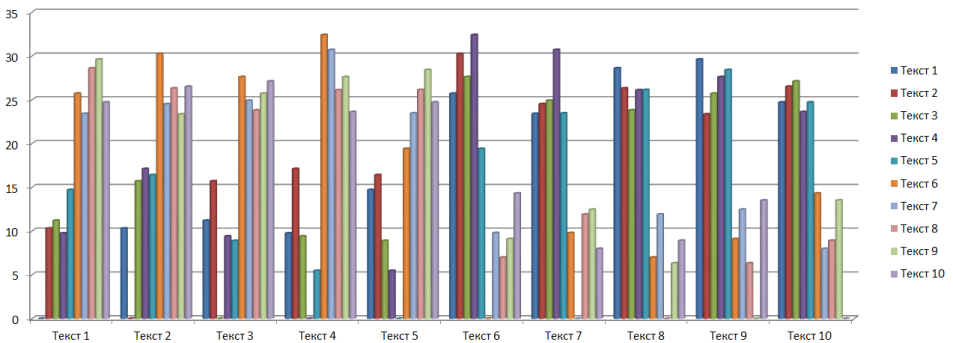


Рисунок 3 – Евклідові відстані між тестовими текстами двох категорій

Таким чином, було розглянуто сучасний стан досліджень, пов'язаних із виявленням цифрового виснаження на основі аналізу множини текстових

повідомлень користувача, зокрема через процедури пошуку ключових слів та ідентифікації іменованих сутностей. На підставі опрацьованих джерел запропоновано власний підхід до визначення ознак цифрового виснаження, що ґрунтується на аналізі цільових об'єктів текстового контенту. Запропонований метод використовує алгоритми машинного навчання для адаптивного виявлення релевантних об'єктів з урахуванням галузевої специфіки, що дає змогу зменшити час обробки даних та знизити ймовірність втрати змістовно важливої інформації. Розроблений підхід орієнтований на автоматизацію процесу виділення значущих елементів із великих текстових масивів, підвищуючи точність та загальну ефективність аналізу.

Метод трансформує вхідні текстові дані та підготовлений збалансований корпус предметної області у множину цільових об'єктів, що включає об'єднання ключових слів, отриманих різними підходами без дублювання, а також згрупованих шляхом лематизації сутностей NER. На відміну від відомих рішень, метод інтегрує як ключові слова, так і предметно орієнтовані іменникові сутності, що дозволило покращити точність виявлення цільових елементів.

Для перевірки ефективності запропонованого підходу сформовано навчальний датасет із 400 текстів українською мовою розмовного стилю. Крім того, створено програмний застосунок для генерування множини цільових об'єктів за текстами тестової вибірки, а також окремий консольний інструмент для роботи з отриманими списками цільових об'єктів і словниками предметних областей, що відповідали структурі датасету.

Проведені експерименти показали, що сформовані методом цільові об'єкти придатні для виконання подальших класифікаційних завдань. На основі оцінювання за метрикою Евклідових відстаней продемонстровано чітке групування текстів певної категорії та збільшення відстані відносно ортогональних класів, що свідчить про практичну цінність та ефективність розробленого підходу. Подальші дослідження доцільно спрямувати на розширення набору категорій та випробування інших метрик оцінювання якості виявлених цільових об'єктів, а також на порівняння результатів із ефективністю сучасних великих мовних моделей.

Перелік посилань

1. Молчанова М.О., Мазурець О.В., Собко О.В., Віт Р.В., Назаров В.В. Алгоритм виявлення аб'юзивного вмісту в україномовному аудіоконтенті для імплементації в об'єктно-орієнтовану інформаційну систему. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2024. №1 (331). С. 101-106.
2. Mazurets O., Sobko O., Vit R., Pasternak V. Practical Approach for Detection by Deep Learning of Target Objects of Subject Area Based on Semantic Connectivity Indicators in Audio Database. Proceedings of XXIV International Scientific and Practical Conference «Modern Scientific Challenges are the Driving Force of the Development of Scientific Research». May 22-24, 2024. Bruges, Belgium. International Scientific Unity. 2024. Pp. 91-96.
3. Shin H. General-use unsupervised keyword extraction model for keyword analysis / H. Shin, J. Lee, S. Cho. // Expert Systems with Applications. 2023. №233. С. 120889.

4. Chen X. Named Entity Recognition via Unified Information Extraction Framework / X. Chen, Z. Zhang, X. Lu. // 4th International Conference on Computer Communication and Artificial Intelligence. 2024. С. 308–313.
5. Мазурець О.В., Віт Р.В. Метод виявлення цільових об'єктів предметної області у текстовому контенті. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2024. №6, Т.1 (343). С. 152-157.
6. Віт Р.В., Мазурець О.В. Метод формування множин цільових об'єктів предметних областей у цифрових текстах засобами машинного навчання. Науковий журнал «Наука і техніка сьогодні». Київ, 2024. №13 (41). С. 926-937.
7. Віт Р.В., Мазурець О.В. Підхід до тематичної класифікації текстової інформації засобами обробки природної мови. Науковий журнал «Наукові праці Донецького національного технічного університету», серія «Проблеми моделювання та автоматизації проектування». 2025. №1 (21). С. 94-99.
8. Мазурець О., Віт Р. Інтелектуальний метод виявлення цільових об'єктів предметної області для класифікації текстової інформації. Матеріали XII Міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології ІУСТ-ОДЕСА-2024». 23-25.09.2024. Одеса. 2024. С.205-208.
9. Віт Р.В., Мазурець О.В. Метод виявлення множин цільових об'єктів предметної області у текстовому контенті. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». 15-16 листопада 2024. Хмельницький, 2024. с. 78-82.
10. Мазурець О.В., Віт Р.В. Дослідження ефективності методу виявлення цільових об'єктів предметної області. Інформаційні технології і автоматизація. Матеріали XVII міжнародної науково-практичної конференції. 31 жовтня – 1 листопада 2024 р. Одеса, ОНТУ. 2024. С.650-653.
11. Віт Р.В., Мазурець О.В. Тематична класифікація текстової інформації засобами обробки природної мови. Збірник наукових праць XXIII Міжнародної наукової конференції «Нейромережні технології та їх застосування НМТіЗ-2024». 11-12 грудня 2024. Краматорськ-Тернопіль, ДДМА. 2024. с. 63-66.
12. Мазурець О.В., Віт Р.В. Інтелектуальний метод виявлення цільових об'єктів предметної області за показниками семантичної зв'язності для класифікації текстової інформації. Розвитки інформаційно-керуючих систем та технологій.: монографія. Львів-Торунь: Lina-Pres, 2024. С.223-244.

УДК 004.85:004.932.7

Вовк С.В., Радюк П.М., Скрипник Т.К.

Хмельницький національний університет

МЕТОД ІНТЕРПРЕТУВАННЯ РЕЗУЛЬТАТІВ ВИЯВЛЕННЯ ФЕЙКОВИХ НОВИН ЗА ВЕЛИКОЮ МОВНОЮ МОДЕЛЛЮ

Запропоновано пояснюваний метод виявлення фейкових новин, що інтегрує великі мовні моделі з модулями пояснюваного штучного інтелекту та концепцією «людина-в-петлі». Метод ґрунтується на послідовній обробці тексту за допомогою трансформерної архітектури DistilBERT для глибокого семантичного аналізу, подальшої класифікації та інтерпретації рішень моделі з використанням SHAP та Integrated Gradients. Це забезпечує високу точність класифікації та прозорість й довіру до системи, дозволяючи експертам розуміти фактори, що впливають на виявлення дезінформації.

An explainable method for detecting fake news is proposed, integrating large language models with explainable artificial intelligence modules and the “human-in-the-loop” concept. The method is based on sequential text processing using the DistilBERT transformer architecture for deep semantic analysis, subsequent classification, and interpretation of model decisions with SHAP and Integrated Gradients. This ensures not only high classification accuracy but also transparency and trust in the system, allowing experts to understand the factors influencing disinformation detection and actively intervene to enhance its effectiveness.

Сучасний інформаційний простір зіткнувся з безпрецедентним викликом – експоненціальним поширенням дезінформації, зокрема фейкових новин. Це явище перетворилося на серйозну загрозу, що здатна дестабілізувати суспільну думку, політичні процеси та навіть національну безпеку. Швидкість, з якою неправдива інформація розповсюджується через соціальні медіа, значно випереджає можливості традиційних методів фактчекінгу, що породжує потребу в створенні ефективних автоматизованих інструментів для протидії [1]. Особливої актуальності ця проблема набуває в умовах гібридних конфліктів і криз, де оперативність та достовірність інформації стають критично важливими.

Традиційні підходи до обробки природної мови (NLP) демонструють обмежену працездатність, оскільки їм бракує здатності глибоко аналізувати контекст, іронію та емоційне забарвлення тексту [2]. Поява великих мовних моделей (LLM) відкрила нові горизонти в автоматизованому аналізі, однак водночас створила проблему «чорної скриньки» – непрозорості процесу ухвалення рішень [3]. Ця особливість підриває довіру до таких систем та ускладнює їх застосування у таких відповідальних сферах, як політика чи охорона здоров'я.

Для подолання цих викликів активно розвиваються методи пояснюваного штучного інтелекту (XAI), зокрема інструменти SHAP та Integrated Gradients, що

дозволяють інтерпретувати рішення моделей [4]. Разом із концепцією «людина-в-петлі» (HITL), яка поєднує автоматизацію з експертним контролем, це створює синергію для підвищення надійності системи [5]. Попри значний прогрес, залишаються невирішеними питання адаптації моделей до багатомовних та емоційно насичених контекстів.

Метою дослідження є підвищення рівня інтерпретованості систем виявлення фейкових новин через проєктування нового методу, який дає змогу експертам інтерактивно аналізувати, валідувати та ітеративно вдосконалювати простір текстових ембедінгів, що лежить в основі класифікаційних рішень.

Запропонований метод поєднує автоматизоване виявлення фейкових новин з інтерпретацією результатів та втручанням людини в процес навчання. Його робота включає шість основних етапів:

1. Попередня обробка тексту – очищення від шумів, нормалізація, лематизація та балансування класів для уникнення упередженості.

2. Перетворення тексту у векторний простір за допомогою DistilBERT, що забезпечує глибоке контекстне розуміння.

3. Класифікація зі застосування щільного шару з функцією активації Softmax та мінімізацією функції втрат на основі крос-ентропії.

4. Пояснення рішень моделі за допомогою локальних методів SHAP та Integrated Gradients для виявлення ключових слів/фраз, що впливають на рішення моделі. Також формуються ROC-криві та матриці помилок для загальної оцінки якості моделі.

5. Візуалізація простору ознак за допомогою UMAP та t-SNE, для проєкції векторних представлень текстів у 2D/3D простір, що дозволяє виявляти кластери фейкових/правдивих новин та аномалії.

6. Інтерактивний цикл «людина-в-петлі», в межах якого експерт аналізує пояснення, коригує помилки й оновлює дані для підвищення точності (>90%).

Для експериментальної перевірки працездатності методу використано репрезентативні корпуси даних: LIAR [6], FakeNewsNet (PolitiFact, GossipCop) [7] та CONSTRAINT-2021 (EN) [8]. Ці набори охоплюють різні типи новин (короткі висловлювання, повноцінні статті), тематичні домени та часові періоди, дозволяючи оцінити здатність моделі до узагальнення.

Запропонований метод продемонстрував стабільне покращення показника F1-міри на 2–4% порівняно з базовими моделями (TF-IDF+SVM, BERT-base, SBERT) на всіх корпусах. Найвищу працездатність було зафіксовано на корпусі CONSTRAINT-2021 ($F1 = 0.97$), що узгоджується з результатами найкращих моделей міжнародних конкурсів [6–8]. Це підтверджує працездатність інтеграції DistilBERT та XAI-фідбеку (таблиця 1).

Експерименти з перепрацюванням новин за допомогою TextFooler та LLM-laundering виявили вразливість трансформерних моделей до семантичних атак: частка зміни класу становила 22% для фейкових та 8% для правдивих новин (рисунок 1). Це вказує на необхідність посилення стійкості моделі.

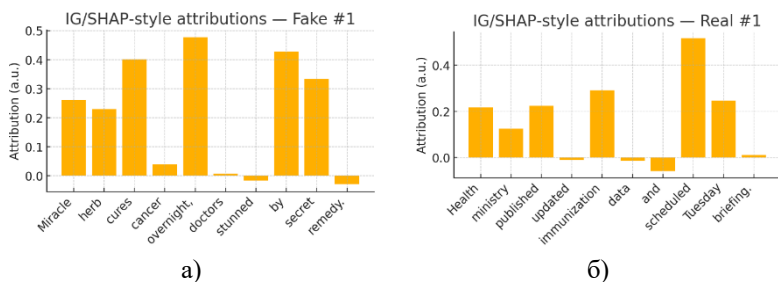
Таблиця 1 – Порівняння базових моделей за F1-мірою на різних корпусах

Корпус/Модель	Класичні методи (TF-IDF + SVM)	BERT-base	SBERT	Запропонований метод
LIAR(бінар.)	0.68	0.78	0.8	0.83
FakeNewsNet – PolitiFact	0.7	0.87	0.88	0.9
FakeNewsNet – GossipCop	0.63	0.84	0.85	0.87
CONSTRAINT-2021 (EN)	0.75	0.95	0.96	0.97

Застосування SHAP та Integrated Gradients дозволило чітко ідентифікувати ключові слова та фрази (рисунки 2–3), які модель використовує для класифікації новин як фейкових (наприклад, сенсаційні, емоційно забарвлені лексеми) або правдивих (фактологічні, нейтральні), що підвищує прозорість та довіру до системи.



Рисунок 1 – Стійкість до перефразування контенту



а)

б)

Рисунок 2 – Порівняння IG/SHAP-атрибуції: а) клас «fake» #1 та б) клас «real» #1

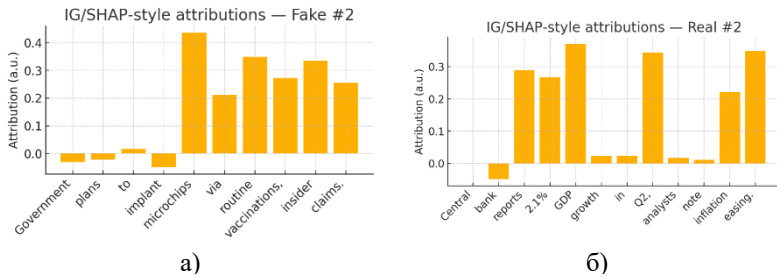


Рисунок 3 – Порівняння IG/SHAP-атрибуції: а) клас «fake» #2 та б) клас «real» #2

У підсумку, у даній роботі було запропоновано та експериментально підтверджено працездатність пояснюваного методу виявлення фейкових новин на основі великих мовних моделей, інтегрованого з підходом «людина-в-петлі». Побудована система забезпечує не лише високу точність класифікації, але й прозорість прийнятих рішень завдяки модулям пояснюваного штучного інтелекту. Це дозволяє експертам розуміти логіку моделі та втручатися для покращення її роботи.

Перелік посилань

1. Explainable deep learning: A visual analytics approach with transition matrices / P. Radiuk et al. Mathematics. 2024. Vol. 12, no. 7. P. 1024. URL: <https://doi.org/10.3390/math12071024> (date of access: 19.10.2025).
2. Shupta A., Radiuk P., Krak I. Feature computation procedure for fake news detection: An LLM-based extraction approach. Proceedings of the 6th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS 2025) : CEUR-Workshop Proceedings, Khmelnytskyi, 4 April 2025. Aachen, 2025. P. 112–124. URL: <https://ceur-ws.org/Vol-3963/paper10.pdf> (date of access: 19.10.2025).
3. Survey on explainable AI: from approaches, limitations and applications aspects / W. Yang et al. Human-Centric Intelligent Systems. 2023. Vol. 3. P. 161–188. URL: <https://doi.org/10.1007/s44230-023-00038-y> (date of access: 19.10.2025).
4. Lyu Q., Apidianaki M., Callison-Burch C. Towards faithful model explanation in NLP: a survey. Computational Linguistics. 2024. Vol. 50, no. 2. P. 1–70. URL: https://doi.org/10.1162/coli_a_00511 (date of access: 19.10.2025).
5. Human-in-the-loop approach based on MRI and ECG for healthcare diagnosis / P. Radiuk et al. Proceedings of the 5th International Conference on Informatics & Data-Driven Medicine : CEUR-Workshop Proceedings, Lyon, 18–20 November 2022. Aachen, 2022. P. 9–20. URL: <https://ceur-ws.org/Vol-3302/paper1.pdf> (date of access: 19.10.2025).
6. Wang W. Y. "Liar, liar pants on fire": a new benchmark dataset for fake news detection. Proceedings of the 55th annual meeting of the association for computational linguistics (Volume 2: short papers), Vancouver, Canada, 30 July – 4 August 2017. Stroudsburg, PA, USA, 2017. P. 422–426. URL: <https://doi.org/10.18653/v1/p17-2067> (date of access: 19.10.2025).
7. FakeNewsNet: A data repository with news content, social context, and spatiotemporal information for studying fake news on social media / K. Shu et al. Big Data. 2020. Vol. 8, no. 3. P. 171–188. URL: <https://doi.org/10.1089/big.2020.0062> (date of access: 19.10.2025).
8. Patwa P. GitHub - parthpatwa/covid19-fake-news-detection: Official repository for data set and baselines for covid19 fake news data. GitHub. URL: <https://github.com/parthpatwa/covid19-fake-news-detection> (date of access: 19.10.2025).

УДК 004.8

Волколуп Б.А., Пасічник О.А., Скрипник Т.К.

Хмельницький національний університет

МЕТОД КЛАСИФІКАЦІЇ НАСТРОЇВ У ТЕКСТАХ СОЦІАЛЬНИХ МЕРЕЖ НА ОСНОВІ РЕКУРЕНТНИХ НЕЙРОННИХ МЕРЕЖ

Розглянуто метод автоматичної класифікації настроїв у текстах соціальних мереж з використанням рекурентних нейронних мереж типу LSTM. Запропонована архітектура включає шар вкладень з попередньо навченими векторами Word2Vec, LSTM шар для захоплення контекстних залежностей та повнозв'язні шари для класифікації. Розроблено модифікацію для покращення обробки емодзі та сленгу через спеціальні словники. Метод забезпечує точність класифікації 89.4%.

A method for automatic sentiment classification in social media texts using LSTM recurrent neural networks is considered. The proposed architecture includes an embedding layer with pre-trained Word2Vec vectors, an LSTM layer for capturing contextual dependencies, and fully connected layers for classification. A modification for improved processing of emoji and slang through specialized dictionaries has been developed. The method achieves classification accuracy of 89.4%.

Автоматичний аналіз настроїв у соціальних мережах є важливим інструментом для моніторингу громадської думки, аналізу відгуків споживачів та виявлення трендів [1, 2]. Традиційні методи класифікації настроїв базуються на словниках емоційно забарвлених слів та лінійних моделях, які не враховують контекстних залежностей між словами [3, 4]. Використання рекурентних нейронних мереж дозволяє автоматично виявляти складні семантичні патерни та контекстні залежності у текстах.

Метою роботи є розробка методу автоматичної класифікації настроїв у текстах соціальних мереж на основі рекурентних нейронних мереж типу LSTM з модифікацією для покращення обробки емодзі та сленгу, який забезпечує високу точність при прийнятній швидкості обробки.

Запропонований метод базується на використанні глибокого навчання для послідовної обробки текстових даних. Вхідними даними є текстові повідомлення з соціальних мереж максимальною довжиною 128 токенів, а вихідними – клас настрою (позитивний, негативний або нейтральний). Метод складається з чотирьох послідовних етапів (рисунок 1): попередня обробка та токенизація тексту, векторизація токенів з використанням Word2Vec, обробка послідовності LSTM шаром для захоплення контекстних залежностей, класифікація повнозв'язними шарами з функцією активації софтмакс.

Етап попередньої обробки включає видалення URL-адрес та згадок користувачів, обробку хештегів (видалення символу # зі збереженням тексту), видалення спеціальних символів та знаків пунктуації, приведення до нижнього

регістру, токенизацію з використанням бібліотеки NLTK та видалення стоп-слів. Модифікація методу передбачає додатковий етап обробки емодзі та сленгу через спеціальні словники. Словник емодзі містить 100 найпоширеніших емодзі з відповідними текстовими описами емоцій (наприклад, 😊 замінюється на "щасливий"). Словник сленгу нормалізує неформальні вирази до стандартних форм (наприклад, "lol" → "laughing out loud").

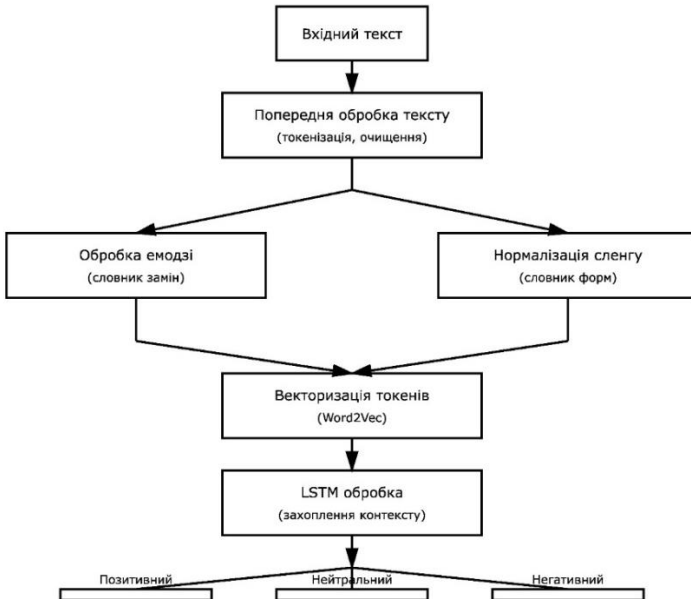


Рисунок 1 – Загальна схема методу класифікації настроїв

Архітектура нейронної мережі. Базова архітектура мережі включає послідовне з'єднання шару вкладень, LSTM шару, шару дропаут та двох повнозв'язних шарів (рисунок 2). Шар вкладень перетворює токени у векторні представлення розмірністю 300, ініціалізовані попередньо навченими векторами Word2Vec. Використовується тонке налаштування вкладень під час навчання для адаптації до специфіки задачі.

LSTM шар є основним компонентом архітектури і має 128 прихованих одиниць. Шар використовує три вентиля для контролю потоку інформації: вентиль забування визначає, яку частину попереднього стану забути; вентиль входу контролює додавання нової інформації; вентиль виходу формує прихований стан.

Після LSTM шару розташований шар дропаут з коефіцієнтом 0.5 для зменшення перенавчання. Перший повнозв'язний шар містить 512 нейронів з активацією ReLU, другий – 256 нейронів також з ReLU. Обидва повнозв'язні шари використовують дропаут 0.5. Вихідний шар має три нейрони з функцією активації софтмакс для формування розподілу ймовірностей по класах настроїв.

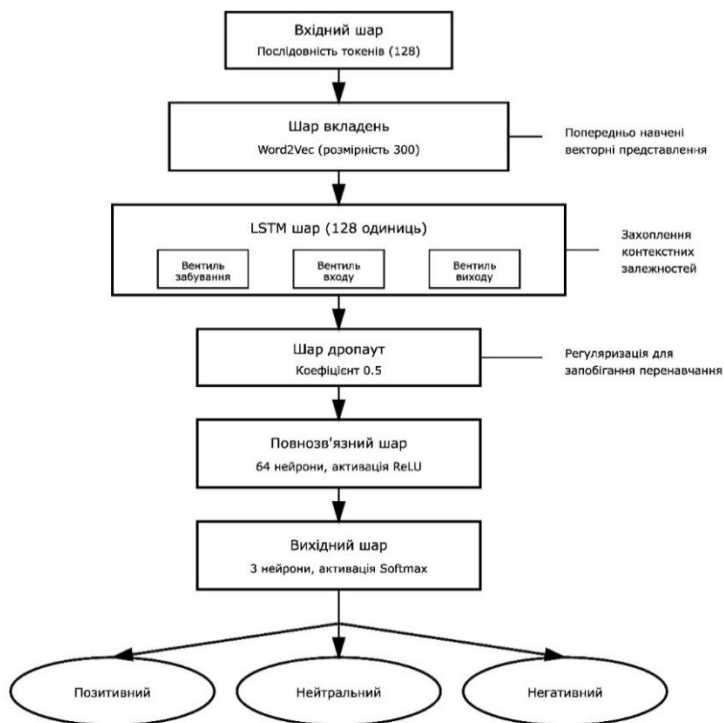


Рисунок 2 – Архітектура моделі класифікації настроїв

Отже, розроблений метод класифікації настроїв на основі рекурентних нейронних мереж LSTM забезпечує точність 89.4%. Модифікація з обробкою емодзі та сленгу через спеціальні словники покращує точність на 1.8% без збільшення обчислювальної складності. Метод є придатним для практичного застосування в системах моніторингу соціальних мереж та аналізу відгуків користувачів.

Перелік посилань

1. Murat Başı. Natural Language Processing for Sentiment Analysis in Social Media Marketing. Economics World. 2025. Vol. 12, No. 1. URL: <https://doi.org/10.17265/2328-7144/2025.01.004>.
2. Nikhil N., Pratik P., Rutuja P., Rutuja P., Suyash W. Sentiment Analysis Using Natural Language Processing. International Journal of Scientific Development and Research. 2022. Vol. 7, No. 5. Pp. 458–462.
3. Shad R., Potter K., Gracias A. Natural Language Processing (NLP) for Sentiment Analysis: A Comparative Study of Machine Learning Algorithms. International Journal of Artificial Intelligence and Machine Learning. 2025. Vol. 5, No. 1. Pp. 58–69. URL: <https://doi.org/10.51483/IJAIML.5.1.2025.58-69>.
4. Muthukumar P., Ibrahim M. A. S. Multimodal Social Media Sentiment Analysis. Stanford CS224N Final Project. 2024. Pp. 1–12.

УДК 004.8

Вонсович Б.А., Багрій Р.О., Пасічник О.А., Скрипник Т.К.

Хмельницький національний університет

МЕТОД ВИЯВЛЕННЯ НЕОДНОЗНАЧНОСТЕЙ У ВИМОГАХ ДО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ВИКОРИСТАННЯМ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ

Запропоновано метод автоматизованого аналізу вимог до програмного забезпечення, що базується на двоагентній LLM-архітектурі. Підхід вирішує проблему низької ефективності прямих запитів, розділяючи процес на два етапи: ідентифікацію потенційних неоднозначностей та їх подальшу глибоку класифікацію з поясненням. В основі методу лежить технологія доповненої генерації (RAG) для надання агентам контекстуальних знань та використання промптингу ланцюжок думок (CoT) для підвищення прозорості та точності результатів.

A method for the automated analysis of software requirements based on a two-agent LLM architecture is proposed. This approach addresses the problem of low efficiency in direct queries by dividing the process into two stages: identification of potential ambiguities and their subsequent deep classification with explanation. The method is based on Retrieval-Augmented Generation (RAG) technology to provide agents with contextual knowledge and the use of Chain-of-Thought (CoT) prompting to increase transparency and accuracy of results.

Якість текстових вимог до програмного забезпечення є критичною для успіху проєкту – неоднозначність у формулюваннях призводить до неправильної інтерпретації, помилок у дизайні та значного зростання витрат на виправлення дефектів [1, 2].

Сучасні великі мовні моделі (LLM) демонструють високий потенціал у обробці природної мови, але дослідження підтверджують, що в задачах, які вимагають багатокрокового міркування, їхня ефективність без структурованих підходів суттєво знижується [3].

У задачах аналізу вимог до ПЗ необхідно не лише виявляти потенційно неоднозначні фрагменти тексту, а й класифікувати тип неоднозначності та оцінювати її вплив на якість вимоги. Практика показує, що виконання всіх етапів аналізу одним запитом до LLM призводить до зниження точності, нестабільності результатів і втрати інформативності [4]. Розділення процесу на послідовні етапи з чітко визначеними ролями є доцільним підходом. Відсутність такого поділу з високою ймовірністю спричиняє або надмірну кількість хибних спрацьовувань на

етапі виявлення, або поверховий аналіз під час класифікації [5]. Запропонований двоетапний підхід усуває ці недоліки: поділ завдань знижує когнітивне навантаження на модель, підвищує точність і забезпечує прозорість процесу.

В основі методу (рис. 1) лежить технологія доповненої генерації (RAG). Кожен агент у системі використовує RAG для отримання динамічних прикладів, що є критично важливим для точного аналізу вимог. Замість статичних прикладів, RAG-система активно шукає у спеціалізованому наборі даних найбільш релевантну інформацію для поточного завдання. Ця інформація динамічно додається до промпту агента, що є ефективною формою навчання в контексті.

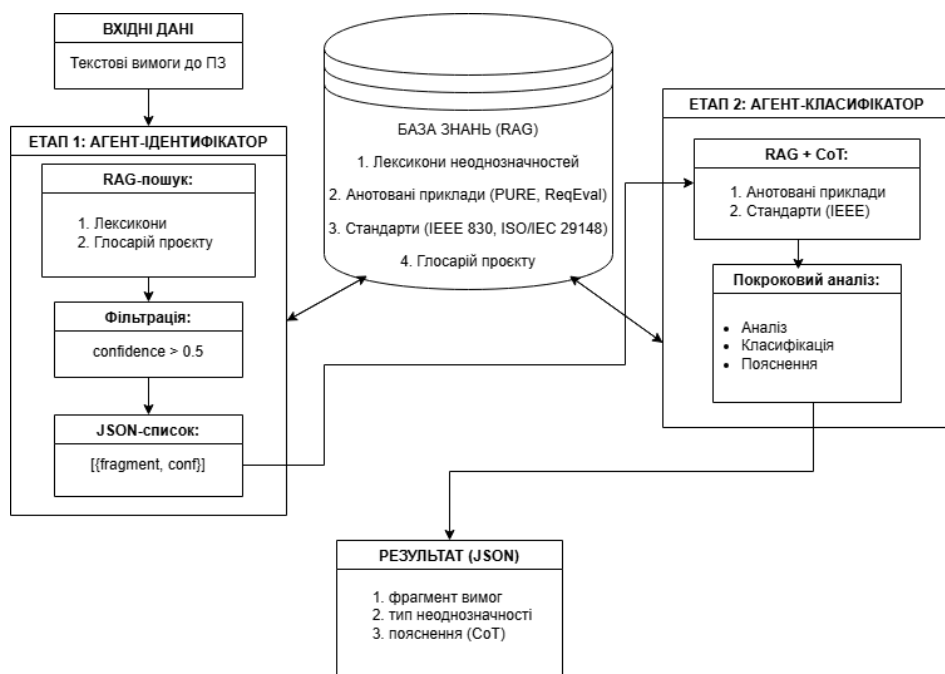


Рисунок 1 – Схема методу виявлення неоднозначності у вимогах

Ефективність системи залежить від якості наповнення цієї бази знань. Для задачі аналізу вимог база знань має бути структурована та містити декілька ключових компонентів. По-перше, це лексикони неоднозначностей – куровані списки слів та фраз, які часто вказують на проблеми (наприклад, «легко», «швидко», «ефективно», «тощо»). По-друге, це анотовані приклади – реальні речення з вимог, розмічені експертами. Для цього можуть бути використані публічні бенчмарки, такі як PURE або спеціалізовані набори даних, як-от ReqEval,

що фокусується на референційній неоднозначності. По-третє, база знань повинна містити стандарти та принципи – витяги з академічних джерел та галузевих стандартів (наприклад, IEEE 830), що описують характеристики якісних вимог, зокрема верифікованість. Нарешті, найважливішим компонентом є база знань проекту/домену – внутрішні глосарії, специфікації та акроніми, специфічні для конкретного проекту, що дозволяє системі адаптуватися до контексту та зменшити кількість помилкових спрацьовувань.

На першому етапі функціонує Агент-ідентифікатор, роль якого полягає в оцінці ризику неоднозначності. Його завдання – провести первинний аналіз тексту вимог та ідентифікувати фрагменти, що мають високий потенціал неоднозначності. Агент виконує роль QA-аналітика з метою ранжування виявлених фраз за шкалою впевненості (від 0.0 до 1.0). Для виконання цього завдання агент використовує технологію RAG, звертаючись до двох спеціалізованих наборів даних: лексикону неоднозначностей та база знань проекту.

Ключова перевага такого підходу полягає у можливості фільтрації. Встановлення порогового значення (наприклад, $\text{confidence} > 0.5$) дозволяє відсіяти шум – кандидати з низькою впевненістю. Це ефективно вирішує поширену проблему автоматизованих аналізаторів, пов'язану з низькою точністю та перевантаженням системи помилковими спрацьовуваннями. Результатом цього етапу є відфільтрований JSON-список кандидатів з високою впевненістю (наприклад, [{"fragment": "швидко реагувати", "confidence": 0.9}]), який передається на наступний, обчислювально дорожчий етап.

На другому етапі в роботу вступає Агент-Класифікатор. Він отримує на вхід відфільтрований список кандидатів і проводить їх глибокий аналіз. Агент діє в ролі експерта з інженерії вимог, що знайомий з галузовими стандартами, такими як IEEE 830. Робота агента базується на методології ланцюжка думок (CoT), яка вимагає від моделі генерації покрокового обґрунтування для кожного рішення. Процес CoT складається з трьох обов'язкових кроків:

Аналіз – ідентифікація конкретного терміну, фрази чи граматичної структури, що спричиняє проблему.

Класифікація – присвоєння точного типу неоднозначності згідно з попередньо визначеною класифікацією неоднозначностей.

Пояснення – формулювання чіткого обґрунтування, чому фраза є неоднозначною в даному контексті, та опис потенційних негативних наслідків (наприклад, «неможливість тестування», «ризик неправильної реалізації»).

Використання CoT є вирішальним, оскільки дослідження показують, що прості запити до LLM можуть не дати адекватного пояснення, тоді як CoT змушує модель генерувати покрокову логіку. Простий тег [Туманність] може бути проігнорований розробником. Однак, покрокове пояснення (CoT), яке логічно

обґрунтовує висновок і посилається на галузеві принципи (наприклад, «не підлягає тестуванню» згідно IEEE 830), демонструє компетентність системи та значно підвищує довіру до її результатів. Для підвищення точності аналізу цей агент також використовує RAG, але вже з іншими джерелами – анотованими прикладами та стандартами. Фінальним результатом роботи системи є структурований JSON-об'єкт з повним детальним аналізом кожної виявленої неоднозначності.

У роботі запропоновано двоагентний LLM-метод для аналізу вимог до ПЗ, який вирішує проблему низької ефективності прямих запитів до моделей. Ключем є декомпозиція задачі: Агент 1 (Ідентифікатор) проводить ефективну фільтрацію "шуму", ранжуючи проблеми за впевненістю, тоді як Агент 2 (Класифікатор) проводить глибокий аналіз відфільтрованих кандидатів. Контекстуальна точність досягається через RAG, що надає агентам доступ до спеціалізованих баз знань (лексикони, стандарти IEEE 830, знання проекту). Прозорість та довіра забезпечуються ланцюжком думок, який змушує другого агента генерувати покрокові пояснення замість простих міток. Таким чином, запропонований метод перетворює LLM на надійний, прозорий та адаптивний інструмент для підвищення якості вимог.

Перелік посилань

1. Femmer, H., Fernández, D. M., Wagner, S., & Eder, S. (2017). Rapid quality assurance with Requirements Smells. *Journal of Systems and Software*, 123, 190–213. <https://doi.org/10.1016/j.jss.2016.02.047>
2. Berry, D. M., & Kamsties, E. (2004). Ambiguity in Requirements Specification. In *Perspectives on Software Requirements* (pp. 7–44). Springer. https://doi.org/10.1007/978-1-4615-0465-8_2
3. Wei, J., Wang, X., Schuurmans, D., et al. (2022). Chain-of-Thought Prompting Elicits Reasoning in Large Language Models. *NeurIPS 2022*. <https://arxiv.org/abs/2201.11903>
4. Yao, S., Zhao, J., Yu, D., et al. (2023). ReAct: Synergizing Reasoning and Acting in Language Models. *ICLR 2023*. <https://arxiv.org/abs/2210.03629>
5. Kojima, T., Gu, S. S., Reid, M., et al. (2022). Large Language Models are Zero-Shot Reasoners. *NeurIPS 2022*. <https://arxiv.org/abs/2205.11916>

УДК 004.8

Гнатюк П.В., Залуцька О.О.

Хмельницький національний університет

ПІДХІД ДО ВИЗНАЧЕННЯ ПСИХОЕМОЦІЙНОЇ ТОНАЛЬНОСТІ УКРАЇНОМОВНИХ ПОВІДОМЛЕНЬ У СОЦІАЛЬНО-ОРІЄНТОВАНИХ СЕРВІСАХ

Подано підхід до автоматизованого визначення психоемоційної тональності українськомовних повідомлень у соціально орієнтованих сервісах із пріоритетом прозорості та відтворюваності. Конвеєр охоплює підготовку даних, виділення ключових термінів за TF-IDF, YAKE і TextRank, зіставлення з лексиконами та навчання класифікатора з подальшим агрегуванням полярності. Ефективність оцінено на незалежних наборах за точністю, повнотою і F_1 з аналізом матриць сплутувань та розбором помилок. Збереження проміжних артефактів і версій параметрів забезпечує аудит і стабільність у реальних потоках. Підхід враховує етичні вимоги щодо мінімізації персональних даних та придатний до масштабованого впровадження.

This work presents a method for automated detection of psycho-emotional sentiment in Ukrainian messages from socially oriented platforms with an emphasis on transparency and reproducibility. The pipeline includes data preparation, key-term extraction using TF-IDF, YAKE and TextRank, lexicon alignment, and classifier training followed by polarity aggregation. Performance is evaluated on independent sets through precision, recall and F_1 together with confusion-matrix inspection and error analysis. Intermediate artifacts and parameter versions are persisted to enable full auditability and robust operation in real streams. The approach adheres to ethical constraints on personal data and is suitable for scalable deployment.

Актуальність теми зумовлена стрімким зростанням ролі соціально орієнтованих цифрових сервісів, де короткі, часто імпульсивні повідомлення стають базовою одиницею суспільної комунікації, самоорганізації спільнот і швидкої координації дій [1, 2]. У таких потоках психоемоційна тональність виконує не другорядну, а формувальну функцію: вона впливає на довіру до джерела, модулює готовність до співпраці, спричиняє ланцюгові реакції підтримки або відторгнення та визначає видимі контури суспільних норм [3]. Для українського сегмента мережі ця проблематика має додатковий вимір через інтенсивну цифровізацію громадянської взаємодії, підвищену чутливість до ризиків дезінформації, а також потребу у відповідальній модератії без придушення легітимної критики.

Соціально орієнтовані сервіси акумулюють висловлювання різної довжини й жанру: від коротких реакцій до мікроесе з емоційними маркерами, емодзі та контекстними натяками. Психоемоційна складова в них не лише супроводжує зміст, а часто і є самим змістом, коли рішення користувача приймаються з огляду на

емоційний сигнал, а не на фактичний опис події [4]. Це вимагає коректних інструментів автоматизованого визначення тональності, здатних працювати зі стисненим контекстом, змішаними регістрами мовлення, активним код-світчингом та нестандартними графічними підсилювачами, не зводячи різноманіття виражальних засобів до грубих полярних бінарів.

Аналіз психоемоційної тональності текстів набуває дедалі більшої значущості в умовах стрімкого зростання кількості цифрової комунікації та підвищення ролі соціально-орієнтованих сервісів у взаємодії між користувачами [5]. Визначення емоційного стану автора повідомлення є важливою складовою побудови безпечного й підтримувального онлайн-середовища [6], виявлення кризових ситуацій [7], модерації контенту та адаптивної персоналізації сервісів [8, 9]. Для українського сегмента цифрових платформ це завдання ускладнюється особливостями морфології, синтаксису та стилістичних варіацій української мови [10], що потребує спеціалізованих методів обробки природної мови.

Сучасні NLP-підходи, зокрема неймережеві моделі [11], демонструють високий потенціал у класифікації емоцій [12], виявленні складних психоемоційних патернів [13] та інтерпретації контексту [14]. Використання трансформерних архітектур дає змогу опрацьовувати довгі залежності в тексті, враховувати латентні емоційні індикатори й точно розпізнавати тональність навіть у випадках іронії, сарказму та змішаних емоційних станів [15]. Значного розвитку набувають також мультимодальні підходи, що поєднують текстові дані з поведінковими або метаданими, що розширює можливості оцінки психоемоційного профілю користувача [16].

Актуальність розроблення методів визначення психоемоційної тональності українськомовних повідомлень зумовлена потребою у створенні локальних мовних моделей, здатних коректно працювати з діалектами, розмовними формами, сленгом та змішаними мовними конструкціями [17]. Наявність таких моделей є критично важливою для підвищення якості аналізу соціальних платформ, освітніх сервісів та систем психологічної підтримки, що інтегрують автоматизовані механізми оцінки стану користувачів [18].

Перспективи розвитку цього напрямку охоплюють конструювання великих українськомовних емоційно розмічених корпусів, удосконалення трансформерних моделей для роботи з низькоресурсними мовами, розроблення інтерпретованих архітектур для пояснення рішень систем та упровадження алгоритмів раннього виявлення емоційної дестабілізації. Сукупність цих напрямів формує базис для створення інтелектуальних соціальних сервісів нового покоління, здатних чутливо й точно реагувати на емоційний стан користувачів.

Українська мова у цифровому вжитку вирізняється багатшаровою варіативністю: співіснуванням літературної норми з розмовними і професійними підсистемами, міжмовними нашаруваннями, регіональними лексемами, активним словотвором і швидким оновленням сленгу. У поєднанні з суспільно значущими темами це породжує складні психоемоційні профілі, де одна й та сама поверхнева

лексема може нести протилежний емоційний знак залежно від локальної інтонації, присутності заперечення чи іронічної рамки [19]. Відповідно, підхід до автоматизованої інтерпретації повинен бути чутливим до контексту короткого висловлювання й не переносити без модифікацій припущення, вироблені на англomовних або багатоконтекстних корпусах.

Практична потреба у надійній психоемоційній аналітиці прямо пов'язана з якістю сервісів модерації, зменшенням токсичності дискусій, підтримкою ментального благополуччя користувачів та підвищенням ефективності зворотного зв'язку між громадянами, органами влади, освітніми та медичними інституціями. Помилки у визначенні тональності мають не тільки методологічну, а й соціальну ціну: вони здатні посилювати поляризацію, хибно флагувати вразливі групи, створювати хибне уявлення про консенсус або кризу, а також провокувати неадекватні управлінські рішення. Коректний інструментарій, навпаки, відкриває можливість тонкого моніторингу настроїв без втручання у свободу висловлювання та з повагою до етичних і правових обмежень.

Суттєвим викликом є характерні для соціальних платформ умови даних: нерівномірна якість текстів, висока частка повторів, кампанійні «накрутки» позитиву чи негативу, а також конвеєрна поява нових меметичних форм. Без попереднього контролю якості корпусів і явної фіксації проміжних артефактів будь-яка модель, у тому числі високорівнева, демонструє нестабільність і деградацію на реальних потоках. Актуальність теми посилюється потребою прозорості та аудиту: автоматичне рішення повинно мати пояснювану структуру, щоб його можна було перевірити, відтворити і коректно оскаржити без апеляції до «чорної скриньки».

Тому, розроблений підхід включає в себе послідовний конвеєр від вхідних повідомлень до узгодженого експертного висновку, у якому кожен етап має власні артефакти й формальні точки контролю (рисунк 1). На вході перебуває масив коротких україномовних повідомлень, що надходять у первинному вигляді без ручного доопрацювання. Матеріал одразу переводиться до підсистеми підготовки, метою якої є створення стабільного представлення тексту для подальшої інтелектуальної обробки.

Перший етап охоплює нормалізацію обраного тексту, побудову мовної моделі для української та векторизацію. Нормалізація забезпечує уніфікацію графематики, усунення службових символів і підготовку до токенізації, завдяки чому знімаються технічні артефакти, що спотворюють частотний профіль. Мовна модель інтерпретує токени у відповідності до українських морфологічних і синтаксичних закономірностей, що підвищує коректність подальших вагових оцінок. Векторизація створює числове подання тексту кількома взаємодоповнюваними способами: частотно-оберненою мірою TF-IDF для стабільної корпусної специфічності, алгоритмом YAKE для відбору термінів із локальною інформативністю та TextRank для графового ранжування ключових одиниць за їхньою зв'язністю. На виході етапу формується узгоджений набір ознак, придатний і для лексиконного зіставлення, і для навчання класифікатора.

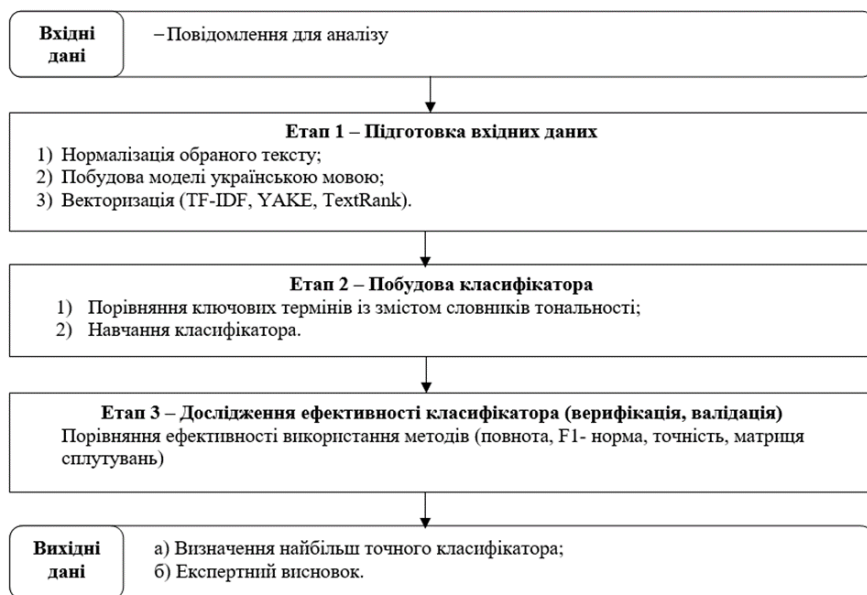


Рисунок 1 – Схема та етапи підходу

Другий етап присвячено побудові класифікатора. Спочатку відбувається порівняння виділених ключових термінів із змістом словників тональності, що дозволяє зафіксувати первинні полярні індикатори та їхні вагові внески. Далі запускається навчання класифікаційної моделі, яка поєднує інформацію з лексиконного зіставлення і векторизованих ознак. Навчання проводиться на репрезентативній вибірці з контролем дисбалансу класів і фіксацією версій параметрів. Проміжним результатом стають натреновані параметри моделі та узгоджені правила прийняття рішень, що переносяться до підсистеми оцінювання.

Третій етап реалізує дослідження ефективності класифікатора. Проводяться незалежні процедури верифікації та валідації з чітким розмежуванням наборів даних, після чого виконується порівняння обраних методів за повнотою, точністю та F1-мірою з додатковим аналізом матриць сплутувань для кожного класу. Окремо здійснюється якісний розбір хибно позитивних і хибно негативних випадків, що дозволяє коректно інтерпретувати числові показники та за потреби повертатися до попередніх етапів для уточнення параметрів нормалізації, вагових порогів або структури ознак. Завершальним продуктом є визначення найбільш точного варіанта класифікатора для заданих умов даних і сформований експертний висновок, у якому фіксуються придатність моделі до експлуатації, межі застосовності та рекомендації щодо подальшого вдосконалення.

У подальшому викладі описуються методи виокремлення ключових термінів, які надалі становитимуть основу семантичного профілю повідомлення та керуватимуть обчисленням психоемоційної тональності. Перший з них спирається на поєднання локальної ваги слова в межах одного повідомлення та його розрізняювальної здатності в масштабі всього корпусу. Інтуїція проста: термін має бути помітним у конкретному тексті, але водночас не належати до тієї частини лексики, яка зустрічається майже всюди і тому не несе змістовного сигналу. Вагове зважування поєднує ці два виміри так, щоб підсилювати слова, характерні саме для цього повідомлення, і послаблювати ті, що є фоновими для всіх документів. Завдяки такій конструкції формується компактний набір лексем і стійких словосполучень, які найкраще репрезентують зміст короткого висловлювання, не втрачаючи чутливості до теми і стилю.

Другий метод зорієнтовано на внутрішньодокументні сигнали релевантності і застосовується після нормалізації тексту та сегментації на речення. Кандидатами на роль ключових одиниць стають як окремі слова, так і короткі фрази, що витримують синтаксичну цілісність. Для кожного кандидата оцінюється низка ознак, які відбивають його поведінку в конкретному документі: позиція у межах тексту, оскільки заголовкові та вступні сегменти часто містять тематичні сигнали; частота появи без штучного «накачування» повтореннями; різноманітність контекстів, що дозволяє відрізнити інформаційні носії від загальних модальних слів; розсіювання по реченнях як індикатор того, що термін підтримує зв'язність повідомлення, а не випадково виникає в одному місці. Додатково зважають на графічні індикатори, зокрема великі літери й абрєвіатури, які часто кодують власні назви або терміни домену. Після агрегування цих ознак кандидат отримує інтегральний бал, що відображає його пріоритетність саме в цьому документі.

Щоб уникнути розщеплення одного поняття на кілька технічних варіантів, результати для морфологічно споріднених форм об'єднуються. Це дає єдиний запис для леми або типової словоформи і запобігає конкуренції між близькими формами, яка спотворює ваги у коротких повідомленнях. На цьому ж кроці проводиться гармонізація написань, що відрізняються дрібними графічними деталями, але мають тотожний зміст. Так підтримується баланс між інтерпретованістю та компактністю словника ключових одиниць.

Практична інтеграція обох підходів відбувається у вигляді злиття ваг із попереднім нормуванням до спільної шкали. Частотно-інверсна схема надає глобальній дисципліни та захищає від переваги універсальних слів, натомість документно орієнтована оцінка підсилює саме ті маркери, що структурно важливі для даного тексту. У поєднанні ці сигнали формують стійкий профіль, здатний відсікти випадкові емоційні індикатори, які не підтримані контекстом, і водночас підхопити змістові осердя, що справді визначають настрої висловлювання.

У модулі визначення психоемоційної тональності цей профіль використовується як керівна маска для подальшого зіставлення зі словниковими валентностями. Високовагові терміни одержують пріоритет під час агрегування

полярності, тоді як другорядні одиниці мають обмежений вплив і не здатні самотужки змінювати знак рішення. Окремо враховуються локальні мовні явища, зокрема заперечення та інтенсифікатори, але їхній внесок модулюється саме ваговою структурою, сформованою на етапі виділення ключових термінів. Це дозволяє уникати хибно позитивних і хибно негативних рішень у випадках, коли одиничний емоційний маркер випадає з тематичної канви повідомлення.

З інженерного погляду усі проміжні артефакти обох методів зберігаються у базі даних разом із версіями параметрів, що забезпечує повний аудит і відтворюваність. У тестуванні це дає змогу порівнювати альтернативні конфігурації відбору, аналізувати чутливість до змін порогів, повертатися до будь-якого прогону та пояснювати природу розбіжностей не на рівні «чорної скриньки», а через прозорий ланцюг вагових рішень. У підсумку поєднання частотно-інверсного зважування та документно орієнтованої оцінки релевантності формує інтерпретовану і стабільну основу, на якій надалі будуються класифікаційні висновки щодо психоемоційної тональності україномовних повідомлень у соціально орієнтованих сервісах. Інтерфейс розробленого ПЗ наведено на рисунку 2.

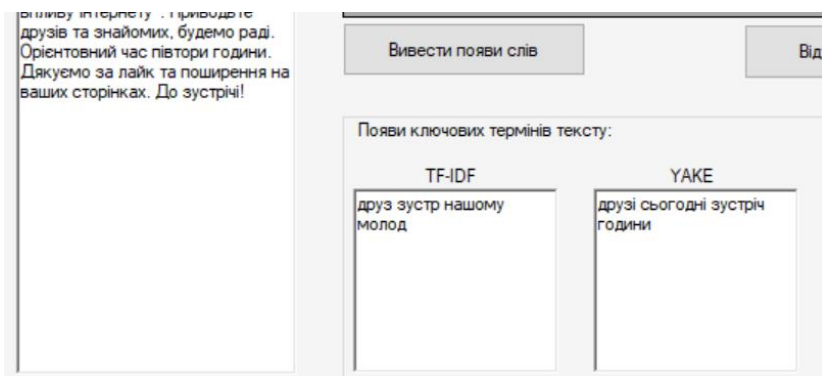


Рисунок 2 – Інтерфейс розробленого застосунку

Окремого значення набувають етичні й правові аспекти. Психоемоційні індикатори можуть трактуватися як чутлива інформація, тож технологічні рішення мають забезпечувати мінімізацію збору персональних даних, працювати з анонімізованими або агрегованими представленнями та виключати дискримінаційні ефекти. Для українського контексту, у якому цифрові платформи часто виконують функції оперативної взаємодії під час надзвичайних ситуацій та громадської мобілізації, відповідальність за інтерпретацію емоційних сигналів особливо висока.

Нарешті, завдання психоемоційного аналізу не зводиться до класифікації повідомлень на позитивні і негативні. Йдеться про побудову стійкої до збурень інфраструктури спостереження за настроями та їхніми змінами у часі, придатної до

розгортання у сервісах різної мети: від освітніх і волонтерських до муніципальних і медіаційних. Саме така рамка робить дослідження не лише науково доцільним, а й суспільно значущим, оскільки надає інструменти для раннього виявлення ескалацій, підтримки конструктивної комунікації та ухвалення рішень на підставі інтерпретованих, а не інтуїтивних емоційних сигналів.

Перелік посилань

1. Bychkov, O., Obrusnik, T., & Dukhnovska, K. (2025). Automatic psychoemotional state analysis of text messages.
2. De Keyser, F., Dens, N., & De Pelsmacker, P. (2017). Don't be so emotional! How tone of voice and service type affect the relationship between message valence and consumer responses to WOM in social media. *Online Information Review*, 41(7), 905-920.
3. Su, L., Tang, B., & Nawijn, J. (2023). How destination social responsibility shapes resident emotional solidarity and quality of life: Moderating roles of disclosure tone and visual messaging. *Journal of Travel Research*, 62(1), 105-120.
4. Roche, J. M., Peters, B., & Dale, R. (2015). "Your tone says it all": The processing and interpretation of affective language. *Speech Communication*, 66, 47-64.
5. Гладун О.В., Мазурець О.В., Залуцька О.О. Аналіз прикладної імплементації методу нейромережевого виявлення емоційного стану людини у режимі реального часу. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». 15-16 листопада 2024. Хмельницький, 2024. с. 142-148.
6. Shevchuk P., Molchanova M., Mazurets O. Software for Text Messages Reliability Analysis Based on the Machine Learning Models Ensemble. *Proceedings of IV International Scientific and Practical Conference «Innovative research and perspectives of the development of science and technology»*. January 29-31, 2024. Stockholm, Sweden. 2024. Pp. 347-354.
7. Молчанова М.О., Мазурець О.В., Собко О.В., Віт Р.В., Назаров В.В. Алгоритм виявлення аб'юзивного вмісту в україномовному аудіоконтенті для імплементації в об'єктно-орієнтовану інформаційну систему. *Науковий журнал «Вісник Хмельницького національного університету»* серія: Технічні науки. Хмельницький, 2024. №1 (331). С. 101-106.
8. Mazurets O., Sobko O., Vit R., Pasternak V. Practical Approach for Detection by Deep Learning of Target Objects of Subject Area Based on Semantic Connectivity Indicators in Audio Database. *Proceedings of XXIV International Scientific and Practical Conference «Modern Scientific Challenges are the Driving Force of the Development of Scientific Research»*. May 22-24, 2024. Bruges, Belgium. International Scientific Unity. 2024. Pp. 91-96.
9. Мазурець О.В., Тимофіїв І.А., Кліменко В.І., Тищенко О.О. Метод виявлення депресивного стану пов'язаного із навчанням у закладах освіти із використанням нейромережі дуальної архітектури. *Науковий журнал «Вісник Херсонського національного технічного університету»*. 2024. №4 (91). С. 311-318.
10. Залуцька О.О., Мазурець О.В. Інформаційний портрет ключових термінів у цифрових навчальних матеріалах. Матеріали III Міжнародної науково-практичної конференції «Сучасні інформаційні технології та інноваційні методики навчання: досвід, тенденції, перспективи». Тернопіль, 2019. С.120-122.
11. Войчишин О.О., Залуцька О.О., Попов Ю.М., Купрійчук В.О. Інформаційна технологія автоматизованого формування семантичного ядра цифрових текстів. *Збірник наукових праць*

за матеріалами XIII Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2021». Хмельницький, 2021. с. 298-305.

12. Молчанова М.О., Мазурець О.В., Собко О.В., Кліменко В.І., Андрощук В.І. Метод нейромережевого виявлення кібербулінгу з використанням хмарних сервісів та об'єктно-орієнтованої моделі. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2024. №2 (333). С. 200-206.

13. Залуцька О.О., Молчанова М.О., Віт Р.В., Мазурець О.В. Конфігурування нейронної мережі для класифікації емоційної тональності текстової інформації за показниками семантичної зв'язності. Збірник наукових праць за матеріалами XV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2023». Хмельницький, 2023. с. 102-107.

14. Mazurets O.V., Sobko O.V., Molchanova M.O., Zalutska O.O., Yurchak A.V. Practical Implementation of Neural Network Method for Stress Features Detection by Social Internet Networks Posts. Global Science: Prospects and Innovations. Proceedings of the II International Scientific and Theoretical Conference «Scientific Review of the Actual Events, Achievements and Problems». May 31, 2024. Berlin, Federal Republic of Germany: International Center of Scientific Research. 2024. Pp. 160-167.

15. Blazhuk V., Mazurets O., Zalutska O. An Approach to Using the mBERT Deep Learning Neural Network Model for Identifying Emotional Components and Communication Intentions. The Impact of Scientific Research on the Development of the Modern World. Proceedings of the XLIV International scientific and practical conference. October 23-25, 2024. Dubrovnik, Croatia. 2024. Pp. 79-84.

16. Юрченко Д.Ю., Мазурець О.В., Залуцька О.О., Безпрозвана Ю.Г. Підхід до візуального пояснення результатів нейромережевого аналізу емоційної тональності повідомлень у соціальних мережах. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». 15-16 листопада 2024. Хмельницький, 2024. с. 565-571.

17. Денисенко Б.О., Залуцька О.О. Інтелектуальні засоби кібербезпеки в інтернет та нейромережеве виявлення дезінформації. Інформаційна, функційна і кібербезпека СКІФіК2024. Матеріали четвертої науково-технічної конференції. 29-30 листопада 2024. Харків. 2024. с. 34-35.

18. Murava V., Zalutska O., Didur V., Mazurets O. Software architecture of information system for exchanging LLM thematic prompts. Global Trends in the Development of Information Technology and Science. Proceedings IV International Scientific and Practical Conference. June 25-27, 2025. Stockholm, Sweden. Pp. 121-127.

19. Залуцька О.О. Метод автоматизованого оцінювання відповідності тональності відгуків на товари в інтернет-магазинах до їх користувацької оцінки з використанням нейромереж. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». 15-16 листопада 2024. Хмельницький, 2024. с. 221-236.

УДК 004.41

Горбатюк І.В., Форкун Ю.В.

Хмельницький національний університет

МЕТОД ПРОЄКТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ АГЕНТНО-ОРІЄНТОВАНОЇ АРХІТЕКТУРИ ДЛЯ БАГАТОКОМПОНЕНТНИХ ПРОГРАМНИХ СИСТЕМ

У роботі розглянуто агентно-орієнтований метод проєктування програмного забезпечення для багатокомпонентних систем. Розроблено процес автоматичного вибору метамodelей і конфігурацій агентів із використанням баєсового пізнання та мультиагентного підходу. Підхід забезпечує узгодженість компонентів, скорочує час проєктування та підвищує ефективність розробки складних програмних систем.

The paper considers an agent-oriented method for software design for multi-component systems. A process for automatic selection of metamodels and agent configurations using Bayesian learning and a multi-agent approach is developed. The approach ensures component consistency, reduces design time, and increases the efficiency of developing complex software systems.

Сучасні інформаційні системи стають дедалі складнішими, поєднуючи різні програмні компоненти, що взаємодіють між собою в умовах децентралізованого управління. Такі системи вимагають нових методів проєктування, орієнтованих на автономність, адаптивність і координацію між частинами. Одним із ефективних підходів є агентно-орієнтована архітектура, яка забезпечує гнучкість, масштабованість і підвищену надійність при створенні багатокомпонентних систем.

Робота присвячена розробці методу проєктування програмного забезпечення, заснованого на агентно-орієнтованій парадигмі. Основна ідея полягає у використанні мультиагентних систем (МАС) для моделювання взаємодії між компонентами програмного комплексу. Кожен агент виступає як автономна сутність із власними цілями, знаннями та можливістю співпраці з іншими агентами.

Метою дослідження є створення автоматизованого механізму вибору оптимальної конфігурації агентів та метамodelей для побудови рішення, що відповідає заданій проблемі. Такий механізм аналізує опис проблеми, зіставляє її характеристики з базою знань про існуючі агентні метамodelі й обирає найбільш сумісний набір компонентів для побудови системи.

У межах дослідження розроблено процес, який складається з трьох основних етапів:

- характеристика опису проблеми та визначення домену рішення;
- оцінювання продуктивності наявних метамodelей для цього домену;

– автоматичне зіставлення проблеми та набору метамodelей за допомогою мультиагентного підходу.

Запропонована архітектура мультиагентної системи містить агенти, які представляють окремі метамodelі та взаємодіють між собою, формуючи групу найбільш сумісних modelей. Кожен агент використовує критерії сумісності для узгодження рішень з іншими агентами. У результаті формується узгоджена група метамodelей, що становить основу запропонованого рішення.

Розроблено прототип інструменту, що реалізує запропонований метод і дозволяє автоматизувати вибір архітектурних компонентів. Для цього застосовано методи кооперативного штучного інтелекту, баєсового пізнання та метааналізу, що враховують невизначеність і статистичні закономірності у прийнятті рішень.

Практичне значення дослідження полягає у можливості використання запропонованого методу для створення складних систем — від сенсорних мереж до автономних керуючих комплексів. Використання агентного підходу дозволяє підвищити надійність програмних систем, забезпечити їх самодостатність і спроможність до адаптації в умовах динамічних середовищ.

Проведені експерименти показали, що застосування розробленого механізму скорочує час проєктування в середньому на від 5 до 15%, зменшує кількість помилок узгодження між компонентами та підвищує стабільність системи під час розгортання.

Запропонований підхід може бути використаний у процесах інженерії програмного забезпечення, особливо при створенні розподілених, адаптивних і високонадійних програмних рішень. Його гнучкість дозволяє масштабувати архітектуру та повторно використовувати окремі компоненти в інших проєктах.

Подальші дослідження планується спрямувати на вдосконалення інструменту автоматичного аналізу, розширення бази знань про метамodelі, а також інтеграцію з сучасними технологіями машинного навчання для підвищення точності рішень і прогнозування ефективності компонентів.

Перелік посилань

1. Blum J. Exploring Arduino: Tools and Techniques for Engineering Wizardry. 2nd ed. Wiley. 2021.
2. McGarry, S. What is Schematic Design? Understanding Schematics and Their Importance. URL: <https://www.autodesk.com/products/fusion-360/blog/schematic-design/>
3. Law A. M. Simulation Modeling and Analysis. 6th ed. New York : McGraw-Hill Education, 2023. 864 p.
4. Бабенко В. О., Попова О. В. Застосування методів системного аналізу та експертних оцінок для оптимізації управлінських рішень. Економіка та суспільство. 2023. № 49.
5. Матвійків О., Ткаченко С., Хаханов В. Інженерне проєктування складних об'єктів і систем. – Львів: НУ «Львівська політехніка», 2021. – 260 с.
6. Lemmon M.D. Lectures for Advanced Control Systems. University of Notre Dame, 2025. 346 p. URL: <https://www3.nd.edu/~lemmon/courses/advanced-control/lecture-book/advanced-control-2025.pdf>.

УДК 004.9

Гордієнко Є.О.

Хмельницький національний університет

АНАЛІЗ ІНСТРУМЕНТІВ ТА ЗАСОБІВ ФОРМАЛІЗАЦІЇ ВИМОГ ПРИ ПРОЕКТУВАННІ ТА РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Розглянуто задачу формалізації вимог до програмного забезпечення, а також інструменти та засоби, що дозволяють здійснювати правильну та чітку системи формалізації вимог. Здійснено аналіз інструментів та засобів системи формалізації вимог.

The article of formalizing software requirements is considered, as well as the tools and means that allow for the implementation of a correct and clear system of formalizing requirements. An analysis of the tools and means of the system of formalizing requirements is carried out.

Формалізація вимог до програмного забезпечення - це критично важливий етап у життєвому циклі розробки, який полягає у систематичному перетворенні неформальних, часто неоднозначних потреб замовника на чіткі, верифіковані, узгоджені та повні технічні специфікації. Це процес, що переводить розпливчасті ідеї та очікування в точну, структуровану мову, яка може бути зрозуміла та використана як розробниками для кодування, так і тестувальниками для перевірки відповідності.

Основне завдання полягає в усуненні двозначності, оскільки вимоги, виражені природною мовою, неминуче містять термінологічну невизначеність, прогалини в логіці та суперечності. Формалізація використовує методи, що дозволяють перевірити кожну вимогу на узгодженість та відповісти на запитання чи не суперечить вона іншим вимогам та визначити повноту, тобто чи описано всі необхідні функції.

Цей процес охоплює кілька ключових дій. Спочатку проводиться детальний аналіз зібраних вимог для їхньої класифікації на функціональні (що система повинна робити) та нефункціональні (як система повинна працювати, включаючи вимоги до продуктивності, безпеки та надійності). Потім відбувається їхнє структурування із застосуванням стандартних шаблонів та нотацій, таких як використання сценаріїв (Use Cases) або мови UML. На цьому етапі вимоги перетворюються на технічні атрибути, коли кожна функціональна вимога повинна мати унікальний ідентифікатор, бути простежуваною до джерела та, що найважливіше, верифікованою, тобто повинна існувати можливість розробити тест, який підтвердить її виконання.

Кінцевим результатом формалізації є створення документу специфікації вимог до програмного забезпечення (SRS), який слугує єдиним джерелом істини та

контрактом між замовником і командою розробки. Без цієї строгої формалізації проєкт неминуче стикається зі збільшенням вартості, затримками та невідповідністю кінцевого продукту початковим очікуванням.

Загалом, дослідники виділяють декілька інструментів із доступністю поза межами проєктів. Також можна виокремити ще один засіб, що доступний як частина набору інструментів COMPASS [1], який спрощує формальну специфікацію вимог у контексті моделей AADL [2].

У [3] дослідники представили інструмент під назвою DODT, розроблений у рамках проєкту CESAR [4], що дозволяє проєкційне редагування та типізацію вимог на основі шаблонного синтаксису (Requirements Specification Language - RSL), атрибутної онтології та предметно-специфічної онтології. Були реалізовані перевірки валідації на основі онтологій, які дозволяють виявляти суперечності шляхом попарного порівняння вимог, іменників, які не визначені в онтології тощо. Хоча DODT не реалізує точного зв'язку шаблонів зі шаблонами властивостей, однак авторами надаються пропозиції щодо шаблонів, які можуть бути придатними для опису заданої вимоги.

Інструмент EARS-CTRL [5] був введений для забезпечення шляхом побудови коректності вимог, написаних з використанням шаблонів Easy Approach to Requirements Syntax (EARS). Інструмент перевіряє, чи можна синтезувати контролер з набору вимог. Якщо контролер неможливо синтезувати, то існують конфліктуючі вимоги. EARS-CTRL дозволяє редагувати проєкційні вимоги на основі глосарію, визначеного для області синтезу контролерів. Вимоги аналізуються як формули LTL. Ефективність аналізу залежить від визначеної користувачем семантичної інформації (наприклад, простих предикатів) для заданого глосарію.

Інструмент RERD [6] підтримує специфікацію вимог та виведення властивостей на основі шаблонів та шаблонів властивостей, а також поступове конструювання систем для реалізації похідних властивостей за допомогою підходу проєктування «знизу вгору». Під час редагування вимог користувач взаємодіє з базовими онтологіями, запитуючи їх та отримуючи доступ до екземплярів їхніх класів для пошуку відповідних термінів. Таким чином, словник шаблонних атрибутів обмежений термінами, які можна ідентифікувати в рамках предметно-специфічних онтологій та онтологій, специфічних для проєктованої системи. Зв'язки шаблонних атрибутів відіграють ключову роль у семантичному аналізі та виведенні властивостей, де кожен шаблон пов'язаний із заздалегідь визначеними шаблонами властивостей, які можуть формально його фіксувати. Для забезпечення дотримання властивостей користувач може вибрати один із доступних шаблонів архітектури та параметризувати їх, вибираючи компоненти з поступово побудованої моделі системи. Потім необхідно перевірити відсутність взаємоблокувань у результатуючій моделі, що пропонується зробити за допомогою спеціального інструменту D-Finder. Для властивостей, які неможливо забезпечити за допомогою існуючих шаблонів архітектури, користувачеві доведеться використовувати зовнішні інструменти, такі як перевірка моделей.

Щодо підходу на основі COMPASS, у [1] дослідники представили інший підхід, згідно з яким формальні властивості не створюються з шаблонів шляхом заміни їхніх заповнювачів станами/подіями, пов'язаними з атрибутами, визначеними шаблоном, а шляхом присвоєння значень атрибутам системної моделі. Більш конкретно, було введено набір властивостей, які дозволяють пов'язувати значення з певними елементами моделі AADL.

Формальна семантика системних властивостей спирається на поведінкову семантику мови SLIM, тоді як логіка, що використовується для визначення більшості з них, є варіантом метричної часової логіки (MTL). Хоча таксономія формальних властивостей порівняно обмежена у виразності, вона повністю усуває необхідність вибору шаблону та винаходження екземпляра. Формальні властивості можна аналізувати на узгодженість між різними рівнями абстракції системної моделі або використовувати як припущення чи гарантії компонентів для проектування на основі контрактів. Для останньої мети COMPASS вимагає додаткової специфікації уточнення контракту, яке пов'язує контракт з його підкомпонентів. Це дозволяє виконувати різні аналізи, такі як узгодженість або наслідки для будь-якої підмножини властивостей контракту, щоб перевірити правильність уточнень контракту, а також звзвити контракт таким чином, щоб уточнення залишалося чинним.

Отже, специфікація вимог може базуватися на онтологіях предметної області, які використовуються для виявлення відсутньої інформації та усунення невідповідностей і випадків недостатньої специфікації. Виведення властивостей залежить від формальної моделі системи, яка може бути поступово побудована за допомогою компонентного процесу проектування.

Перелік посилань

1. M. Bozzano, H. Bruintjes, A. Cimatti, J.-P. Katoen, T. Noll, S. Tonetta Compass 3.0. Tools and algorithms for the construction and analysis of systems (TACAS), Springer, Cham (2019), pp. 379-385.
2. V. Bos, H. Bruintjes, S. Tonetta. Catalogue of system and software properties. Computer safety, reliability, and security, Springer, Cham (2016), pp. 88-101.
3. N. Mahmud, C. Seceleanu, O. Ljungkrantz Resa : an ontology-based requirement specification language tailored to automotive systems 10th IEEE int. Symp. On industrial embedded systems (2015), pp. 1-10.
4. Rajan, T. Wahl CESAR-cost-efficient methods and processes for safety-relevant embedded systems Springer (2013).
5. L. Lucio, S. Rahman, C. Cheng, A. Mavin. Just formal enough? automated analysis of EARS requirements. NFM 2017 (2017), pp. 427-434. NASA formal methods - 9th int. Symp.
6. E. Stachtari, A. Mavridou, P. Katsaros, S. Bliudze, J. Sifakis. Early validation of system requirements and design through correctness-by-construction. J Syst Software, 145 (2018), pp. 52-78.

УДК 004.8

Грінчук М.О.¹, Залуцька О.О.²

¹ Новолабунський ліцей Полонської міської ради

² Хмельницький національний університет

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ДІАГНОСТУВАННЯ ХВОРОБ ЛИСТЯ ТОМАТА ЗА НЕЙРОМЕРЕЖЕВИМ АНАЛІЗОМ ФОТОЗОБРАЖЕНЬ

Робота присвячена створенню інформаційної технології для автоматизованого виявлення хвороб листя томату за зображеннями із застосуванням глибоких нейронних мереж. Запропонований підхід підвищує ефективність діагностики рослин порівняно з традиційними методами, що потребують значного часу та експертних знань, і є актуальним напрямом розвитку аграрних інформаційних систем.

The paper is devoted to the creation of information technology for automated detection of tomato leaf diseases based on images using deep neural networks. The proposed approach increases the efficiency of plant diagnostics compared to traditional methods, which require considerable time and expert knowledge, and is a relevant direction for the development of agricultural information systems.

Сільське господарство, зокрема овочівництво, має ключове значення для продовольчої безпеки, економічного розвитку регіонів та експорту багатьох країн [1]. Томат є однією з наймасовіших овочевих культур, що вирощується для свіжого споживання та промислової переробки [2, 3].

Водночас урожай томатів суттєво знижується через численні хвороби грибової, бактеріальної та вірусної природи, які вражають листя, стебла та плоди. У багатьох випадках втрати можуть досягати значних масштабів, що призводить до погіршення якості продукції та збільшення витрат на її захист [4].

Особливої актуальності ця проблема набуває в Україні, де через зміни умов виробництва, логістики та доступності земель необхідно підвищувати ефективність вирощування культур у нових регіонах. Це вимагає сучасних рішень для моніторингу стану посівів і запобігання втратам.

Розвиток цифрових технологій, комп'ютерного зору [5] та штучного інтелекту [6] відкриває якісно нові можливості для агросектору. Інтелектуальні системи можуть здійснювати моніторинг стану рослин, своєчасно виявляти ознаки захворювань і допомагати аграріям оперативного реагувати на загрози.

Автоматизована діагностика хвороб листя томату на основі аналізу зображень сприяє підвищенню точності контролю, зменшенню людського впливу, економії ресурсів і переходу до принципів точного землеробства. Це робить

впровадження таких технологій важливим кроком для забезпечення сталого розвитку овочівництва.

Нейронні мережі є ключовою технологією сучасного штучного інтелекту [7], оскільки здатні навчатися та робити висновки на основі даних, моделюючи роботу біологічних нейронів [8]. Їхня ефективність зумовлена можливістю адаптувати ваги між зв'язками для мінімізації похибки під час навчання. Історичний розвиток нейромережевих підходів привів до появи глибокого навчання [9], яке дозволило моделювати складні нелінійні залежності та стало основою сучасних систем комп'ютерного зору.

У аграрному секторі глибокі нейронні мережі широко застосовуються для класифікації стану рослин, виявлення шкідників і діагностики захворювань за зображеннями листя. На відміну від класичних алгоритмів машинного навчання, які потребують ручного виділення ознак, сучасні CNN-архітектури самостійно вилучають релевантні характеристики [10], що є критично важливим у складних польових умовах. Архітектури AlexNet, VGG, ResNet, Inception, DenseNet і MobileNet підтвердили свою результативність у задачах визначення хвороб різних культур, включно з томатами.

Паралельно розвиваються трансформерні моделі, серед яких Vision Transformer (ViT) є одним із найперспективніших рішень для аналізу зображень. Завдяки механізму self-attention ViT здатна враховувати глобальні просторові взаємозв'язки між частинами зображення та ефективно розпізнавати ознаки, які проявляються нерівномірно на поверхні листка. Для порівняння з ним доцільним є використання легких згорткових моделей, таких як MobileNetV2, оптимізованих для пристроїв із обмеженими ресурсами [11].

Інтеграція таких моделей із безпілотними платформами, польовими роботами й мобільними застосунками сприяє розвитку точного землеробства, де рішення приймаються на основі даних. Це дозволяє зменшити втрати врожаю, оптимізувати витрати та забезпечити своєчасну діагностику захворювань, підвищуючи ефективність і сталий розвиток агровиробництва, зокрема в Україні.

Для автоматизованого виявлення хвороб листя томатів важливо ідентифікувати характерні візуальні ознаки, що свідчать про розвиток патологічних процесів у рослині. Як правило, симптоми проявляються у вигляді зміни кольору, появи плям, порушення структури або деформації листової поверхні. Для класифікації таких зображень використовується попередньо навчена модель глибокого навчання, здатна аналізувати та розпізнавати зазначені особливості. Загальну схему підходу до визначення захворювань листя томату подано на рисунку 1.

Вхідними даними є зображення листя томатів із різними типами захворювань і здорові зразки. Перед аналізом зображення проходять стандартну попередню обробку: масштабування, нормалізацію та фільтрацію шумів. Далі дані

подаються у попередньо навчені моделі ViT-B/12 і MobileNetV2, які автоматично виділяють ознаки та визначають клас захворювання. Результат подається у вигляді ймовірності належності до кожного класу, що дає можливість швидко та точно визначати стан рослин без участі експертів.

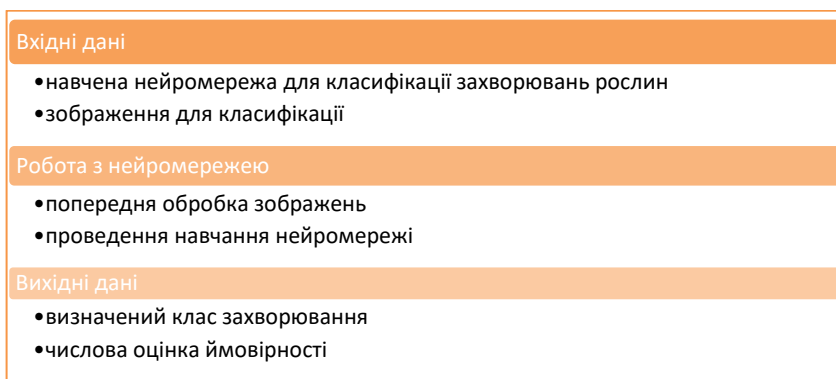


Рисунок 1 – Послідовність дій при класифікації захворювань листя томату

Для розпізнавання захворювань листя томатів застосовуються моделі ViT-B/12 та MobileNetV2, навчені на датасеті Tomato Leaves Dataset [12], що містить зображення здорових рослин і різних типів уражень. Дані попередньо обробляються: зображення приводяться до розміру 224×224 пікселів, нормалізуються та розподіляються на навчальну (80 %) і валідаційну (20 %) вибірки. Такий підхід забезпечує якісне формування моделі для точної класифікації захворювань.

Другим етапом є налаштування і тренування двох обраних архітектур – Vision Transformer та MobileNetV2. ViT використовує механізм самоуваги для аналізу зображень, розбитих на патчі, тоді як MobileNetV2 є легкою згортковою мережею, оптимізованою для швидкої роботи на пристроях із невеликими ресурсами. Обидві моделі навчаються з використанням оптимізатора Adam і категоріальної кросентропії, а для запобігання перенавчанню застосовуються Dropout, Weight Decay та Early Stopping. Після навчання проводиться оцінювання за метриками Accuracy, Precision, Recall, F1-score та матрицею помилок. У результаті отримуються дві готові моделі, що дозволяють визначити найоптимальнішу для використання в системі діагностики захворювань листя томатів.

Для оцінювання ефективності запропонованого підходу розроблено експериментальне програмне забезпечення на Python у середовищі PyCharm з використанням TensorFlow, Keras і PyTorch. Система включає модуль підготовки

даних, модуль навчання моделей і модуль класифікації нових зображень. На етапі підготовки було видалено файли в некоректних форматах, після чого сформовано навчальну вибірку з 25 844 зображень і валідаційну – з 6 683. Навчання моделей Vision Transformer та MobileNetV2 виконується автоматизованим скриптом, який охоплює передобробку, аугментацію даних та підбір гіперпараметрів (рисунок 2).

```
Epoch 1/15
808/808 [=====] - 720s 889ms/step - loss: 1.3107 - accuracy: 0.5547 - val_loss: 0.8498 - val_accuracy: 0.7265
Epoch 2/15
808/808 [=====] - 670s 830ms/step - loss: 0.8664 - accuracy: 0.7096 - val_loss: 0.7498 - val_accuracy: 0.7512
Epoch 3/15
808/808 [=====] - 504s 624ms/step - loss: 0.7742 - accuracy: 0.7405 - val_loss: 0.6853 - val_accuracy: 0.7738
Epoch 4/15
808/808 [=====] - 489s 605ms/step - loss: 0.7327 - accuracy: 0.7527 - val_loss: 0.6274 - val_accuracy: 0.7989
Epoch 5/15
808/808 [=====] - 436s 540ms/step - loss: 0.7077 - accuracy: 0.7607 - val_loss: 0.6207 - val_accuracy: 0.7934
```

Рисунок 2 – Процес навчання нейромережевої моделі MobileNetV2

Під час навчання контролювалися ключові метрики точності класифікації – Accuracy, Precision, Recall та F1-score. Після завершення моделі було збережено у форматах .h5 та .pt для зручної подальшої інтеграції. Для роботи з навченими мережами реалізовано користувацький інтерфейс модуля класифікації, який забезпечує розпізнавання захворювань за новими зображеннями листа томатів.

На рисунку 3 наведено реалізоване програмне забезпечення для класифікації захворювань листа томату.

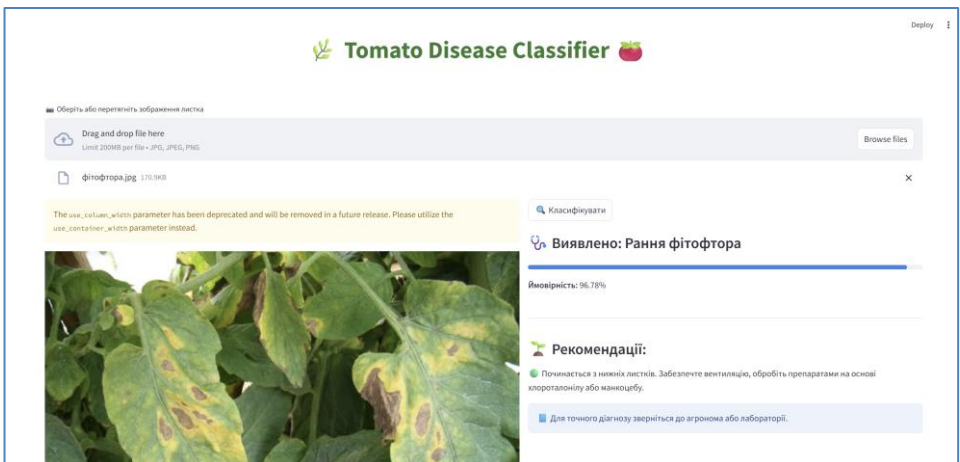


Рисунок 3 – Інтерфейс модуля класифікації захворювань листа томату

Для оцінювання ефективності створеної інформаційної технології проведено експерименти з використанням двох моделей – Vision Transformer і MobileNetV2. Обидві архітектури навчалися на однаковому датасеті, що охоплює 11 класів захворювань і здорового листя. Узагальнені результати навчання подано в таблиці 1.

Було розроблено інформаційну технологію для автоматизованої класифікації захворювань листя томату на основі методів комп'ютерного зору та глибокого навчання. Проведені дослідження підтвердило високу ефективність використання сучасних нейромережових моделей у задачах діагностики агрокультурних хвороб.

Таблиця 1 – Результати проведення навчання нейромереж

Назва моделі	Accuracy	Loss	F1-score
ViT-B/12	0.9717	0.0984	0.9717
MobileNetV2	0.8243	0.5328	0.8224

Розроблене програмне забезпечення реалізує повний цикл автоматичної діагностики – від обробки вхідних зображень до отримання результату класифікації в інтерфейсі користувача. Це дає можливість оперативно визначати тип хвороби та підвищує ефективність процесу ухвалення рішень в агровиробництві.

Таким чином, проведені дослідження підтвердило доцільність застосування штучного інтелекту для моніторингу стану томатних посівів і відкрило перспективи подальшого розвитку подібних систем.

Перелік посилань

1. Das, A., Pathan, F., Jim, J. R., Kabir, M. M., & Mridha, M. F. (2025). Deep learning-based classification, detection, and segmentation of tomato leaf diseases: A state-of-the-art review. *Artificial Intelligence in Agriculture*.
2. Ramesh Babu, P., Srikrishna, A., & Gera, V. R. (2024). Diagnosis of tomato leaf disease using OTSU multi-threshold image segmentation-based chimp optimization algorithm and LeNet-5 classifier. *Journal of Plant Diseases and Protection*, 131(6), 2221-2236.
3. Ahmed, M. R., Haque, R., Rahman, S. A., Afridi, S., Abir, M. F. F., Hossain, M. F., ... & Uddin, M. M. (2024, May). Towards automated detection of tomato leaf diseases. In *2024 6th International Conference on Electrical Engineering and Information & Communication Technology (ICEEICT)* (pp. 387-392). IEEE.
4. Assaduzzaman, M., Bishshash, P., Nirob, M. A. S., Al Marouf, A., Rokne, J. G., & Alhajj, R. (2025). XSE-TomatoNet: An explainable AI based tomato leaf disease classification method using EfficientNetB0 with squeeze-and-excitation blocks and multi-scale feature fusion. *MethodsX*, 14, 103159.

5. Собко О.В., Кліменко В.І., Мазурець О.В., Залуцька О.О., Гладун О.В. Особливості програмної інженерії та тестування програмного забезпечення для нейромережевого аналізу фотоданих залишків зруйнованих будівель із роботизованої техніки. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №4 (45). С. 1566-1581.
6. Kharysh I., Sobko O., Mazurets O. Designing CNN Neural Network Model for Detecting Fractures of Lower Extremities by X-ray Images. The Impact of Scientific Research on the Development of the Modern World. Proceedings of the XLIV International scientific and practical conference. October 23-25, 2024. Dubrovnik, Croatia. 2024. Pp. 91-96.
7. Zharnovskiy O., Mazurets O., Sobko O. Approach to Identification of Artificial Intelligence-Generated People Images by Means of Machine Learning. Key Aspects of the Development of Scientific Research in Modern Conditions. Proceedings of the XLV International scientific and practical conference. October 30 – November 1, 2024. Constanta, Romania. 2024. Pp. 69-73.
8. Mazurets O. V., Klimenko V. I., Molchanova M. O., Sultanov A. V. Object-Oriented Intelligent System for Neural Network Detection of Sugar Crystallization Zones. Global Science: Prospects and Innovations. Proceedings of the 10th International scientific and practical conference. Cognum Publishing House. Liverpool, United Kingdom. 2024. Pp. 198-207.
9. Мазур Є.В., Мазурець О.В., Кліменко В.І., Собко О.В., Залуцька О.О. Алгоритми та програмна архітектура інформаційної системи нейромережевого аналізу постави людини. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2025. №3. Т.1. С. 275-284.
10. Kok I.A., Kadyńska V.D., Zalutská O.O., Mazurets O.V. Object-Oriented Intelligent System for Automated Control of Smoking by Video Data. Current scientific goals, approaches and challenges. Proceedings of IV International Scientific and Theoretical Conference. June 13, 2025. Dresden, Federal Republic of Germany. Pp. 156-164.
11. Hladun O.V., Molchanova M.O., Zalutská O.O., Mazurets O.V. Effectiveness research of using ViT neural network architecture for classifying the destroyed buildings remains. Achievements of Science and Applied Research. Proceedings of 2nd International Scientific and Theoretical Conference. May 19-21, 2025. Dublin, Ireland. Pp. 96-100.
12. Kaggle.com. Tomato Leaves Dataset. URL:
<https://www.kaggle.com/datasets/ashishmotwani/tomato/data>

УДК 004

Гуляєв Н.Ю.

Кам'янський енергетичний фаховий коледж

МЕТОДИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

У сучасному цифровому світі інформація стала одним із найцінніших ресурсів, а її захист – пріоритетним завданням для держав, бізнесу та приватних осіб. Щодня у глобальних комп'ютерних мережах передаються мільярди повідомлень, фінансових транзакцій, персональних даних. З розвитком кіберзлочинності та технічних можливостей зловмисників традиційні методи захисту інформації (паролі, обмеження доступу, антивіруси) стають недостатніми.

In today's digital world, information has become one of the most valuable resources, and its protection is a priority for states, businesses, and individuals. Billions of messages, financial transactions, and personal data are transmitted across global computer networks every day. With the development of cybercrime and the technical capabilities of attackers, traditional methods of information protection (passwords, access restrictions, antiviruses) are becoming insufficient.

Криптографія – наука про методи перетворення даних із метою їх захисту – є фундаментом сучасних систем безпеки. Вона забезпечує конфіденційність, цілісність, автентичність і невідомість інформації.

Метою даної доповіді є аналіз сучасних методів криптографічного захисту, їх класифікації, особливостей застосування в комп'ютерних системах та тенденцій розвитку цієї галузі.

Основні поняття криптографічного захисту:

Криптографія (від грец. *kryptos* – «прихований», *grapho* – «пишу») – це сукупність методів і алгоритмів, які забезпечують захист інформації шляхом її математичного перетворення.

Основні цілі криптографічного захисту:

Конфіденційність – захист від несанкціонованого ознайомлення.

Цілісність – недопущення несанкціонованої модифікації.

Автентичність – підтвердження справжності джерела даних.

Невідомість – неможливість відмови від авторства чи факту відправлення.

Зазвичай криптографічні методи реалізуються програмно або апаратно, інтегруються у протоколи зв'язку, операційні системи, хмарні сервіси та банківські додатки.

Класифікація методів криптографічного захисту:

1. Симетричні алгоритми шифрування

У симетричних системах для шифрування та дешифрування використовується один і той самий ключ. Основна перевага – висока швидкість обробки даних, недолік – складність безпечного розповсюдження ключів.

Найпоширеніші симетричні алгоритми:

AES (Advanced Encryption Standard) – сучасний стандарт США, підтримує довжину ключа 128, 192 та 256 біт.

Blowfish, Twofish, IDEA, RC6 – альтернативні варіанти із різним рівнем продуктивності та безпеки.

Симетричне шифрування активно використовується у VPN, Wi-Fi (WPA2, WPA3), хмарних сховищах та месенджерах.

2. Асиметричні алгоритми шифрування

Асиметричні системи базуються на парі ключів: публічному та приватному. Публічний використовується для шифрування або перевірки підпису, приватний – для дешифрування або створення підпису.

Основні алгоритми:

RSA – класичний алгоритм, стійкість якого базується на складності факторизації великих чисел.

ElGamal, ECC (еліптичні криві) – сучасні схеми з вищою ефективністю.

Перевагою асиметричної криптографії є зручність управління ключами, а недоліком – більші обчислювальні витрати.

3. Хешування та цифровий підпис

Хеш-функція перетворює довільне повідомлення на фіксований бітовий рядок – «відбиток» або «хеш». Приклад – алгоритми SHA-2, SHA-3, BLAKE2.

Цифровий підпис, своєю чергою, забезпечує автентичність та невідомність. Його використовують у системах електронного документообігу, банківських платформах, державних порталах (наприклад, «Дія»).

Сучасні напрями розвитку криптографії:

1. Квантова криптографія – створення систем, стійких до атак квантових комп'ютерів. Зокрема, алгоритми на основі решіток (*lattice-based*) та багаточленів.

2. Гомоморфне шифрування – можливість виконувати обчислення над зашифрованими даними без їх розшифрування.

3. Криптографія з нульовим розголошенням (Zero-Knowledge Proofs) – використовується у блокчейнах для підвищення приватності.

4. Квантові протоколи розподілу ключів (QKD) – практичне застосування квантової фізики для безпечної передачі ключів.

Застосування криптографічних методів у комп'ютерних системах

Банківські системи та електронна комерція: шифрування платежів, захист карткових даних (протоколи SSL/TLS).

Мобільні додатки та месенджери: наскрізне (end-to-end) шифрування у WhatsApp, Signal, Telegram.

Хмарні сервіси: шифрування даних клієнтів на серверах Google, Microsoft, AWS.

Державні інформаційні системи: використання електронного підпису, сертифікованих криптопровайдерів.

Криптографічні методи є невід'ємною складовою систем інформаційної безпеки. Вони забезпечують надійний захист даних у процесі зберігання, передавання та обробки.

Сучасний етап розвитку криптографії характеризується переходом від класичних алгоритмів до постквантових і хмарних рішень, що здатні протидіяти новим загрозам. Для України розвиток власних криптографічних стандартів і впровадження сертифікованих засобів захисту інформації є стратегічно важливим напрямом кібербезпеки.

Перелік посилань

1. Stallings W. Cryptography and Network Security: Principles and Practice. – 8th ed. – Pearson, 2023.
1. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. – CRC Press, 2022.
2. Національний стандарт України ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації.
3. NIST. Post-Quantum Cryptography Project. – <https://csrc.nist.gov/projects/post-quantum-cryptography>.
4. Кузнецов С.Ю. Системи захисту інформації: навчальний посібник. – Київ: НАУ, 2021.

УДК 004.8

Держак В.В., Мазурець О.В.

Хмельницький національний університет

ПРОЄКТУВАННЯ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ КЛАСИФІКАЦІЇ ПОБУТОВОГО СМІТТЯ ЗА ВІЗУАЛЬНИМИ ДАНИМИ

У роботі розглянуто особливості проектування інтелектуальної системи класифікації побутового сміття за візуальними даними в умовах змішаних потоків, змінного освітлення та фонових завад. Запропоновано підхід, у якому якість зображень розглядається як структурний елемент процесу навчання: формалізовано вектор якості (різкість, контраст, експозиційна збалансованість, рівень фонові «засміченості») та побудовано механізм адаптивної фільтрації вибірки за інтегральним балом. Архітектура системи реалізована як модульний конвеєр, що включає підсистему підготовки даних, тренувальний контур з порівняльним донавчанням моделей на сирому й очищеному датасетах, модуль оцінювання з використанням збалансованих метрик та прикладний вебінтерфейс для інтерактивного тестування.

The paper addresses the design features of an intelligent visual system for household waste classification operating under mixed waste streams, variable illumination and background clutter. The proposed approach treats image quality as a structural component of the training process: a formal quality vector (sharpness, contrast, exposure balance, background clutter level) is introduced and an adaptive filtering mechanism based on an integral quality score is implemented. The system architecture is organised as a modular pipeline comprising a data preparation subsystem, a training loop with comparative fine-tuning of models on raw and cleaned datasets, an evaluation module employing balanced performance metrics, and an application-level web interface for interactive testing.

Інтенсивне зростання обсягів побутових відходів і нормативний тиск щодо збільшення частки перероблення висувають підвищені вимоги до автоматизації сортування на сортувальних лініях та в смарт-інфраструктурі поводження з відходами [1]. Критичним елементом таких рішень є інтелектуальні системи класифікації побутового сміття за візуальними даними, здатні працювати в умовах змішаних потоків, змінного освітлення, фонових завад, деформацій і забруднень об'єктів [2]. У цих умовах якість зображень та організація програмної архітектури системи стають не другорядним, а визначальним чинником досягнення стабільної точності й відтворюваності результатів [3]. У цьому контексті комп'ютерне зір [4] і нейромережеві методи [5] відкривають нові перспективи для об'єктивного аналізу візуальної інформації, що містить зображення побутових відходів [5, 6].

Сучасні конволюційні нейронні мережі здатні ефективно виділяти локальні та глобальні ознаки зі складних візуальних даних [7], стійкі до шумів [8] і змінних

умов освітлення [9], що характерні для фотозображень. Адаптивні конвеєри обробки зображень [10], які враховують показники якості, такі як різкість, контраст, експозиційна збалансованість і рівень фонових завад, дозволяють оптимізувати процес тренування моделей, підвищуючи точність класифікації навіть при наявності спотворених або частково некоректних даних [11]. Поєднання базових архітектур CNN із модулями донавчання на очищених і сирих датасетах забезпечує більш гнучке узагальнення патернів [12] і зменшує вплив артефактів та шумів [13] на рішення моделі.

Важливим аспектом є модульна побудова системи [14], яка дозволяє інтегрувати попередню обробку зображень, навчальні контури, оцінку якості та прикладні інтерфейси для інтерактивного тестування [15]. Такий підхід відкриває можливості для впровадження нейромережових рішень, де потрібно автоматизовано оцінювати численні візуальні параметри [16, 17]. Подальший розвиток включає вдосконалення механізмів пояснюваності рішень моделей [18, 19], інтеграцію з мультимодальними даними [20], такими як відео та аудіо, а також створення адаптивних систем, що здатні навчатися на нових даних без повного перенавчання, що суттєво підвищує їхню практичну цінність [21].

Метою роботи є обґрунтування та реалізація підходу до проектування інтелектуальної системи класифікації побутового сміття за візуальними даними, у якій забезпечено інтеграцію якісно-обізнаного препроцесингу, нейромережової класифікації та прикладного інтерфейсу користувача в єдиний модульний контур. Об'єктом дослідження виступає процес автоматизованої класифікації побутових відходів за зображеннями, а предметом – архітектурні та алгоритмічні рішення, що забезпечують підвищення точності та стійкості класифікації за рахунок формалізованого контролю якості вхідних даних і раціональної побудови програмних компонентів.

Ключовою особливістю запропонованого підходу є трактування якості зображень не як допоміжного параметра, а як структурного елемента процесу навчання. На відміну від типових рішень, де препроцесинг обмежується нормалізацією розміру та базовими аугментаціями, у запропонованій системі передбачено формальну модель відбору зображень за вектором якості, що включає різкість, контрастність, експозиційну збалансованість та показник фонові «засміченості» сцени. Інтегральний бал якості, обчислений із використанням вагових коефіцієнтів, слугує основою для адаптивного порога фільтрації, який динамічно налаштовується на основі статистики датасету [22]. Це дає змогу вилучати зображення, що знижують внутрішньокласову однорідність і ускладнюють узагальнення моделі, зберігаючи при цьому репрезентативність кожного класу [23].

Архітектура системи (рисунок 1) побудована як сукупність узгоджених модулів: підсистема підготовки даних (імпорт, перевірка структури, обчислення метрик якості, формування очищеного датасету), тренувальний контур (донавчання базової нейромережової моделі на сирих та очищених даних із можливістю

порівняльних експериментів), модуль оцінювання (розрахунок сукупності метрик – accuracy, balanced accuracy, macro/micro F_1 , аналіз матриць плутанини) та прикладний інтерфейс для інтерактивного тестування. Така декомпозиція дозволяє незалежно модифікувати та повторно використовувати окремі компоненти, переносити систему на інші датасети та інтегрувати її у прототипи виробничих рішень.

У неймережевій частині системи застосовано трансферне навчання легковагових згорткових архітектур (зокрема MobileNetV2/EfficientNet) на основі відкритого датасету Recyclable and Household Waste Classification, який містить 30 класів відходів у контрольованих та реалістичних умовах зйомки. Доновчання виконується окремо на сирій та очищеній вибірках, що дає змогу кількісно оцінити вплив формалізованого відбору зображень на поведінку моделі, зокрема щодо рідкісних і візуально складних класів. Порівняння метрик на двох конфігураціях моделі дозволяє виявити класи, найчутливіші до шуму, та обґрунтувати доцільність інтеграції механізмів контролю якості в промислові конвеєри класифікації.

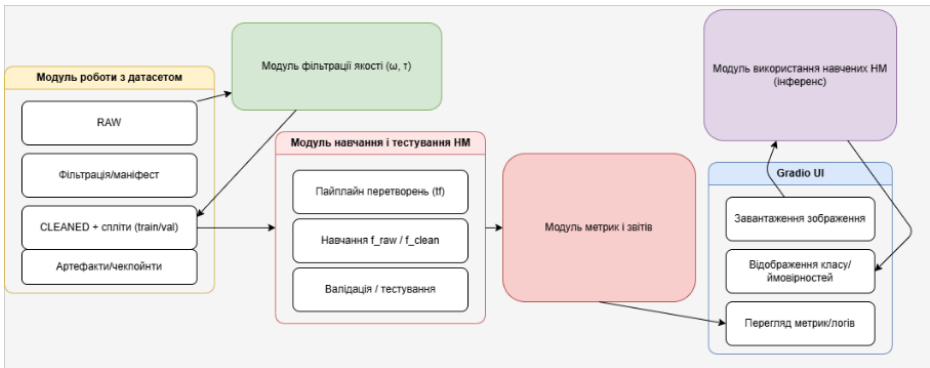


Рисунок 1 – Схема взаємодії компонентів інтелектуальної системи

Особливе значення в контексті проектування має вибір технологічного стека. Для реалізації обчислювальної частини застосовано Python з використанням бібліотек PyTorch, NumPy, Pandas, OpenCV та Matplotlib, що забезпечують повний цикл роботи з даними – від попередньої обробки зображень до навчання й оцінювання моделей. Середовище Google Colab використано як основну платформу для експериментів завдяки доступу до GPU, інтеграції з хмарним сховищем та можливості відтворення результатів. Для побудови інтерфейсу інтерактивного тестування впроваджено вебкомпонент на основі Gradio, який дає змогу не лише завантажувати зображення користувачем, а й візуально демонструвати результати класифікації у формі, придатній для подальшої інженерної інтеграції.

Експериментальні дослідження підтверджують, що врахування якості зображень на етапі формування вибірки дозволяє підвищити збалансовану точність

та macro-F1, зменшити систематичні помилки між близькими матеріальними класами та стабілізувати поведінку моделі для рідкісних категорій. З погляду проектування це означає, що інтелектуальна система класифікації побутового сміття має розглядатися не лише як «модель + інтерфейс», а як цілісний конвеєр, у якому модулі контролю якості даних, навчання та валідації взаємопов'язані й спільно визначають рівень надійності рішення в реальних виробничих сценаріях.

Перелік посилань

1. Global Waste Management Outlook / United Nations Environment Programme. United Nations Environment Programme, 2015. URL: <https://www.unccllearn.org/wp-content/uploads/library/unep23092015.pdf>
2. What a Waste 2.0: A Global Snapshot of Solid Waste Management to 2050 / S. Kaza et al. Washington, DC: World Bank, 2018. URL: <https://doi.org/10.1596/978-1-4648-1329-0>
3. Maalouf A., Mavropoulos A. Re-assessing global municipal solid waste generation. Waste Management & Research: The Journal for a Sustainable Circular Economy. 2022. P. 0734242X2210741.
4. Kok I.A., Kadynska V.D., Zalutska O.O., Mazurets O.V. Object-Oriented Intelligent System for Automated Control of Smoking by Video Data. Current scientific goals, approaches and challenges. Proceedings of IV International Scientific and Theoretical Conference. June 13, 2025. Dresden, Federal Republic of Germany. Pp. 156-164.
5. Bas I.S., Kadynska V.D., Klimenko V.I., Mazurets O.V. Convolutional Neural Network Transfer Learning Method for Aircraft Image Classification. Scientific method: reality and future trends of researching. Proceedings of VI International Scientific and Theoretical Conference. June 6, 2025. Montreal, Canada. Pp. 147-155.
6. Mushtyn O., Sobko O., Molchanova M., Mazurets O. Convolutional Neural Network Architecture for Image-Based Architectural Style Recognition. Evolving Science: Theories, Discoveries and Practical Outcomes. Proceedings of 4th International Scientific and Practical Conference. June 9-11, 2025. Zurich, Switzerland. Pp. 130-143.
7. Дідур В.О., Молчанова М.О., Мазурець О.В. Спосіб виявлення та класифікації залишків зруйнованих будівель та будівельного сміття за фотографіями з використанням моделей CNN. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №1 (42). С. 1162-1175.
8. Дидо Р.А., Мазурець О.В. Метод ідентифікації особистості на основі розпізнавання обличчя в реальному часі для систем кібербезпеки. Інформаційна, функційна і кібербезпека СКІФіК2024. Матеріали IV Всеукраїнської науково-технічної конференції. 29-30 листопада 2024. Харків. 2024. с. 36-37.
9. Похитун А.В., Мазурець О.В., Молчанова М.О., Бармак О.В. Підхід до формування датасету для нейромережевого виявлення модифікованих фотографій облич людей. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». 15-16 листопада 2024. Хмельницький, 2024. с. 428-433.
10. Мазурець О.В., Петровський С.С., Дидо Р.А. Нейромережева модель для ідентифікації особистості за зображенням обличчя у реальному часі Інформаційні технології і автоматизація. Матеріали XVII міжнародної науково-практичної конференції. 31 жовтня – 1 листопада 2024 р. Одеса, ОНТУ. 2024. С.655-658.
11. Мазурець О.В., Жарновський О.В., Гладун О.В., Собко О.В. Нейромережеве виявлення фейкових зображень людей. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2025. №5. Т.1. С. 416-422.

12. Молчанова М.О., Мазурець О.В., Шурипа М.О. Об'єктно-орієнтований підхід до нейромережевого виявлення та відстеження БПЛА з використанням хмарних технологій. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №9 (50). С. 1346-1360.
13. Мазур Є.В., Мазурець О.В., Кліменко В.І., Собко О.В., Залуцька О.О. Алгоритми та програмна архітектура інформаційної системи нейромережевого аналізу постави людини. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2025. №3. Т.1. С. 275-284.
14. Malaydakh V., Molchanova M., Shevchuk P., Mazurets O. Deep learning neural network architecture for determining sunflower growth stage from visual data. Modern Scientific Research: Theoretical and Practical Aspects. Proceedings II International Scientific and Practical Conference. May 26-28, 2025. Riga, Latvia. Pp. 143-148.
15. Мазурець О.В., Собко О.В., Дидо Р.А., Молчанова М.О., Тищенко О.О. Проектування структури бази даних для інтелектуальної системи нейромережевого виявлення та локалізації на фотозображеннях ділянок із залишками зруйнованих будівель. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №4 (45). С. 1242-1258.
16. Ostapchenko N., Tyschenko O., Denysenko B., Mazurets O. Semantic search of relevant images using vector databases. Modern Scientific Research: Theoretical and Practical Aspects. Proceedings II International Scientific and Practical Conference. May 26-28, 2025. Riga, Latvia. Pp. 161-165.
17. Dydo R., Sobko O., Klimenko V., Mazurets O. Datalogic structure for intelligent system for areas localization in photos with the remains of buildings using neural network. Modern Scientific Research: Theoretical and Practical Aspects. Proceedings II International Scientific and Practical Conference. May 26-28, 2025. Riga, Latvia. Pp. 123-127.
18. Молчанова М.О., Дідур В.О., Мазурець О.В., Тищенко О.О., Залуцька О.О. Інформаційна технологія використання хмарних обчислень для класифікації залишків зруйнованих будівель засобами нейронних мереж за візуальними даними з безпілотних літальних апаратів. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №4 (45). С. 1259-1272.
19. Didur V., Molchanova M., Mazurets O. Research on the effectiveness of neural network detection of plots with the destroyed buildings remains. Modern technologies and science: problems, new and relevant developments. Proceedings XXI International Scientific and Practical Conference. May 26, 2025. Zaragoza, Spain. Pp. 245-251.
20. Hladun O.V., Molchanova M.O., Zalutska O.O., Mazurets O.V. Effectiveness research of using ViT neural network architecture for classifying the destroyed buildings remains. Achievements of Science and Applied Research. Proceedings of 2nd International Scientific and Theoretical Conference. May 19-21, 2025. Dublin, Ireland. Pp. 96-100.
21. Собко О.В., Кліменко В.І., Мазурець О.В., Залуцька О.О., Гладун О.В. Особливості програмної інженерії та тестування програмного забезпечення для нейромережевого аналізу фотоданих залишків зруйнованих будівель із роботизованої техніки. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №4 (45). С. 1566-1581.
22. Hladun O., Zalutska O., Klimenko V., Mazurets O. Research on the effectiveness of classifying the remains of destroyed buildings using MobileNetV3 neural network architecture. Innovations in Science: From Theoretical Foundations to Practical Impact. Proceedings 1st International Scientific and Practical Conference. May 12-14, 2025. Antwerp, Belgium. Pp. 158-162.
23. Synchansky S. O. Bringing the legislation of Ukraine on hazardous waste management in line with the requirements of the European Union law. Uzhhorod National University Herald. Series: Law. 2025. Vol. 3, no. 86. P. 180–189.

УДК 004.8

Дидо Р.А., Собко О.В.

Хмельницький національний університет

МЕТОД ПОБУДОВИ АУДИОПОТОКУ ДОПОВНЕНОЇ РЕАЛЬНОСТІ ДЛЯ ПОКРАЩЕННЯ ОРІЄНТАЦІЇ ТА БЕЗПЕКИ ЛЮДЕЙ ІЗ ПРОБЛЕМАМИ ЗОРУ

Розглянуто метод побудови аудіопотоку доповненої реальності для покращення орієнтації та безпеки людей із проблемами зору. Метод ґрунтується на використанні моделі YOLOv8S для виявлення об'єктів у відеопотоці та згорткової нейронної мережі для класифікації названих осіб, що дає змогу забезпечити пріоритизоване озвучування небезпечних об'єктів та персоніфіковане інформування користувача в реальному часі. Розроблений програмний прототип продемонстрував високі показники точності під час експериментального дослідження, підтвердивши ефективність методу як інструменту підвищення автономності та безпеки людей із зоровими порушеннями.

The method for constructing an augmented reality audio stream to improve orientation and safety for people with vision problems is considered. The method is based on the use of the YOLOv8S model for detecting objects in a video stream and a convolutional neural network for classifying named individuals, which allows for prioritized voicing of dangerous objects and personalized user information in real time. The developed software prototype demonstrated high accuracy rates during experimental research, confirming the effectiveness of the method as a tool for increasing the autonomy and safety of people with visual impairments.

У дослідженні представлено науково обґрунтований метод побудови аудіопотоку доповненої реальності для покращення орієнтації та безпеки людей із проблемами зору шляхом аналізу відеопотоку в реальному часі та озвучування пріоритетної інформації про об'єкти довкілля й ідентифікованих осіб. Зростання глобальної кількості людей із порушеннями зору, складність самостійної навігації, недостатня адаптованість інфраструктури [1] та обмежені можливості існуючих цифрових асистивних технологій формують потребу у створенні інтегрованих систем, здатних синтезувати зорову інформацію у зручний аудіоформат [2, 3]. Такий підхід має особливе значення в умовах нестабільного чи небезпечного середовища, де швидкість та точність повідомлень впливають на безпеку користувача [4].

Зростання інтересу до технологій доповненої реальності у поєднанні з інтелектуальними системами аналізу даних відкриває нові можливості для підтримки людей із порушеннями зору [5]. Одним із перспективних напрямів є формування аудіопотоку доповненої реальності, у якому вербальні описи, попередження та контекстні підказки синтезуються на основі багаторівневої

обробки інформації про довкілля [6]. Розвиток технологій комп'ютерного зору відкриває нові можливості для створення систем доповненої реальності, орієнтованих на підтримку людей із порушеннями зору. Актуальність цієї тематики зумовлена потребою забезпечити безпечну та інформативну взаємодію таких користувачів з оточенням у режимі реального часу [7]. Комп'ютерний зір дозволяє автоматично аналізувати просторову структуру сцени, визначати ключові об'єкти, оцінювати їхню відстань, тип, поведінкові характеристики та потенційну небезпеку [8]. Для людей з порушеннями зору ці можливості є критично важливими, оскільки формують основу для побудови аудіопотоку доповненої реальності, який компенсує брак візуальної інформації.

Сучасні підходи, засновані на глибинному навчанні, забезпечують високу точність розпізнавання об'єктів [9], виявлення перешкод [10], семантичної сегментації [11] та відстеження рухомих елементів сцени [12]. Це дозволяє не лише описувати статичне оточення, а й розпізнавати динамічні ситуації, що особливо важливо для навігації у міському середовищі, громадських будівлях чи транспортних вузлах [13]. Отримані комп'ютерним зором дані можуть бути конвертовані у структуровані текстові описи, які далі трансформуються в аудіопідказки – від коротких попереджень до детальних інструкцій, залежно від рівня складності ситуації та індивідуальних потреб користувача.

Перспективи розвитку таких систем пов'язані з інтеграцією мультимодальних моделей [14], здатних одночасно обробляти відеопотоки [16], просторові карти оточення та контекстні дані [15], що дозволить генерувати ще точніші та релевантні мовні повідомлення [17]. Такі технології здатні суттєво підвищити рівень мобільності та безпеки людей із порушеннями зору, створюючи інтелектуальний аудіонавігаційний простір, що природно інтегрується у їхню повсякденну взаємодію із навколишнім світом.

Наукова новизна дослідження полягає у поєднанні пріоритизованої ідентифікації об'єктів та персоніфікованої класифікації осіб із подальшим перетворенням цієї інформації на аудіопотік доповненої реальності. Такий підхід забезпечує адаптивну взаємодію користувача із середовищем, розширює можливості асистивних технологій, а також створює умови для більшої автономності осіб із порушеннями зору. Розроблений метод сприяє реалізації Цілей сталого розвитку ООН №3, №10 та №11 [18], оскільки підтримує збереження здоров'я, зменшує соціальну нерівність і сприяє формуванню інклюзивних міських середовищ.

Практична значущість роботи полягає у створенні програмного прототипу, який доводить застосовність методу в реальному режимі. Такий підхід може бути інтегрований в мобільні застосунки, системи навігації та інклюзивні інформаційні сервіси.

Запропонований метод базується на використанні моделі YOLOv8S для виявлення об'єктів у відеопотоці та згорткової нейронної мережі для класифікації названих осіб. Його структурна організація охоплює попередню обробку

відеоданих, виявлення та фільтрацію об'єктів за порогом довіри, персоніфіковану ідентифікацію та формування аудіопотоку з урахуванням пріоритетності потенційно небезпечних об'єктів. Ключовою особливістю є встановлення динамічної ієрархії класів, що визначає порядок озвучування залежно від рівня загрози, яку конкретні об'єкти можуть створювати для користувача. Це дозволяє оперативно привертати увагу до факторів ризику, підтримуючи безпечну траєкторію руху. Додатково, можливість класифікації названих осіб забезпечує персоніфіковану взаємодію з оточенням, що є важливим як у повсякденних ситуаціях, так і в контексті соціальної інтеграції.

Експериментальні дослідження виконано на основі створеного програмного прототипу (рисунок 1), що включає підсистеми попередньої обробки відеопотоку, виявлення об'єктів, класифікації названих осіб, навчання моделей і користувацького інтерфейсу [19].

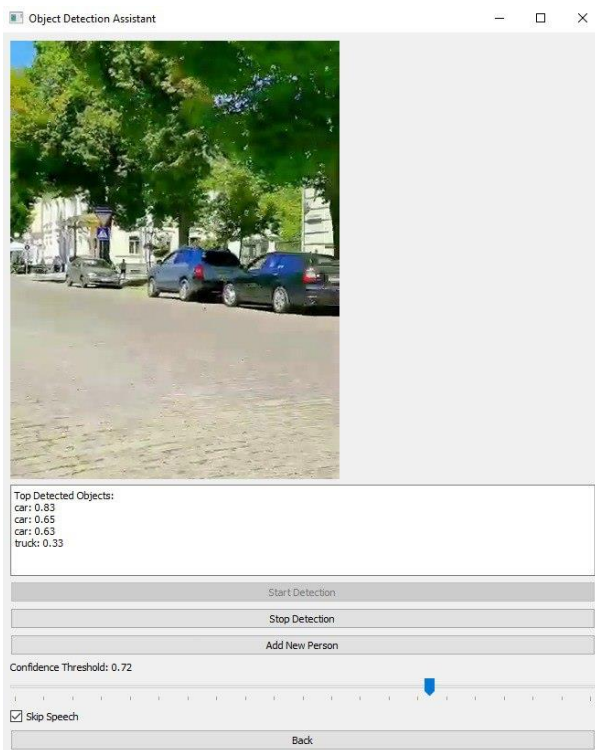


Рисунок 1 – Програмний прототип запропонованого методу

Отримані значення макропоказників для моделі YOLOv8S підтвердили її ефективність, зокрема Precision 0.77, Recall 0.62, mAP@0.5 0.73 та mAP@0.5:0.95

0.5604. Аналіз мікропоказників для об'єктів із підвищеним рівнем небезпеки засвідчив переважно високу точність моделі, хоча для окремих класів виявлено доцільність подальшого донавчання для підвищення стабільності. Водночас CNN-модель для класифікації названих осіб продемонструвала практично безпомилкову роботу, що підтверджують макропоказники Accuracy 0.97, Precision 0.98, Recall 0.97 та F_1 -score 0.98. Високі результати для класів «Person 1» та «Person 2» свідчать про надійність моделі, тоді як оптимізація вибірки для класу «Other» може підвищити повноту розпізнавання.

Подальший розвиток дослідження передбачає впровадження новітніх нейромережових архітектур, зокрема YOLO12, розширення та балансування датасетів для високопріоритетних класів, створення мобільного застосунку з адаптивною конфігурацією та розроблення підходів до динамічного контекстного аналізу середовища, що дозволить формувати більш точні й ситуативно релевантні аудіоповідомлення.

Отримані результати підтверджують ефективність запропонованого методу як перспективного рішення для систем підтримки безпеки та орієнтації осіб із порушеннями зору. Очікується, що запропонований метод створюватиме умови для безпечнішої інтеграції в соціальний простір, підвищуватиме якість життя користувачів і закладає основу для розвитку нових інтелектуальних асистивних технологій.

Перелік посилань

1. World Health Organization. Blindness and Visual Impairment. WHO. URL: <https://www.who.int/news-room/fact-sheets/detail/blindness-and-visual-impairment>
2. BBC News Ukraina. Yak suchasni tekhnolohii dopomahaiut liudiam z invalidnistiu. URL: https://www.bbc.com/ukrainian/science/2016/02/160202_tech_disability_ko
3. Omelchuk N., Dorohyi I. Intelligent System of Support for People with Visual Impairments. Scientific Papers of Donetsk National Technical University. Series: Computer Engineering and Automation. 2024. Pp. 4–17.
4. Dembitska S., Sievert I. Digital Accessibility in Education: Challenges and Prospects. Pedagogy of Security. 2024. Vol. 9, No. 2. Pp. 57–63.
5. Дидо Р.А., Мазурець О.В. Метод ідентифікації особистості на основі розпізнавання обличчя в реальному часі для систем кібербезпеки. Інформаційна, функційна і кібербезпека СКІФіК2024. Матеріали IV Всеукраїнської науково-технічної конференції. 29-30 листопада 2024. Харків. 2024. с. 36-37.
6. Kok I.A., Kadyńska V.D., Zalutka O.O., Mazurets O.V. Object-Oriented Intelligent System for Automated Control of Smoking by Video Data. Current scientific goals, approaches and challenges. Proceedings of IV International Scientific and Theoretical Conference. June 13, 2025. Dresden, Federal Republic of Germany. Pp. 156-164.
7. Hladun O., Zalutka O., Klimenko V., Mazurets O. Research on the effectiveness of classifying the remains of destroyed buildings using MobileNetV3 neural network architecture. Innovations in Science: From Theoretical Foundations to Practical Impact. Proceedings 1st International Scientific and Practical Conference. May 12-14, 2025. Antwerp, Belgium. Pp. 158-162.

8. Mushtyn O., Sobko O., Molchanova M., Mazurets O. Convolutional Neural Network Architecture for Image-Based Architectural Style Recognition. *Evolving Science: Theories, Discoveries and Practical Outcomes. Proceedings of 4th International Scientific and Practical Conference*. June 9-11, 2025. Zurich, Switzerland. Pp. 130-143.
9. Malaydakh V., Molchanova M., Shevchuk P., Mazurets O. Deep learning neural network architecture for determining sunflower growth stage from visual data. *Modern Scientific Research: Theoretical and Practical Aspects. Proceedings II International Scientific and Practical Conference*. May 26-28, 2025. Riga, Latvia. Pp. 143-148.
10. Didur V., Molchanova M., Mazurets O. Research on the effectiveness of neural network detection of plots with the destroyed buildings remains. *Modern technologies and science: problems, new and relevant developments. Proceedings XXI International Scientific and Practical Conference*. May 26, 2025. Zaragoza, Spain. Pp. 245-251.
11. Hladun O.V., Molchanova M.O., Zalutska O.O., Mazurets O.V. Effectiveness research of using ViT neural network architecture for classifying the destroyed buildings remains. *Achievements of Science and Applied Research. Proceedings of 2nd International Scientific and Theoretical Conference*. May 19-21, 2025. Dublin, Ireland. Pp. 96-100.
12. Kharysh I., Sobko O., Mazurets O. Designing CNN Neural Network Model for Detecting Fractures of Lower Extremities by X-ray Images. *The Impact of Scientific Research on the Development of the Modern World. Proceedings of the XLIV International scientific and practical conference*. October 23-25, 2024. Dubrovnik, Croatia. 2024. Pp. 91-96.
13. Zharnovskiy O., Mazurets O., Sobko O. Approach to Identification of Artificial Intelligence-Generated People Images by Means of Machine Learning. *Key Aspects of the Development of Scientific Research in Modern Conditions. Proceedings of the XLV International scientific and practical conference*. October 30 – November 1, 2024. Constanta, Romania. 2024. Pp. 69-73.
14. Mazurets O. V., Klimenko V. I., Molchanova M. O., Sultanov A. V. Object-Oriented Intelligent System for Neural Network Detection of Sugar Crystallization Zones. *Global Science: Prospects and Innovations. Proceedings of the 10th International scientific and practical conference*. Cognum Publishing House. Liverpool, United Kingdom. 2024. Pp. 198-207.
15. Pokhytun A., Mazurets O., Molchanova M., Tyschenko O. Method for Neural Network Detecting Changed Images of People's Faces Using CNN. *New Horizons in Scientific Research: Challenges and Solutions. Proceedings of the 1st International scientific and practical conference*. October 21-23, 2024. Marseille, France. 2024. Pp. 35-40.
16. Похитун А.В., Мазурець О.В., Дидо Р.А., Молчанова М.О. Програмна архітектура для нейромережевого виявлення модифікованих фотографій облич людей. *Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки*. Хмельницький, 2025. №3. Т.2. С. 493-500.
17. Dydo R., Sobko O., Klimenko V., Mazurets O. Datalogic structure for intelligent system for areas localization in photos with the remains of buildings using neural network. *Modern Scientific Research: Theoretical and Practical Aspects. Proceedings II International Scientific and Practical Conference*. May 26-28, 2025. Riga, Latvia. Pp. 123-127.
18. Gyimah P., Appiah K. O., Appiagyei K. Unraveling Contemporary Trends on United Nations Sustainable Development Goals: A New Global Bibliometric and Literature Review Analysis. *Sustainable Development*. 2025. Vol. 33, No. 2. Pp. 2579–2598.
19. Мазурець О.В., Собко О.В., Дидо Р.А., Молчанова М.О., Тищенко О.О. Проектування структури бази даних для інтелектуальної системи нейромережевого виявлення та локалізації на фотозображеннях ділянок із залишками зруйнованих будівель. *Науковий журнал «Наука і техніка сьогодні»*. Київ, 2025. №4 (45). С. 1242-1258.

УДК 004.891

Добрицький І.Д., Юрейко К.Ю., Міліція Б.М., Джулій В.М.

Хмельницький національний університет

МОДЕЛЬ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПОДАННЯ ПРЕДМЕТНОЇ ОБЛАСТІ

Модель інформаційного забезпечення предметної області призначена для управління процесами придбання та використання знань, що дозволяє враховувати корисності інформаційних елементів і дидактичні зв'язки між ними. Запропоновано спосіб формування інформаційного забезпечення, призначений для ієрархічного мережевого представлення предметної області, що дозволяє структурувати контент інформаційно-довідкових та інших систем, які відрізняються від відомих використанням взаємопов'язаних етапів відбору, кластеризації та впорядкування контенту.

The model of information support of the subject area is intended for management of processes of acquisition and use of knowledge, which allows to take into account the usefulness of information elements and didactic connections between them. A method of formation of information support is proposed, intended for hierarchical network representation of the subject area, which allows to structure the content of information and reference and other systems, which differ from the known ones by using interconnected stages of selection, clustering and ordering of content.

Якість інформаційного забезпечення можна розглядати в двох аспектах – зміст і структура. Остання, в свою чергу, включає в себе модель інформаційно-довідкового контенту і послідовність його застосування [1,2]. Зважаючи на великий обсяг доступних інформаційних ресурсів, актуальним стає питання розробки процедур, що дозволяють підвищити результативність засвоєння інформації, зокрема, за рахунок створення умов для найбільш успішного освоєння контенту предметної області за допомогою підвищення якості підготовки інформаційного забезпечення для технічних додатків в промислових системах.

Опис предметної області за допомогою лише мережевих або ієрархічних моделей не є достатнім для подання інформаційного забезпечення, тому запропонована для використання узагальнена ієрархічна мережева модель. Залежно від виду вхідних даних розглянемо можливі способи формування ієрархічних мережевих моделей інформаційного забезпечення [3,4,5].

В першому випадку вхідні дані представлені множиною інформаційних елементів, кількість яких порівняно невелика і є припустимою для застосування

експертних методів. Сукупність етапів побудови ієрархічної мережевої моделі приведено на рисунку 1.

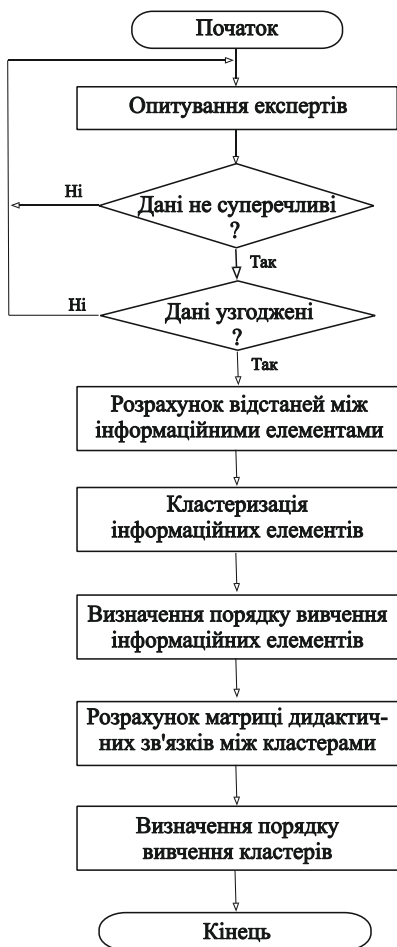


Рисунок 1 – Алгоритм побудови ієрархічної мережевої дворівневої моделі інформаційного забезпечення

В другому варіанті вхідні дані представлені «деревом знань», тобто, ієрархічною моделлю інформаційного забезпечення. Сукупність етапів побудови ієрархічної мережевої моделі наведена на рисунку 2. Визначення структури інформаційного забезпечення та порядку засвоєння знань предметної області представлена на рисунку 3, де W – матриця ваг дидактичних зв'язків між

інформаційними елементами (ІЕ), D – матриця відстаней між ІЕ, R – порядок вивчення ІЕ, C_L – кластери інформаційних елементів, що є інформаційними фрагментами (ІФ), W_L – матриця ваг дидактичних зв'язків між кластерами на рівні L , r_{if} – порядок вивчення ІФ.

Процедура визначення структури інформаційного забезпечення складається з наступних кроків: визначення близькості між ІЕ; кластеризація усієї множини відібраних навчальних елементів (формування ІФ); визначення дидактичних зв'язків між ІФ та формування структури контенту верхнього рівня; впорядкування ІЕ всередині кластерів; визначення близькості між кластерами; впорядкування кластерів.

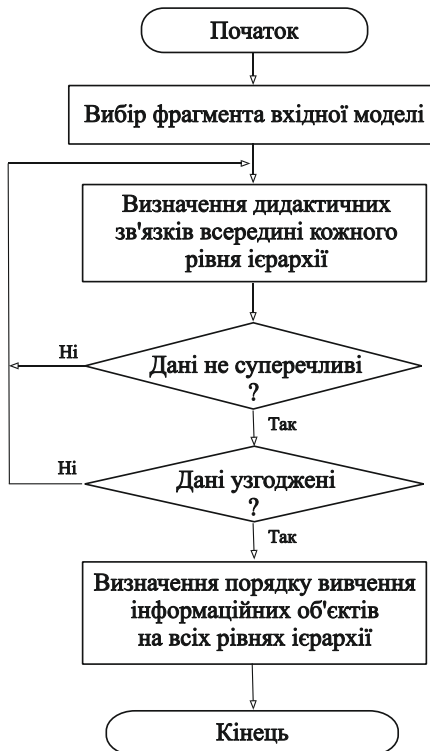


Рисунок 2 – Алгоритм побудови ієрархічної мережевої моделі

На основі отриманої ієрархічної мережевої моделі інформаційного забезпечення, необхідно сформуванати траєкторію роботи з об'єктами предметної області (ІФ та ІЕ). На кожному з ієрархічних рівнів, визначається лінійний порядок

їх застосування або вивчення. На кожному з рівнів модель дидактичних зв'язків між ІФ (ІЕ) представлена квадратною матрицею W_L . Для вирішення задачі формування траєкторії роботи з інформаційними об'єктами предметної області можуть застосовуватися алгоритми побудови ярусно-паралельної форми графу, зокрема, алгоритми топологічної сортування. Задача топологічного сортування графу полягає в наступному: вказати такий лінійний порядок на його вершинах, щоб будь-яке ребро було спрямоване від вершини з меншим номером до вершини з більшим номером. Очевидно, якщо в графі є цикли, то такого порядку не існує.

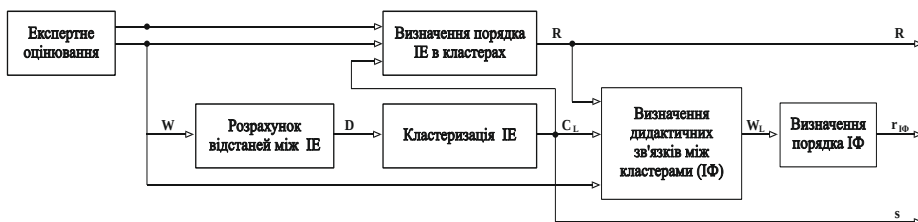


Рисунок 3 – Визначення структури та порядку освоєння знань предметної області

Якщо при вирішенні задачі визначення траєкторії засвоєння матеріалу необхідно розглянути всі ІЕ з деякої предметної області, то задача може бути сформульована як варіант задачі комівояжера. В даному випадку задача комівояжера є асиметричною, оскільки моделюється орієнтованою граф-структурою, яка є незамкненою, тому що повертатися до стартової вершини не вимагається. При цьому "критерій вигідності маршруту" відображає логічність (тобто, дидактичну впорядкованість) розгляду матеріалу, сприяючи кращому його сприйняттю яке можна трактувати відповідно до семантичної теорії інформації Шрейдера. Для успішного засвоєння деякого ІЕ потрібно вивчити всі ІЕ, від яких в моделі дидактичних зв'язків є дуги до поточного ІЕ. Порушення цієї умови призводить до погіршення характеристик розглянутого маршруту, тобто до зменшення значення цільової функції, що характеризує траєкторію засвоєння матеріалу.

Одним з етапів побудови ієрархічної мережевої моделі інформаційного забезпечення є відбір інформаційних елементів, які забезпечують формування заявлених цілей інформаційного забезпечення. залежно від виду вхідних даних запропоновано два можливі способи формування ієрархічних мережевих моделей інформаційного забезпечення [3, 4].

Для вхідних даних, представлених множиною інформаційних елементів, кількість яких порівняно невелика і є придатною для застосування експертних методів, запропонований алгоритм побудови ієрархічної мережевої дворівневої

моделі інформаційного забезпечення [4,5]. Експертним шляхом встановлюються дидактичні зв'язки між ІЕ, що відображають відношення парної впорядкованості при розгляді (застосуванні) ІЕ. Виконуються перевірки на несуперечливість та узгодженість (якщо експертів було декілька). В результаті формується мережева модель інформаційного забезпечення. Якщо експертами застосовувалися не бінарні оцінки парної дидактичної впорядкованості, то формується зважена мережева модель інформаційного забезпечення.

Для досягнення цілей інформаційного забезпечення запропоновано шляхи підвищення ефективності набуття знань, зокрема, за допомогою аналізу і синтезу структури інформаційного забезпечення та визначення послідовності інформаційних об'єктів предметної області. Також запропонований підхід визначення такої траєкторії освоєння матеріалу, яка безпосередньо сприяє досягненню мети інформаційного забезпечення на основі вже наявних знань.

Отримані результати можуть бути використані для підтримки прийняття рішень при придбанні та застосуванні знань, а саме: при створенні інформаційного забезпечення виробничих процесів, в частині розробки елементів методичного забезпечення інформаційних систем, в корпоративних системах навчання персоналу; при розробці програм окремих курсів підвищення кваліфікації; при розробці та наступним коригуванням навчальних планів; формуванні навчальних, довідкових матеріалів, курсів лекцій для окремих дисциплін.

Перелік посилань

1. Приймак В. Управління знаннями: підручник. К.: Київський національний університет імені Тараса Шевченка, 2019. 240с..
2. Остроухов В.В. Інформаційна безпека: підручник. К.: Ліра-К, 2021. 412 с.
3. Литвин В.В., Басюк Т.М. Машинне навчання. Львів:Новий світ, 2025.315 с.
4. Шаховська Н. Б., Кунанець Н. Е. Сховища та простори даних. Книга 2: Простори даних : підручник. Львів : «Новий Світ-2000», 2025. 360 с.
5. Джулій В.М., Солодєєва Л.В., Мірошніченко О.В. Метод класифікації додатків інтернет - трафіка комп'ютерних мереж в умовах невизначеності. Збірник наукових праць ВІКНУ ім. Т. Шевченка. 2022. №74. С. 73-82.

УДК 004

Жураковська Д.О.

Кам'янський енергетичний фаховий коледж

ЗАСТОСУВАННЯ АЛГОРИТМУ ISOLATION FOREST ДЛЯ ПОБУДОВИ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ В ІОТ-МЕРЕЖІ

У статті досліджується проблема забезпечення безпеки мереж Інтернету Речей (IoT). Проаналізовано основні загрози, властиві IoT-мережам, такі як низька обчислювальна потужність пристроїв, різноманітність протоколів та масштабованість атак. Запропоновано підхід до виявлення аномалій на основі алгоритму ізоляційного лісу (Isolation Forest). Метою роботи є підвищення точності та швидкості виявлення невірогідних подій у мережевому трафіку IoT порівняно з традиційними сигнатурними методами. Проведено експеримент на публічно доступному наборі даних IoT-23, який показав зменшення часу аналізу на 15% та досягнення метрики F1-score на рівні 0.94. Результати вказують на перспективність використання запропонованого методу для побудови адаптивних систем захисту.

The article investigates the problem of security in Internet of Things (IoT) networks. The main threats inherent to IoT networks are analyzed, such as low device computational power, protocol diversity, and attack scalability. An approach for anomaly detection based on the Isolation Forest algorithm is proposed. The goal of the work is to increase the accuracy and speed of detecting malicious events in IoT network traffic compared to traditional signature-based methods. An experiment was conducted on the publicly available IoT-23 dataset, which showed a 15% reduction in analysis time and achieved an F1-score of 0.94. The results indicate the promise of using the proposed method for building adaptive security systems.

Стрімке зростання кількості пристроїв Інтернету Речей (IoT) у всіх сферах життя призводить до появи нових векторів кібератак. Традиційні системи захисту, такі як мережеві екрани та системи виявлення вторгнень (IDS), що базуються на сигнатурах, неефективні проти нових, невідомих атак та адаптивних загроз. Це створює нагальну потребу в розробці інтелектуальних систем, здатних виявляти аномальну поведінку в реальному часі.

Питання безпеки IoT досліджували такі вчені, як [1, 2]. У роботі [1] для виявлення атак використовується метод опорних векторів (SVM), але його обчислювальна складність є перешкодою для реального часу. Дослідження [2] пропонує використання кластеризації для виявлення відхилень, однак цей метод може бути чутливим до шуму в даних. Незважаючи на існуючі роботи, залишається невирішеною проблема створення легкого та ефективного механізму виявлення аномалій, адаптованого саме для специфіки IoT-трафіку, який характеризується великою кількістю дрібних пакетів та періодичністю.

Метою даної роботи є розробка та експериментальна перевірка моделі виявлення аномальної мережевої активності в IoT-мережах на основі алгоритму машинного навчання без учителя, спрямованої на підвищення точності та швидкодії порівняно з базовими підходами.

В якості основного алгоритму було обрано ізоляційний ліс (Isolation Forest) [3]. Його перевагою є здатність ефективно виявляти аномалії в даних з високою розмірністю при невеликих обчислювальних витратах, що критично важливо для обмежених ресурсів IoT-середовищ. Для експерименту було використано набір даних IoT-23, що містить як легітимний трафік, так і трафік, згенерований різними бот-мережами.

На етапі підготовки даних було виокремлено ключові ознаки мережевого трафіку: тривалість сесії, кількість відправлених/отриманих пакетів, середній розмір пакета, використання нестандартних портів. Після цього дані були нормалізовані. Модель була навчена на безетикеткових даних, що імітує реальні умови, де мітки "нормальний/аномальний" зазвичай відсутні.

Результати експерименту показали, що запропонована модель досягла метрики F1-score 0.94, що на 7% вище, ніж у традиційного методу k-NN, використаного для порівняння. Час класифікації одного запису склав у середньому 0.8 мс. Отримані результати підтверджують ефективність обраного підходу для швидкого та точного виявлення аномалій.

В рамках даного дослідження було розроблено модель виявлення аномалій для IoT-мереж на основі алгоритму Isolation Forest. Експериментально доведено, що запропонований підхід забезпечує високу точність (F1-score = 0.94) та низький час відгуку, що робить його придатним для використання в системах реального часу. Перспективою подальших досліджень є вдосконалення моделі шляхом додавання механізмів напівконтрольованого навчання для адаптації до мінливих умов мережі та інтеграція запропонованого рішення в архітектуру програмно-визначених мереж (SDN) для централізованого керування безпекою.

Перелік посилань

1. Smith J., Doe A. IoT Network Security Using SVM-Based Intrusion Detection // IEEE Access. – 2022. – Vol. 10. – P. 12345-12356.
2. Kowalski M., Nowak T. Unsupervised Clustering for Anomaly Detection in Smart Home IoT Systems // Proc. of International Conference on Computer Science. – 2023. – P. 234-241.
3. Liu F. T., Ting K. M., Zhou Z. H. Isolation Forest // 2008 Eighth IEEE International Conference on Data Mining. – 2008. – P. 413–422.
4. IoT-23 Dataset: A labeled dataset with malicious and benign IoT network traffic. [Електронний ресурс]. – Режим доступу: <https://www.stratosphereips.org/datasets-iot23>.

УДК 004.8

Загурський Б.З., Манзюк Е.А., Скрипник Т.К.

Хмельницький національний університет

МЕТОД АНАЛІЗУ ТОНАЛЬНОСТІ ВІДГУКІВ КЛІЄНТІВ З ВИКОРИСТАННЯМ ГІБРИДНОЇ МОДЕЛІ МАШИННОГО НАВЧАННЯ

Розглянуто метод автоматизованого аналізу тональності відгуків клієнтів з використанням гібридної моделі, що поєднує метод опорних векторів та нейронну мережу. Запропонована архітектура враховує контекст слів через аналіз біграм та забезпечує точність класифікації 81.5% при обробці позитивних, негативних та нейтральних відгуків.

A method for automated sentiment analysis of customer reviews using a hybrid model combining support vector machines and neural networks is considered. The proposed architecture accounts for word context through bigram analysis and achieves classification accuracy of 81.5% when processing positive, negative, and neutral reviews.

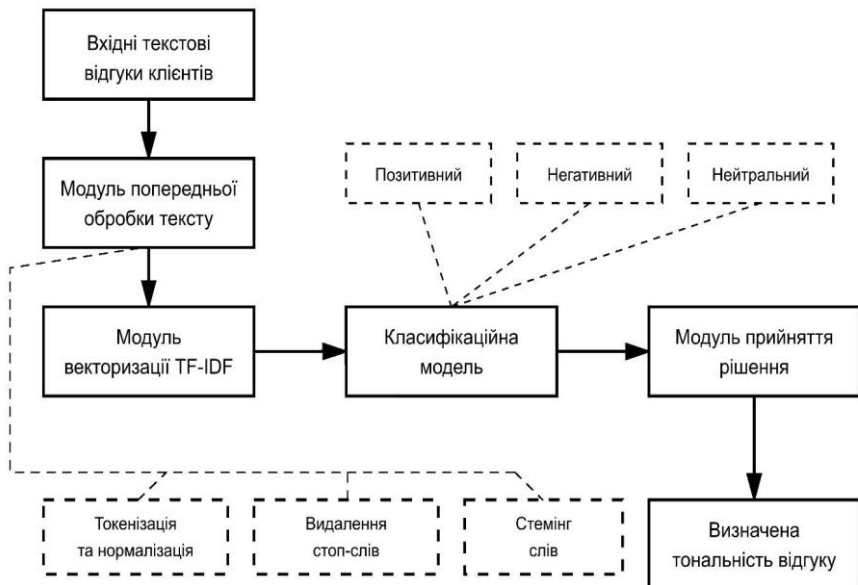
Аналіз тональності відгуків клієнтів є актуальною задачею для бізнесу, який прагне зрозуміти ставлення споживачів до своїх продуктів та послуг [1-3]. Відгуки клієнтів містять цінну інформацію про сильні та слабкі сторони продукту, проте їх ручна обробка стає неможливою при великих обсягах даних. Автоматизація цього процесу за допомогою машинного навчання дозволяє швидко та ефективно обробляти тисячі відгуків, виявляючи загальні тенденції у думках споживачів. Сучасні дослідження в області штучного інтелекту демонструють ефективність пояснюваних підходів до аналізу складних даних [4-6], методів візуальної аналітики для розробки моделей [7-9] та інтеграції контекстних дескрипторів для збагачення семантичних зв'язків [10-12]. Адаптивні методи машинного навчання успішно застосовуються для розпізнавання патернів у різних предметних областях [13-15], включаючи медичну діагностику та оптимізацію процесів прийняття рішень [16-18]. Зокрема, підходи до кластерного аналізу та розпізнавання високоточних патернів [19-21] показують можливості для покращення якості класифікації текстових даних, а багатофакторний аналіз поведінкових ознак [22] демонструє ефективність методів обробки природної мови для вирішення задач класифікації тональності.

Метою роботи є розробка методу автоматизованого аналізу тональності відгуків, який забезпечує точну класифікацію емоційного забарвлення тексту з

урахуванням контекстних особливостей мови та здатний розрізняти позитивні, негативні та нейтральні висловлювання.

Розроблений метод базується на припущенні, що емоційне забарвлення тексту можна визначити через аналіз закономірностей у словах та їх комбінаціях. Основна ідея полягає у навчанні моделі розпізнавати характерні ознаки кожного класу тональності на основі набору попередньо розмічених відгуків. Метод вирішує задачу тризначної класифікації, де відгуки поділяються на позитивні, негативні та нейтральні.

Метод складається з чотирьох послідовних етапів обробки інформації, показаних на рисунку 1. Перший етап включає збір та попередню обробку текстових даних, де виконується очищення тексту від непотрібних символів, приведення до нижнього регістру, видалення стоп-слів та токенизація. Другий етап здійснює перетворення оброблених текстових даних у числове векторне представлення за допомогою методу TF-IDF з додаванням аналізу біграм для врахування контексту слів. Третій етап передбачає навчання гібридної класифікаційної моделі на підготовлених векторних представленнях. Четвертий етап застосовує навчену модель для класифікації нових відгуків з визначенням ймовірності належності до кожного класу тональності.



Рисунк 1 – Загальна схема методу аналізу тональності

Вхідні дані надходять у вигляді необроблених текстових відгуків клієнтів різної довжини та структури. Відгуки можуть варіюватися від коротких оцінок з декількох слів до розгорнутих текстів з детальним описом досвіду використання продукту. Ці відгуки проходять через модуль попередньої обробки, де виконується послідовність трансформацій для приведення тексту до стандартизованого вигляду. Після попередньої обробки дані потрапляють у модуль векторизації, де текст перетворюється на числові вектори з використанням статистичних характеристик слів та їх комбінацій.

Важливою особливістю методу є його модульність, де кожен етап обробки може бути модифікований або замінений без суттєвих змін в інших частинах системи. Така архітектура забезпечує гнучкість та можливість подальшого вдосконалення через інтеграцію нових алгоритмів векторизації або класифікації. Метод розроблявся з урахуванням балансу між точністю класифікації та швидкістю обробки, намагаючись знайти оптимальне співвідношення для практичного застосування у системах реального часу.

Якість роботи моделі машинного навчання критично залежить від якості підготовки вхідних даних. Для навчання використовується датасет з платформи Kaggle, який містить приблизно п'ять тисяч відгуків клієнтів з відповідними мітками тональності. Структура датасету включає три основні поля: унікальний ідентифікатор відгуку для відстеження записів, власне текст відгуку змінної довжини та мітку тональності, яка приймає одне з трьох значень: позитивна, негативна або нейтральна. Розподіл класів у датасеті є відносно збалансованим, що забезпечує рівномірне навчання моделі на всіх типах тональності.

Попередня обробка текстових даних виконується через п'ять послідовних етапів трансформації, кожен з яких спрямований на покращення якості представлення тексту. Перший етап полягає в приведенні всього тексту до нижнього регістру, що забезпечує однакову обробку слів незалежно від їх написання. Без цього кроку модель розглядала б варіанти "Добре", "добре" та "ДОБРЕ" як три різні слова, що призводило б до надмірного збільшення словника та розпорошення статистичної інформації про важливі терміни.

Параметри векторизації налаштовані експериментально для досягнення оптимального балансу між повнотою представлення та обчислювальною ефективністю. Максимальний розмір словника встановлено на рівні трьох тисяч найбільш частотних термінів, що забезпечує охоплення основної лексики відгуків без надмірного збільшення розмірності векторів. Мінімальна частота появи терміну для включення до словника дорівнює двом, що означає фільтрацію дуже рідкісних слів, які можуть бути опечатками або специфічними термінами. Максимальна

частота обмежена на рівні вісімдесяти відсотків для виключення надто частих слів, які з'являються майже в кожному документі та не несуть дискримінативної інформації для класифікації.

Після векторизації кожен відгук представлений у вигляді розрідженого вектора розмірністю три тисячі, де кожен елемент відповідає TF-IDF значенню відповідного терміну у словнику. Більшість елементів цього вектора дорівнюють нулю, оскільки конкретний відгук містить лише невелику частину всього словника. Використання розрідженого представлення дозволяє ефективно зберігати та обробляти такі вектори без витрат пам'яті на зберігання нульових значень.

Підготовлений датасет розділяється на три частини з використанням стратифікованого підходу. Навчальна вибірка містить сімдесят відсотків всіх даних і використовується безпосередньо для навчання моделі на виявлення закономірностей тональності. Валідаційна вибірка становить п'ятнадцять відсотків даних і використовується для підбору гіперпараметрів та контролю перенавчання під час тренування моделі. Тестова вибірка з решти п'ятнадцяти відсотків використовується для фінальної оцінки якості моделі на даних, які вона ніколи не бачила під час навчання. Розподіл виконується випадковим чином з фіксованим seed для забезпечення відтворюваності результатів, при цьому зберігається пропорція класів у кожній вибірці для коректного навчання та оцінювання.

Для вирішення задачі аналізу тональності обрано гібридний підхід, що поєднує традиційні методи машинного навчання з елементами глибокого навчання. Архітектура складається з декількох послідовно та паралельно з'єднаних компонентів, кожен з яких виконує специфічну функцію в процесі класифікації та компенсує обмеження інших компонентів.

Базова архітектура гібридної моделі показала прийнятні результати на тестових даних, проте аналіз помилок класифікації виявив можливості для покращення. Основна проблема полягає в недостатньо точній класифікації нейтральних відгуків, які часто помилково відносяться до позитивного або негативного класу через нездатність моделі врахувати контекст слів. Стандартна TF-IDF векторизація враховує лише частоту появи слів у документі та їх рідкість у всьому корпусі, але не враховує контекст та взаємозв'язки між сусідніми словами.

Запропонована модифікація спрямована на покращення обробки ознак через введення додаткового етапу аналізу біграм перед основною векторизацією. Біграми являють собою послідовності з двох сусідніх слів у тексті, які дозволяють частково захопити контекст та взаємозв'язки між термінами. Врахування біграм особливо важливе для розпізнавання заперечних конструкцій та модифікаторів, які кардинально змінюють значення слів. Наприклад, словосполучення "не добре" та "дуже добре" містять слово "добре", але мають протилежну або посилену

тональність відповідно. Використання біграм допомагає моделі правильно інтерпретувати такі конструкції.

Отже, розроблено метод автоматизованого аналізу тональності відгуків клієнтів, який поєднує гібридну архітектуру на основі методу опорних векторів та нейронної мережі з розширеним векторним представленням через аналіз біграм. Метод забезпечує точну класифікацію емоційного забарвлення текстів через врахування контекстних особливостей мови та взаємозв'язків між словами.

Запропонована гібридна архітектура використовує переваги обох підходів до класифікації, де метод опорних векторів забезпечує ефективну роботу з високорозмірними даними та побудову оптимальної розділяючої гіперплощини, а нейронна мережа виявляє складні нелінійні залежності в даних та забезпечує точність класифікації 81.5% при обробці позитивних, негативних та нейтральних відгуків. Комбінація передбачень через зважене об'єднання результатів дозволяє компенсувати слабкості кожного окремого класифікатора та підвищити загальну стабільність і точність передбачень.

Перелік посилань

1. Kung H. Were You Helpful – Predicting Helpful Votes from Amazon Reviews. arXiv preprint arXiv:2412.02884. DOI: 10.48550/arXiv.2412.02884. URL: <https://arxiv.org/abs/2412.02884>.
2. Kumar S., Roy P. P., Dogra D. P., Kim B.-G. A Comprehensive Review on Sentiment Analysis: Tasks, Approaches and Applications. arXiv preprint arXiv:2311.11250. DOI: 10.48550/arXiv.2311.11250. URL: <https://arxiv.org/abs/2311.11250>.
3. Guo X. Sentiment Analysis Based on RoBERTa for Amazon Review: An Empirical Study on Decision Making. arXiv preprint arXiv:2411.00796. DOI: 10.48550/arXiv.2411.00796. URL: <https://arxiv.org/abs/2411.00796>.
4. Barmak O., Krak I., Yakovlev S., Manziuk E., Radiuk P., Kuznetsov V. Toward explainable deep learning in healthcare through transition matrix and user-friendly features // *Frontiers in Artificial Intelligence*. — 2024. — Vol. 7. — Pp. 1482141. — URL: <https://doi.org/10.3389/frai.2024.1482141>.
5. Chaban O., Manziuk E., Markevych O., Petrovskiy S., Radiuk P. EMTKD at the edge: An adaptive multi-teacher knowledge distillation for robust cardiac MRI classification // *CEUR Workshop Proceedings*. — 2025. — Pp. 42–57.
6. Chaban O., Manziuk E. Enhancing medical NLI with integrated domain knowledge and sentiment analysis // *CEUR Workshop Proceedings*. — 2024. — Vol. 3790. — Pp. 262–272.
7. Krak I., Barmak O., Manziuk E. Using visual analytics to develop human and machine-centric models: A review of approaches and proposed information technology // *Computational Intelligence*. — 2022. — Vol. 38, No. 3. — Pp. 921–946. — URL: <https://doi.org/10.1111/coin.12289>.
8. Krak I., Zalutskaya O., Molchanova M., Mazurets O., Manziuk E., Barmak O. Method for neural network detecting propaganda techniques by markers with visual analytic // *CEUR Workshop Proceedings*. — 2024. — Vol. 3790. — Pp. 158–170.
9. Manziuk E., Barmak O., Krak I., Petliak N., Jin Z., Radiuk P. Explainable Deep Learning for Interpretable Brain Tumor Diagnosis from MRI Images // *Lecture Notes on Data Engineering and Communications Technologies*. — Cham : Springer Nature Switzerland, 2024. — Pp. 326–348. — URL: https://doi.org/10.1007/978-3-031-70959-3_17.

10. Manziuk E., Barmak O., Radiuk P., Kuznetsov V., Krak I. Representation of Trustworthiness Components in AI Systems: A Formalized Approach Considering Interconnections and Overlap // CEUR Workshop Proceedings. — 2024. — Vol. 3777. — Pp. 405–417.
11. Manziuk E., Barmak O., Radiuk P., Kuznetsov V., Krak I., Yakovlev S. Integration of Contextual Descriptors in Ontology Alignment for Enrichment of Semantic Correspondence // 2024 14th International Conference on Dependable Systems, Services and Technologies (DESSERT), October 2024. — Pp. 1–7. — URL: <https://doi.org/10.1109/DESSERT65323.2024.11122179>.
12. Manziuk E., Krak I., Barmak O., Mazurets O., Kuznetsov V., Pylypiak O. Structural alignment method of conceptual categories of ontology and formalized domain // CEUR Workshop Proceedings. — 2021. — Vol. 3003. — Pp. 11–22.
13. Pavlyshyn V., Manziuk E., Barmak O., Krak I., Daamasevicius R. Modeling environment intelligent transport system for eco-friendly urban mobility // CEUR Workshop Proceedings. — 2024. — Vol. 3675. — Pp. 118–136. — URL: <https://ceur-ws.org/Vol-3675/paper9.pdf>.
14. Radiuk P., Barmak O., Manziuk E., Krak I. Explainable Deep Learning: A Visual Analytics Approach with Transition Matrices // Mathematics. — 2024. — Vol. 12, No. 7. — Pp. 1–32. — URL: <https://doi.org/10.3390/math12071024>.
15. Radiuk P., Barmak O., Manziuk E., Krak I. Explainable Artificial Intelligence: Transitioning DL Model Decisions to User-Understandable Features in Healthcare // Proceedings of the 4th International Workshop of IT-professionals on Artificial Intelligence (ProFIT AI 2024), Cambridge, MA, USA, September 25, 2024. — CEUR Workshop Proceedings. — 2024. — Vol. 3777. — Pp. 185–199. — URL: <https://ceur-ws.org/Vol-3777/paper12.pdf>.
16. Radiuk P., Kovalchuk O., Slobodzian V., Manziuk E., Barmak O., Krak I. Human-in-the-Loop Approach Based on MRI and ECG for Healthcare Diagnosis // CEUR Workshop Proceedings. — 2022. — Vol. 3302. — Pp. 9–20.
17. Ryzhanskyi O., Manziuk E., Barmak O., Krak I., Bačanin N. An Approach to Optimizing CO2 Emissions in Traffic Control via Reinforcement Learning // CEUR Workshop Proceedings. — 2024. — Vol. 3675. — Pp. 137–155. — URL: <https://ceur-ws.org/Vol-3675/paper10.pdf>.
18. Ryzhanskyi O., Pavlyshyn V., Radiuk P., Manziuk E., Barmak O., Krak I. AI-Driven Traffic Signal Control System to Reduce CO2 Emissions // CEUR Workshop Proceedings. — 2025. — Vol. 3974. — Pp. 18–27. — URL: <https://ceur-ws.org/Vol-3974/paper02.pdf>.
19. Pavlyshyn V., Ryzhanskyi O., Manziuk E., Radiuk P., Barmak O., Krak I. Establishing Patterns of the Urban Transport Flows on Clustering Analysis // Proceedings of the Second International Conference of Young Scientists on Artificial Intelligence for Sustainable Development (YAISD 2025). — 2025. — Vol. 3974. — Pp. 1–9. — URL: <https://ceur-ws.org/Vol-3974/paper01.pdf>.
20. Pavlyshyn V., Manziuk E., Barmak O., Radiuk P., Krak I. An Adaptive Machine Learning Approach to Sustainable Traffic Planning: High-Fidelity Pattern Recognition in Smart Transportation Systems // Future Transportation. — 2025. — Vol. 5, No. 4. — URL: <https://doi.org/10.3390/futuretransp5040152>.
21. Pavlyshyn V., Manziuk E., Barmak O., Radiuk P., Krak I. Adaptive Cascade Clustering for High-Fidelity Urban Traffic Pattern Recognition // Computer Science and Mathematics. — 2025. — Preprint. — URL: <https://doi.org/10.20944/preprints202508.0637.v1>.
22. Manziuk E. A., Sobko O. V., Podhorniuk I. O., Molchanova M. O., Mazurets O. V. Multifactorial analysis of mobbing behavioral signs in educational environments posts by NLP means // Journal of Physics: Conference Series. — 2025. — Vol. 3105, No. 1. — Pp. 012025. — URL: <https://doi.org/10.1088/1742-6596/3105/1/012025>.

УДК 534.843:004.9

Задорожний М.О., Крак Ю.В.

Київський національний університет імені Тараса Шевченка

ПІДВИЩЕННЯ ГЕНЕРАЛІЗАЦІЇ МОДЕЛІ РОЗПІЗНАВАННЯ ДАКТИЛЕМ УКРАЇНСЬКОЇ ЖЕСТОВОЇ МОВИ В УМОВАХ ОБМЕЖЕНИХ ДАНИХ

Розглянуто підхід до підвищення генералізації моделей глибокого навчання при розпізнаванні дактилем української жестової мови за умов обмеженої кількості даних. Запропоновано використання архітектури X3D-M, попередньо навченої на масштабних відеодатасетах, що забезпечує стабільність розпізнавання та зменшує ризик перенавчання. Експерименти показали точність класифікації до 91% F1-score при значній стійкості моделі до варіацій фону та положень руки.

An approach to improving the generalization capability of deep learning models for Ukrainian sign language fingerspelling recognition under limited data conditions is presented. The use of the X3D-M architecture pre-trained on large-scale video datasets is proposed, providing stable recognition and reduced overfitting. Experiments demonstrated classification quality up to 91% F1-score and significant robustness to variations in background and hand position.

Актуальність автоматичного розпізнавання української жестової мови (УЖМ) зумовлена потребою забезпечення рівного доступу до інформації та комунікації для людей із порушеннями слуху, які щоденно стикаються з бар'єрами у взаємодії з чуючими людьми та цифровими сервісами. В Україні тисячі нечуючих громадян використовують жестову мову як основний засіб спілкування, проте через відсутність стандартних технологічних рішень ефективна комунікація з оточуючими часто ускладнена. Розробка систем автоматичного розпізнавання УЖМ дозволяє перекладати жести у текст або мовлення в реальному часі, відкриваючи нові можливості для освіти, медіа, державного обслуговування та соціальної взаємодії.

Автоматичне розпізнавання жестів є складною задачею через значну варіативність положень і рухів руки, а також змінність умов освітлення та фону. Попередні підходи, що базувалися на класичних методах комп'ютерного зору (HOG[1], «мішок ознак»[2], розділення гіперплощинами[3]), виявилися надто чутливими до змін середовища.

Використання згорткових нейромереж значно підвищує стійкість до зовнішніх факторів, проте потребує масштабних навчальних вибірок. Для української жестової мови відчувається значний дефіцит датасетів, а тому більшість наявних моделей навчені на недостатньо репрезентативних вибірках та

демонструють ефективність лише в контрольованих умовах, втрачаючи точність при роботі з реальними відео.

Тому метою даної роботи є розробка легкої моделі глибокого навчання для розпізнавання дактилем української жестової мови з фокусом на підвищенні генералізації при нестачі навчальних даних.

У роботі використано архітектуру X3D-M, що є складовою сімейства моделей Expand 3D[4], розробленого Facebook AI Research. Ключовою особливістю сімейства є поступове та оптимізоване розширення по 3D-простору, що забезпечує високу ефективність відеорозпізнавання при помірних обчислювальних витратах.

Усі моделі Expand 3D, включаючи X3D-M, навчалися з нуля на датасеті розпізнавання дій людини Kinetics-400[5], без використання ImageNet опори. Kinetics-400 містить близько 240 тисяч навчальних, 20 тисяч валідаційних та 35 тисяч тестових відео, що охоплюють 400 класів людських дій. Тренування виключно на відеоданих застосовано щоб уникнути упередженості від статичних зображень і отримати «чистіше» навчання саме для відеоаналізу.

Для донавчання на потрібний домен використано модифіковану версію датасету[6] українських дактилем, розширену до понад 3000 відео (Рис.1). Аугментації проводилися «на льоту», включають обрізання з масштабуванням, повороти, зміни яскравості, контрасту, насиченості, відтінку, додання розмиття та шумів.



Рисунок 1 – демонстрація навчальної вибірки, фрейми

Результати показали покласово середнє top-1 F1-score приблизно рівним 91% на тестовій вибірці (рисунок 2). Найкраще розпізнаються жести з чіткими візуальними відмінностями, тоді як подібні форми рук потребують додаткової генералізації навчальних прикладів.



Рисунок 2 – Демонстрація тестової вибірки, фрейми

Отримані результати ставлять застосування архітектури X3D-M та навчання з перенесенням як перспективну стартову точку для задачі розпізнавання дактилем української жестової мови в умовах малої кількості даних. Подальші дослідження спрямовуватимуться на розширення навчального набору, використання генеративних моделей для синтетичних даних та підвищення стабільності класифікації жестів.

Перелік посилань

1. Prasuhn L., Oyamada Y., Mochizuki Y., Ishikawa H. Система розпізнавання жестів руки на мобільному пристрої на основі HOG. Proc. IEEE Int. Conf. on Image Processing (ICIP). 2014. С. 3973–3977. DOI: <https://doi.org/10.1109/ICIP.2014.7025807>
2. Dardas N. H., Georganas N. D. Виявлення та розпізнавання жестів руки в реальному часі з використанням методу «мішок ознак» і техніки опорних векторів. IEEE Transactions on Instrumentation and Measurement. 2011. Т. 60, № 11. С. 3592–3607. DOI: <https://doi.org/10.1109/TIM.2011.2161140>
3. Krak I., Kudin G., Kulias A. Баратовимірне масштабування за допомогою псевдообернених операцій. Cybernetics and Systems Analysis. 2019. Т. 55, № 1. С. 22–29. DOI: <https://doi.org/10.1007/s10559-019-00108-9>
4. Feichtenhofer C. X3D: Розширення архітектур для ефективного розпізнавання відео. Proc. IEEE/CVF Conf. on Computer Vision and Pattern Recognition (CVPR). 2020. С. 203–213. DOI: <https://doi.org/10.1109/CVPR42600.2020.00028>
5. Kay W., Carreira J., Simonyan K., Zhang B., Hillier C., Vijayanarasimhan S., Viola F., Green T., Back T., Natsev P., Suleyman M., Zisserman A. Набір даних відео людських дій Kinetics Human Action Video Dataset. 2017. URL: <https://arxiv.org/abs/1705.06950>
6. Kondratiuk S., Krak I., Kuznetsov V., Kulias A. Використання часових даних і тривимірних згорток для розпізнавання абетки жестової мови. Proc. CMIS 2022 : зб. наук. пр. за матеріалами конф. 2022. С. 78–87. DOI: <https://doi.org/10.32782/cm2022/3137-7>

УДК 004.8

Залуцька О.О., Скрипльонов С.Д.

Хмельницький національний університет

ПРОЄКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ СЕМАНТИЧНОЇ ОБРОБКИ ТЕКСТІВ ДЛЯ ВИЗНАЧЕННЯ ТОНАЛЬНОСТІ

Подано проєкт інформаційної системи семантичної обробки україномовних коротких повідомлень для визначення тональності, зорієнтований на керованість, відтворюваність і прозорість. Архітектуру побудовано як багатошаровий застосунок з чітким розмежуванням відповідальностей: прийом і буферування даних, підготовка та нормалізація тексту, семантична аналітика з формуванням ознак, агрегування індикаторів тональності, збереження результатів і артефактів аудиту. Логічна модель даних включає сутності документів, токенів, словосполучень, частотних і вагових профілів, лексиконних значень, проміжних агрегатів і фінальних вердиктів, пов'язані з версіями конфігурацій і довідників. Інтерфейси розділено на інтеграційні та експертні з фіксованими контрактами і підтримкою міграцій. Передбачено телеметрію, політики доступу за ролями, незмінювані журнали та механізми відновлення, а також стратегії кешування і матеріалізації для забезпечення продуктивності та масштабованості. Запропонована специфікація створює інженерне підґрунтя для промислового впровадження системи з повним аудитним слідом та керованим життєвим циклом конфігурацій.

The paper presents the design of an information system for semantic processing of short Ukrainian texts aimed at sentiment determination with emphasis on controllability, reproducibility and transparency. The architecture follows a layered application with strict separation of concerns, covering data intake and buffering, text preparation and normalization, semantic analytics for feature formation, aggregation of sentiment indicators, and persistent storage of results and audit artifacts. The logical data model defines entities for documents, tokens, phrases, frequency and weight profiles, lexicon values, intermediate aggregates and final verdicts, all tied to versioned configurations and reference resources. System interfaces are split into integration and expert endpoints with stable contracts and migration support. The design embeds telemetry, role based access control, immutable logs and recovery mechanisms, together with caching and materialization strategies to ensure performance and scalability. The specification provides an engineering foundation for production deployment with a complete audit trail and a governed configuration lifecycle.

Сучасні методи обробки природної мови (NLP) є ключовою технологічною основою для побудови інформаційних систем семантичного аналізу, що здатні автоматично інтерпретувати емоційно-оцінні компоненти тексту [1, 2]. За останнє десятиріччя NLP перейшло від використання традиційних статистичних підходів до глибинних нейронних моделей [3], які оперують контекстними представленнями

мовних одиниць та забезпечують суттєве підвищення точності аналізу тональності, семантичного структурування та класифікації текстових даних [4].

У контексті проєктування інформаційної системи для визначення тональності особливу роль відіграють моделі трансформерної архітектури (BERT, RoBERTa, XLM-R) [5, 6], що дозволяють відтворювати глибокі семантичні залежності та враховувати контекст на рівні всього документа [7]. Застосування таких моделей забезпечує здатність до коректного трактування полісемії, довгострокових залежностей [8], змішаних мовних реєстрів та паралінгвістичних маркерів емоційності [9], що є критично важливим для задач точного визначення тональності природної мови [10, 11].

Окремої уваги потребує специфіка україномовних текстів, які характеризуються високою морфологічною варіативністю, наявністю просторіччя, діалектних елементів та активним розвитком неологізмів у цифрових комунікаціях [12]. Ці фактори створюють додаткові виклики при розробленні систем автоматичної тональної класифікації [13], однак одночасно стимулюють розвиток україномовних лінгвістичних ресурсів та спеціалізованих моделей [14, 15]. Поява українських BERT-подібних моделей і зростання обсягів розмічених корпусів суттєво розширюють можливості побудови високоточних інформаційних систем семантичної обробки текстів [16, 17].

Актуальність розробки інформаційної системи семантичної обробки текстів визначається необхідністю стабільного і відтворюваного аналізу тональності у реалістичних потоках даних [18]. Виробничі сценарії потребують не лише точності на контрольних вибірках, а передусім керованості параметрами, прозорості прийняття рішень і можливості аудиту. Проєктування такої системи передбачає цілісну узгодженість між архітектурою застосунку, схемою зберігання проміжних артефактів, семантичними модулями та методикою тестування. Центральним принципом стає документування кожного кроку обробки у вигляді відтворюваних артефактів, завдяки чому будь-який результат може бути пояснений і відтворений за ідентичних умов.

Метою проєктування є створення керованої, відтворюваної та прозорої системи, здатної приймати короткі україномовні повідомлення, стабілізувати їх уніфікованим поданням, формувати семантичні ознаки та обчислювати тональність із фіксацією усіх проміжних станів. Вимоги формуються як інженерні обмеження до архітектури, моделі даних, інтерфейсів і експлуатаційних властивостей. Ключовими принципами є розмежування відповідальностей, версіонування конфігурацій і словників, матеріалізація артефактів для аудиту, відсутність прихованих побічних ефектів і можливість детермінованого повторного прогону за часовою міткою.

Архітектурну основу становить багатoshаровий застосунок із чіткою ізоляцією контурів. На зовнішньому периметрі розміщується підсистема прийому, що працює з потоками коротких текстів і забезпечує нормалізоване, безпечне буферування. Далі діє шар підготовки, задачі якого включають уніфікацію графематики, стабілізацію токенизації та побудову службових метаданих для подальшого трасування. Шар семантичної аналітики відповідає за формування ознак та обчислення індикаторів тональності за узгодженими контрактами. Шар прийняття рішень агрегує сигнали в остаточне подання тональності та передає результат у підсистему збереження. Паралельно працює контур спостережності, що накопичує журнали параметрів, артефакти проміжних обчислень і довідники з їхніми версіями. Така композиція забезпечує локалізацію змін і дозволяє модернізувати окремі модулі без каскадного впливу на весь конвеєр.

Модель даних проектується як логічно зв'язана схема, орієнтована на прозорість і повторюваність. Передбачено сутності для документів, токенів, словосполучень, профілів частот, вагових оцінок ознак, лексиконних значень, проміжних агрегатів і фінальних вердиктів. Кожний запис пов'язується з конфігураційною сесією, що має часову мітку, і з набором версій довідників. Залежності організовано таким чином, щоб важкі у перерахунку об'єкти могли бути матеріалізовані та повторно використані. Це зменшує латентність і дає можливість виконувати локальні перебудови, зберігаючи стабільність загальної поведінки. Схема підтримує повний шлях пояснюваності, оскільки у ній фіксуються як вихідні повідомлення, так і їхні нормалізовані представлення, ключові одиниці, значення ваг, параметри порогів і остаточні рішення. Схема таблиць бази даних наведена на рисунку 1.

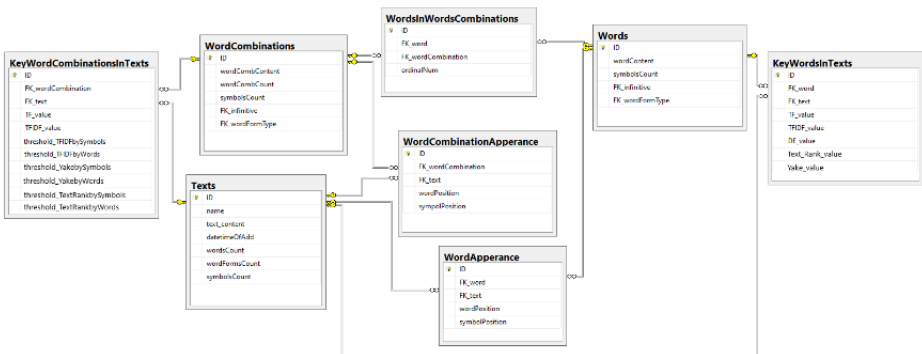


Рисунок 1 – Схема бази даних

Схема бази даних спроектована як нормалізована предметна модель для зберігання первинних текстових даних, морфологічних одиниць, їхніх поєднань і позицій у повідомленнях, а також проміжних і підсумкових артефактів семантичного аналізу. Логічний центр становить таблиця *Texts*, що акумулює короткі цифрові повідомлення у вигляді ідентифікованих записів із назвою, повним текстом, часовою міткою додання та агрегованими характеристиками довжини за словами і символами. Ця сутність є джерелом зв'язків для всіх подальших артефактів аналізу, забезпечуючи відтворюваність на рівні конкретного документа.

Лексична інформація представлена таблицею *Words*, де кожне слово зберігається як незалежна семантична одиниця з текстовою формою та довжиною. Посилання на *Infinitives* та *FormTypes* дозволяють відокремити лемму й тип словоформи від поверхневої форми, що усуває надлишковість і фіксує морфологічну норму для подальших зіставлень. Модель підтримує сценарії, коли кілька різних словоформ відносяться до одного інфінітива, а також розрізняє граматичні варіанти через окремий довідник типів форм.

Фразеологічний рівень подано сутністю *WordCombs*, яка описує словосполучення як окремі інформаційні носії з власним текстовим представленням, довжиною та лічильником зустрічей. Зв'язок між словосполученням і словами, що його утворюють, реалізовано через проміжну таблицю *WordsInCombinations*: тут для кожної комбінації фіксуються складові слова і порядок їх розташування, що дає можливість відтворити структурну форму та відокремити її від конкретних появ у документах. Така декомпозиція підтримує канонічне збереження шаблону словосполучення та унеможливорює дублювання даних.

Позиційні відомості зберігаються двома взаємодоповнювальними сутностями. Таблиця *WordApperance* (у подальшому доцільно уніфікувати написання як *WordAppearance*) відображає появи слів у межах конкретного повідомлення, фіксуючи посилання на слово та текст разом із позиціями за словами і символами. Аналогічно, *WordCombApperance* (*WordCombAppearance*) відстежує входження словосполучень у текстах із прив'язкою до абсолютних позицій. Розмежування цих двох рівнів дозволяє, з одного боку, реконструювати точну послідовність лексем у повідомленні, а з іншого — аналізувати сталі фрагменти як окремі ознаки, не втрачаючи їх прив'язки до первинних даних.

Шар семантичних обчислень реалізовано через спеціалізовані сутності для ключових одиниць. У *KeyWordsInMessages* зберігаються зв'язки між текстом і словом, що набуло статусу ключового, разом із чисельними показниками, отриманими на етапі векторизації. Передбачено поля для значень TF-IDF та порогових критеріїв відсікання за різними методами й різними шкалами позиціонування. Схема симетрично підтримує параметри для символорієнтованого

та словоорієнтованого підрахунку, що дає змогу відтворювати умови експерименту й проводити регресійні порівняння. Для багатослівних ознак аналогічні дані акумулює KeyWordCombinationsInTexts, де ключовою одиницею виступає словосполучення, пов'язане з відповідним текстом і доповнене набором порогових атрибутів для застосованих методів відбору. Вказані сутності виконують роль «аудитних таблиць» векторизації: вони не лише тримають підсумкові значення, а й відображають конфігураційний контекст ухвалення рішень.

Реляційна структура дотримується принципів третьої нормальної форми: текст, слово, словосполучення та їхні появи розведені у відокремлені сутності; довідникова інформація про лема та типи форм винесена за межі операційних таблиць; числові метрики зберігаються поруч із ключами, що визначають їхню область чинності. Первинні ключі забезпечують унікальність записів, тоді як зовнішні ключі фіксують цілісність посилань між рівнями лінгвістичної абстракції й конкретними документами. Для забезпечення продуктивності індекси доцільно створити на полях зв'язків FK_text, FK_word, FK_wordComb, а також на текстових полях wordContent та wCombContent з урахуванням налаштувань сортування та мовної локалі. Для позиційних таблиць доречно встановити унікальні обмеження на композиції (FK_text, wordPosition) і (FK_text, sympolPosition), що унеможливило б дублювати та гарантує однозначність координат у межах повідомлення.

Семантика часової прив'язки реалізується через поле дати й часу у Texts, яке визначає базову мітку для відтворення прогонів. Усі похідні артефакти можуть бути додатково з'єднані з конфігураційними версіями й словниковими релізами через відповідні довідники, що забезпечує повний аудит параметрів обчислень. Узгодженість імен і типів даних підтримує детермінованість обмінних контрактів між прикладними модулями, а розділення на словникові, позиційні та метрик-орієнтовані сутності знижує зв'язаність і полегшує еволюцію схеми без порушення цілісності історичних даних.

Інтерфейси системи поділяються на інтеграційні та експертні. Інтеграційні інтерфейси приймають повідомлення з зовнішніх сервісів у стандартизованому форматі та повертають структуровану відповідь із тональністю і базовими метаданими. Експертні інтерфейси забезпечують доступ до трас рішень, включаючи перелік ключових одиниць з їхніми вагами, застосовані конфігурації та пов'язані журнали. Контракти між шарами визначаються як стабільні схеми обміну, що унеможливають неявні зміни структури даних. Внутрішні API фіксують версії, підтримують міграції та валідацію вхідних параметрів, щоб запобігати розходженням між модулями під час оновлень.

Нижче наведено спроектовану діаграму класів для системи визначення тональності (рисунк 2).

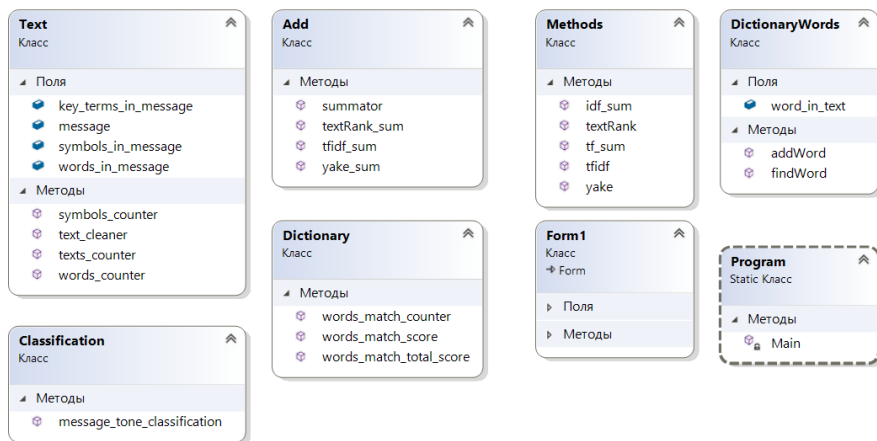


Рисунок 2 – Діаграма класів

Робота ініціюється з точки входу класу Program, який відповідає за коректне завантаження конфігурацій, підготовку середовища виконання та запуск основної форми користувацького інтерфейсу. Графічний інтерфейс реалізовано у вигляді форми Form1, що виконує роль центрального вузла взаємодії з користувачем. Форму організовано навколо тематичних вкладок, які охоплюють повний цикл опрацювання коротких україномовних повідомлень: від первинного завантаження і стабілізації тексту до семантичної інтерпретації та узагальнення результатів. Така композиція забезпечує логічну послідовність дій, мінімізує контекстні перемикання та робить процедури обробки відтворюваними.

Вкладка, присвячена роботі з базою повідомлень, уможливорює імпорт, попередній перегляд і добір матеріалу для аналізу з фіксацією метаданих. Тут відбувається підготовка корпусу й перевірка технічної придатності записів до подальшого опрацювання. Вкладка появ семантичних одиниць формує для вибраних текстів їхнє стабілізоване подання, фіксує токенізацію, частотні профілі та вектори ключових одиниць і надає користувачеві інспектовані проміжні результати. На вкладці аналізу повідомлень здійснюється зіставлення із словниковими ресурсами, агрегування сигналів і формування підсумкової класифікації з одночасним збереженням трас пояснюваності. Кожен елемент інтерфейсу пов'язаний із конкретним шаром логіки, що гарантує однозначну відповідність між дією користувача і викликаними сервісами.

Функції первинної обробки тексту інкапсульовано в окремому класі Text, який утворює стабільне підґрунтя для подальшої семантичної обробки. Методи класу виконують нормалізацію шляхом усунення цифрових і службових символів,

уніфікації реєстру та очищення невидимих артефактів кодування, що могли б викривляти частотний профіль. Окремі процедури відповідають за підрахунок кількості доступних повідомлень, слів і символів, завдяки чому формується базова статистика для контролю якості та налаштування порогів допуску. Сукупність цих операцій забезпечує інваріантність подальшої токенизації та робить результати наступних шарів порівнянними між різними джерелами даних.

Видобування інформативних ознак реалізовано в класі *Methods*, де зосереджено алгоритмічні засоби для побудови векторних представлень. Локальна помітність терміна визначається через частотні характеристики, тоді як глобальна розрізняювальна здатність регулюється інверсним зважуванням, що знижує вплив повсюдних лексем. Паралельно застосовуються безвчительні процедури, орієнтовані на внутрішньодокументні сигнали, зокрема механізми, які оцінюють позиційні ефекти, контекстну різноманітність та графову зв'язність кандидатів. Після узгодження шкал отримується композитний вектор ключових одиниць, придатний як для лексиконного зіставлення, так і для подачі на класифікаційні модулі. Такий дизайн забезпечує баланс між корпусною дисципліною і чутливістю до риторичної структури коротких повідомлень.

Робота зі словниками інтерпретації тональності зосереджена у класі *Dictionary*, який відповідає за операції зіставлення та агрегування оцінок. Спочатку визначаються перетини між відібраними ключовими одиницями і записами словника з урахуванням нормалізованих форм та можливих морфологічних варіантів. Далі кожній знайденій відповідності надається вагове значення згідно з валентною шкалою, після чого підрахунок інтегрується у зважений підсумок для всього повідомлення. Клас зберігає проміжні внески на рівні окремих термінів, що формує прозорі підстави для подальшої інтерпретації та спрощує аналіз джерел впливу на підсумковий знак.

Фінальне узгодження ознак у тональний вердикт виконує клас *Classification*, який здійснює перетворення підсумкової оцінки на категоріальне рішення та супровідні ймовірнісні показники. Перетворення враховує нейтральну зону з фіксованими порогамі, що запобігає поспішним рішенням у прикордонних випадках і підвищує стабільність поведінки на неоднорідних потоках. Результат подається у вигляді структурованого висновку, який містить категорію тональності, інтенсивність сигналу, посилання на використані версії словників і параметрів та скорочену трасу пояснюваності з переліком провідних семантичних одиниць.

Міжкласові взаємодії опрацьовано через чіткі контрактні інтерфейси. *Form1* ініціює операції класу *Text* для підготовки даних, передає стабілізовані тексти у *Methods* для формування ознак, скеровує отримані профілі до *Dictionary* для зіставлення зі словниками та, нарешті, викликає *Classification* для одержання підсумкового рішення. Кожний крок супроводжується фіксацією параметрів

виконання і часових міток, що уможливило аудит і відтворюваність. Така послідовність забезпечує низьку зв'язаність між підсистемами, високу когерентність усередині класів і локалізованість змін під час модернізації окремих алгоритмічних компонентів.

Експлуатаційні вимоги враховують продуктивність, масштабованість і стійкість. Для зменшення затримок застосовується кешування результатів підготовки і семантичних обчислень, а також матеріалізація часто використовуваних представлень. Обробка організується пакетами з лінійною залежністю часу від обсягу вхідних даних. Стратегія масштабування передбачає горизонтальне рознесення підсистем за функціональними ролями, що дозволяє окремо збільшувати ресурси підготовки, семантики або прийняття рішень залежно від профілю навантаження. Усі компоненти проєктуються з урахуванням відмовостійкості, передбачено механізми повторних спроб, ідемпотентність обробки та консистентні транзакції для критичних операцій запису.

Безпека і відповідність етичним вимогам закладаються на рівні проєктних рішень. Система працює з анонімізованими або агрегованими представленнями, мінімізує обсяг персональних даних і розділяє доступ до технічних і змістових артефактів. Політика контролю доступу визначається ролями та підтримує принцип мінімальних привілеїв. Усі експортовані результати супроводжуються метаданими про версії конфігурацій і часові мітки, що забезпечує можливість зовнішнього аудиту. Журнали доступу та зміни параметрів зберігаються у незмінюваному вигляді, що гарантує довіру до відтворюваності.

Управління конфігураціями та довідниками є окремим аспектом проєктування. Кожна зміна порогів, словників, правил нормалізації або форматів контрактів оформлюється як версійована подія із вказанням причини, відповідального і кола впливу. Підтримується можливість повернення до попереднього стану за однією командою. Для критичних оновлень застосовується подвійний запуск у паралельному контурі, що дає змогу порівнювати виходи різних версій на однакових вхідних потоках до моменту повного переключення.

Спостережність і керованість забезпечуються єдиним шаром телеметрії. У ньому акумулюються технічні метрики затримок та використання ресурсів, статистика по класах і зведення щодо відсотка повідомлень у нейтральній зоні. Артефакти трас зберігаються з прив'язкою до ключів сесії, що дозволяє реконструювати повний шлях рішення для будь-якого повідомлення. Передбачено механізм сигналів про деградацію, який ініціює захисні сценарії, наприклад автоматичне розширення нейтральної зони або переключення на попередню стабільну конфігурацію до завершення аналізу причин.

Розгортання системи планується у конфігурації з поділом середовищ. Окреме середовище використовується для розробки та інтеграційного узгодження

контрактів, окреме для передпромислової валідації з доступом до повних трас і незмінюваних журналів, а окреме для промислової експлуатації з обмеженим доступом і жорсткими політиками версіювання. Міграції схеми даних проводяться за сценаріями, що не потребують зупинки сервісу, а всі зміни контрактів супроводжуються автоматичною перевіркою сумісності.

Підсумовуючи, проєктування інформаційної системи семантичної обробки текстів для визначення тональності зосереджується на архітектурній ясності, відтворюваності і керованості. Узгоджена багатоваріантова структура, прозора модель даних із матеріалізованими артефактами, стабільні інтерфейси, дисципліна версіювання і вбудована спостережність формують інженерне підґрунтя для подальшого масштабованого впровадження без компромісів щодо прозорості прийняття рішень і можливості аудиту.

Перелік посилань

1. Siino M., Falco M., Croce D., Rosso P. Exploring LLMs Applications in Law: A Literature Review on Current Legal NLP Approaches. IEEE Access. 2025.
2. Akter Semi M. M., Uddin M. B., Sultana S., Tamanna M., Uddin A., Ahmed K. R. AI-Driven Education: Integrating Machine Learning and NLP to Transform Child Learning Systems. International Journal of Advanced Computer Science & Applications. 2025. Vol. 16, No. 6.
3. Yu J. H., Chauhan D. Trends in NLP for Personalized Learning: LDA and Sentiment Analysis Insights. Education and Information Technologies. 2025. Vol. 30, No. 4. Pp. 4307–4348.
4. Poddar S., Koley P., Misra J., Ganguly N., Ghosh S. Towards Sustainable NLP: Insights from Benchmarking Inference Energy in Large Language Models. Proceedings of the 2025 Conference of the Nations of the Americas Chapter of the Association for Computational Linguistics: Human Language Technologies. April 2025. Pp. 12688–12704.
5. Timoneda J. C., Vera S. V. BERT, RoBERTa, or DeBERTa? Comparing Performance Across Transformers Models in Political Science Text. The Journal of Politics. 2025. Vol. 87, No. 1. Pp. 347–364.
6. Shevchuk P., Molchanova M., Mazurets O. Software for Text Messages Reliability Analysis Based on the Machine Learning Models Ensemble. Proceedings of IV International Scientific and Practical Conference «Innovative research and perspectives of the development of science and technology». January 29-31, 2024. Stockholm, Sweden. 2024. Pp. 347-354.
7. Mazurets O., Sobko O., Vit R., Pasternak V. Practical Approach for Detection by Deep Learning of Target Objects of Subject Area Based on Semantic Connectivity Indicators in Audio Database. Proceedings of XXIV International Scientific and Practical Conference «Modern Scientific Challenges are the Driving Force of the Development of Scientific Research». May 22-24, 2024. Bruges, Belgium. International Scientific Unity. 2024. Pp. 91-96.
8. Молчанова М.О., Мазурець О.В., Собко О.В., Кліменко В.І., Андрощук В.І. Метод неймережевого виявлення кібербулінгу з використанням хмарних сервісів та об'єктно-орієнтованої моделі. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2024. №2 (333). С. 200-206.

9. Mazurets O.V., Sobko O.V., Molchanova M.O., Zalutska O.O., Yurchak A.V. Practical Implementation of Neural Network Method for Stress Features Detection by Social Internet Networks Posts. Global Science: Prospects and Innovations. Proceedings of the II International Scientific and Theoretical Conference «Scientific Review of the Actual Events, Achievements and Problems». May 31, 2024. Berlin, Federal Republic of Germany: International Center of Scientific Research. 2024. Pp. 160-167.
10. Sobko O., Mazurets O., Didur V., Chervonchuk I. Recurrent Neural Network Model Architecture for Detecting a Tendency to Atypical Behavior Of Individuals by Text Posts. Theoretical and Practical Aspects of Modern Research. Proceedings of XXVI International scientific and practical conference. June 5-7, 2024. International Scientific Unity. Ottawa, Canada. 2024. Pp. 113-117.
11. Mazurets O., Molchanova M., Klimenko V., Prosvitliuk M Practice Implementation of Neural Network Model BART-Large-CNN for Text Annotation. Prospects of Scientific Research in the Conditions of the Modern World. Proceedings of XXVII International scientific and practical conference. June 12-14, 2024. Rotterdam, Netherlands. 2024. Pp. 97-102.
12. Blazhuk V., Mazurets O., Zalutska O. An Approach to Using the mBERT Deep Learning Neural Network Model for Identifying Emotional Components and Communication Intentions. The Impact of Scientific Research on the Development of the Modern World. Proceedings of the XLIV International scientific and practical conference. October 23-25, 2024. Dubrovnik, Croatia. 2024. Pp. 79-84.
13. Tymofiiiev I., Mazurets O., Hardysh D., Molchanova M. Neural Network Dual Architecture for Depression Detection Using Cloud Services. Scientific Research in the Era of Digital Technologies: Challenges and Opportunities. Proceedings of the XLVI International scientific and practical conference. November 6-8, 2024. Barcelona, Spain. 2024. Pp. 84-88.
14. Yurchenko D., Mazurets O., Didur V., Molchanova M. Approach to Using Cloud Services for Visual Analytics of Neural Network Analysis of Texts Emotional Tonality. The Future of Scientific Discoveries: New Trends and Technologies. Proceedings of the XLVII International scientific and practical conference. November 13-15, 2024. Marseille, France. 2024. Pp. 108-113.
15. Mazurets O., Tymofiiiev I., Dydo R. медвApproach for Using Neural Network BERT-GPT2 Dual Transformer Architecture for Detecting Persons Depressive State. Ricerche scientifiche e metodi della loro realizzazione: esperienza mondiale e realtà domestiche. Raccolta di articoli scientifici con gli atti della VI Conferenza scientifica e pratica internazionale. 15 novembre, 2024. Bologna, Repubblica Italiana. 2024. Pp. 147-151.
16. Hladun O., Mazurets O., Molchanova M., Sobko O. Real Time Detection the Person Emotion State Using Neural Network. Scientific Research: Modern Innovations and Future Perspectives. Proceedings of the 2 International scientific and practical conference. November 25-27, 2024. Montreal, Canada. 2024. Pp. 119-123.
17. Mazurets O., Vit R. Practical Application of Method of Thematic Classification of Text Information Using LDA. Information Technology and Implementation (Satellite). Proceedings 11th International Conference. November 21, 2024. Kyiv, Ukraine. 2024. Pp. 151-152.
18. Murava V., Zalutska O., Didur V., Mazurets O. Software architecture of information system for exchanging LLM thematic prompts. Global Trends in the Development of Information Technology and Science. Proceedings IV International Scientific and Practical Conference. June 25-27, 2025. Stockholm, Sweden. Pp. 121-127.

УДК 004.056.5

Зарицька О.А.¹, Лада М.Р.¹, Чешун В.М.¹, Чешун Д.В.²

¹Хмельницький національний університет

²Хмельницький фаховий економіко-технологічний коледж УЕП

ПЕРЕХІД ВІД КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ДО АВТОРИЗАЦІЇ З БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Робота присвячена дослідженню трансформації підходів до забезпечення кібербезпеки в Україні, акцентовано на суттєвих змінах у законодавстві (Закон № 4336-IX, 2025 р.), що призвели до скасування комплексної системи захисту інформації, та на впровадженні нової моделі, яка замінює статичний формалізм на ризик-орієнтований підхід, гармонізований з ISO 27001 та NIST. Ключовим інструментом є Авторизація з безпеки на основі профілів безпеки, що підвищує гнучкість, ефективність використання ресурсів та кіберстійкість критичних державних систем.

The work is devoted to the study of the transformation of approaches to ensuring cybersecurity in Ukraine, focusing on significant changes in legislation (Law № 4336-IX, 2025), which led to the abolition of the comprehensive information protection system, and on the implementation of a new model that replaces static formalism with a risk-based approach harmonized with ISO 27001 and NIST. The key tool is Security Authorization based on security profiles, which increases flexibility, resource efficiency, and cyber resilience of critical government systems.

Актуальність організації комплексного захисту інформації в державних структурах та комерційних визначається потужним і незворотним процесом цифровізації публічних послуг, який, з одного боку, є імперативом сучасності, а з іншого – створює безпрецедентні виклики у сфері кібербезпеки. Прагнення держав до створення ефективного та прозорого електронного урядування вимагає акумулювання у взаємопов'язаних цифрових системах величезних обсягів чутливої інформації, розпочинаючи із персональних даних громадян, фінансових і майнових реєстрів, завершуючи даними стратегічної державної таємниці. Цифровізація підвищує зручність та інклюзивність державних сервісів, мінімізує корупційні ризики й прискорює взаємодію з суспільством, проте водночас перетворює державні інформаційні ресурси на пріоритетну мішень для зловмисників.

Стрімке впровадження новітніх технологій, на жаль, часто випереджає розвиток адекватних та багаторівневих систем захисту, що призводить до виникнення критичних вразливостей. Сучасні кіберзагрози давно вийшли за межі

звичайного хакерства – вони стали інструментом державного кібершпionажу та елементом гібридної війни, про що свідчать численні цілеспрямовані та складні атаки на критичну інфраструктуру та державні реєстри. Метою таких атак є не лише викрадення секретних даних, а й порушення функціонування життєво важливих державних сервісів, підри́в довіри громадян до інститутів влади та дестабілізація суспільства. Крім того, державні установи постійно стикаються із загрозами, пов'язаними з програмами-вимагачами та несанкціонованим доступом до даних, що часто стає можливим через використання застарілих систем (Legacy) та низьку обізнаність персоналу. Таким чином, забезпечення кіберстійкості та захисту інформаційних активів держави, відповідно до жорстких міжнародних стандартів, є не просто технічним завданням, а ключовим фактором національної безпеки та умовою успішного функціонування держави в цифрову епоху.

Успішне функціонування державних структур в умовах інтенсивної цифровізації та зростання кіберзагроз вимагає принципово нового підходу до забезпечення інформаційної безпеки, який має бути комплексним, багаторівневим і стандартизованим. Недостатньо просто захистити окремі сервери чи встановити антивірус. Потрібна цілісна система управління інформаційною безпекою (СУІБ), що охоплює всі аспекти діяльності установи. Комплексний підхід означає інтеграцію організаційних, правових, кадрових та технологічних заходів, де безпека розглядається не як одноразовий проєкт, а як безперервний процес, вбудований у щоденну роботу. Це вимагає розробки чітких політик, процедур та інструкцій, які регулюють доступ, обробку та зберігання всіх видів інформації.

В Україні відбулася кардинальна трансформація підходів до забезпечення захисту інформації в державних та комерційних структурах, що знайшла своє відображення у суттєвих змінах до Закону України «Про захист інформації в інформаційно-комунікаційних системах» [1] (зокрема, згідно із Законом № 4336-ІХ, що набрав чинності у 2025 році [2]). Ключовим нововведенням є відмова від застарілої моделі комплексної системи захисту інформації (КСЗІ) та перехід до більш гнучкого та сучасного інструменту – авторизації з безпеки інформаційних систем.

Деінституалізація КСЗІ орієнтована на перехід від формалізму в організації комплексного захисту до управління ризиками.

Донедавна захист державних інформаційних ресурсів та інформації з обмеженим доступом був нерозривно пов'язаний з обов'язковою наявністю КСЗІ та її атестату відповідності. Ця модель, хоча й забезпечувала високий рівень безпеки на момент атестації, часто критикувалася за її формалізм та статичність. Процес створення КСЗІ був тривалим, ресурсоємним і зосередженим на документальному

підтвердженні відповідності вимогам на певний момент часу, тоді як реальні кіберзагрози розвиваються експоненційно.

Оновлене законодавство 2025 року радикально змінює цей підхід, скасовуючи обов'язковість КСЗІ. Цей крок є рухом до управління ризиками, гармонізованим з міжнародними фреймворками, такими як NIST [3] та ISO 27001 [4], де безпека є безперервним процесом, а не одноразовим проектом. Тепер акцент зміщується з оцінки заходів захисту (як це було в КСЗІ) на оцінку забезпечення безпеки системи протягом усього її життєвого циклу.

Впровадження авторизації базується на двох положеннях: гнучкість та профілі безпеки.

Новий механізм авторизації з безпеки систем стає ключовим елементом, який дозволяє експлуатувати системи, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом. Цей процес безпосередньо пов'язаний із запровадженням інституту профілів безпеки, що є абсолютною новачією для українського законодавства.

Процедура авторизації тепер базується на використанні трьох рівнів профілів безпеки, які визначають необхідний мінімум заходів захисту, залежно від категорії системи та виду інформації [1, 2, 5]:

базовий профіль безпеки розробляється Адміністрацією Державної служби спеціального зв'язку та захисту інформації України і є загальним стандартом, який залежить від виду обмеження доступу до інформації та функціонального призначення системи;

– галузевий профіль безпеки розробляється на основі базового профілю для відповідних категорій систем у конкретній галузі (наприклад, медицина, фінанси);

– цільовий профіль безпеки – це профіль, який розробляється безпосередньо для конкретної системи, що підлягає авторизації, з урахуванням її унікальних особливостей, на основі базового або галузевого профілю.

Авторизація з безпеки підтверджує, що система, відповідно до обраного профілю, забезпечує відповідність вимогам законодавства, національним стандартам та нормам технічного й криптографічного захисту. Це дозволяє державним органам та власникам критичної інформаційної інфраструктури швидше адаптувати заходи безпеки до змін і технологічних інновацій, оскільки Профілі безпеки, як очікується, будуть більш гнучкими, ніж застарілі НД ТЗІ. Відтепер Державна служба спеціального зв'язку та захисту інформації України здійснює ведення Переліку авторизованих систем з безпеки, що вносить елемент прозорості та контролю [6].

Перехід від КСЗІ до авторизації та профілів безпеки відображає стратегічний намір України перейти від застарілого підходу, заснованого на

суворих (іноді застарілих) технічних стандартах, до ризик-орієнтованої моделі. Ця модель дозволяє більш ефективно використовувати фінансові та кадрові ресурси, зосереджуючись на найбільш актуальних кіберзагрозах і забезпечуючи неперервне функціонування критично важливих державних систем. Таким чином, оновлення законодавства 2025 року є ключовим кроком до модернізації системи кіберзахисту, роблячи її більш динамічною та стійкою до сучасних викликів.

Перелік посилань

1. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР : редакція від 20.04.2025. URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text> (дата звернення: 28.10.2025).
2. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури. Закон України від 27.03.2025 № 4336-IX. URL: <https://zakon.rada.gov.ua/laws/show/4336-20#Text> (дата звернення: 28.10.2025).
3. NIST SP 800-61 Rev.2 — Computer Security Incident Handling Guide. URL: <https://csrc.nist.gov/pubs/sp/800/61/r2/final> (date of access: 25.10.2025).
4. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. URL: <https://www.iso.org/standard/27001> (дата звернення: 28.10.2025).
5. Про затвердження Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем та Порядку розроблення та затвердження профілів безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем. Постанова Кабінету Міністрів України від 18 червня 2025 р. № 712. URL: <https://zakon.rada.gov.ua/laws/show/z1140-25#Text> (дата звернення: 28.10.2025).
6. Про затвердження Порядку ведення переліку авторизованих систем з безпеки. Наказ Адміністрації Держспецв'язку від 11.07.2025 № 424. URL: <https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-11-07-2025-424-pro-zatverdzhennya-poryadku-vedennya-pereliku-avtorizovanih-sistem-z-bezpeki> (дата звернення: 28.10.2025).

УДК 004.056.55:004.804.4

Ісаєв Т.С., Лисенко С.М., Лисенко Н.С.

Хмельницький національний університет

ІНТЕЛЕКТУАЛЬНА АДАПТИВНА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ АВТОМАТИЧНОГО ОНОВЛЕННЯ МОДЕЛЕЙ ВІЯВЛЕННЯ ЗАГРОЗ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Розглянуто прикладні аспекти розробки інтелектуальної адаптивної інформаційної технології, що забезпечує автоматичне оновлення моделей виявлення загроз у комп'ютерних системах. Запропонована технологія дозволяє підвищити точність і актуальність виявлення атак за рахунок використання методів машинного навчання, інкрементного оновлення та аналізу поведінкових характеристик. Система адаптується до нових типів загроз без участі користувача, зменшуючи кількість хибнопозитивних спрацювань.

Applied aspects of intelligent adaptive information technology development for automatic threat detection model updating in computer systems are considered. The proposed technology improves the accuracy and relevance of attack detection through machine learning methods, incremental updates, and behavioral analysis. The system adapts to new types of threats without user intervention, reducing the number of false positives.

З розвитком кіберзагроз та ускладненням їх структури традиційні системи виявлення атак втрачають ефективність. Це зумовлює потребу в адаптивних технологіях, здатних автоматично оновлювати моделі на основі нових даних. Запропонована технологія включає модулі збору подій, класифікації, генерації нових ознак та оновлення моделей.

Метою роботи є розробка інтелектуальної адаптивної інформаційної технології автоматичного оновлення моделей виявлення загроз, яка забезпечує підвищення ефективності кіберзахисту.

Для досягнення поставленої мети було проаналізовано існуючі підходи до побудови систем виявлення загроз, зокрема сигнатурні, поведінкові та гібридні моделі. Основним недоліком більшості з них є статичність – моделі не оновлюються автоматично, що призводить до втрати актуальності та зниження точності виявлення. Зважаючи на усе це, було запропоновано технологію, яка дозволяє здійснювати автоматичне оновлення моделей на основі нових даних, що надходять у реальному часі.

Ключовим елементом технології є механізм оцінки релевантності нових ознак, які можуть бути включені до моделі. Така оцінка базується на

інформаційному прирості та складності інтеграції ознаки. Формально це можна представити наступним чином:

$$R(fi) = \frac{IG(fi)}{C(fi)}, \quad (1)$$

де $IG(fi)$ – інформаційний приріст ознаки fi , що характеризує її внесок у покращення класифікації, а $C(fi)$ – складність її інтеграції в існуючу модель (наприклад, обчислювальні витрати, конфлікти з поточними правилами тощо).

Загальну архітектуру даної моделі можна представити візуально (рис. 1).



Рисунок 1 – Архітектура адаптивної технології оновлення моделей

Існує безліч способів адаптувати модель та навчити її, вале було виокремлено лише декілька найбільш дієвих способів, які покажуть кращий результат (таблиця 1).

Таблиця 1 – Підходи до адаптації моделей виявлення загроз

Підхід	Опис
Інкrementне навчання	Оновлення моделі без повного перенавчання, з урахуванням нових даних
Поведінкова класифікація	Виявлення аномалій на основі профілю користувача та системної активності
Генерація ознак	Автоматичне створення нових параметрів для моделі на основі статистики та контексту

Запропоновані підходи до адаптації моделей виявлення загроз дозволяють забезпечити гнучкість та масштабованість системи в умовах змінного середовища. Інкrementне навчання дає змогу оновлювати класифікатори без повного перенавчання, що суттєво знижує обчислювальні витрати та час реакції на нові типи атак. Поведінкова класифікація, у свою чергу, дозволяє виявляти аномалії, які не мають чітких сигнатур, шляхом аналізу відхилень від типових профілів користувачів або систем.

Особливу увагу приділено генерації нових ознак, які можуть бути як статистичними (наприклад, частота доступу до певних ресурсів), так і контекстними (наприклад, взаємозв'язок між подіями у часовому інтервалі). Для оцінки доцільності включення таких ознак до моделі використовується механізм релевантності, що враховує як їх інформаційний внесок, так і складність інтеграції.

Крім того, технологія передбачає автоматичне формування правил на основі виявлених закономірностей, що дозволяє системі самостійно адаптуватися до нових загроз без участі експерта. Це відкриває перспективи для побудови самонавчальних систем кіберзахисту, здатних ефективно функціонувати в умовах обмеженого людського ресурсу.

Отже, запропонована технологія дозволяє автоматизувати процес оновлення моделей виявлення загроз, забезпечуючи адаптацію до нових умов та підвищення ефективності кіберзахисту. Подальші дослідження спрямовані на інтеграцію технології в промислові програмні комплекси, розширення її функціональності та забезпечення масштабованості для великих корпоративних мереж.

Перелік посилань

1. KAVITHA, D.; THEJAS, S. Ai enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation. *IEEE Access*, 2024, 12: 173127-173136.
2. CHEN, Heyao, et al. Threat detection driven by artificial intelligence: Enhancing cybersecurity with machine learning algorithms. 2024, 6: 1-13.
3. ALZAABI, Fatima Rashed; MEHMOOD, Abid. A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. *IEEE Access*, 2024, 12: 30907-30927.
4. MADUPATI, Bhanuprakash. AI-Driven Threat Detection in Cybersecurity. Available at SSRN 5076610, 2024, 2: 1-20.
5. OFOEGBU, Kingsley David Onyewuchi, et al. Real-Time Cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach. *Computer Science & IT Research Journal*, 2024, 4: 478-501.
6. AMINU, Muritala, et al. Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. *International Journal of Computer Applications Technology and Research*, 2024, 13.8: 11-27.
7. RAMESH, Sai Kiran Arcot; KIRAN, Sai. AI-Enhanced Cyber Threat Detection. *International Journal of Computer Trends and Technology (IJCTT)*, 2024, 72.6: 64-71.
8. AKINBOLAJI, TAIWO JOSEPH. Advanced integration of artificial intelligence and machine learning for real-time threat detection in cloud computing environments. *Iconic Research and Engineering Journals*, 2024, 6.10: 980-991.
9. KHAN, Muhammad Ismaeel; ARIF, Aftab; KHAN, Ali Raza A. AI-Driven Threat Detection: A Brief Overview of AI Techniques in Cybersecurity. *BIN: Bulletin of Informatics*, 2024, 2.2: 248-261.
10. OKOLI, Ugochukwu Ikechukwu, et al. Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews*, 2024, 21.1: 2286-2295

УДК 004.8

Ільчишин В.В., Манзюк Е.А., Скрипник Т.К.

Хмельницький національний університет

МЕТОД ВИЯВЛЕННЯ ШАХРАЙСЬКИХ БАНКІВСЬКИХ ОПЕРАЦІЙ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

Розглянуто метод автоматизованого виявлення шахрайських банківських операцій з використанням алгоритму випадкового лісу та техніки балансування класів SMOTE. Запропонована архітектура поєднує ансамблеве навчання з попередньою обробкою даних та генерацією синтетичних зразків для вирішення проблеми незбалансованості класів.

A method for automated detection of fraudulent banking operations using Random Forest algorithm and SMOTE class balancing technique is considered. The proposed architecture combines ensemble learning with data preprocessing and synthetic sample generation to address class imbalance problem.

Виявлення шахрайських банківських операцій є критично важливою задачею для фінансових установ, які щорічно втрачають мільярди доларів через фродові транзакції [1-3]. Традиційні підходи, що базуються на ручному аналізі та статичних правилах, не справляються з великими обсягами транзакцій та еволюцією методів шахрайства. Використання алгоритмів машинного навчання дозволяє автоматизувати процес виявлення шахрайства та адаптуватися до нових патернів фродової активності. Сучасні дослідження в області штучного інтелекту демонструють ефективність адаптивних підходів до розпізнавання складних патернів у різних застосуваннях [4-6]. Зокрема, методи машинного навчання успішно використовуються для аналізу поведінкових ознак [7, 8] та оптимізації процесів прийняття рішень [9-11]. Пояснюване глибоке навчання забезпечує інтерпретацію результатів моделей [12], що є критично важливим для фінансового сектору.

Метою роботи є розробка методу автоматизованого виявлення шахрайських операцій, який забезпечує високу точність при роботі з незбалансованими даними та може працювати в режимі реального часу для захисту фінансових систем від фродових атак.

Розроблений метод базується на припущенні, що шахрайські операції мають специфічні характеристики та патерни поведінки, які відрізняють їх від легальних транзакцій. Ці відмінності проявляються у таких аспектах як сума операції, час здійснення, географічне розташування, кількість спроб входу в систему та зміна технічних параметрів доступу. Основна ідея методу полягає у навчанні моделі на історичних даних з подальшим використанням для класифікації нових операцій.

Метод складається з шести послідовних етапів, показаних на рисунку 1.

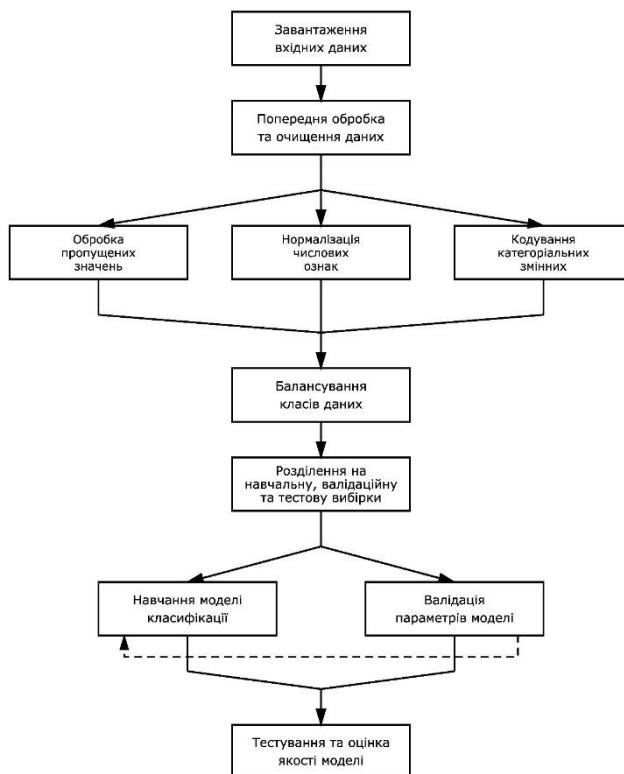


Рисунок 1 – Загальна схема методу виявлення шахрайських операцій

Перший етап включає завантаження та аналіз вхідних даних, де відбувається ознайомлення зі структурою датасету та виявлення потенційних проблем. Другий етап присвячено попередній обробці даних, що включає нормалізацію, кодування змінних та обробку пропущених значень. Третій етап передбачає генерацію міток класів на основі системи правил виявлення аномалій. Четвертий етап застосовує техніку SMOTE для балансування класів у навчальній вибірці. П'ятий етап виконує навчання моделі випадкового лісу на підготовлених даних. Шостий етап здійснює класифікацію нових транзакцій з визначенням ймовірності шахрайства.

Ключовою особливістю методу є його модульна структура, що дозволяє незалежно змінювати окремі компоненти без перебудови всієї системи. Така архітектура забезпечує гнучкість у налаштуванні параметрів та можливість адаптації до специфічних вимог різних банківських установ.

Початковий датасет містить інформацію про банківські транзакції з такими характеристиками: сума операції, тип рахунку, час здійснення, географічне

розташування, IP-адреса, ідентифікатор пристрою, кількість спроб входу, тривалість виконання та стан балансу. Кожна транзакція описується набором числових та категоріальних ознак, які потребують спеціальної обробки перед використанням у моделі машинного навчання.

Особливістю використовуюваного датасету є відсутність готових міток класів, що вимагає їх автоматичного визначення. Розроблено систему з восьми критеріїв для виявлення підозрілих транзакцій, представлену в таблиці 1. Перший критерій аналізує кількість спроб входу в систему, де значення більше трьох спроб отримує один бал підозрілості. Другий критерій оцінює незвичайність суми операції шляхом порівняння з історичними даними рахунку, присвоюючи бал транзакціям, що перевищують середнє значення більш ніж на два стандартних відхилення.

Таблиця 1 – Критерії визначення шахрайських операцій

Критерій	Умова аномалії	Бали
Спроби входу	Більше 3 спроб	1
Незвичайна сума	Перевищує $\mu + 2\sigma$ від історії	1
Часовий інтервал	Менше 1 хвилини між операціями	1
Географічна аномалія	Фізично неможливе переміщення	1
Зміна IP-адреси	Нова, раніше не використовувана	1
Зміна пристрою	Новий ідентифікатор	1
Тривалість операції	Менше 5 секунд або більше 2 хвилин	1
Зміна балансу	Зменшення понад 80% або від'ємний	1

Третій критерій перевіряє часовий інтервал між послідовними транзакціями одного рахунку, де інтервал менше однієї хвилини вказує на можливу автоматизовану атаку. Четвертий критерій аналізує географічну консистентність, виявляючи фізично неможливі переміщення користувача між локаціями за короткий проміжок часу. П'ятий та шостий критерії відстежують зміни технічних параметрів доступу, таких як IP-адреса та ідентифікатор пристрою, що можуть свідчити про несанкціонований доступ до рахунку.

Сьомий критерій оцінює тривалість виконання транзакції, де надто швидкі операції менше п'яти секунд можуть вказувати на автоматизовані скрипти, а занадто тривалі операції більше двох хвилин можуть бути ознакою проблем з легітимністю. Восьмий критерій аналізує стан балансу після транзакції, де різке зменшення більш ніж на вісімдесят відсотків або від'ємний баланс вказують на спробу максимально вивести кошти.

Фінальна мітка класу визначається на основі сумарного балу підозрілості. Транзакції, які набирають три або більше балів з восьми можливих, класифікуються як шахрайські. Такий підхід дозволяє уникнути помилкової класифікації операцій з лише однією незвичною характеристикою та забезпечує реалістичне співвідношення класів на рівні одного-п'яти відсотків шахрайських операцій від загальної кількості.

Для класифікації банківських транзакцій обрано алгоритм випадкового лісу, який є ансамблевим методом машинного навчання. Вибір цього алгоритму

обумовлений декількома важливими факторами. По-перше, випадковий ліс демонструє високу точність класифікації на різних типах даних та добре справляється з задачами, де присутня велика кількість ознак. По-друге, алгоритм є стійким до перенавчання завдяки своїй ансамблевій природі, де помилки окремих дерев компенсуються правильними передбаченнями інших. По-третє, випадковий ліс може працювати з даними, які містять як числові, так і категоріальні ознаки, що є важливим для банківських транзакцій.

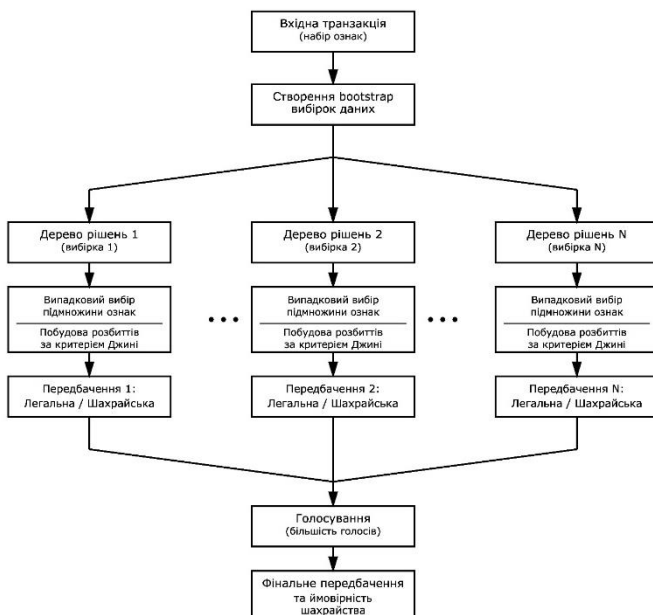


Рисунок 2 – Архітектура моделі класифікації транзакцій

Архітектура випадкового лісу базується на побудові множини дерев рішень, кожне з яких навчається на випадковій підвибірці вхідних даних. Процес починається зі створення навчальних підвибірок методом бутстрепа, який полягає у випадковому відборі зразків з поверненням. Це означає, що один і той самий зразок може потрапити у вибірку декілька разів, що забезпечує різноманітність навчальних даних для кожного дерева.

Модель також надає ймовірнісну інтерпретацію результатів класифікації. Ймовірність належності транзакції до класу шахрайських операцій обчислюється як частка дерев, які класифікували транзакцію як шахрайську, від загальної кількості дерев в ансамблі. Така оцінка дозволяє встановлювати порогові значення для прийняття рішення та гнучко налаштовувати баланс між виявленням шахрайства та кількістю помилкових спрацювань залежно від потреб банківської установи.

Важливою характеристикою випадкового лісу є можливість оцінки важливості ознак для класифікації. Це досягається шляхом вимірювання того, наскільки зменшується помилка при використанні конкретної ознаки для розбиття вузлів дерев. Ознаки, які часто використовуються і призводять до значного покращення класифікації, отримують вищі оцінки важливості. Ця інформація корисна для розуміння того, які характеристики транзакцій найбільш критичні для виявлення шахрайства.

Для вирішення проблеми дисбалансу класів застосовано техніку передискретизації меншого класу під назвою SMOTE, яка означає синтетичну передискретизацію меншого класу. Ця техніка дозволяє збільшити кількість зразків шахрайських транзакцій у вибірці шляхом генерації синтетичних прикладів. Основна ідея методу полягає в створенні нових зразків не шляхом простого копіювання існуючих шахрайських транзакцій, а через інтерполяцію між сусідніми зразками в просторі ознак, що забезпечує різноманітність генерованих даних.

Комбінація техніки передискретизації SMOTE та налаштування вагових коефіцієнтів забезпечує найкращі результати у виявленні шахрайських операцій. Ці два підходи доповнюють один одного синергетично, оскільки SMOTE збільшує кількість навчальних зразків шахрайських транзакцій та їх різноманітність, а вагові коефіцієнти впливають на процес навчання моделі, підвищуючи важливість правильної класифікації цих зразків та зменшуючи схильність до пропуску шахрайських операцій.

Оцінювання якості роботи методу виявлення шахрайських банківських операцій потребує використання спеціальних метрик, які враховують специфіку задачі класифікації з незбалансованими класами. Стандартна метрика точності класифікації, яка обчислюється як відношення правильно класифікованих зразків до загальної кількості зразків, не є достатньо інформативною для такої задачі. Модель може досягти точності дев'яносто дев'ять відсотків, просто класифікуючи всі транзакції як легальні, що не відповідає меті виявлення шахрайства.

Для всебічної оцінки якості використовується набір метрик, які базуються на матриці помилок. Ця матриця містить чотири основні категорії передбачень. Істинно позитивні результати відповідають шахрайським транзакціям, які правильно класифіковано моделлю як шахрайські. Істинно негативні результати представляють легальні операції, які коректно визначено як легальні. Хибно позитивні результати виникають, коли легальна транзакція помилково класифікується як шахрайська, що призводить до блокування операції клієнта та погіршення користувацького досвіду. Хибно негативні результати відповідають шахрайським операціям, які модель не змогла виявити та класифікувала як легальні, що призводить до фінансових втрат.

Отже, розроблено метод автоматизованого виявлення шахрайських банківських операцій, який поєднує алгоритм випадкового лісу з технікою балансування класів SMOTE для ефективної роботи з незбалансованими даними. Метод вирішує фундаментальну проблему значної незбалансованості класів через генерацію синтетичних зразків шахрайських транзакцій шляхом лінійної інтерполяції між існуючими зразками в багатовимірному просторі ознак.

Модульна структура методу забезпечує гнучкість у налаштуванні окремих компонентів без необхідності перебудови всієї системи. Метод передбачає можливість адаптації до змін у характері шахрайських операцій шляхом періодичного перенавчання моделі на нових даних та коригування правил класифікації, що є критично важливим для протидії еволюції методів шахрайства у банківській сфері.

Перелік посилань

1. Al-Hashedi, A. Hybrid feature selection framework for enhanced credit card fraud detection // PLOS ONE. – 2025. – Vol. 20, № 7. – DOI: 10.1371/journal.pone.0326975.
2. Relational AI Team. Credit Card Fraud Identification Using Machine Learning on Graphs // Relational AI Resources. – 2024. – URL: <https://relational.ai/resources/credit-card-fraud-detection-machine-learning-graphs>.
3. West, J. A systematic review of AI-enhanced techniques in credit card fraud detection // Journal of Big Data. – 2025. – Vol. 12, № 1. – P. 1-10. – DOI: 10.1186/s40537-024-01048-8.
4. Ryzhanskyi O., Pavlyshyn V., Radiuk P., Manziuk E., Barmak O., Krak I. AI-Driven Traffic Signal Control System to Reduce CO2 Emissions / CEUR Workshop Proc., CEUR-WS, 2025. Pp. 18–27. URL: <https://ceur-ws.org/Vol-3974/paper02.pdf>.
5. Pavlyshyn V., Ryzhanskyi O., Manziuk E., Radiuk P., Barmak O., Krak I. Establishing Patterns of the Urban Transport Flows on Clustering Analysis. In Proceedings of the Second International Conference of Young Scientists on Artificial Intelligence for Sustainable Development (YAISD 2025). 2025. Vol. 3974. Pp. 1–9. URL: <https://ceur-ws.org/Vol-3974/paper01.pdf>.
6. Pavlyshyn V., Manziuk E., Barmak O., Radiuk P., Krak I. An Adaptive Machine Learning Approach to Sustainable Traffic Planning: High-Fidelity Pattern Recognition in Smart Transportation Systems. Future Transportation. 2025. Vol. 5, No. 4. URL: <https://doi.org/10.3390/futuretransp5040152>.
7. Pavlyshyn V., Manziuk E., Barmak O., Radiuk P., Krak I. Adaptive Cascade Clustering for High-Fidelity Urban Traffic Pattern Recognition. Computer Science and Mathematics, 2025. URL: <https://doi.org/10.20944/preprints202508.0637.v1>.
8. Manziuk E. A., Sobko O. V., Podhorniuk I. O., Molchanova M. O., Mazurets O. V. Multifactorial analysis of mobbing behavioral signs in educational environments posts by NLP means. Journal of Physics: Conference Series. 2025. Vol. 3105, No. 1. Pp. 012025. URL: <https://doi.org/10.1088/1742-6596/3105/1/012025>.
9. Chaban O., Manziuk E., Radiuk P. Method of adaptive knowledge distillation from multi-teacher to student deep learning models. Journal of Edge Computing. 2025. URL: <https://doi.org/10.55056/jec.978>.
10. Chaban O., Manziuk E., Markevych O., Petrovskyi S., Radiuk P. EMTKD at the edge: An adaptive multi-teacher knowledge distillation for robust cardiac MRI classification / Proceedings of the 5th Edge Computing Workshop (doors 2025), Zhytomyr, Ukraine, April 04, 2025. Pp. 42–57. URL: <https://ceur-ws.org/Vol-3943/paper09.pdf>.
11. Ryzhanskyi O., Manziuk E., Barmak O., Krak I., Bačanin N. An Approach to Optimizing CO2 Emissions in Traffic Control via Reinforcement Learning. CEUR Workshop Proceedings. 2024. Vol. 3675. Pp. 137–155. URL: <https://ceur-ws.org/Vol-3675/paper10.pdf>.
12. Radiuk P., Barmak O., Manziuk E., Krak I. Explainable Deep Learning: A Visual Analytics Approach with Transition Matrices. Mathematics. 2024. Vol. 12, No. 7. Pp. 1–32. URL: <https://doi.org/10.3390/math12071024>.

УДК 004.8

Іщук-Яшурина С.Я.¹, Кліменко В.І.², Мазурець О.В.²

¹ Комунальний заклад загальної середньої освіти
«Ліцей №7 Хмельницької міської ради»

² Хмельницький національний університет

ПОЯСНЕНИЙ ПІДХІД ДО НЕЙРОМЕРЕЖЕВОЇ КЛАСИФІКАЦІЇ ДІАБЕТИЧНОЇ РЕТИНОПАТІЇ ЗА ЗОБРАЖЕННЯМИ ОЧНОГО ДНА

Робота присвячена поясненній нейромережевій класифікації діабетичної ретинопатії за зображеннями очного дна, орієнтованій на потреби масового скринінгу. Запропоновано підхід, у якому багатокласова модель глибокого навчання доповнюється картами значущості, що візуалізують внесок локальних патологічних змін у класифікаційне рішення та дозволяють зіставити його з офтальмологічною оцінкою. Узгодженість пояснень перевіряється на підбірці зображень з експертною розміткою, що дає змогу виявити залежність моделі від артефактів і підвищити довіру лікарів до автоматизованої системи. Отримані результати формують основу для інтеграції пояснених нейромережевих рішень у клінічні протоколи скринінгу діабетичної ретинопатії.

The study focuses on explainable neural network-based classification of diabetic retinopathy from fundus images in the context of large-scale screening. A multiclass deep learning model is augmented with saliency maps that highlight the contribution of local pathological changes to the final prediction, enabling alignment between automated decisions and ophthalmologists' visual assessment. Consistency of the explanations is evaluated on a subset of images with expert lesion annotations, which helps reveal model dependence on artefacts and increases clinicians' trust in the system. The results provide a basis for integrating explainable deep learning tools into clinical screening protocols for diabetic retinopathy.

Діабетична ретинопатія є однією з провідних причин незворотної втрати зору у працездатному віці, причому клінічно значущі зміни сітківки тривалий час залишаються безсимптомними [1, 2]. Це зумовлює потребу в інструментах раннього виявлення патології на основі зображень очного дна, здатних працювати у масових скринінгових програмах [3]. Традиційні методи скринінгу, що базуються на ручному аналізі зображень очного дна фахівцями-офтальмологами, є трудомісткими, залежними від суб'єктивної оцінки та не завжди здатні задовольнити потреби масового скринінгу у великих популяціях. У цьому контексті автоматизовані методи комп'ютерного зору, зокрема нейромережеві моделі

глибокого навчання, демонструють значний потенціал у швидкому й точному виявленні ознак патологій на ретинальних зображеннях [4].

Використання згорткових нейронних мереж [5, 6] дозволяє ефективно виявляти локальні та глобальні патерни, характерні для різних стадій діабетичної ретинопатії, забезпечуючи багатокласову класифікацію з високою точністю [7, 8]. Пояснювані методи, такі як карти значущості або теплові мапи, доповнюють нейромережеві підходи можливістю ідентифікувати ключові регіони зображення [9], які вплинули на рішення моделі, що робить результати більш прозорими для клінічних спеціалістів. Такий підхід сприяє підвищенню довіри лікарів до автоматизованих систем, дозволяє виявляти потенційні артефакти та помилки моделі, а також забезпечує інтеграцію результатів у існуючі клінічні протоколи.

Загалом, нейромережеві моделі демонструють високу точність класифікації стадій діабетичної ретинопатії, однак їх застосування у клінічній практиці стримується «чорним ящиком» прийняття рішень [10, 11]. Відсутність прозорих пояснень, які б узгоджувались із офтальмологічними уявленнями про морфологічні зміни сітківки, знижує довіру лікарів до автоматизованих систем і ускладнює інтеграцію таких рішень у регламентовані діагностичні протоколи.

Метою роботи є формування поясненого підходу до нейромережевої класифікації діабетичної ретинопатії за зображеннями очного дна, у якому кінцеві діагностичні рішення доповнюються інтерпретованими візуальними та кількісними поясненнями, релевантними клінічній практиці. Для досягнення цієї мети пропонується узгоджена обчислювальна схема, що поєднує попередню нормалізацію та стандартизацію зображень, багатокласову нейромережеву модель класифікації стадій ураження та модулі пояснення, орієнтовані на виявлення та візуалізацію патологічних структур.

На рівні класифікації використовується глибока згорткова або трансформерна архітектура, адаптована до особливостей кольорових фундус-знімків: моделюється глобальний стан сітківки та локальні патологічні утворення, зокрема мікроаневризми, крововиливи, тверді й м'які ексудати, неоваскуляризація. Балансування навчальної вибірки, підбір аугментацій та контроль якості вхідних зображень спрямовані на стабілізацію роботи моделі для різних джерел даних і оптичних систем. Вихідною величиною є не лише класова мітка стадії діабетичної ретинопатії, а й вектор впевненостей, що надалі використовується у модулі пояснення.

Поясненість досягається за рахунок поєднання локальних і глобальних інтерпретацій. Локальні пояснення формуються у вигляді карт значущості, побудованих методами градієнтно-активаційної візуалізації та інтегрованих градієнтів. Такі карти проєктуються на вихідне зображення очного дна, виділяючи

ділянки, що найбільше вплинули на віднесення до певної стадії, та дозволяють лікарю співвіднести нейромережеве рішення з реальною локалізацією патологічних змін. Глобальні пояснення реалізуються на основі агрегованого аналізу багатьох зображень: оцінюються типові патерни активації моделі для кожного класу, характерні ділянки сітківки, які найчастіше виявляються релевантними, а також розподіл значущості між основними морфологічними ознаками.

Важливим компонентом поясненого підходу є перевірка узгодженості пояснень з експертною офтальмологічною оцінкою. Для цього передбачається формування підвибірки зображень з незалежною розміткою патологічних утворень лікарями-експертами. На цій підвибірці аналізується ступінь накладання карт значущості на вручну позначені області інтересу, а також якісно оцінюється відповідність візуалізованих патернів очікуваній клінічній картині. Такий підхід дозволяє виявляти випадки, коли модель досягає прийнятних метрик точності за рахунок небажаних «шорткатів», пов'язаних не з патологією, а з артефактами зображення чи особливостями збору даних.

Запропонована концепція поясненої нейромережевої класифікації діабетичної ретинопатії створює підґрунтя для розроблення клінічно орієнтованих систем підтримки прийняття рішень, у яких високі показники автоматизованого розпізнавання поєднуються з прозорістю, відтворюваністю та можливістю експертного контролю. Очікується, що інтеграція таких систем у скринінгові програми сприятиме ранньому виявленню пацієнтів з ризиком прогресування діабетичної ретинопатії, підвищенню ефективності направлення до офтальмолога та оптимізації використання ресурсів охорони здоров'я, зберігаючи при цьому ключову роль лікаря в інтерпретації та верифікації результатів

Перелік посилань

1. Muthusamy, D., & Palani, P. (2024). Deep learning model using classification for diabetic retinopathy detection: an overview. *Artificial Intelligence Review*, 57(7), 185.
2. Youldash, M., Rahman, A., Alsayed, M., Sebiany, A., Alzayat, J., Aljishi, N., ... & Alqahtani, M. (2024). Early Detection and Classification of Diabetic Retinopathy: A Deep Learning Approach. *AI*, 5(4).
3. Thanikachalam, V., Kabilan, K., & Erramchetty, S. K. (2024). Optimized deep CNN for detection and classification of diabetic retinopathy and diabetic macular edema. *BMC Medical Imaging*, 24(1), 227.
4. Saproo, D., Mahajan, A. N., & Narwal, S. (2024). Deep learning based binary classification of diabetic retinopathy images using transfer learning approach. *Journal of Diabetes & Metabolic Disorders*, 23(2), 2289-2314.
5. Mushtyn O., Sobko O., Molchanova M., Mazurets O. Convolutional Neural Network Architecture for Image-Based Architectural Style Recognition. *Evolving Science: Theories*,

- Discoveries and Practical Outcomes. Proceedings of 4th International Scientific and Practical Conference. June 9-11, 2025. Zurich, Switzerland. Pp. 130-143.
6. Hladun O.V., Molchanova M.O., Zalutska O.O., Mazurets O.V. Effectiveness research of using ViT neural network architecture for classifying the destroyed buildings remains. Achievements of Science and Applied Research. Proceedings of 2nd International Scientific and Theoretical Conference. May 19-21, 2025. Dublin, Ireland. Pp. 96-100.
7. Malaydakh V., Molchanova M., Shevchuk P., Mazurets O. Deep learning neural network architecture for determining sunflower growth stage from visual data. Modern Scientific Research: Theoretical and Practical Aspects. Proceedings II International Scientific and Practical Conference. May 26-28, 2025. Riga, Latvia. Pp. 143-148.
8. Дідур В.О., Молчанова М.О., Мазурець О.В. Спосіб виявлення та класифікації залишків зруйнованих будівель та будівельного сміття за фотографіями з використанням моделей CNN. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №1 (42). С. 1162-1175.
9. Pokhytun A., Mazurets O., Molchanova M., Tyschenko O. Method for Neural Network Detecting Changed Images of People's Faces Using CNN. New Horizons in Scientific Research: Challenges and Solutions. Proceedings of the 1st International scientific and practical conference. October 21-23, 2024. Marseille, France. 2024. Pp. 35-40.
10. Mazurets O. V., Klimenko V. I., Molchanova M. O., Sultanov A. V. Object-Oriented Intelligent System for Neural Network Detection of Sugar Crystallization Zones. Global Science: Prospects and Innovations. Proceedings of the 10th International scientific and practical conference. Cognum Publishing House. Liverpool, United Kingdom. 2024. Pp. 198-207.
11. Запорожець М.В., Молчанова М.О., Скрипник Т.К. Метод виявлення патологій мозку за зображеннями магнітно-резонансної терапії нейромережевими засобами. Збірник наукових праць за матеріалами XV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2023». Хмельницький, 2023. с. 108-110.

УДК 004.8

Кадинська В.Д., Молчанова М.О.

Хмельницький національний університет

АДАПТОВАНИЙ НЕЙРОМЕРЕЖЕВИЙ ПІДХІД ДО ВИЯВЛЕННЯ ФРАГМЕНТІВ БУДІВЕЛЬНИХ ВІДХОДІВ НА ЗОБРАЖЕННЯХ РЕАЛЬНИХ СЦЕН

У роботі розглянуто задачу автоматизованого виявлення фрагментів будівельних відходів на зображеннях реальних сцен, актуальну в контексті післявоєнної відбудови та зростання навантаження на системи управління відходами. Показано обмеженість класичних алгоритмів комп'ютерного зору, що ґрунтуються на порогових правилах та сконструйованих вручну ознаках, у сценах зі складним фоном, змінним освітленням і частковими перекриттями. Запропоновано адаптований нейромережевий підхід на основі одностадійного детектора YOLO.

The paper addresses the problem of automated detection of construction and demolition waste fragments in real-world images, which is highly relevant in the context of post-war reconstruction and increasing pressure on municipal waste management systems. It is shown that classical computer vision approaches based on hand-crafted features, thresholding and simple morphological rules are unreliable in scenes with complex backgrounds, varying illumination and partial occlusions. An adapted deep learning approach based on a one-stage YOLO detector is proposed.

Інтенсивне зростання обсягів будівництва, реконструкції та демонтажу об'єктів інфраструктури, а також масштабні процеси післявоєнної відбудови сформували якісно новий контекст для задач моніторингу будівельних відходів [1, 2]. Потоки уламків конструкцій, змішаного будівельного сміття та вторинних матеріалів дедалі частіше розподіляються у просторі нерівномірно, виникають стихійні скупчення, тимчасові склади, локальні звалища на периферійних територіях [3, 4]. За таких умов ефективне управління будівельними відходами потребує не лише регламентів і логістичних рішень, а й інструментів автоматизованого виявлення зон накопичення за візуальними даними, здатних працювати у реалістичних сценах із неконтрольованими умовами зйомки [5].

Швидке зростання обсягів будівельних відходів та необхідність їх ефективного виявлення у середовищах реального світу роблять задачі автоматизованої візуальної ідентифікації особливо актуальними. Традиційні методи контролю стану будівельних майданчиків і територій після демонтажів є

трудомісткими, потребують значних людських ресурсів та характеризуються низькою оперативністю. Використання комп'ютерного зору в поєднанні з глибокими нейронними мережами відкриває можливості створення автоматичних систем моніторингу, здатних ідентифікувати фрагменти будівельних відходів на зображеннях із високою точністю навіть у складних умовах освітлення, за варіантності форм, кольорів та фону.

Згорткові нейронні мережі є ключовою технологією для задач класифікації [6], сегментації [7] та детекції об'єктів на зображеннях [8]. Їхня здатність навчатись інваріантним до масштабу та поворотів ознакам дозволяє моделювати складну структуру будівельних відходів – уламків бетону, дерева, металевих конструкцій, мінеральної вати тощо. Однак реальні сцени містять значну кількість шумів [9], неоднорідний фон [10] та різноманітні погодні або технічні фактори [11], що впливають на якість зображень, тому актуальними стають адаптовані нейромережеві підходи, орієнтовані на роботу з даними такої варіативності [12]. Модифіковані CNN-архітектури, доповнені attention-модулями або багаторівневими фіч-блоками, здатні підвищувати точність локалізації та розпізнавання дрібних або частково перекритих об'єктів [13, 14].

Класичні підходи комп'ютерного зору, що спираються на сконструйовані вручну ознаки, порогове виділення областей інтересу [15], прості морфологічні перетворення та евристичні правила, виявляються нестійкими до складного фону, змінного освітлення, затінених ділянок і часткових перекриттів об'єктів. Будівельні відходи характеризуються великою варіативністю форм, розмірів, кольорів і фактур, можуть бути частково вкриті ґрунтом, снігом або рослинністю, змішуватися з побутовим сміттям і природними об'єктами [16]. Це призводить до того, що традиційні алгоритми мають або надмірно жорсткі налаштування, які пропускають значну частину уламків, або надто чутливі параметри, що генерують численні хибнопозитивні спрацювання.

На цьому тлі очевидною стає доцільність використання глибоких нейромережевих детекторів, які поєднують у собі автоматичне виділення ознак і локалізацію об'єктів. Одностадійні детектори типу YOLO зарекомендували себе як придатні для задач, де необхідне поєднання прийнятної точності та високої швидкодії, включно з аналізом відеопотоків у реальному часі. Однак без доменно-орієнтованої адаптації навіть сучасні архітектури демонструють лише обмежену якість виявлення будівельних відходів, оскільки базові набори даних для їх попереднього навчання не містять специфічної категорії «фрагменти будівельних уламків», а візуальні ознаки цих об'єктів часто маскуються складним фоном [17].

Проблема ускладнюється тим, що в операційному сенсі первинним завданням для муніципальних служб і систем підтримки прийняття рішень є не

стільки детальна класифікація матеріалів, скільки надійне виявлення самих зон накопичення будівельного сміття. На початковому етапі аналізу важливіше сформувати карту регіонів, де присутні значущі обсяги будівельних відходів, ніж відразу розрізняти бетон, цеглу, дерево чи метал [18]. Це обґрунтовує підхід, за якого нейромережевий детектор налаштовується на бінарну постановку «фрагмент будівельних відходів / фон», а деталізація матеріалів може розглядатися як наступний рівень аналізу, що виходить за межі даних тез.

Мета роботи полягає у розробленні, обґрунтуванні та експериментальній перевірці адаптованого нейромережевого підходу до виявлення фрагментів будівельних відходів на зображеннях реальних сцен із використанням одностадійного детектора YOLO, який спеціально донавчається на основі ручної дорозмітки зразків. Під адаптацією у даному контексті розуміється не лише формальне трансферне навчання з повторним налаштуванням ваг моделі, а й цілеспрямоване переформулювання задачі, уточнення критеріїв віднесення об'єктів до цільового класу, побудова збалансованого навчального набору, розроблення процедури поетапної ручної корекції розмітки та узгодження параметрів аугментації з реальними умовами експлуатації.

Дослідження базується на колекції зображень, отриманих у реалістичних умовах: на будівельних майданчиках, у зонах демонтажу зруйнованих споруд, на тимчасових складах будівельних відходів, а також на ділянках міського середовища, де будівельне сміття змішується з іншими типами відходів. Джерела візуальних даних включають знімки, отримані з рівня землі на мобільні пристрої та цифрові камери, а також окремі кадри з відеопотоків. У вибірці присутні сцени з різною щільністю відходів, різним масштабом об'єктів і широтою поля зору, що імітує спектр практичних сценаріїв від детального огляду окремих ділянок до узагальнених панорам. В межах підходу виконувалась ідентифікація класів, наведених на рисунку 1.

Особливе значення в рамках запропонованого підходу має процедура ручної дорозмітки. Початкова розмітка формувалася за схемою, близькою до спрощених евристичних правил, коли оператори виділяли у кадрі домінантні скупчення уламків із мінімальною деталізацією меж. Така розмітка виявилася недостатньо точною, оскільки значна частина рамок включала великі фрагменти фону, а дрібні уламки, які з точки зору експлуатаційних потреб є суттєвими, часто залишалися неврахованими. Для подолання цих обмежень було застосовано поетапний підхід: використовуючи попередньо навчену базову модель YOLO, на зображеннях генерувалися первинні пропозиції областей інтересу, після чого експерти вручну коригували межі рамок, вилучали очевидні хибнопозитивні

спрацювання, додавали пропущені фрагменти, що мають явно виражені ознаки будівельних відходів.

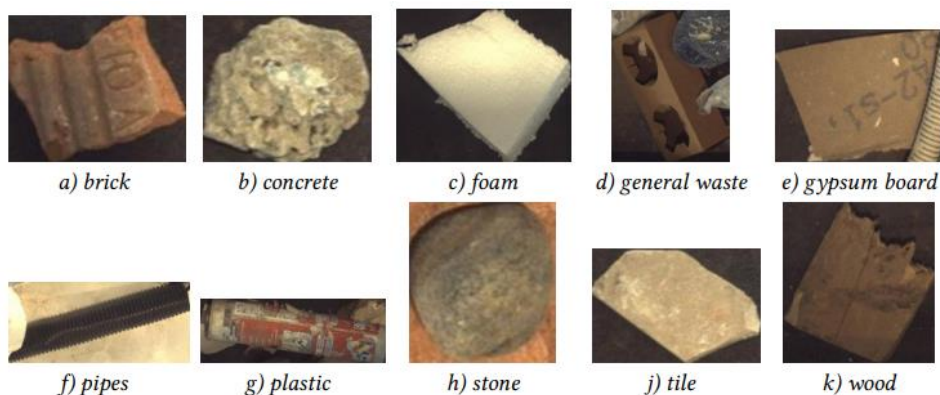


Рисунок 1 – Види будівельних відходів для ідентифікації

Ручна дорозмітка супроводжувалася детально розробленим протоколом, спрямованим на узгодженість і відтворюваність рішень між різними анотаторами. Було сформульовано критерії віднесення об'єкта до фрагмента будівельного сміття, де підкреслювалася необхідність фокусування на уламках конструкцій, які мають реальне значення з точки зору логістики прибирання та вторинної переробки. Надто дрібні часточки, пилові утворення та неоднозначні текстурні вclusions не позначалися як окремі об'єкти, аби не перевантажувати модель шумовими прикладами. Натомість структурні уламки цегли, бетону, плитки, дерев'яних елементів, металевих деталей і змішаних фрагментів розглядалися як цільові об'єкти, навіть якщо вони були частково перекриті іншими предметами або частково заглиблені у ґрунт.

Для забезпечення контролю якості розмітки застосовувався підхід, близький до експертної валідації. Вибірка анотованих зображень перевірялася незалежним експертом, який оцінював повноту охоплення уламків, точність позиціонування рамок та відсутність систематичних перекосів, наприклад, систематичної відмови від позначення певних типів матеріалів. За необхідності виконувалася повторна корекція найпроблемніших знімків, що дозволило сформувати підмножину високоякісних еталонних прикладів, придатних для подальшого трансферного навчання.

На основі підготовленого датасету було здійснено адаптацію базової моделі YOLO у режимі трансферного навчання. Вихідні ваги, отримані під час

попереднього навчання на універсальних наборах даних, використовувалися як початкова точка, що забезпечує загальну здатність моделі виділяти вузли, межі та текстурні патерни. На першому етапі навчання фіксувалися всі глибинні шари, відповідальні за низькорівневе та середньорівневе виділення ознак, тоді як оновленню підлягали лише параметри «голови» детектора, які контролюють формування рамок і бінарне рішення щодо наявності цільового об'єкта. Такий режим дозволяє швидко адаптувати модель до нової предметної області без значного ризику руйнування попередньо сформованого простору ознак.

Подальші етапи адаптації передбачали поступове «розморожування» частини проміжних шарів. Це дало змогу гнучкіше підлаштувати репрезентації під специфіку будівельних відходів, що мають характерні, але водночас різноманітні текстури. Для уникнення перенавчання було застосовано регуляризаційні прийоми, зокрема вагове згасання та контрольовану інтенсивність аугментації. Розмір входу детектора, параметри сітки передбачень і порогові значення для коефіцієнта перетину над об'єднанням налаштовувалися з урахуванням того, що цільові об'єкти можуть бути як відносно великими, так і дрібними, але операційно значущими.

Процес навчання супроводжувався цілеспрямованим застосуванням аугментації даних. Варіювалися яскравість, контраст, насиченість і колірний відтінок зображень, що моделювало різні погодні та освітлювальні умови, характерні для відкритих міських сцен. Використовувалося масштабування із збереженням пропорцій і подальшим довільним обрізанням, завдяки чому модель навчалася працювати з різними масштабами і ракурсами відносно зон накопичення відходів. Легке розмиття та шум дозволяли імітувати знижену якість зображення, властиву кадрам із відеопотоків камер спостереження або дронів. При цьому параметри аугментації підбиралися таким чином, щоб не зруйнувати ті ознаки, які є ключовими для відокремлення будівельних уламків від фону.

Оцінювання якості адаптованої моделі проводилося на відкладеній тестовій вибірці, яка формувалася з урахуванням різноманітності сцен і не брала участі в процесі навчання. Основними кількісними показниками слугували середня точність виявлення при фіксованому пороговому значенні коефіцієнта перетину над об'єднанням, повнота детекції та узагальнена оцінка, що характеризує баланс між пропусками та хибнопозитивними спрацюваннями. Додатково аналізувалися сценарії, де будівельні відходи займають значну частину кадру, і сценарії, де вони розташовані фрагментарно та змішуються з іншими об'єктами міського середовища. Такий розріз дозволив отримати уявлення про стабільність роботи моделі в умовах різної складності сцени.

Отримані результати засвідчили, що адаптація через ручну дорозмітку та поетапне донавчання призводить до помітного підвищення якості виявлення

порівняно з базовою моделлю без фахової адаптації. У сценах із неоднорідним фоном і частковими перекриттями фрагментів було зафіксовано зростання повноти детекції за збереження прийнятного рівня точності, що є критичним для задач моніторингу, де небажаними є пропуски значущих скупчень відходів. Зменшилася кількість хибних спрацювань на природних структурах, таких як каміння, оголені корені дерев або уламки асфальту, які на етапі попередніх експериментів часто помилково трактувалися як будівельне сміття.

Якісний аналіз типових помилок показав, що найбільшу складність для моделі становлять сцени, де фрагменти будівельних відходів частково вкриті ґрунтом, снігом або шаром пилу, а також зони з сильними відбиттями сонячного світла на металевих поверхнях. У таких випадках текстурні ознаки стають менш інформативними, а локальні перенасичення або провали яскравості ускладнюють процес виділення контурів об'єктів. Частина помилок пов'язана з дрібними фрагментами, які за розміром наближаються до шумових кластерів пікселів, і потребує або зміни параметрів сітки детектора, або залучення методів, орієнтованих на виявлення дуже малих об'єктів.

Важливим компонентом дослідження стало оцінювання обчислювальної доцільності запропонованого підходу. Одностадійна природа детектора YOLO дозволяє застосовувати адаптовану модель у режимах, близьких до реального часу, що відкриває можливості інтеграції в системи відеоспостереження, мобільні додатки для польових інспекторів, програмні комплекси для аналізу даних з безпілотних літальних апаратів. У роботі було проаналізовано варіанти розгортання моделі як на серверних обчислювальних вузлах, так і на відносно обмежених апаратних платформах. Встановлено, що за певної оптимізації параметрів і використання полегшених модифікацій архітектури модель може бути придатною для застосування у розподілених системах моніторингу, де частина попередньої обробки виконується на периферійних пристроях, а детальніший аналіз здійснюється на центральному сервері.

Адаптований неймерережевий підхід, описаний у роботі, можна розглядати як базовий рівень ширшої системи підтримки прийняття рішень у сфері управління будівельними відходами. Первинне автоматизоване виявлення зон із наявністю уламків формує вхідну інформацію для модулів, які оцінюють динаміку накопичення відходів, моделюють навантаження на інфраструктуру вивезення та переробки, аналізують дотримання екологічних обмежень у різних районах. Наявність достовірних карт виявлених зон будівельного сміття полегшує планування маршрутів спецтехніки, дозволяє оперативно виявляти стихійні звалища, підтримує прозорість контролю за діяльністю підрядних організацій.

Перспективи подальших досліджень пов'язані з декількома важливими напрямками. Одним із них є розширення й диверсифікація навчального набору шляхом включення даних із різних географічних регіонів, сезонів та типів забудови, що має підвищити узагальнюваність моделі. Іншим перспективним напрямом є інтеграція додаткових модальностей, зокрема використання глибинної інформації або даних тепловізійних камер, які допомогли б відокремлювати об'єкти з різною фізичною структурою за непрямими ознаками. Не менш актуальним є дослідження підходів до активного навчання, коли модель, розгорнута в експлуатаційному середовищі, пропонує оператору для ручної дорозмітки найінформативніші кадри, що дозволить із мінімальними зусиллями підтримувати її актуальність за умови змінних сценаріїв застосування.

Таким чином, результати проведеного дослідження демонструють, що поєднання сучасних одностадійних нейромережових детекторів із ретельно організованою процедурою ручної дорозмітки та трансферного навчання дає змогу сформувати адаптований інструмент для виявлення фрагментів будівельних відходів на зображеннях реальних сцен. Ретельно опрацьована анотація даних, узгодженість критеріїв виділення цільових об'єктів і доменно орієнтована адаптація моделі виявляються ключовими чинниками, що визначають стабільність і практичну корисність системи, часто не менш важливими, ніж вибір конкретної архітектури нейромережі. Запропонований підхід може слугувати основою для побудови комплексних рішень моніторингу будівельних відходів у контексті сталої урбаністичної політики та післявоєнної відбудови.

Перелік посилань

1. Zhuang, Z., Bi, J., & Wang, F. (2020). The Whole Process Management Monitoring and Control of Construction Waste. In IOP Conference Series: Earth and Environmental Science (Vol. 435, No. 1, p. 012001). IOP Publishing.
2. Cha, G. W., Kim, Y. C., Moon, H. J., & Hong, W. H. (2017). The effects of data collection method and monitoring of workers' behavior on the generation of demolition waste. *International journal of environmental research and public health*, 14(10), 1216.
3. Lu, W., Chen, X., Peng, Y., & Shen, L. (2015). Benchmarking construction waste management performance using big data. *Resources, Conservation and Recycling*, 105, 49-58.
4. Yuan, H., Lu, W., & Hao, J. J. (2013). The evolution of construction waste sorting on-site. *Renewable and Sustainable Energy Reviews*, 20, 483-490.
5. Bang, S., & Andersen, B. S. (2022). Utilising artificial intelligence in construction site waste reduction.
6. Кліменко В.І., Собко О.В., Мазурець О.В., Кадинська В.Д. Алгоритми та програмна архітектура експертної системи з продукційною моделлю подання знань. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №9 (50). С. 1252-1264.

7. Дидо Р.А., Мазурець О.В. Метод ідентифікації особистості на основі розпізнавання обличчя в реальному часі для систем кібербезпеки. Інформаційна, функційна і кібербезпека СКІФіК2024. Матеріали IV Всеукраїнської науково-технічної конференції. 29-30 листопада 2024. Харків. 2024. с. 36-37.
8. Молчанова М.О., Дідур В.О., Мазурець О.В., Тищенко О.О., Залуцька О.О. Інформаційна технологія використання хмарних обчислень для класифікації залишків зруйнованих будівель засобами нейронних мереж за візуальними даними з безпілотних літальних апаратів. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №4 (45). С. 1259-1272.
9. Мазурець О.В., Жарновський О.В., Гладун О.В., Собко О.В. Нейромережеве виявлення фейкових зображень людей. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2025. №5. Т.1. С. 416-422.
10. Мазурець О.В., Собко О.В., Дидо Р.А., Молчанова М.О., Тищенко О.О. Проєктування структури бази даних для інтелектуальної системи нейромережевого виявлення та локалізації на фотозображеннях ділянок із залишками зруйнованих будівель. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №4 (45). С. 1242-1258.
11. Похитун А.В., Мазурець О.В., Молчанова М.О., Бармак О.В. Підхід до формування датасету для нейромережевого виявлення модифікованих фотографій обличчя людей. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». 15-16 листопада 2024. Хмельницький, 2024. с. 428-433.
12. Мазурець О.В., Петровський С.С., Дидо Р.А. Нейромережева модель для ідентифікації особистості за зображенням обличчя у реальному часі Інформаційні технології і автоматизація. Матеріали XVII міжнародної науково-практичної конференції. 31 жовтня – 1 листопада 2024 р. Одеса, ОНТУ. 2024. С.655-658.
13. Похитун А.В., Мазурець О.В., Дидо Р.А., Молчанова М.О. Програмна архітектура для нейромережевого виявлення модифікованих фотографій обличчя людей. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2025. №3. Т.2. С. 493-500.
14. Молчанова М.О., Мазурець О.В., Шурипа М.О. Об'єктно-орієнтований підхід до нейромережевого виявлення та відстеження БПЛА з використанням хмарних технологій. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №9 (50). С. 1346-1360.
15. Мазур Є.В., Мазурець О.В., Кліменко В.І., Собко О.В., Залуцька О.О. Алгоритми та програмна архітектура інформаційної системи нейромережевого аналізу постави людини. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2025. №3. Т.1. С. 275-284.
16. Собко О.В., Кліменко В.І., Мазурець О.В., Залуцька О.О., Гладун О.В. Особливості програмної інженерії та тестування програмного забезпечення для нейромережевого аналізу фотоданих залишків зруйнованих будівель із роботизованої техніки. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №4 (45). С. 1566-1581.
17. Molchanova M., Didur V., Mazurets O., Sobko O., Zakharkevich O. Method for Construction and Demolition Waste Classification Using Two-Factor Neural Network Image Analysis. CEUR Workshop Proceedings, 2025, vol. 3970, pp. 168-182.
18. Дідур В.О., Молчанова М.О., Мазурець О.В. Спосіб виявлення та класифікації залишків зруйнованих будівель та будівельного сміття за фотографіями з використанням моделей CNN. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №1 (42). С. 1162-1175.

УДК 004.8

Казмірчук Я.М., Микитюк М.О., Мазурець О.В.

Хмельницький національний університет

АЛГОРИТМ МАСШТАБУВАННЯ ЗОБРАЖЕНЬ ПРИНТІВ НЕЙРОМЕРЕЖЕВИМИ ЗАСОБАМИ ДЛЯ ТРАФАРЕТНОГО ДРУКУ

Запропоновано нейромережевий алгоритм масштабування зображень текстильних принтів, орієнтований на вимоги промислового трафаретного друку щодо роздільної здатності та чіткості контурів. Алгоритм інтегрується в конвеєр препресу між сегментацією принта та етапами кольороподілу, поєднуючи нормалізацію зображення, виділення «чистої» області принта, суперрезолюцію на основі CNN ESPCN та контурно-орієнтовану постобробку. Експериментальні результати на корпоративному наборі принтів показали суттєве підвищення чіткості дрібних деталей, стабільності контурів і сумісності з подальшими етапами кольороподілу порівняно з класичними методами інтерполяції. Розроблене рішення зменшує залежність від ручного масштабування й ретуші та створює передумови для більш повної автоматизації тракту «цифровий макет – друкарський шар».

A neural network-based algorithm for scaling textile print images is proposed, tailored to the industrial screen-printing requirements for spatial resolution and contour sharpness. The algorithm is integrated into the prepress pipeline between print segmentation and colour separation, combining image normalization, extraction of the “clean” print area, super-resolution via a lightweight ESPCN CNN, and contour-oriented post-processing. Experiments on a corporate print dataset demonstrate a substantial improvement in fine-detail clarity, contour stability, and compatibility with downstream colour separation compared to classical interpolation-based scaling. The proposed solution reduces reliance on manual resizing and retouching and paves the way toward more complete automation of the “digital artwork–printing layer” workflow.

Сучасна текстильна індустрія дедалі активніше переходить до цифровізованих виробничих циклів, у яких ключові етапи препресу мають бути максимально автоматизованими, відтворюваними та незалежними від суб'єктивних рішень оператора [1]. Однією з критичних задач у цьому контексті є масштабування зображень принтів для трафаретного друку [2], оскільки вимоги до роздільної здатності, чіткості контурів та коректності дрібних елементів безпосередньо впливають на якість друкарського шару та стабільність процесу кольороподілу [3]. Традиційні методи масштабування на основі інтерполяції часто не здатні забезпечити достатній рівень деталізації, що ускладнює подальшу підготовку друкарських форм, спричиняє появу артефактів на межах кольорів та потребує значного обсягу ручної ретуші [4].

У цих умовах методи комп'ютерного зору [5], а особливо нейронні мережі для суперрезолюції зображень [6, 7], відкривають можливості якісно нового рівня обробки дизайнерських принтів. Архітектури типу CNN [8] здатні не лише підвищувати номінальну роздільну здатність зображення [9], а й відновлювати структурні особливості текстильних патернів, що є принциповим для технологічної точності трафаретного друку. Глибокі моделі демонструють здатність адаптуватися до різних стилів принтів, зберігати локальні контурні характеристики та мінімізувати спотворення [10], які критичні для подальших етапів кольороподілу.

Перспективи використання нейромережових підходів у даному напрямку пов'язані з їхньою здатністю формувати стійкі та стандартизовані робочі процеси [11, 12], інтегровані у виробничий конвеєр [13]. Поєднання сегментації принтів, нормалізації, суперрезолюції та контурно-орієнтованої корекції створює основу для комплексної автоматизації препресу, зменшення ризиків браку й оптимізації витрат часу на підготовку друкарських форм [14]. Використання CNN-моделей також відкриває шлях до створення адаптивних систем препресу, що можуть враховувати тип матеріалу, очікувані характеристики друку та специфіку дизайну, забезпечуючи стабільну якість друку незалежно від складності вхідного зображення.

Важливим є і те, що сучасні глибокі моделі [15, 16] здатні враховувати статистичні властивості реальних корпоративних наборів принтів, адаптуючись до стилістичних особливостей конкретного виробництва. Це відкриває можливість створення кастомізованих моделей суперрезолюції [17], які оптимізуються не лише на абстрактні метрики якості, а й на критерії технологічної сумісності зі специфічними процесами кольороподілу та виготовлення трафаретних форм. Відмова від універсальних інтерполяційних методів [18] на користь спеціалізованих нейромережових рішень [19, 20] дає змогу значно скоротити потребу в ручному коригуванні, зменшити кількість помилок на препрес-етапі та забезпечити прогнозованість результатів друку.

Цифрова підготовка макетів до трафаретного друку висуває жорсткі вимоги до роздільної здатності й чіткості контурів принта: растрові зображення, отримані зі стандартних дизайнів або веб-ресурсів, часто мають недостатню якість для прямого перенесення на друкарські шари. Традиційні методи масштабування (bilinear, bicubic) згладжують дрібні деталі, «розмивають» краї елементів і призводять до втрати дрібного штриха, що безпосередньо позначається на якості трафаретів і збільшує частку ручної дорисовки. Це зумовлює потребу у спеціалізованому алгоритмі масштабування зображень принтів, орієнтованому саме на задачі промислового трафаретного друку та інтегрованому в загальний нейромережовий конвеєр препресу.

Метою роботи є розроблення нейромережового алгоритму масштабування зображень принтів, який забезпечує збільшення роздільної здатності збереженням різкості контурів і текстурних елементів, узгоджене з технологічними параметрами трафаретного друку (розмір сітки, мінімальна товщина лінії, допуски суміщення).

Алгоритм розглядається як окремий модуль у складі системи автоматизованої підготовки друкарських шарів, що працює після сегментації принта та до етапів кольороподілу й формування трафаретів.

Запропонований алгоритм включає кілька послідовних кроків. На етапі попередньої обробки виконується нормалізація яскравості й кольору, пригнічення шумів та приведення вхідного зображення до уніфікованого робочого формату. Для відокремлення принта від фону тканини використовуються результати попередньої сегментації (нейромережеві моделі класу SAM або аналогічні), що дозволяє працювати з «чистою» областю принта без складок, тіней і сторонніх об'єктів. На цій масці формується набір фрагментів-тайлів із фіксованим розміром, які далі подаються на вхід моделі суперрезолюції.

Ядром алгоритму є легковагова CNN-архітектура типу ESPCN, адаптована до домену текстильних принтів [21]. Мережа навчається відновлювати високороздільні фрагменти принта за їх даунсемпльованими версіями з урахуванням характерних властивостей трафаретної графіки: різких переходів між заливками, наявності дрібного растрового «зерна» та тонких ліній. Для цього формуються навчальні пари «HR–LR» з високоякісних зображень принтів, отриманих у максимально можливій роздільності, після чого до них застосовується контрольоване пониження роздільної здатності з моделюванням типових артефактів (розмиття, JPEG-компресія). Навчання спрямоване на мінімізацію комбінованої функції втрат, що поєднує піксельні метрики (MSE) з структурними показниками подібності, орієнтованими на збереження контуру.

На етапі інференсу зображення принта розбивається на перекривні тайли, кожен з яких проходить через нейромережевий блок суперрезолюції з заданим коефіцієнтом масштабування. Після цього результати збираються в єдине зображення з використанням згладжування в зонах перекриття для уникнення швів. Додатково застосовується контурно-орієнтована постобробка, яка коригує поодинокі спотворення на краях заливок та шрифтових елементів, забезпечуючи технологічно коректні границі для подальшого формування трафаретних масок.

Експериментальна перевірка алгоритму на корпоративному наборі принтів показала, що нейромережева суперрезолюція дозволяє суттєво підвищити візуальну чіткість дрібних деталей і стабільність контурів порівняно з класичними інтерполяційними методами. Масштабовані зображення демонструють кращу сумісність із подальшим кольороподілом і кластеризацією, зменшується потреба у ручній ретуші дрібних дефектів, а відтворюваність дрібного штриха на готових трафаретах підвищується. Інтеграція алгоритму в уже наявний конвеєр препроцесингу, сегментації, кластеризації кольорів та генерації друкарських шарів підтвердила його придатність для роботи в умовах реального виробництва.

Таким чином, розроблений алгоритм масштабування зображень принтів нейромережевими засобами формує спеціалізований інструмент для трафаретного друку, який поєднує доменно адаптовану суперрезолюцію, сегментаційну підтримку та контурно-орієнтовану постобробку. Він зменшує залежність від

ручного масштабування й ретуші, підвищує точність і відтворюваність препрес-процесів, створює передумови для подальшої повної автоматизації тракту «цифровий макет – друкарський шар» у текстильній промисловості. Подальший розвиток пов'язується з розширенням навчального корпусу за рахунок реальних виробничих сцен, впровадженням метризованих критеріїв оцінки якості саме з позицій графаретного друку та інтеграцією алгоритму з модулями інтелектуального кольороподілу.

Перелік посилань

1. Guidelines for using print production standards. Committee. URL: <https://committee.iso.org/files/live/sites/tc130/files/Resources/Guidelines%20for%20using%20print%20production%20standards%20v2%20Jan%202024.pdf>
2. A Fabric Defect Segmentation Model Based on Improved Swin-Unet with Gabor Filter / H. Xu et al. Applied Sciences. 2023. Vol. 13, no. 20. P. 11386. URL: <https://doi.org/10.3390/app132011386>
3. Adaloglou N., Michels F., Kalisch H., Kollmann M. Exploring the limits of deep image clustering using pretrained models // arXiv preprint arXiv:2303.17896. – 2023. – URL: <https://papers.bmvc2023.org/0297.pdf>
4. Nay D. J. B. Single Image Super Resolution using ESPCN – With SSIM Loss. SSRN Electronic Journal. 2021. URL: <https://doi.org/10.2139/ssrn.3898913>
5. Мазурець О.В., Жарновський О.В., Гладун О.В., Собко О.В. Нейромережеве виявлення фейкових зображень людей. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2025. №5. Т.1. С. 416-422.
6. Молчанова М.О., Мазурець О.В., Шурипа М.О. Об'єктно-орієнтований підхід до нейромережевого виявлення та відстеження БПЛА з використанням хмарних технологій. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №9 (50). С. 1346-1360.
7. Мазур Є.В., Мазурець О.В., Кліменко В.І., Собко О.В., Залуцька О.О. Алгоритми та програмна архітектура інформаційної системи нейромережевого аналізу постави людини. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2025. №3. Т.1. С. 275-284.
8. Kok I.A., Kadynska V.D., Zalutska O.O., Mazurets O.V. Object-Oriented Intelligent System for Automated Control of Smoking by Video Data. Current scientific goals, approaches and challenges. Proceedings of IV International Scientific and Theoretical Conference. June 13, 2025. Dresden, Federal Republic of Germany. Pp. 156-164.
9. Bas I.S., Kadynska V.D., Klimenko V.I., Mazurets O.V. Convolutional Neural Network Transfer Learning Method for Aircraft Image Classification. Scientific method: reality and future trends of researching. Proceedings of VI International Scientific and Theoretical Conference. June 6, 2025. Montreal, Canada. Pp. 147-155.
10. Mushtyn O., Sobko O., Molchanova M., Mazurets O. Convolutional Neural Network Architecture for Image-Based Architectural Style Recognition. Evolving Science: Theories, Discoveries and Practical Outcomes. Proceedings of 4th International Scientific and Practical Conference. June 9-11, 2025. Zurich, Switzerland. Pp. 130-143.
11. Malaydakh V., Molchanova M., Shevchuk P., Mazurets O. Deep learning neural network architecture for determining sunflower growth stage from visual data. Modern Scientific Research: Theoretical and Practical Aspects. Proceedings II International Scientific and Practical Conference. May 26-28, 2025. Riga, Latvia. Pp. 143-148.

12. Ostapchenko N., Tyschenko O., Denysenko B., Mazurets O. Semantic search of relevant images using vector databases. Modern Scientific Research: Theoretical and Practical Aspects. Proceedings II International Scientific and Practical Conference. May 26-28, 2025. Riga, Latvia. Pp. 161-165.
13. Dydo R., Sobko O., Klimenko V., Mazurets O. Datalogic structure for intelligent system for areas localization in photos with the remains of buildings using neural network. Modern Scientific Research: Theoretical and Practical Aspects. Proceedings II International Scientific and Practical Conference. May 26-28, 2025. Riga, Latvia. Pp. 123-127.
14. Didur V., Molchanova M., Mazurets O. Research on the effectiveness of neural network detection of plots with the destroyed buildings remains. Modern technologies and science: problems, new and relevant developments. Proceedings XXI International Scientific and Practical Conference. May 26, 2025. Zaragoza, Spain. Pp. 245-251.
15. Hladun O.V., Molchanova M.O., Zalutska O.O., Mazurets O.V. Effectiveness research of using ViT neural network architecture for classifying the destroyed buildings remains. Achievements of Science and Applied Research. Proceedings of 2nd International Scientific and Theoretical Conference. May 19-21, 2025. Dublin, Ireland. Pp. 96-100.
16. Hladun O., Zalutska O., Klimenko V., Mazurets O. Research on the effectiveness of classifying the remains of destroyed buildings using MobileNetV3 neural network architecture. Innovations in Science: From Theoretical Foundations to Practical Impact. Proceedings 1st International Scientific and Practical Conference. May 12-14, 2025. Antwerp, Belgium. Pp. 158-162.
17. Мазурець О.В., Собко О.В., Дидо Р.А., Молчанова М.О., Тищенко О.О. Проєктування структури бази даних для інтелектуальної системи нейромережевого виявлення та локалізації на фотозображеннях ділянок із залишками зруйнованих будівель. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №4 (45). С. 1242-1258.
18. Молчанова М.О., Дідур В.О., Мазурець О.В., Тищенко О.О., Залуцька О.О. Інформаційна технологія використання хмарних обчислень для класифікації залишків зруйнованих будівель засобами нейронних мереж за візуальними даними з безпілотних літальних апаратів. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №4 (45). С. 1259-1272.
19. Собко О.В., Кліменко В.І., Мазурець О.В., Залуцька О.О., Гладун О.В. Особливості програмної інженерії та тестування програмного забезпечення для нейромережевого аналізу фотоданих залишків зруйнованих будівель із роботизованої техніки. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №4 (45). С. 1566-1581.
20. Дідур В.О., Молчанова М.О., Мазурець О.В. Спосіб виявлення та класифікації залишків зруйнованих будівель та будівельного сміття за фотографіями з використанням моделей CNN. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №1 (42). С. 1162-1175.
21. Дидо Р.А., Мазурець О.В. Метод ідентифікації особистості на основі розпізнавання обличчя в реальному часі для систем кібербезпеки. Інформаційна, функційна і кібербезпека СКІФіК2024. Матеріали IV Всеукраїнської науково-технічної конференції. 29-30 листопада 2024. Харків. 2024. с. 36-37.

УДК 004.4:612.845

Канішев В.О., Мельников О.Ю.

Донбаська державна машинобудівна академія

ВДОСКОНАЛЕННЯ ОБ'ЄКТНО-ОРІЄНТОВАНОЇ МОДЕЛІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ОЦІНКИ ЯКОСТІ ФОНОВОГО ОФОРМЛЕННЯ САЙТІВ ДЛЯ ЛЮДЕЙ ІЗ ДАЛЬТОНІЗМОМ

Стаття присвячена вдосконаленню об'єктно-орієнтованої моделі програмного забезпечення для оцінки кольорового оформлення вебсайтів з урахуванням потреб користувачів з кольоровою сліпотю. У роботі досліджуються методи моделювання порушень кольорового зору та розробляються алгоритми аналізу контрастності, зручності сприйняття та доступності вебресурсів. Запропонована система була реалізована у вигляді інтерактивного вебдодатка, що дозволяє моделювати три основні типи кольорової сліпоти – протанопію, дейтеранопію та тританопію – та проводити кількісну оцінку доступності кольорів. Розробка базується на клієнт-серверній архітектурі з використанням мови програмування JavaScript та уніфікованої мови моделювання UML для проектування структури системи. Проведений аналіз показав, що вдосконалена модель підвищує точність ідентифікації проблемних поєднань кольорів і надає користувачеві зрозумілі рекомендації щодо поліпшення візуальної доступності вебсайтів. Отримані результати можуть бути використані для розробки інструментів перевірки доступності вебресурсів та в освітніх цілях для підвищення інклюзивності цифрового середовища.

The article is devoted to improving the object-oriented software model for evaluating the color design of websites, taking into account the needs of users with color blindness. The paper explores methods for modeling color vision disorders and develops algorithms for analyzing the contrast, perceptual comfort, and accessibility of web resources. The proposed system was implemented as an interactive web application that allows modeling three main types of color blindness – protanopia, deuteranopia, and tritanopia – and conducting a quantitative assessment of color accessibility. The development is based on client-server architecture using the JavaScript programming language and the unified modeling language UML for designing the system structure. The analysis showed that the improved model increases the accuracy of identifying problematic color combinations and provides the user with clear recommendations for improving the visual accessibility of websites. The results can be used to develop tools for checking the accessibility of web resources and for educational purposes to increase the inclusiveness of the digital environment.

Дальтонізм є генетичним порушенням, яке впливає на спроможність розрізняти певні кольори [1]. Є низка методів та програмних засобів для виявлення аномалій визначення кольорів [2], але окремою проблемою є створення доступного середовища для людей з особливими потребами. На сучасному рівні це означає наявність електронних ресурсів (інтернет-сайтів), що будуть цілком задовольняти потреби людей із порушенням кольоросприйняття [3].

Поставлено задачу створення застосунку для аналізу рівня задоволення сайтами людей з деякими особливими потребами (а саме – з порушеннями кольоросприйняття) [4-5]. Застосунок може бути реалізовано у вигляді спеціального сайту, де обробку здійснюватиме скрипт на мові JAVASCRIPT [6].

Програмне рішення буде реалізовано за клієнт-серверною архітектурою, що складається з вебінтерфейсу та серверної частини [7]. Для створення інформаційної моделі програмного забезпечення використаємо мову UML [8]. Діаграма варіантів використання ілюструє взаємодію користувача з основними компонентами застосунку та демонструє повний спектр можливостей системи.

Система надаватиме користувачу два основні способи введення даних: вказати URL вебресурсу для перевірки його колірної схеми або завантажити графічний файл. Після введення посилання система автоматично каталогізує всі кольорові значення вебсторінки, включаючи текст, фон та графічні елементи. Користувач може швидко копіювати HEX або RGB значення кольорів безпосередньо з інтерфейсу [9].

Для налаштування та тестування колірних комбінацій буде доступне введення через RGB-формат або hex-код. Функціонал редагування дозволить налаштовувати кольори тексту та фону з подальшим аналізом їх контрастності та придатності.

Ключовою функцією є симуляція відтінків кольорів при різних типах дальтонізму [10]. Система підтримуватиме окремі режими візуалізації для протанопії, дейтеранопії та тританопії, відображаючи результати з візуалізацією та числовими показниками контрастності. Така структура забезпечує інтуїтивний робочий процес від простого введення даних до детального аналізу колірних комбінацій з урахуванням потреб людей з порушеннями кольоросприйняття. Діаграма варіантів використання показана на рисунку 1.

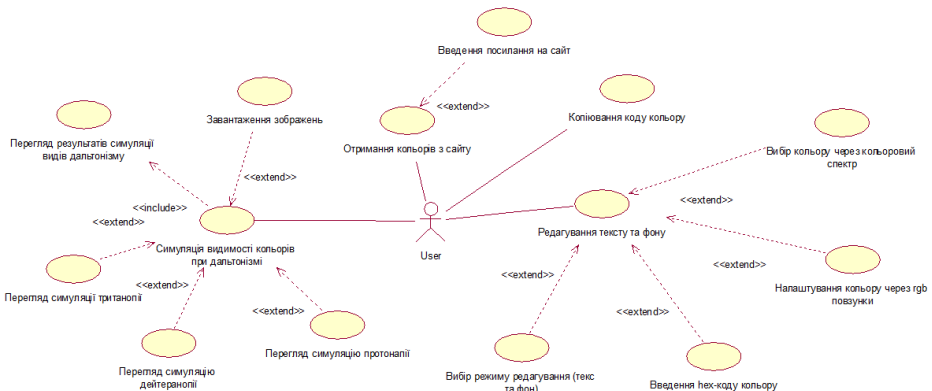


Рисунок 1 – Діаграма варіантів використання

Діаграма класів представляє статичну архітектуру програмної моделі, відображаючи структурні зв'язки між компонентами системи на етапі проектування [11]. Архітектура застосунку побудована навколо семи основних класів, кожен з яких відповідає за конкретний аспект функціональності.

Клас `UIController` виступає центральним координатором користувацького інтерфейсу, керуючи режимом редагування, синхронізацією слайдерів, оновленням кольірних значень та обробкою введення даних. Він безпосередньо взаємодіє з користувачем та координує роботу інших компонентів системи.

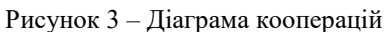
`WebServer` забезпечує серверну частину, обробляючи HTTP-запити та керуючи комунікацією між клієнтською та серверною частинами [12].

Для отримання даних використовуються два спеціалізовані класи: `SiteFetcher` працює з вебресурсами, завантажуючи HTML та CSS контент, витягуючи вбудовані стилі та санітизуючи дані, тоді як `ImageProcessor` обробляє графічні файли, виконуючи завантаження, зміну розміру та конвертацію у RGB-формат. `ColorAnalyzer` витягує кольорову інформацію з отриманого контенту, валідує кольірні значення та проводить комплексний аналіз вебсайтів.

Центральним елементом системи є `ColorblindnessSimulator`, який містить матриці трансформації для різних типів дальтонізму та реалізує методи симуляції кольірної сліпоти, обчислення видимості та оновлення попереднього перегляду. Для математичних обчислень він використовує `ColorUtility`, що надає функції конвертації між форматами HEX та RGB, розрахунку яскравості, обчислення коефіцієнта контрастності та визначення класу видимості.

Взаємодія компонентів відбувається наступним чином: `WebServer` отримує запити через `UIController` та передає їх `SiteFetcher` або `ImageProcessor` залежно від типу вхідних даних, `ColorAnalyzer` витягує кольори, `ColorblindnessSimulator` обробляє їх з використанням `ColorUtility`, а результати повертаються через `UIController` для відображення користувачу, формуючи замкнутий цикл обробки від введення до візуалізації. Діаграма класів показана на рисунку 2.

Наступною діаграмою буде діаграма кооперацій, вона демонструє динамічну взаємодію між об'єктами системи через послідовність пронумерованих повідомлень [13]. Процес починається з дії користувача (`updateColor`), яка ініціює ланцюг викликів через `UIController` до `WebServer`. Сервер активує `SiteFetcher` для завантаження вебконтенту (`fetchWebsite`, `extractInlineStyles`), після чого `ColorAnalyzer` виконує аналіз кольорів (`analyzeWebsite`, `extractColors`). Паралельно `ImageProcessor` обробляє зображення (`loadImage`, `convertToRGB`). Центральний компонент `ColorblindnessSimulator` координує симуляцію дальтонізму (`simulateColorBlindness`), звертаючись до `ColorUtility` для математичних обчислень (`rgbToHex`, `calculateLuminance`, `calculateContrastRatio`) та розрахунку видимості (`calculateVisibility`). Результати застосовуються через `applyFilter` та повертаються до `UIController` методом `updatePreview` для синхронізації інтерфейсу (`syncSliders`). Діаграма кооперацій зображена на рисунку 3.



Вертикальні пунктирні лінії представляють лінії життя кожного об'єкта (ColorAnalyzer, Colorblindness, ColorUtility, ImageProcessor, WebServer, SiteFetcher,

UIController), а горизонтальні стрілки показують повідомлення між ними у послідовності від 1 до 16.

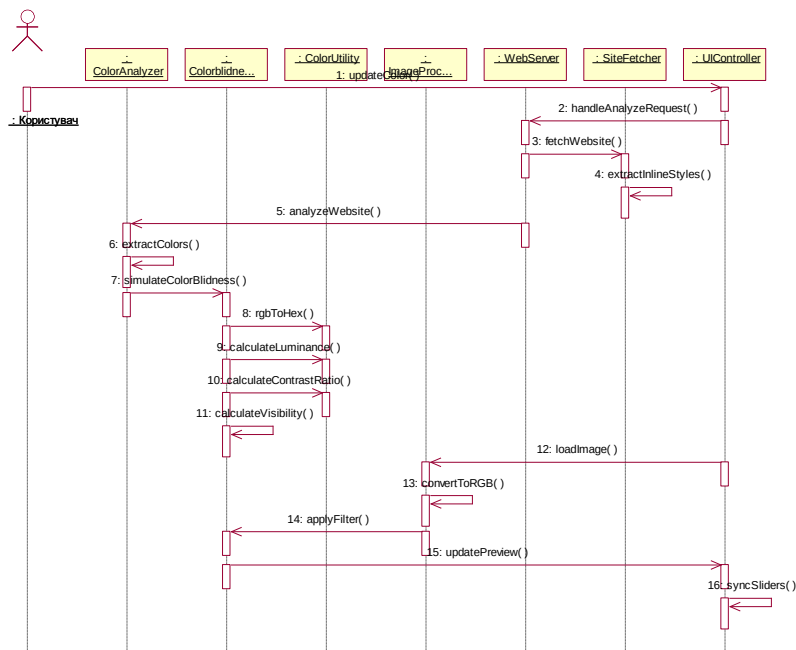


Рисунок 4 – Діаграма послідовностей

Процес розпочинається з ініціації користувачем через UIController, який передає запит на WebServer для обробки (handleAnalyzeRequest). Далі відбувається паралельна робота: SiteFetcher завантажує та обробляє вебконтент (fetchWebsite, extractInlineStyles), а ImageProcessor працює з графікою (loadImage, convertToRGB). ColorAnalyzer виконує аналіз кольорів (analyzeWebsite, extractColors), після чого Colorblindness компонент застосовує симуляцію (simulateColorBlindness), звертаючись до ColorUtility для математичних розрахунків (rgbToHex, calculateLuminance, calculateContrastRatio, calculateVisibility). Завершується процес оновленням інтерфейсу через updatePreview та syncSliders, демонструючи повний цикл обробки запиту від початку до кінця. Діаграма зображена на рисунку 4.

Діаграма станів ілюструє життєвий цикл системи [14]. Вона відображає всі можливі стани застосунку та переходи між ними. Процес розпочинається з початкового стану та проходить через послідовність станів від введення даних до відображення результатів. Діаграма станів зображена на рисунку 5.

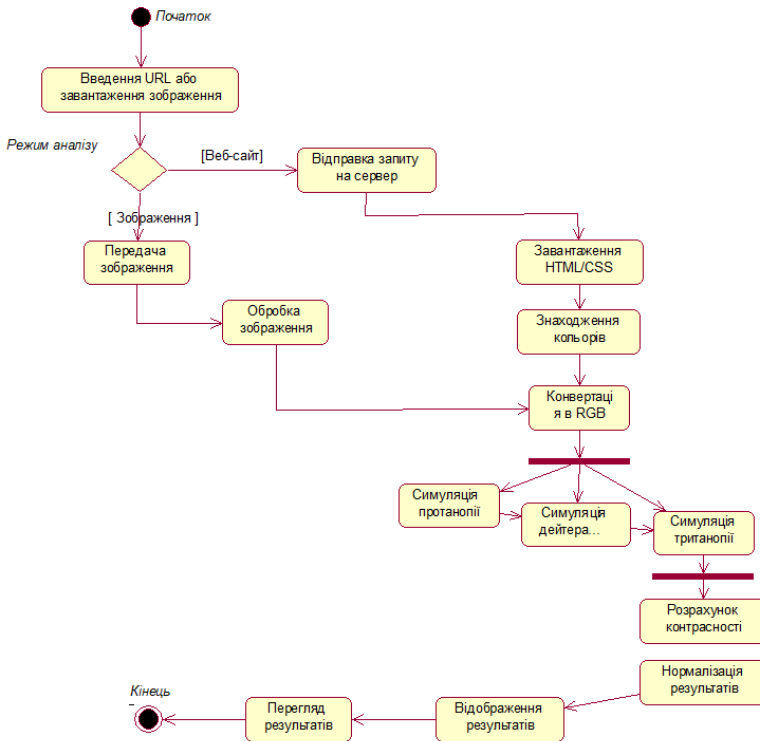


Рисунок 5 – Діаграма станів

Останньою буде діаграма діяльності [15]. Вона демонструє потік виконання операцій у системі від початку до завершення, визначаючи послідовність дій та точки прийняття рішень. Процес стартує з введення URL або завантаження зображення, після чого система розгалужується залежно від обраного режиму аналізу. При виборі режиму вебсайту відбувається відправка запиту на сервер, завантаження HTML/CSS контенту та знаходження кольорів [16-17]. Якщо обрано режим зображення, система виконує передачу та обробку графічного файлу. Обидві гілки збігаються в активності конвертації у RGB-формат, яка є обов'язковою для подальшої обробки незалежно від джерела даних. Далі система входить у фазу паралельної обробки, де одночасно виконуються три незалежні потоки симуляції: протанопії, дейтеранопії та тританопії. Після завершення паралельних процесів відбувається синхронізація результатів, розрахунок контрастності та нормалізація отриманих даних. Фінальні активності включають відображення результатів користувачу та перегляд підсумкової інформації, після чого процес завершується переходом у кінцевий стан. Діаграма зображена на рисунку 6.

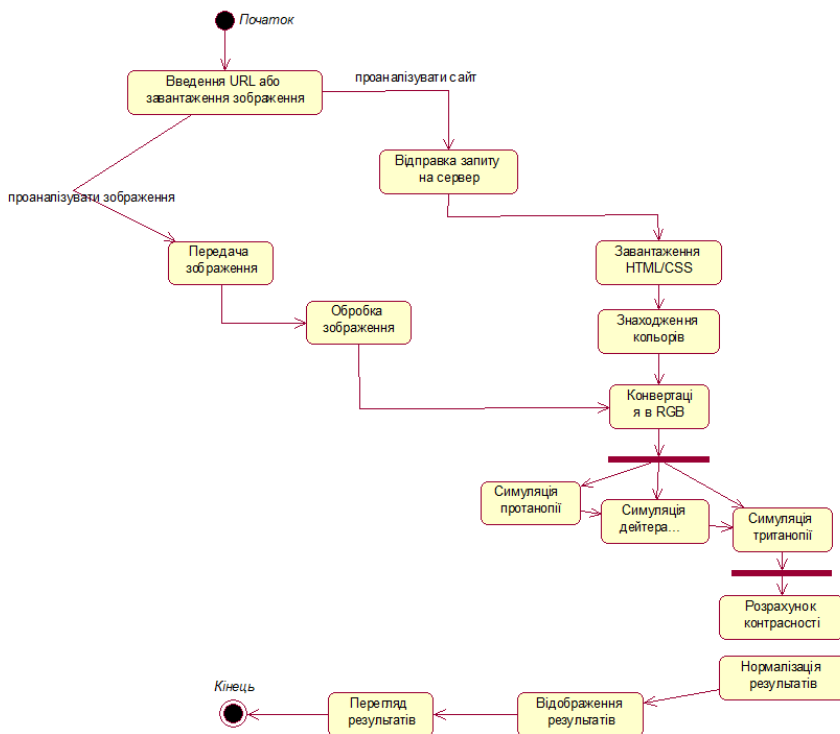


Рисунок 6 – Діаграма діяльності

Спроектowana система аналізу доступності кольорів може бути інтегрована в вебплатформи та системи аудиту доступності вебсайтів, що сприятиме підвищенню інклюзивності цифрового середовища та поліпшенню сприйняття інформації користувачами з порушеннями кольорового зору.

Перелік посилань

1. Дальтонізм: відповіді та питання. [Електронний ресурс]. URL: <https://doc.ua/ua/news/articles/daltonizm-voprosy-i-otvety>. Дата звернення: 7.04.2025.
2. О. Ю. Мельников, В. О. Канішев, “Система підтримки прийняття рішень для виявлення аномалій визначення кольорів”, Automation of Technological and Business Processes, Одеса: ОНТУ, № 16 (3), с. 58–68, 2024, DOI: <https://doi.org/10.15673/atbp.v16i3.2921>
3. А. М. Горло, І. С. Мінтій, “Адаптація дизайну сайту для людей із порушенням кольоросприйняття”, Новітні комп'ютерні технології, Кривий Ріг: Видавничий центр ДВНЗ «Криворізький національний університет», т. XVI, с. 182–187, 2018.

4. Канішев В. О., Мельников О. Ю. Об'єктно-орієнтоване проєктування програмного забезпечення для оцінки якості фонового оформлення сайтів для людей із дальтонізмом // Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XXV Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 17-18 квітня 2025 р. – Одеса, Видавництво ОНТУ
5. Мельников О. Ю., Канішев В. О. Алгоритм для відображення видів дальтонізму в системі оцінки якості фонового оформлення сайтів // Інформаційні технології в культурі, мистецтві, освіті, науці, економіці та бізнесі: матеріали X Міжнародної науково-практичної конференції / М-во освіти і науки України; Київ. нац. ун-т культури і мистецтв. Київ : Видавничий центр КНУКіМ, 2025. – С. 29–31
6. В. О. Канішев, О. Ю. Мельников, “Постановка задачі створення застосунку для аналізу рівня задоволення сайтами людей із порушенням кольоросприйняття”, Сучасні інформаційні системи та технології: матеріали VII Всеукр. наук.-практ. інтернет-конф. за тематикою «Сучасні комп'ютерні системи та мережі в управлінні» (29 листопада 2024 р., м. Херсон, м. Хмельницький) / за ред. А. А. Григорової, Херсон: Книжкове видавництво ФОП Вишемирський В. С., с. 180–181, 2024.
7. С. В. Буртовий, В. А. Чубенко, С. В. Василюк-Зайцева Використання нейромереж у розпізнаванні та діагностиці навчальних здібностей здобувачів освіти. Академічні візії. №29, 2024, 2–3 с. URL: <https://academy-vision.org/index.php/av/article/view/971/884> (Дата звернення 22.10.2025)
8. Канішев В. О., Мельников О. Ю. Вебзастосунок для розрахунку ступеня бачення дизайну сайтів для людей з порушенням кольоросприйняття // Розвиток науки – простір для відновлення регіону: збірник тез наукової конференції молодих вчених 19 грудня 2024 р., – м. Краматорськ: Донецька обласна державна адміністрація, Рада молодих вчених при Донецькій облдержадміністрації, 2024. – С. 76–79.
9. О. Ю. Мельников, “Об'єктно-орієнтований аналіз і проєктування інформаційних систем: посібник для студентів спеціальностей «Системний аналіз» та «Інформаційні системи та технології». – Вид. 3-є, перероб. та доп.”, Краматорськ: ДДМА, 208 с., 2020.
10. RGB – ВІКІПЕДІЯ URL:
11. <https://uk.wikipedia.org/wiki/RGB>
12. Види дальтонізму – OCHI CLINIC URL: <https://www.ochiclinic.com.ua/publications/daltonizm-yak-bachat-daltoniki-i-yaki-kolori-ne-rozriznuayut>
13. Діаграма класів – ВІКІПЕДІЯ URL: https://uk.wikipedia.org/wiki/Діаграма_класів
14. HTTP – Вікіпедія URL:
15. <https://uk.wikipedia.org/wiki/HTTP>
16. Діаграма кооперацій – StudFiles URL:
17. <https://studfile.net/preview/5010027/page:4>
18. Діаграма станів (UML) – ВІКІПЕДІЯ URL:
19. [https://uk.wikipedia.org/wiki/Діаграма_станів_\(UML\)](https://uk.wikipedia.org/wiki/Діаграма_станів_(UML))
20. Діаграма діяльності – ВІКІПЕДІЯ URL:
21. https://uk.wikipedia.org/wiki/Діаграма_діяльності
22. HTML – ВІКІПЕДІЯ URL:
23. <https://uk.wikipedia.org/wiki/HTML>
24. CSS – ВІКІПЕДІЯ URL:
25. <https://uk.wikipedia.org/wiki/CSS>

УДК 004.4

Коржан М.М., Підченко С.К.

Хмельницький національний університет

ІНФОКОМУНІКАЦІЙНА СИСТЕМА ЕКЗАМЕНАЦІЙНО-ТРЕНІНГОВОГО ЦЕНТРУ ІНОЗЕМНИХ МОВ

Розглянуто методи захисту інформаційних систем від загрозових програм на основі механізмів контролю доступу та розмежувальних політик. Запропоновано підхід до побудови багаторівневої системи захисту, що поєднує дискреційний, мандатний та рольовий контроль доступу з динамічними політиками безпеки. Результати дослідження демонструють, що правильно налаштовані механізми контролю доступу можуть суттєво знизити ймовірність успішного зараження системи та обмежити масштаби можливих наслідків.

Methods of protecting information systems from malicious programs based on access control mechanisms and separation policies are considered. An approach to building a multi-level protection system is proposed, combining discretionary, mandatory, and role-based access control with dynamic security policies. The results of the study demonstrate that properly configured access control mechanisms can significantly reduce the likelihood of successful system infection and limit the scale of possible consequences.

Забезпечення функціонування інфокомунікаційних систем (ІКС), в тому числі освітніх, покладено на всебічне використання програмних, апаратних та мережевих засобів [1-2]. Незалежно від масштабу та форми власності закладу освіти (ЗО), такі технології покращують якість надання послуг здобувачам освіти (студентам) за рахунок автоматизації процесів.

Відповідно до досліджень [3-4], використання ІКС для вивчення іноземних мов сприяє підвищенню мотивації, ефективності взаємодії учасників освітнього процесу, а також дозволяє моделювати реальні комунікаційні ситуації в штучному середовищі.

Такі інструменти особливо корисні для вивчення іноземних мов, де акцент робиться на розмовній практиці, аудіюванні та культурному обміні, а також для атестації знань студентів через, автоматизовану оцінку та персоналізований зворотний зв'язок.

Практика свідчить, що застосування ІКС в освіті сприяє розвитку від монотонного заучування до появи інтегральних методів, що суттєво підвищують якість освітніх послуг.

Природною є класифікація засобів підтримки ІКС на апаратні і програмні [3].

Представимо ІКС I_S у вигляді трійки:

$$I_s = \{X, Y, Z\}, \quad (1)$$

де X – множина вхідних потоків даних (Inputs);

Y – множина вихідних потоків (Outputs);

Z – параметри системи, що в свою чергу згідно методології SADT поділяють на сигнали контролю (Controls – C) та механізми виконання (Mechanisms – M):

$$Z = \{C, M\}. \quad (2)$$

Схематично система може бути представлена у спрощеному вигляді, на основі базової моделі «чорного ящика» з подальшою розробкою контекстної діаграми (A-0), яка описує всю систему у вигляді єдиного блоку активності Activity A-0: «Керування реєстрацією на курси іноземних мов та екзамени».

Ця активність охоплює всі взаємодії з користувачами, обробку даних та адміністративні функції через веб-додаток на основі триступеневої архітектури (Model-View-Controller, MVC), БД (доступ до якої здійснюється через драйвер з пулом підключень) та асинхронні обробники (для паралельного виконання).

З огляду на важливість забезпечення безвідмовного доступу ПЗ до БД, розглянемо моделі резервування програмних компонентів для підключення програмного додатку до БД.

Відома модель мікросервісів [5], згідно якої архітектура ПЗ розділяється на множину окремих компонентів (сервісів), що функціонують паралельно в єдиній екосистемі. Використання таких сервісів сприяє підвищенню надійності системи та спрощення структури окремих сервісів, які виконують кожен свою просту функцію (спрощено).

Представимо механізм доступу до БД у вигляді програмного модуля з багатосервісною архітектурою, що функціонує з метою, наприклад, використання одним додатком декількох БД, розташованих фізично на різних серверних платформах.

Об'єктно-орієнтована модель ПЗ дозволяє абстрагуватись від конкретної системи управління базою даних (СУБД), її драйвера та параметрів підключення, інкапсулюючи ці дані у вигляді об'єкта підключення.

На Рисунку 1 показана структура вищезазначених програмних компонентів, де головним елементом є пул підключень до БД, який складається із N об'єктів підключень та K резервних об'єктів. Метод резервування в загальному випадку може бути довільним, на розсуд архітектора або розробника ПЗ, однак, в рамках даної роботи обмежимося доволі простим випадком відновлювальної резервованої системи з резервом кратності $1/2$. Така система складається із трьох елементів різної надійності.

Як видно із Рисунку 1, концепція використання пулу підключень до БД полягає у постійному використанні підключень для нормальної роботи

програмного додатку, а також у забезпеченні резервного копіювання даних між основними та резервними сховищами для можливості найшвидшого відновлення у випадку відмови.

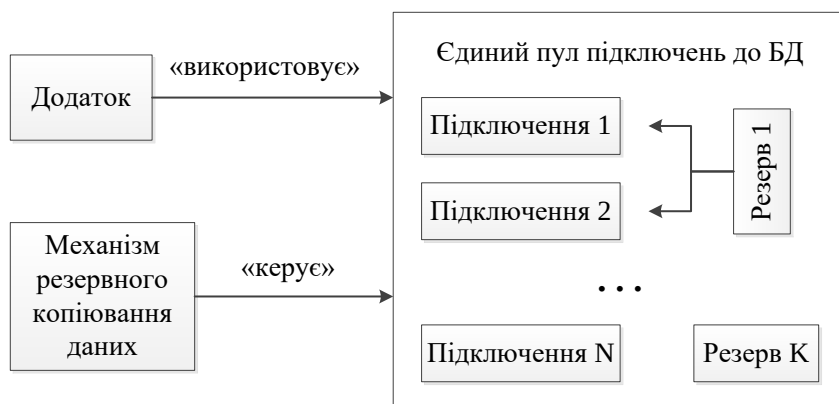


Рисунок 1 – Структура програмного модуля

Виконаємо моделювання такої системи в умовах високого навантаження невеликим часом напрацювання відмови програмних компонентів. В Таблиці 1 подані відповідні параметри надійності.

Таблиця 1 – Параметри надійності елементів системи

Параметр № Елемента	1	2	3
Назва	Підключ. 1	Підключ. 1	Резерв 1
Середній час напрацювання на відмові (Mean Time Between Failures, MTBF), години	12	8	8
Середній час відновлення (Mean Time To Recovery, MTTR), хвилини	10	10	5
Середня інтенсивність відмови, λ_i , год ⁻¹	0,083	0,125	0,125
Середня інтенсивність відновлення μ_i , год ⁻¹	6	6	12

Над вершинами графу 6-11 позначені номери елементів, які відмовили. Так, до прикладу, «1» означає випадок відмови першого елементу за роботи решти двох. Після відновлення неробочого елементу система переходить у стан справності усіх елементів, однак штатно працюватимуть перший та третій елементи.

На Рисунок 2 стани, що відповідають справності усіх елементів розміщені скраю зліва рисунку, наприклад «01» означає, що перший елемент знаходиться в резерві, а працюють другий і третій елементи і т.д. Стани, які позначені прямокутниками, відповідають відмовам.

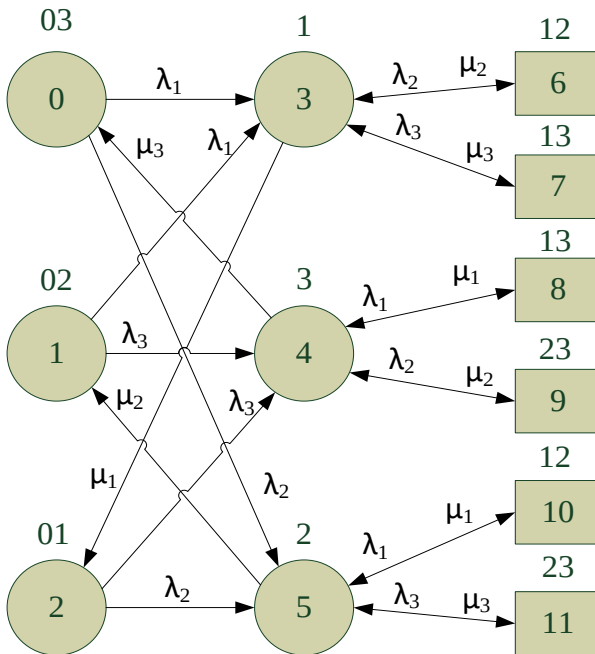


Рисунок 2 – Граф станів системи

Провівши серію імітаційних моделювань, отримуємо вектор стаціонарних ймовірностей P , значення якого наведені на Рисунок 3.

Відповідно до моделі на Рисунок 2, робочими є стани 0-5, отже, коефіцієнт готовності становить суму відповідний ймовірностей:

$$K_s = \sum_{k=0}^5 P_k = 99,92 \% .$$
 З середнім часом напрацювання на відмові 154 год. 20 хв та часом відновлення 7 хв.50 сек.

Функціональний граф станів системи показано на Рисунок 3. Стани системи показані вершинами графу 0-11.

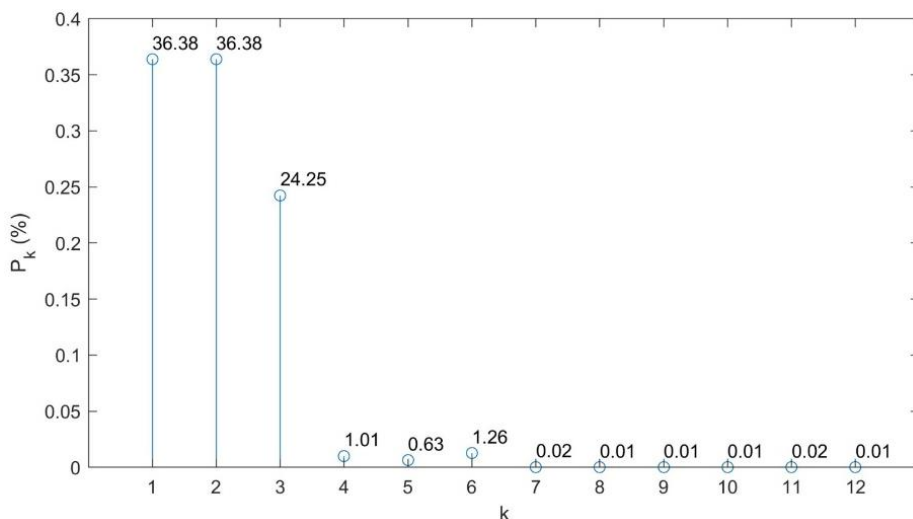


Рисунок 3 – Розраховані стаціонарні ймовірності перебування системи в k -му стані

Отже, запропонований метод дозволяє збільшити середній час напрацювання на відмову до 154 годин (більше 6 днів), що понад у 12 разів більше за відповідний показник для лише одного елемента із базовими показниками надійності, з середнім часом відновлення не більше 8 хвилин.

Перелік посилань

1. Довбиш А. С. Вступ до інформаційного аналізу і синтезу інфокомунікаційних систем : [монографія] / А. С. Довбиш. – Київ, 2016.
2. Осадча Ю. В. Аналіз програмного та інфокомунікаційного забезпечення освітнього процесу : [монографія] / Ю. В. Осадча. – Київ, 2022.
3. Classification of Technology-based Language Learning Resources according to Pedagogical and Functional Criteria / R. Seiz Ortiz, M. L. Carrió Pastor // Revista Electrónica de Lingüística Aplicada. – 2025. – Vol. 23, Iss. 1. – [Електронний ресурс]. – Режим доступу: <https://matrix.aesla.org.es/RAEL/article/view/676>. – DOI: <https://doi.org/10.58859/rael.v23i1.676>.
4. Information and communication technologies in foreign language learning [Електронний ресурс]. – Режим доступу: <https://eprints.soton.ac.uk/192773/>. – Дата звернення: 08.10.2025.
5. Microservice Architecture pattern / C. Richardson // Microservices.io. – [Електронний ресурс]. – Режим доступу: <https://microservices.io/patterns/microservices.html>. – Дата звернення: 08.10.2025.

УДК 004.4

Катревич О.Б.

Хмельницький національний університет

МЕТОД ІНТЕГРАЦІЇ RAG-КОМПОНЕНТІВ У МУЛЬТИАГЕНТНІ СИСТЕМИ

Розглянуто прикладні аспекти розробки методу інтеграції RAG-компонентів у мультиагентні системи програмного забезпечення, що забезпечує поведінку агентів, релевантність відповідей, узгодженість даних і якісну взаємодію із зовнішніми базами знань. Запропонований метод дозволяє ефективно інтегрувати LLM-знання у агентну архітектуру, підвищує адаптивність системи до змін у базі знань і забезпечує зростання якості відповіді у порівнянні з типовими реалізаціями.

Applied aspects of developing a method for integrating RAG components into multi-agent software systems are considered, which ensures agent behavior, relevance of responses, data consistency, and high-quality interaction with external knowledge bases. The proposed method allows for the effective integration of LLM knowledge into agent architecture, increases the system's adaptability to changes in the knowledge base, and ensures an increase in response quality compared to typical implementations.

Сучасний розвиток штучного інтелекту визначається широким поширенням великих мовних моделей (Large Language Models, LLM), які поступово перетворилися з експериментальних досліджень у фундаментальний інструмент для створення інтелектуальних програмних систем.

Відомо, що LLM часто продукують помилкові твердження (так звані “галюцинації”), що значно обмежує можливості їх практичного використання.

Одним із найперспективніших рішень цієї проблеми стала архітектура Retrieval-Augmented Generation (RAG), яка поєднує генеративні можливості моделей із пошуковими механізмами та зовнішніми базами знань.

Паралельно розвивається інший напрямок — мультиагентні системи (MAS), що ґрунтуються на ідеї взаємодії автономних агентів, здатних координувати свої дії, співпрацювати та розподіляти завдання для досягнення спільної мети.

Більшість існуючих рішень розраховані на роботу з одним агентом, тоді як у багатокомпонентному середовищі виникають такі виклики як необхідність узгодженості дій агентів, що одночасно звертаються до баз знань, розмежування функціональної відповідальності між агентами (витягування, генерація, валідація, координація), забезпечення масштабованості при зростанні кількості агентів та обсягів даних, а також потреба у трасованості й відтворюваності результатів у рамках життєвого циклу програмного забезпечення.

Мета дослідження – розробка методу інтеграції RAG-компонентів у мультиагентні системи програмного забезпечення з урахуванням принципів узгодженості, масштабованості та забезпечення якості функціонування.

Загальна архітектура інтеграції RAG-компонента в мультиагентну систему зображена нижче (рисунок 1), де показано послідовність взаємодії агентів із зовнішнім джерелом знань через спільний пошуковий інтерфейс.

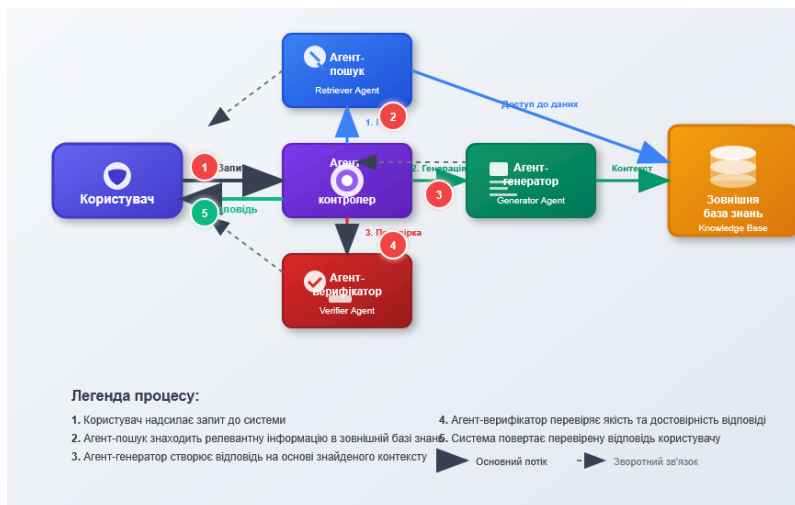


Рисунок 1 – Загальна архітектура інтеграції RAG-компонента в мультиагентну систему

Запропонована архітектура забезпечує асинхронну взаємодію через паралельну обробку запитів декількома агентами одночасно та неблокуючі операції, що усуває простой під час очікування відповідей від зовнішніх сервісів.

Для стабільності (англ. stability) відповідей використовуються метрики, що вимірюють варіації результатів при незначній зміні контексту, запиту або знань:

Δ -variation score — абсолютна зміна відповіді при зміні контексту:

$$\Delta_r = \frac{1}{n} \sum_{i=1}^n \text{sim}(r_i, r'_i) \rightarrow m$$

де r_i — початкова відповідь, r'_i — відповідь після зміни, sim — функція подібності (наприклад, cosine similarity).

Залежність середнього й максимального часу відповіді від кількості паралельних користувачів (Рисунок 2). Крива показує плавне зростання часу відповіді, без різких стрибків чи деградацій.

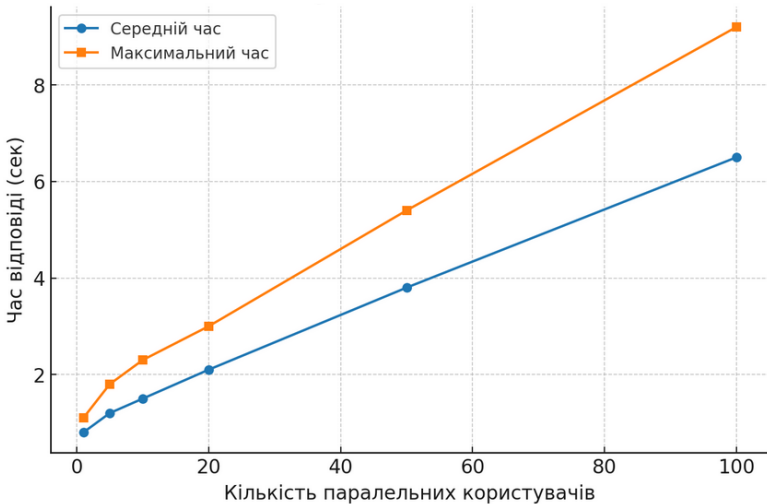


Рисунок 2 - Залежність середнього й максимального часу відповіді від кількості паралельних користувачів

Отже, запропонований підхід дозволяє поєднувати сильні сторони генеративних моделей та систем витягування знань, мінімізуючи їхні недоліки та забезпечуючи більш високу точність і стабільність результатів.

Перелік посилань

1. Вулдрідж М. Вступ до мультиагентних систем / М. Вулдрідж. – 2-е вид. – Чичестер : Wiley, 2009. – 484 с.
2. Басс Л., Клементс П., Казман Р. Архітектура програмного забезпечення на практиці / Л. Басс, П. Клементс, Р. Казман. – 4-е вид. – Бостон : Addison-Wesley, 2021. – 704 с.
3. Jennings N. R., Sycara K., Wooldridge M. A roadmap of agent research and development // Autonomous Agents and Multi-Agent Systems. – 1998. – № 1. – P. 7–38.
4. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. – 4th ed. – Pearson, 2021. – 1152 p.
5. Lewis P., Perez E., Piktus A. Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks // Advances in Neural Information Processing Systems (NeurIPS). – 2020.
6. Karpukhin V., Oguz B., Min S. Dense Passage Retrieval for Open-Domain Question Answering // EMNLP. – 2020.
7. Stone P., Veloso M. Multiagent systems: A survey from a machine learning perspective // Autonomous Robots. – 2000. – Vol. 8. – P. 345–383.
8. Sutton R., Barto A. Reinforcement Learning: An Introduction. – 2nd ed. – MIT Press, 2018. – 552 p.

УДК 004.8

Кашперук Т.Р., Мазурець О.В.

Хмельницький національний університет

МЕТОД ВИЗНАЧЕННЯ МОВНО-ДЕТЕРМІНОВАНОГО ІНДЕКСУ СУБ'ЄКТИВНОГО БЛАГОПОЛУЧЧЯ З ВИКОРИСТАННЯМ NLP

Запропоновано метод визначення мовно-детермінованого індексу суб'єктивного благополуччя з використанням NLP та відповідну програмну реалізацію. Метою інтелектуальної системи є визначення рівня задоволеності життям за описом користувача за допомогою методу SVM, який визначає оцінку. На підставі оцінки створюється опис стану користувача. Використання розробленого методу дає можливість користувачу отримати оцінку щодо свого стану та за потреби прийняти рішення щодо необхідності його покращення. Програма реалізація методу забезпечує виконання функцій: аналіз тексту та визначення оцінки задоволеності життям за описом; збір та обробка внесеної користувачем інформації; перегляд використаних датасетів; перегляд моделей та інформація щодо них; можливість внесення змін у датасети.

The method for determining a language-determined subjective well-being index using NLP and a corresponding software implementation are proposed. The purpose of the intelligent system is to determine the level of life satisfaction based on the user's description using the SVM method, which determines the assessment. Based on the assessment, a description of the user's state is created. Using the developed method allows the user to obtain an assessment of their state and, if necessary, make a decision on the need to improve it. The program implementing the method provides the following functions: text analysis and determination of the assessment of life satisfaction based on the description; collection and processing of information entered by the user; viewing used datasets; viewing models and information about them; the ability to make changes to datasets.

Вже протягом тривалого часу люди усвідомлюють важливість розуміння свого емоційного стану та стеження за ним, оскільки емоційний стан безпосередньо впливає на психологічне благополуччя особи. Це усвідомлення призвело до створення окремої науки, яка вивчає та аналізує емоційний стан людини - психології. Наукові дослідження різних аспектів людської психіки та їх впливу на відчуття комфорту і задоволення є важливими елементами визначення психологічного комфорту. Центральними аспектами для визначення рівня задоволеності життям є стан і психологічний комфорт людини, а фахівці, які допомагають досягти цього комфорту, є психологами.

В деяких сферах діяльності, де використовуються алгоритмічні системи, вже відбувається активне впровадження ШІ, наприклад, у медичній сфері його використання полягає в автоматизації діагностики за зображеннями медичних знімків (наприклад, рентгенівських знімків), в сфері фінансів використовується для прогнозування ринкових трендів, управління портфелем інвестицій, в автомобільній промисловості - для розробки систем автопілоту та безпеки на дорозі. Психологія не є винятком.

ШІ вже широко використовується і продовжує активно вбудовуватись в психологічну практику. Наприклад, розробляються моделі, які аналізують сприйняття та обробку інформації людиною [1]. Як відзначає практикуючий психолог Десмонд Сох, ШІ допоможе автоматизувати рутинні завдання, такі як психометричні оцінки або IQ-тести, тим самим звільняючи час для інших видів діяльності [2]. Згідно з Робертом Солсо, у когнітивній психології проблематика ШІ розглядається переважно як інструмент самопізнання та рефлексії [3]. Крім того, ШІ можна використати для розпізнавання емоцій, що сприятиме визначенню рівня задоволеності життям.

Задоволеність життям є складним показником, що включає загальне щастя та задоволеність людини життєвими обставинами [4]. Рівень життєрадісності можна визначити за тестами, такими як, наприклад, ті, які розроблені англійським психологом В. Коулманом або за шкалою американського психолога Керола Дайана. Суть таких тестів полягає в аналізі їх результатів та формулювання висновків.

Отже, наведені дані підтверджують важливість розуміння та стеження за своїм емоційним станом для досягнення психологічного благополуччя. З розвитком інформаційних технологій відкриваються нові можливості в автоматизації рутинних завдань, таких як психометричні оцінки та розпізнавання емоцій, що визначить рівень задоволеності життям. Таким чином, автоматизація цих процесів сприятиме більш ефективному визначенню та підтримці психологічного комфорту і задоволеності життям.

Методи обробки природної мови (NLP) продемонстрували значний потенціал у задачах автоматизованого аналізу текстових даних [5, 6], що робить їх одним із ключових інструментів сучасних досліджень у сфері соціальних наук, психології та комп'ютерної лінгвістики [7, 8]. Значний обсяг комунікації людини – від приватних повідомлень до публічних дописів у соціальних мережах – представлений у текстовій формі [9], що перетворює текст на цінне джерело інформації про емоційний стан [10, 11], поведінкові патерни [12] та рівень суб'єктивного благополуччя особи.

Сучасні NLP-підходи ґрунтуються на використанні статистичних і нейромережових моделей, які здатні виявляти приховані семантичні та емоційні маркери, недоступні для класичних лінгвістичних методів [13, 14]. Моделі трансформерної архітектури, такі як BERT, RoBERTa, GPT та їхні україномовні адаптації, забезпечують контекстуально залежне кодування текстів, що дозволяє ефективно інтерпретувати багатовимірні сигнали: тональність висловлювань, риторичні конструкції, частоту лексем, індикатори емоційної валентності та когнітивного стилю [15]. Ці характеристики є релевантними для оцінювання таких психологічних категорій, як рівень життєвої задоволеності, суб'єктивний добробут чи емоційне благополуччя.

У контексті визначення мовно-детермінованого індексу суб'єктивного благополуччя NLP надає можливість об'єктивувати та формалізувати текстові ознаки, що відображають індивідуальні оцінки життєвої ситуації [16]. Застосування моделей класифікації, регресійних предикторів та Zero-/Few-Shot-підходів дозволяє автоматично зіставляти мовні патерни з відомими психологічними шкалами (такими як SWLS, PANAS, WHO-5), забезпечуючи відтворюваність і масштабованість оцінювання [17].

Перспективи використання NLP у цій сфері охоплюють:

- створення універсальних моделей оцінки благополуччя, здатних адаптуватися до різних соціокультурних контекстів;
- інтеграцію мультимодальних даних (текст + аудіо/відео) для підвищення точності визначення емоційного стану;
- розроблення індикаторів раннього виявлення психологічних ризиків, що можуть бути корисними в клінічній психології, HR-аналітиці, соціальних дослідженнях;
- використання генеративних моделей для побудови інтерпретованих пояснень, що покращує прозорість і валідність NLP-систем;
- автоматизацію аналізу великих обсягів соціальних даних, що відкриває можливість проводити масштабні дослідження суб'єктивного благополуччя на популяційному рівні.

Таким чином, NLP виступає ефективним інструментом не лише для описової інтерпретації текстів, а й для побудови кількісних моделей психологічних характеристик [18, 19]. Це робить можливим розроблення методів визначення мовно-детермінованих індексів суб'єктивного благополуччя, що забезпечують новий рівень глибини аналізу та відкривають перспективи для міждисциплінарних застосувань [20, 21].

Для більш чіткого розуміння підходу було спроектовано схеми та діаграму методу визначеності рівня задоволеності життям людини за текстовим описом.

Планування та відображення процесів змін кроків є одним з невід'ємних частин створення програми. Усі схеми та діаграми, отримані в результаті аналізу, слугуватимуть основою для подальшого розвитку програмного продукту. Ознайомившись з ними, виникає чітке уявлення про те, як саме функціонує дане програмне забезпечення. Наступна схема відображає метод, за допомогою якого буде визначатись рівень задоволеності життям.

На рисунку 1 вхідними даними методу визначення мовно-детермінованого індексу суб'єктивного благополуччя з використанням NLP є текстовий опис користувача та набори навчених класифікаторів, з яким у наступних етапах будуть здійснюватися операції.

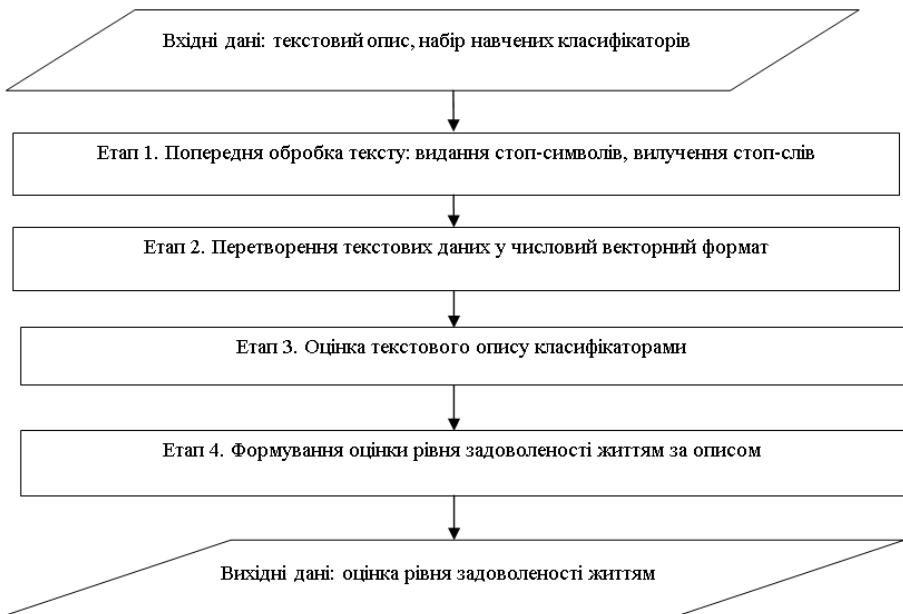


Рисунок 1 – Схема методу визначення мовно-детермінованого індексу суб'єктивного благополуччя

На першому етапі відображено підготовку даних, які включає в себе видалення стоп-символів та слів. Цей етап є обов'язковим перед використанням алгоритму SVM для аналізу текстових даних. Попередня обробка тексту дозволяє забезпечити зручні умови для подальшого використання алгоритму та оптимальну роботу класифікатора. Далі відбувається перетворення текстових даних у числовий векторний формат – векторизація даних, а саме: побудова векторного простору, де кожне слово представлене унікальним індексом. Третій крок – оцінка текстового

опису класифікаторами. Програма видає оцінку згідно навчених моделей та проаналізованого тексту. Останнім етапом є формування оцінки рівня задоволеності життям людини.

Вихідними даними є сама оцінка рівня задоволеності життям за шкалою від нуля до одиниці, в залежності від емоційної забарвленості опису. Якщо текст більше негативний, ніж позитивний – бал буде наближений до нуля, а якщо більш позитивний – до одиниці.

У схемі рисунку 2 показано більш деталізовано хід роботи алгоритму SVM: схема навчання класифікатора. Вхідними даними є датасет. Наступним кроком є вибір ядра. Вибір ядра був можливий з чотирьох основних типів ядра: лінійне, радіально базисне, поліноміальне та сигмоїдне. Для навчання було обрано лінійне ядро, оскільки воно має швидку обчислювальну складність та є ефективним для роздільних даних.

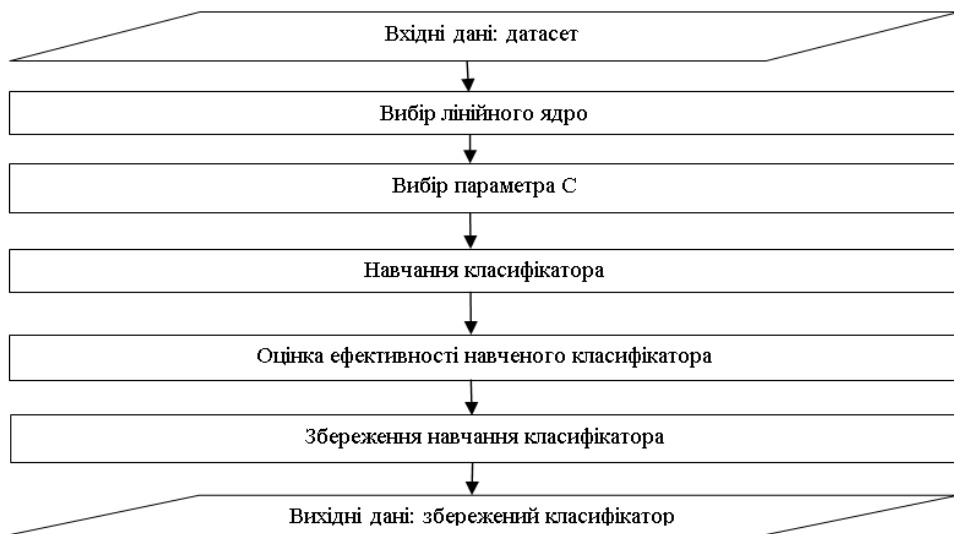


Рисунок 2 – Схема навчання типового класифікатора SVM

Наступним кроком є вибір параметра що визначає компроміс між рівнем точності на навчальному наборі та загальною здатністю моделі до узагальнення на нові дані. Значення параметра визначає рівень штрафу за помилки класифікації. Чим вище параметр, тим більший вплив має штраф на неправильну класифікацію, на процес підгонки моделі до навчальних даних. Після оптимізації параметрів, за допомогою вибраного ядра та оптимізованих параметрів SVM відбувається

побудова роздільної гіперплощини в просторі ознак, що найкращим чином розділяє класи даних.

Четвертий етап – навчання класифікатора. У випадку лінійної моделі навчання відбувається на навчальних даних шляхом максимізації ширини маржі між класами. Для цього використовується метод оптимізації, який мінімізує функцію втрат та враховує обмеження маржі.

П'ятий етап – це оцінка ефективності навченого класифікатора. Після завершення навчання модель оцінюється на тестових даних, щоб оцінити її точність та інші метрики ефективності, такі як точність, відновлення тощо. Останнім етапом є збереження навчання класифікатора. Вихідними даними є збережений класифікатор, який у подальшому буде використано у аналізі опису користувача для прорахунку оцінки рівня задоволеності життям.

За результатами досліджень було створено графіки та таблиці, що відображають результат функціонування програми, наведеної на рисунку 3.

Текст для аналізу:

У мене жакхливий настрій. Я постійно слухаю сумну музику. Боюсь, що так буде завжди. Зараз йде дощ...

Визначити рівень задоволеності життям

Результати аналізу:

Ймовірність радості: 0.02
Ймовірність любові: 0.37
Ймовірність страху: 1.00
Ймовірність смутку: 1.00
Коефіцієнт задоволеності рівня життя: 0.10
Рівень задоволеності життям: Ви повністю незадоволені життям. Життя вам уже довгий час здається сірим, сумним та безнадійним, тому рекомендуємо звернутись до фахівця для отримання допомоги

Перегляд навчальних датасетів

Приклад моделей

Рисунок 3 – Інтелектуальна система визначення мовно-детермінованого індексу суб'єктивного благополуччя

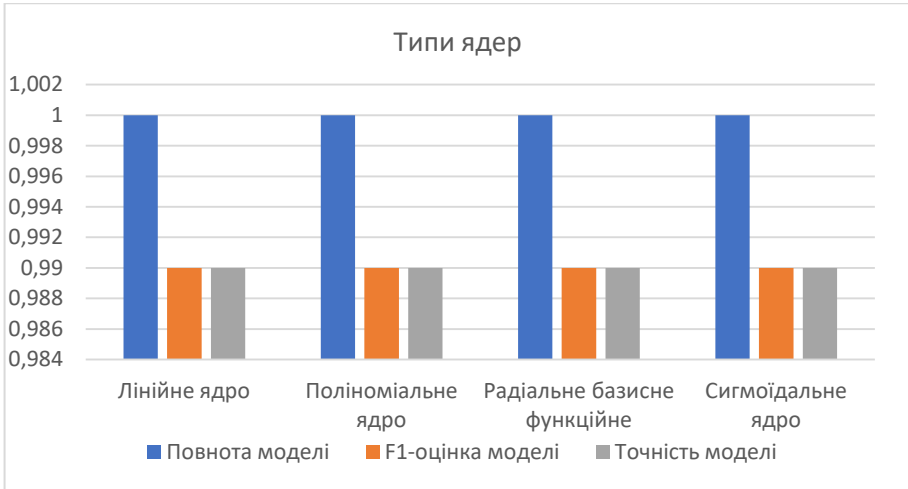


Рисунок 4 – Діаграма характеристик ядер

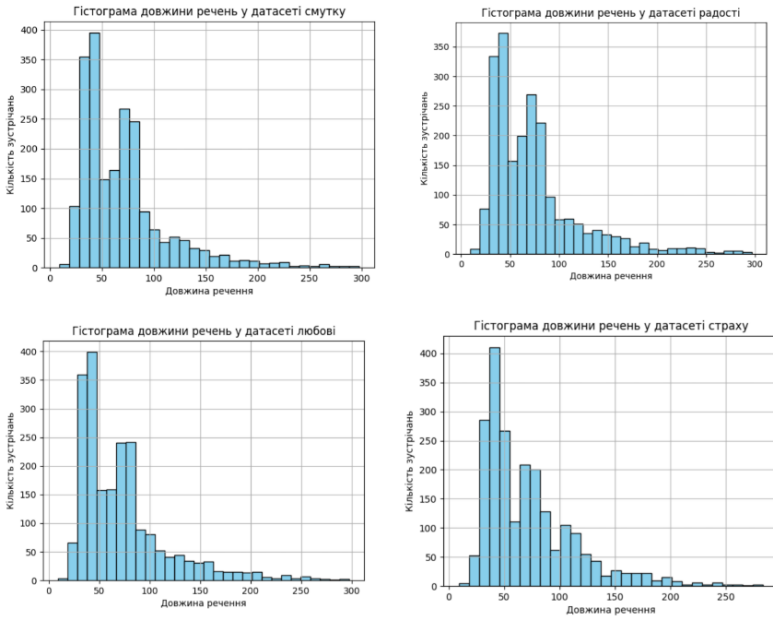


Рисунок 5 – Гістограми довжини речень датасетів

Для написання методу визначення рівня задоволеності життям людини було використано метод SVM, що має для навчання декілька типів ядра, і було протестовано різні варіанти ядра та їх вплив на кінцевий результат (рисунок 4).

З рисунка 4 видно, що характеристики у різних ядрах однакові, що свідчить що дані, що аналізуються, добре розділяються у просторі ознак за допомогою кожного з використовуваних ядер.

Також було проаналізовано довжину чотирьох датасетів, що зображено на рисунку 5

Усі чотири гістограми подібні одна до одного, що говорить про добре розподілення речень у датасетах та їх якісне навчання. На рисунку 6 зображено діаграми найпопулярніших слів у датасетах згідно проведеного аналізу.

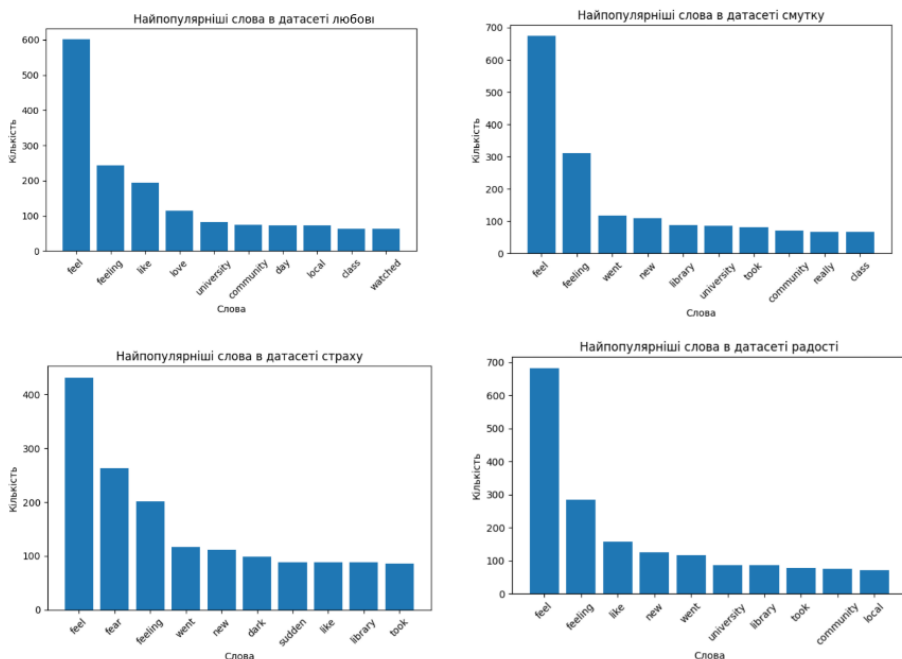


Рисунок 6 – Діаграми найпопулярніших слів у датасетах

Як видно з рисунка 6, кожна діаграма має свій набір слів. Далі було створено хмари слів на основі датасетів, які відображені на рисунку 7.



Рисунок 7 – Хмари слів

У кожній хмарі слів на рисунку 7 відображені від найбільш повторювані слова у датасетах до менш повторюваних, що видно з розмірах слів.

Отже, було спроектовано і реалізовано метод визначення мовно-детермінованого індексу суб'єктивного благополуччя з використанням NLP та відповідне ПЗ. Метою програми є визначення рівня задоволеності життям за описом користувача за допомогою методу SVM, який визначає оцінку. На підставі оцінки програма створює опис стану користувача. Використання розробленого ПЗ дає можливість користувачу отримати оцінку щодо свого стану та за потреби прийняти рішення щодо необхідності його покращення. Програма виконує наступні функції: аналіз тексту та визначення оцінки задоволеності життям за описом; збір та обробка внесеної користувачем інформації; перегляд використаних датасетів; перегляд моделей та інформація щодо них; можливість внесення змін у датасети.

Програма є перспективною, оскільки задоволеність життям та щастя людини прямо впливає на психологічний добробут і загальне здоров'я. Один із напрямків застосування може бути психологія. У майбутньому є шляхи удосконалення ПЗ, такі як збільшення обсягу даних для більш точної оцінки, збільшення кількості емоцій та інше.

Перелік посилань

1. Psykholoh. Штучний інтелект. URL: <https://www.psykholoh.com/post/штучний-інтелект-це>
2. Liga.net. Психологія майбутнього. Як штучний інтелект допоможе у боротьби зі стресом та депресією. URL: <https://life.liga.net/poyasnennya/news/psihologiya-buduschego-kak-iskusstvennyy-intellekt-pomojet-v-borbe-so-stressom-i-depressiy>
3. Solso R. L. Cognitive Psychology: Pearson New International. United Kingdom: Pearson Education, 2013. 532 p.
4. Voxukraine. Віднайти щастя: визначення ключових факторів задоволеності життям серед українців. URL: <https://voxukraine.org/vidnajty-shhastya-vyznachennya-klyuchovyh-faktoriv-zadovolenosti-zhyttiam-sered-ukrayintsiv>
5. Денисенко Б.О., Молчанова М.О., Мазурець О.В. Інтелектуальна система виявлення дезінформації з застосуванням штучних нейронних мереж. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». 15-16 листопада 2024. Хмельницький, 2024. с. 167-174.
6. Шевчук П.О., Мазурець О.В. Метод аналізу достовірності текстових повідомлень для інтелектуальних систем кібербезпеки. Інформаційна, функційна і кібербезпека СКІФіК2024. Матеріали IV Всеукраїнської науково-технічної конференції. 29-30 листопада 2024. Харків. 2024. с. 118-119.
7. Mazurets O., Vit R. Practical Application of Method of Thematic Classification of Text Information Using LDA. Information Technology and Implementation (Satellite). Proceedings 11th International Conference. November 21, 2024. Kyiv, Ukraine. 2024. Pp. 151-152.
8. Віт Р.В., Мазурець О.В. Тематична класифікація текстової інформації засобами обробки природної мови. Збірник наукових праць XXIII Міжнародної наукової конференції «Нейромережні технології та їх застосування НМТіЗ-2024». 11-12 грудня 2024. Краматорськ-Тернопіль, ДДМА. 2024. с. 63-66.
9. Овчарук О.М., Мазурець О.В. Нейромережеве діагностування проявів ПТСР у текстовому контенті з використанням помилко-орієнтованого навчального набору даних. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2024. №6, Т.1 (343). С. 195-200.
10. Крак Ю.В., Дідур В.О., Молчанова М.О., Мазурець О.В., Собко О.В., Залуцька О.О., Бармак О.В. Метод виявлення політичної пропаганди в інтернет-контенті нейромережевими засобами обробки природної мови. Науковий журнал «Проблеми програмування». Київ, 2024, №2-3. с. 288-295.
11. Овчарук О.М., Мазурець О.В. Нейромережева архітектура з квантовим шаром для аналізу текстових повідомлень на прояви посттравматичного стресового розладу. Науковий журнал «Наука і техніка сьогодні». Київ, 2024. №13 (41). С. 1192-1204.
12. Юрченко Д.Ю., Овчарук О.М., Мазурець О.В., Шевчук П.О. Метод використання нейромережі гібридної архітектури для визначення емоційної тональності текстових повідомлень. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». № 2, 2025. с. 136-141.
13. Віт Р.В., Мазурець О.В. Метод виявлення психологічного цифрового перевантаження за аналізом текстових даних нейромережевими моделями глибокого навчання. Науковий

- журнал «Вісник Херсонського національного технічного університету». 2025. №2 (93). Т. 2. С. 107-114.
14. Мазурець О.В., Тимофієв І.А., Кліменко В.І., Тищенко О.О. Метод виявлення депресивного стану пов'язаного із навчанням у закладах освіти із використанням нейромережі дуальної архітектури. Науковий журнал «Вісник Херсонського національного технічного університету». 2024. №4 (91). С. 311-318.
15. Віт Р.В., Мазурець О.В. Підхід до тематичної класифікації текстової інформації засобами обробки природної мови. Науковий журнал «Наукові праці Донецького національного технічного університету», серія «Проблеми моделювання та автоматизації проектування». 2025. №1 (21). С. 94-99.
16. Овчарук О.М., Мазурець О.В. Нейромережевий метод діагностування психологічних розладів за аналізом повідомлень на основі роздільного підходу до класифікації. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». № 1, 2025. с. 210-216.
17. Murava V., Zalutska O., Didur V., Mazurets O. Software architecture of information system for exchanging LLM thematic prompts. Global Trends in the Development of Information Technology and Science. Proceedings IV International Scientific and Practical Conference. June 25-27, 2025. Stockholm, Sweden. Pp. 121-127.
18. Віт Р.В., Мазурець О.В. Метод виявлення комунікаційних об'єктів як індикаторів цифрової втоми. Інтелектуальний метод виявлення цільових об'єктів предметної області для класифікації текстової інформації. Матеріали XIII Міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології ІУСТ-ОДЕСА-2025». 24-26.09.2025. Одеса. 2025. С.119-121.
19. Залуцька О.О., Молчанова М.О., Мазурець О.В., Мельник О.І., Скрипник Т.К. Метод інтелектуального аналізу емоційної тональності текстової інформації для визначення поведінкових намірів нейромережевими засобами. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2023. №5 (325). Т.1. С. 67-73.
20. Мазурець О.В., Козенко О.В., Собко О.В. Метод автоматизованого підбору відповідей на користувачські запитання за семантичною подібністю. Матеріали XII Всеукраїнської науково-практичної конференції «Глушковські читання». Київ – 2023. с. 106-109.
21. Shevchuk P., Molchanova M., Mazurets O. Software for Text Messages Reliability Analysis Based on the Machine Learning Models Ensemble. Proceedings of IV International Scientific and Practical Conference «Innovative research and perspectives of the development of science and technology». January 29-31, 2024. Stockholm, Sweden. 2024. Pp. 347-354.

УДК 004.8

Кириченко О.М.

Хмельницький національний університет

ІНТЕРПРЕТОВАНА НЕЙРОННА МЕРЕЖА ДЛЯ КЛАСИФІКАЦІЇ МРТ-ЗОБРАЖЕНЬ З ГЕНЕРАЦІЄЮ КЛІНІЧНО РЕЛЕВАНТНИХ ПОЯСНЕНЬ

Представлено підхід до побудови прозорих інтелектуальних систем для виявлення новоутворень головного мозку на МРТ-знімках з використанням принципу локальної узгодженості рішень. Комбінована структура на базі VGG-16 та DRN досягає показника правильності діагностування 95.2% зі збереженням можливості формування медично обґрунтованих тлумачень через систему логічних висловлювань. Рівень локальної узгодженості 89.3% демонструє достовірність інтерпретацій для окремих клінічних ситуацій.

A transparent intelligent system design approach for brain neoplasm detection in MRI scans using local decision consistency principle is presented. The combined VGG-16/DRN structure achieves 95.2% diagnostic correctness while maintaining medically justified interpretation generation through logical statement systems. Local consistency level of 89.3% demonstrates interpretation reliability for individual clinical situations.

Сучасний етап розвитку автоматизованої діагностики характеризується суперечністю між технологічними можливостями нейромережових архітектур та їх обмеженою прийнятністю для практичного медичного застосування [1-3]. Моделі глибинного навчання виявляють патологічні зміни з високою результативністю, проте відсутність зрозумілих пояснень створює бар'єр довіри з боку медичного персоналу.

Завдання розпізнавання типів внутрішньочерепних новоутворень демонструє цю проблему особливо чітко [4, 5, 6]. Складні нейромережі успішно диференціюють патології, але їхня внутрішня логіка залишається недоступною для розуміння спеціалістів. Законодавчі норми європейського простору вимагають забезпечення прозорості алгоритмічних рішень у медичній сфері [7].

Існуючі напрацювання у напрямку інтерпретації включають post-hoc методики (LIME, SHAP), котрі генерують апроксимовані тлумачення з проблемами стабільності. Альтернативою виступають природно інтерпретовані архітектури (деревоподібні структури, лінійні залежності), що поступаються у точності на візуальних завданнях [8, 9].

Мета дослідження полягає у формуванні методології конструювання прозорих інтелектуальних систем нейроонкологічної діагностики за томографічними зображеннями, яка поєднує високу результативність розпізнавання з генерацією клінічно значущих обґрунтувань через механізм локальної узгодженості між моделями різної складності.

Розроблений підхід ґрунтується на ідеї локального узгодження висновків між точністю складною архітектурою $F_{complex}$ та спрощеною інтерпретованою структурою F_{simple} [8]. На відміну від стратегій глобального узгодження, методологія концентрується на забезпеченні відповідності для окремих діагностичних епізодів:

$$F_{complex}(x_i) = F_{simple}(x_i) \text{ для } x_i \in S_{local}, \quad (1)$$

де S_{local} становить підмножину S .

Загальна архітектура системи представлена на рисунку 1, який ілюструє взаємодію між основними компонентами та потік обробки даних.

Система реалізується через три взаємопов'язані компоненти. Базовим елементом виступає згортовка архітектура VGG-16, налаштована для чотирикласової категоризації томографічних зрізів мозку: гліома, менінгіома, аденома гіпофіза, відсутність патології.

Архітектура VGG-16 складається з п'яти згорткових блоків з послідовним збільшенням кількості фільтрів, що забезпечує ієрархічне виділення візуальних ознак від простих текстур до складних патологічних паттернів. Кожен блок включає згортковий шар з фільтрами розміром 3×3 , функцію активації ReLU, батч-нормалізацію та операцію максимального пулінгу для зменшення просторової розмірності. Навчання мережі виконувалося з використанням функції втрат крос-ентропії та оптимізатора Adam з адаптивною швидкістю навчання, що забезпечило стабільну збіжність при обробці різномірних МРТ-зображень.

Другий компонент здійснює перетворення внутрішніх репрезентацій глибокої мережі у множину інтерпретованих характеристик стандарту IBSI методом екстракції глибинних ознак: $F = F_t(F_{complex}, S)$. Формується загальна сукупність дескрипторів F обсягом 64 елементи (16 характеристик матриці зон сірих рівнів, 16 параметрів матриці довжин серій, 18 статистичних показників, 14 морфометричних властивостей), з якої виконується селекція для локального випадку $F_{local} \subset F$, причому $|F_{local}|$ значно менше $|F|$.

Третім компонентом виступає мережа Decision Rules Network, призначена для конструювання інтерпретованої моделі на виокремлених ознаках. Архітектура DRN організована у два яруси: початковий рівень містить нейронні елементи, що представляють логічні конструкції умовного типу, завершальний рівень формує

підсумковий висновок шляхом диз'юнктивного об'єднання правил початкового рівня. Конструювання F_{simple} відбувається ітеративно до моменту досягнення достатньої локальної узгодженості.

Механізм формування правил базується на пороговій активації нейронів першого рівня, де кожен нейрон навчається визначати специфічну комбінацію бінаризованих ознак. Позитивні вагові коефіцієнти відповідають умовам "більше порогу", негативні - "менше порогу", а нульові ваги виключають ознаку з правила. Застосування L1-регуляризації з коефіцієнтом $\lambda=0.01$ забезпечує розрідженість правил, обмежуючи кількість активних ознак у кожному правилі до 2-4 елементів, що критично важливо для когнітивної сприйнятності медичними фахівцями. Другий рівень реалізує логічну диз'юнкцію через softmax-активацію, дозволяючи системі комбінувати кілька правил для формування остаточного діагностичного висновку з відповідними ймовірностями для кожного класу патології.

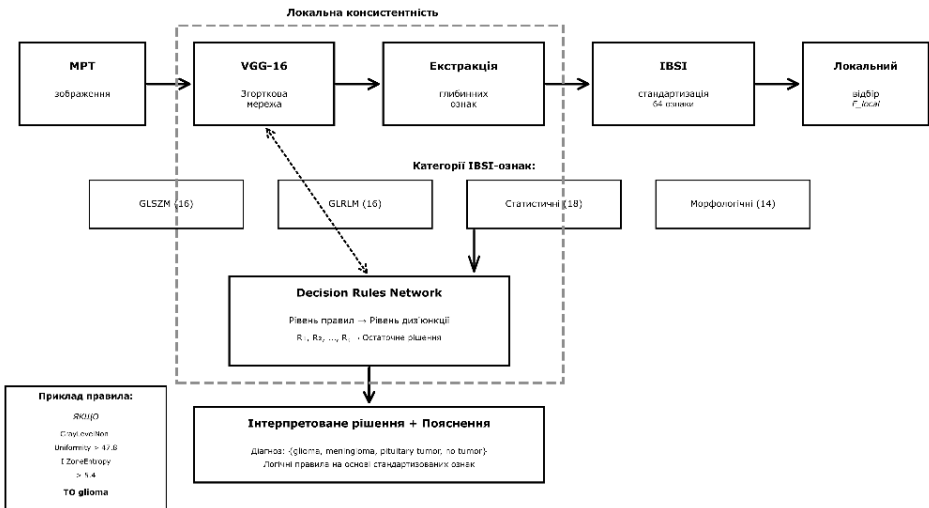


Рисунок 1 – Архітектура системи інтерпретованої діагностики пухлин мозку

Як видно з рисунка 1, система забезпечує послідовну обробку МРТ-зображень через базову зорткову мережу VGG-16, екстракцію глибинних ознак, їх стандартизацію відповідно до IBSI та локальний відбір найбільш інформативних характеристик. Пунктирна рамка позначає блок локальної консистентності, що забезпечує узгодження між рішеннями високоточної моделі (VGG-16) та інтерпретованої моделі (DRN) для конкретних клінічних випадків.

Таким чином, розроблений метод формування інтерпретованих інтелектуальних систем нейроонкологічної діагностики забезпечує синтез високої результативності з прозорістю висновків через локальну узгодженість. Комбінована архітектура VGG-16/DRN формує клінічно обґрунтовані тлумачення у вигляді логічних конструкцій на базі уніфікованих IBSI-дескрипторів. Методологія придатна для практичного використання у клінічному середовищі як засіб підтримки діагностичних рішень.

Перелік посилань

1. Liu K., Tao D. The roles of trust, personalization, loss of privacy, and anthropomorphism in public acceptance of smart healthcare services // *Computers in Human Behavior*. 2022. Vol. 127. <https://doi.org/10.1016/j.chb.2021.107026>
2. Albahri A.S. et al. A systematic review of trustworthy and explainable artificial intelligence in healthcare // *Information Fusion*. 2023. P. 156-191/ <https://doi.org/10.1016/j.inffus.2023.03.008>
3. Hatherley J.J. Limits of trust in medical AI // *Journal of Medical Ethics*. 2020. Vol. 46(7). Pp. 478–481. <https://doi.org/10.1136/medethics-2019-105935>
4. Manziuk E.A. et al. Approach to creating an ensemble on a hierarchy of clusters using model decisions correlation // *Przegląd Elektrotechniczny*. 2020. Vol. 96(9). Pp. 108–113. <https://doi.org/10.15199/48.2020.09.23>
5. Kaur D. et al. Trustworthy explainability acceptance: A new metric to measure the trustworthiness of interpretable AI medical diagnostic systems // *Complex, Intelligent and Software Intensive Systems*. 2021. Pp. 35–46. https://doi.org/10.1007/978-3-030-79725-6_4
6. Manziuk E. et al. Structural alignment method of conceptual categories of ontology and formalized domain // *CEUR Workshop Proceedings*. 2021. Vol. 3003. Pp. 11–22. <http://ceur-ws.org/Vol-3003/paper2.pdf>
7. Lakkaraju H., Bastani O. "How do I fool you?" Manipulating user trust via misleading black box explanations // *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*. 2020. Pp. 79–85. <https://doi.org/10.1145/3375627.3375833>
8. Qiao L., Wang W., Lin B. Learning accurate and interpretable decision rule sets from neural networks // *Proceedings of the AAAI Conference on Artificial Intelligence*. 2021. Vol. 35(5). Pp. 4303–4311. <https://doi.org/10.1609/aaai.v35i5.16555>
9. Holzinger A. et al. Information fusion as an integrative cross-cutting enabler to achieve robust, explainable, and trustworthy medical artificial intelligence // *Information Fusion*. 2022. Vol. 79. Pp. 263–278. <https://doi.org/10.1016/j.inffus.2021.10.007>.

УДК 621.396.67

Коваль М.О., Підченко С.К.

Хмельницький національний університет

АНТЕННА РЕШІТКА GPS-СИГНАЛУ НА БАЗІ СПІРАЛЬНИХ АНТЕН

У роботі розглянуто розробку та моделювання антенної решітки для прийому GPS-сигналів на основі спіральних конусних антен. Обґрунтовано актуальність використання таких антен у сучасних супутникових навігаційних системах завдяки їхній круговій правій поляризації (RHCP), високій спрямованості та здатності забезпечувати стабільний прийом сигналів.

The paper considers the development and modeling of an antenna array for receiving GPS signals based on spiral cone antennas. The relevance of using such antennas in modern satellite navigation systems is substantiated due to their right-hand circular polarization (RHCP), high directivity, and ability to provide stable signal reception.

У сучасних системах супутникової навігації (зокрема GPS) дедалі зростають вимоги до антенної частини: підвищена чутливість, великий коефіцієнт підсилення, широка кутова зона відслідковування супутників, стійкість до шумів антени для мобільних, авіаційних і космічних застосувань.

Спіральні конусні антени можуть забезпечувати задовільні характеристики у смузі L-діапазону (близько 1.2 – 1.6 ГГц). Проте одна спіральна антена має обмежений коефіцієнт підсилення і відносно широку діаграму випромінювання, що може зменшувати ефективність прийому слабких супутникових сигналів у присутності завад і шумів або коли супутники мають низький кут над горизонтом.

Тому актуальною стає ідея створення антенної решітки (масиву) на базі спіральних антен, яка поєднує переваги спіральних елементів (RHCP, простота конструкції) з можливістю підвищення підсилення, формування спрямованого діаграми, керованої або фіксованої, і покращеної стійкості до перешкод. Така антена-масив може бути використана не лише в системах GPS-навігації, а також у інших глобальних навігаційних супутникових системах (наприклад, GPS, GLONASS, Galileo, Beidou) для підвищення точності та надійності позиціонування.

Метою даного дослідження є розробка і моделювання антенної решітки на базі спіральних конусних антен, оптимізованої для прийому сигналів супутникової навігації (зокрема GPS)

У літературі описані різні конфігурації масивів спіральних антен. Зокрема, LaCalli [1] запропонував фазований 2×2 масив спіральних антен для CubeSat (робота на частоті Wi-Fi, ~ 2.4 ГГц) з можливістю керування спрямованістю променя. Dinkić et al. [2] розробили оптимізований квадратно-симетричний масив неоднорідних спіральних антен, отримавши коефіцієнт підсилення близько 20.5 дБі у смузі 0.9–1.1 ГГц. Водночас ці роботи не були орієнтовані на роботу в GPS-діапазоні (1.1–1.6 ГГц). Отже, спеціалізована розробка антенної решітки зі спіралей кінчної форми для частот GPS L1/L2 є актуальним.

Виникають питання оптимального фазування елементів, їх просторового розміщення та взаємодії із середовищем. Для вирішення цих задач доцільно застосовувати чисельні методи і оптимізаційні алгоритми (як це зроблено в [2] при оптимізації 3D-моделі масиву).

При розробці і моделюванні антенної решітки на базі спіральних конусних антен, передбачається забезпечення таких характеристик:

- високого коефіцієнта підсилення і спрямованості (для підвищення співвідношення сигнал/шум при слабких навігаційних сигналах);
- кругової правої поляризації (RHCP), сумісної з GPS/GHCC-сигналами;
- широкої кутової області покриття (зокрема для супутників з низьким кутом над горизонтом) або можливості формування/керування діаграмою в масиві;
- мінімізації впливу шумів та перешкод (через форму діаграми, бокові пелюстки, взаємозв'язок елементів);

У дослідженні використовується спіральна конусна антена (рисунок 1) як елемент решітки: параметри включають діаметр витка D , крок витка S (або кут нахилу спіралі α), кількість витків N , загальна висота спіралі L , а також основа (рефлектор, екран) і тип фідера. Важливим є підбір параметрів для роботи у діапазоні GPS L1 (~ 1.575 ГГц) або багаточастотного (L1/L2) режиму.

Далі формується масив (решітка) з кількох спіральних елементів (2×2), відстань між елементами $d = 1,5\lambda$, схема живлення та фазування. Використовується програма моделювання WIPL-D для обчислення характеристик.

При розробці прототипу антенної решітки спіральних антен для GPS-навігації одержано такі результати:

- підсилення масиву на 4дБ більше, ніж від одної спіральної антени за аналогічних умов, що дозволяє більш надійно приймати слабкі супутникові сигнали.
- діаграма випромінювання має звужену зону і зменшені бокові пелюстки.
- поляризація RHCP, що забезпечує сумісність із GPS-сигналами.

Проведені аналітичні і чисельні розрахунки свідчать, що сумісне використання спіральних антен у масиві дає синергійний ефект: кожний елемент

спеціалізується на поляризації і прийомі супутникового сигналу, тоді як масив забезпечує підсилення і спрямованість. Зменшення бокових пелюсток і підвищення підсилення прямо впливають на підвищення відношення сигнал/шум в навігаційних приймачах, що може забезпечити покращену точність позиціонування і підвищену стійкість до перешкод (наприклад, джерел інтерференції поза головним променем).

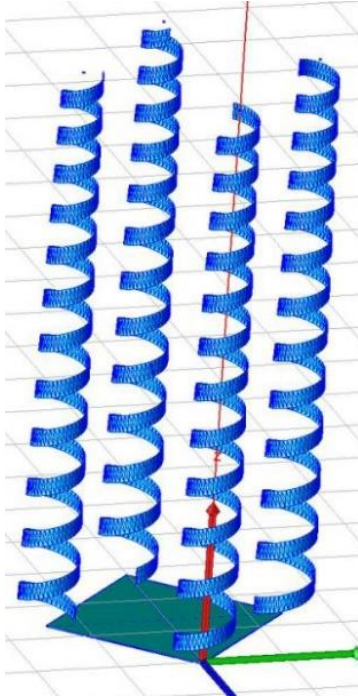


Рисунок 1 – Модель антенної решітки

Науковою новизною є використання конусних спіральних антен в антенній решітці і адаптація масиву спіральних антен саме під GPS/ГНСС-навігацію із врахуванням практичних обмежень. Результати показують, що оптимізація параметрів (діаметр, крок, кількість витків, відстань між елементами, фази живлення) дозволяє досягти балансу між габаритами та характеристиками антени.

Висновки. Розроблена антена-решітка на базі спіральних конусних антен показує обґрунтовану доцільність для систем GPS/ГНСС: вона дозволяє підвищити підсилення, покращити спрямованість і зменшити вплив небажаних компонентів сигналу (бокові пелюстки, шуми).

У порівнянні з одиночними спіральними антенами, застосування масиву дає переваги у більшості характеристик — особливо в умовах слабких сигналів, перешкод або обмеженого поля зору супутників.

Водночас реалізація масиву супроводжується низкою практичних викликів — точне розміщення елементів, узгодження фідерів і фаз, а також вплив взаємозв'язку елементів. Коректне проектування і калібрування мають вирішальне значення.

Отримані результати свідчать, що антена-решітка на базі спіральних конусних антен може бути ефективним рішенням для навігаційних приймачів, а також для спеціалізованих навігаційних систем, що вимагають підвищеної надійності і продуктивності.

Перспективи подальших досліджень. Подальші дослідження спрямовані на оптимізацію конструкції за допомогою сучасних алгоритмів для підбору параметрів масиву (розмір, крок, фаза), з метою покращення характеристик.

Дослідження варіантів матеріалів, легких конструкцій та інтеграційних рішень (наприклад, друковані спіральні антени, 3D-друк корпусу) для зменшення ваги і габаритів.

Перелік посилань

1. Phased Helical Antenna Array for CubeSat Application / Kameron LaCalli // Undergraduate Honors Theses. 32.
2. High-Gain Quad Array of Nonuniform Helical Antennas / Jelena Lj. Dinkić, Dragan I. Olćan, Antonije R. Djordjević, and Alenka G. Zajić // Hindawi International Journal of Antennas and Propagation Volume 2019, Article ID 8421809, 12 pages.
3. Optimization of Helical Antennas / Antonije R. Djordjević, Alenka G. Zajić, Milan M. Ilić, and Gordon L. Stüber // IEEE Antennas and Propagation Magazine, vol. 48, no. 6, pp. 107-116, December 2006.
4. Широкопasmовa планарна спіральна антена з периферійним збудженням / Цалієв Т. А., Сідень С. В. // Наукові праці ОНАЗ ім. О.С. Попова, 2018, № 1 UDC 621.396.677.8.

УДК 004.056.5

Коваль О.В.¹, Олексюк Д.А.², Чешун Д.В.², Чешун В.М.¹

¹Хмельницький національний університет

²Хмельницький фаховий економіко-технологічний коледж УЕП

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ DEVSECOPS ДЛЯ ЗМЕНШЕННЯ ВРАЗЛИВОСТЕЙ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

У роботі розглянуто інтеграцію практик безпеки в усі етапи життєвого циклу розробки програмного забезпечення в межах концепції DevSecOps. Проаналізовано підходи до виявлення вразливостей (SAST, DAST, IAST, пентест), їх переваги та недоліки. Описано стандарти OWASP, CVSS, MITRE ATT&CK і CWE як основу комплексної стратегії захисту. Запропоновано практичні рекомендації щодо тестування безпеки із застосування технологій DevSecOps.

The paper examines the integration of security practices into all stages of the software development lifecycle within the DevSecOps concept. Vulnerability detection approaches (SAST, DAST, IAST, pentest), their advantages and disadvantages are analyzed. OWASP, CVSS, MITRE ATT&CK, and CWE standards are described as the basis for a comprehensive security strategy. Practical recommendations for security testing using DevSecOps technologies are proposed.

У сучасному циклі розробки ПЗ інтеграція практик безпеки є критично важливою для зменшення ризиків. Підхід, відомий як DevSecOps [1], означає перенесення відповідальності за безпеку з кінця циклу розробки на його початок, інтегруючи інструменти та процеси безпеки на кожному етапі. Мета DevSecOps – зробити безпеку спільним завданням для всієї команди, забезпечуючи швидкість розробки (DevOps) без шкоди для надійності та захищеності продукту.

Ключові етапи інтеграції безпеки DevSecOps:

– етап планування та дизайну (Shift Left) ПЗ орієнтований на моделювання загроз та визначення вимог безпеки: В ході моделювання загроз команди аналізують архітектуру програми, визначають можливі активи та ідентифікують потенційні вектори атак, що дозволяє проактивно включити вимоги безпеки в дизайн. Визначення вимог безпеки: може бути реалізоване через включення стандартів, таких як OWASP ASVS, у технічне завдання;

– етап розробки та кодування – розробники використовують інструменти тестування безпеки програмного забезпечення, інтегровані безпосередньо в їхнє середовище розробки (IDE), щоб отримувати миттєвий зворотний зв'язок про потенційні вразливості, коли вони пишуть код. Також здійснюється

автоматизований аналіз сторонніх бібліотек та залежностей для виявлення відомих вразливостей та проблем ліцензування;

- етап тестування та збірки (CI/CD) – на кожному етапі збірки та розгортання в конвеєр CI/CD вбудовуються сканери, здійснюється тестування інфраструктури як коду (IaC) і перевірка налаштувань безпеки хмарних ресурсів і конфігураційних файлів;

- етап розгортання та моніторингу базується на таких технологіях захисту, як захист під час виконання (Runtime Protection) та постійний моніторинг (постійний моніторинг). Захист під час виконання передбачає використання брандмауерів веб-додатків (WAF) та інструментів RASP (Runtime Application Self-Protection), які відстежують виконання програми та можуть блокувати атаки.

Вибір методу виявлення вразливостей залежить від багатьох факторів, зокрема від етапу життєвого циклу, наявності вихідного коду та типу вразливостей, які очікується знайти. Існують три основні автоматизовані підходи (SAST, DAST, IAST) та ручне тестування [2-4].

- SAST (Static Application Security Testing – статичне тестування безпеки додатків) аналізує вихідний код, байт-код або бінарні файли програми без її запуску. SAST шукає потенційні вразливості, помилки конфігурації та недоліки кодування, які можуть призвести до проблем безпеки. Ідеальний для інтеграції на ранніх етапах життєвого циклу розробки, оскільки знаходить дефекти "біля джерела";

- DAST (Dynamic Application Security Testing – динамічне тестування безпеки додатків) аналізує програму під час її виконання. DAST взаємодіє з додатком як звичайний користувач (або зловмисник), надсилаючи різні вхідні дані та відстежуючи відповіді для виявлення вразливостей, таких як ін'єкції або міжсайтовий скриптинг (XSS). Ефективний для тестування того, що бачить зловмисник, і виявлення проблем у виконанні (наприклад, помилки конфігурації сервера, проблеми аутентифікації);

- IAST (Interactive Application Security Testing – інтерактивне тестування безпеки додатків) поєднує елементи SAST та DAST, працює під час виконання програми, як і DAST, але завдяки впровадженню агентів (сенсорів) у додаток він також має доступ до вихідного коду та внутрішніх процесів, як і SAST. Це дозволяє більш точно визначати, які рядки коду є причиною виявленої вразливості. IAST надає швидкий та точний зворотний зв'язок у процесі тестування, мінімізуючи "хибно-позитивні" спрацьовування.

Ручне тестування (також відоме як тестування на проникнення або пентест) передбачає залучення висококваліфікованих фахівців з безпеки (пентестерів), які вручну досліджують додаток, використовуючи свій досвід і креативність для пошуку складних або невідомих (zero-day) вразливостей, які автоматизовані

інструменти можуть пропустити. Переваги – здатність виявляти складні логічні помилки та унікальні вразливості, які залежать від бізнес-логіки. Ручне тестування критично важливе для додатків із високими вимогами до безпеки або для підтвердження результатів автоматизованих сканувань.

Проведений авторами аналіз демонструє ключові відмінності у принципах роботи, перевагах та недоліках кожного методу. Для побудови комплексної стратегії захисту важливо також розуміти їхню практичну ефективність проти різних класів загроз.

Для класифікації загроз часто використовують загальноновизнані стандарти, такі як OWASP Top 10 [5].

OWASP Top 10 є періодично оновлюваним переліком найкритичніших ризиків безпеки веб-додатків. Цей список допомагає розробникам і тестувальникам пріоритезувати зусилля, зосереджуючись на найбільш поширених і небезпечних вразливостях.

Окрім OWASP Top 10, для класифікації, оцінки та управління загрозами застосовують інші важливі стандарти та фреймворки:

- OWASP ASVS (Application Security Verification Standard – стандарт верифікації безпеки додатків) надає детальний, багаторівневий перелік вимог, яким додаток повинен відповідати для досягнення певного рівня безпеки;

- CVSS (Common Vulnerability Scoring System – загальна система оцінки вразливостей) представляє собою відкритий промисловий стандарт, який використовується для кількісної оцінки серйозності вразливостей програмного забезпечення;

- MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge – тактики, техніки та загальнодоступні знання противників) – це фреймворк, який більше орієнтований на кібератаки на рівні підприємства (після проникнення), він використовується для класифікації та документування тактик і технік, які використовують зловмисники, що допомагає командам безпеки зрозуміти та змодельовати потенційні вектори атак на їхні додатки.

- CWE (Common Weakness Enumeration – загальний перелік слабких місць) слугує формальним словником типових слабких місць у програмному забезпеченні та апаратній частині. Кожне слабе місце має унікальний ідентифікатор (наприклад, CWE-79 для XSS), що допомагає стандартизувати звітування про дефекти безпеки, які часто лежать в основі загроз, описаних у OWASP Top 10.

Ці стандарти забезпечують єдину мову та методологію для ідентифікації, класифікації та реагування на загрози, роблячи процес тестування безпеки додатків (Application Security Testing) більш структурованим та результативним, а також

дозволяють робити порівняльну оцінку ефективності методів виявлення проти класів вразливостей (таблиця 1).

Аналіз таблиці та наукових джерел дозволяє зробити однозначний висновок, що не існує єдиного "найкращого" методу. Ефективна стратегія виявлення вразливостей завжди є комплексною та багатошаровою, поєднуючи статичний аналіз на етапі розробки, динамічний аналіз на етапі тестування та регулярне ручне тестування.

Базуючись на аналізі методів та враховуючи технічні можливості інфраструктури можна сформулювати практичні пропозиції та рекомендації для ефективного виявлення вразливостей програмного забезпечення, що полягають у впровадженні циклічного процесу тестування безпеки. Цей процес поєднує автоматизовані інструменти та ручний аналіз. Використовуючи такий підхід, можна добитись швидких результатів і скорегувати їх вручну, якщо будуть виникати відхилення на етапі тестування.

Таблиця 1 – Оцінка ефективності методів проти класів вразливостей

Клас вразливостей	SAST	DAST	Ручне тестування
Вразливості коду: SQL Ін'єкція, XSS(Cross-Site Scripting) [6]	Висока	Середня / Висока	Висока
Вразливості часу виконання, помилки конфігурації сервера, слабке управління сесіями.	Низька	Висока	Висока
Маніпуляції цінами, обхід етапів авторизації. IDOR [7]	Низька	Низька	Висока

Практичне застосування DAST є першим кроком для розгорнутого застосунку. В умовах лабораторії це реалізується шляхом розгортання навмисно вразливого вебзастосунку у ізольованій «пісочниці» Кіберполігону.

Використання утиліти OWASP ZAP, яка надсилає тисячі тестових запитів до всіх виявлених точок входу, намагаючись знайти поширені вразливості є другим етапом. Після завершення роботи утиліти, фахівець має вручну перевірити кожну знайдену вразливість "високого" та "середнього" ризику, підтвердивши її реальну експлуатованість.

Застосування SAST буде ефективним, якщо є доступ до вихідного коду досліджуваного ПЗ. Паралельно запускається SAST-інструмент SonarQube або Snyk. Це дозволяє знайти вразливості, які DAST міг пропустити, що найважливіше – точно вказати на проблемний рядок коду, що значно прискорює виправлення.

Для запобігання XSS всі дані, що надходять від користувача, мають проходити валідацію на дозволені символи. Всі дані, що відображаються на сторінці, мають проходити контекстно-залежне кодування HTML, URL та JavaScript.

Автоматизація запуску SAST та DAST-сканерів у процесі безперервної інтеграції дозволяє виявляти вразливості при кожній зміні коду, що відповідає сучасним підходам до кіберзахисту.

Для критично важливих додатків необхідно проводити регулярне глибоке ручне тестування щонайменше раз на рік або після значних оновлень функціоналу для пошуку логічних вразливостей, як це зазначено в таблиці 1.

Перелік посилань

1. DevSecOps. URL: <https://www.devsecops.org/> (date of access: 10.10.2025).
2. Yuan Li, Peisen Yao, Kan Yu, Chengpeng Wang, Yaoyang Ye, Song Li, Meng Luo, Yepang Liu, Kui Ren. Understanding Industry Perspectives of Static Application Security Testing (SAST). Proceedings of the ACM on Software Engineering. Volume 2, Issue FSE. Article № FSE134. P.3033-3056. DOI: <https://dl.acm.org/doi/abs/10.1145/3729404> (date of access: 23.10.2025).
3. Yi Shen, Jian Zhang, Jieyun Huang, Shuming Shi, Wenjing Zhang, Jiangze Yan, Ning Wang, Kai Wang, Zhaoxiang Liu, Shiguo Lian. DAST: Difficulty-Adaptive Slow-Thinking for Large Reasoning Models. arXiv. 2025. №2503.04472v2. DOI: <https://arxiv.org/abs/2503.04472> (date of access: 20.10.2025)
4. Anoop Gupta, Sivakumar Ponnusamy. Cybersecurity and Ethical Hacking Harnessing AI. IJGIS. November 2024. DOI: <https://doi.org/10.21428/e90189c8.35100e4b> (date of access: 25.10.2025)
5. Anna Ilienکو, Denys Spys, Liliia Halata, Olena Dubchak. System approach to web application security: analysis of threats and methods of cyber protection. Vol. 26 №2 (2024): Ukrainian Information Security Research Journal. P. 277-293. URL: <https://h7.cl/1iBLW> (date of access: 17.10.2025).
6. Rabee Alqura'n, Mahmoud AlJamal, Issa Al-Aiash Ayoub Alsarhan Bashar Khassawneh Mohammad Aljaidi Rakan Alanazi Advancing XSS Detection in IoT over 5G: A Cutting-Edge Artificial Neural Network Approach. IoT. 2024. №5(3). P. 478-508. DOI: <https://www.mdpi.com/2624-831X/5/3/22> (date of access: 20.10.2025).
7. Bhutani V., Ghassemi Toosi F., Buckley J. Analysing the Analysers: An Investigation of Source Code Analysis Tools. Applied Computer Systems. 2024. Vol. 29, Issue 1. DOI: <https://h7.cl/1iC7i>(date of access: 21.10.2025).

УДК 004.8

Кок І.А., Поліщук Д.С., Кліменко В.І., Бармак О.В.

Хмельницький національний університет

НЕЙРОМЕРЕЖЕВА СИСТЕМА АВТОМАТИЗОВАНОГО КОНТРОЛЮ ЗА ТЮТЮНОПАЛІННЯМ У ПУБЛІЧНИХ МІСЦЯХ

У роботі розглянуто нейромережеву систему автоматизованого контролю за тютюнопалінням у публічних місцях, орієнтовану на підтримку реалізації антитютюнової політики в умовах сучасної урбанізованої інфраструктури. Ядром рішення є модель на основі Vision Transformer, попередньо навчена на великомасштабному наборі зображень і донавчена методом трансферного навчання на спеціалізованому корпусі кадрів із курцями та некурцями. Для підвищення прозорості роботи системи та придатності результатів до використання в адміністративних процедурах інтегровано модифікований Grad-CAM, що забезпечує візуалізацію найбільш інформативних ділянок кадру. Показано, що запропонований підхід створює підґрунтя для інтеграції контролю за тютюнопалінням у платформи «розумного міста» та подальшого розвитку мультимодальних систем моніторингу поведінкових порушень.

The paper presents the neural network-based system for automated control of smoking in public spaces, designed to support tobacco control policy within modern urban environments. Its core is a Vision Transformer model pre-trained on a large-scale image dataset and fine-tuned via transfer learning on a domain-specific corpus of images containing smokers and non-smokers. To ensure decision transparency and suitability of the outputs for administrative procedures, a modified Grad-CAM method is integrated, providing visual explanations that highlight the most informative regions of each frame. The proposed approach forms a basis for integrating smoking control into smart city platforms and for further development of multimodal AI systems for monitoring behaviour-related violations in public spaces.

Актуальність застосування методів комп'ютерного зору та глибокого навчання для автоматизованого контролю за тютюнопалінням у публічних місцях зумовлена зростаючими вимогами до дотримання антитютюнового законодавства та необхідністю оперативного моніторингу поведінкових порушень у багатолюдних урбанізованих просторах [1]. Поширення мереж відеоспостереження в містах створює передумови для впровадження інтелектуальних систем відеоаналітики [2], які здатні автономно виявляти ризиковані чи заборонені дії, однак традиційні алгоритми комп'ютерного зору, засновані на ручних ознаках, виявляються недостатньо стійкими до варіацій освітлення, ракурсів, динамічних сцен та поведінкової різноманітності [3]. Тютюнопаління характеризується поєднанням дрібних локальних об'єктів (сигарета, дим) і складних позо-жестових патернів, що

робить задачу виявлення нетривіальною та потребує використання високорівневих моделей, здатних до глибинної інтерпретації просторово-часових даних.

Сучасні конволюційні нейронні мережі [4] та трансформерні архітектури [5] відкривають можливість моделювання складних візуальних залежностей, інтегруючи як локальні текстури, так і глобальні контексти сцени [6]. CNN, зокрема ResNet, EfficientNet або MobileNet, демонструють високу продуктивність у завданнях детекції дрібних об'єктів та класифікації поведінкових ознак [7], тоді як Vision Transformer забезпечує ширшу контекстуальну узагальненість і стійкість до шумів відеопотоку [8]. Комбінація цих підходів дозволяє створювати моделі, здатні виявляти сигарету навіть за умов часткового перекриття об'єкта, низької якості кадру або нерегулярної появи диму, що суттєво підвищує точність системи порівняно з класичними методами [9].

У контексті цієї роботи ключовою є можливість масштабування архітектур глибокого навчання до режиму безперервного аналізу відеопотоків у реальному часі [10, 11]. Оптимізовані CNN дозволяють виконувати інференс з високою пропускну здатністю, що є критичним для використання в міських системах відеоспостереження, де кількість камер може сягати тисяч. Додаткові переваги створює застосування трансферного навчання, яке дає змогу швидко адаптувати попередньо навчені моделі до спеціалізованих корпусів відеоданих, що містять унікальні патерни тютюнопаління, притаманні конкретним середовищам спостереження. Такі моделі здатні ураховувати контекст локації, характерні жести користувачів, типи сигаретних виробів, що підсилює їхню робастність та зменшує кількість хибних спрацьовувань [12].

Не менш важливим аспектом є питання інтерпретованості, яке вирішується завдяки використанню теплових карт уваги, зокрема модифікованих варіантів Grad-CAM. Це забезпечує прозорість прийняття рішень системою та робить можливим використання результатів у юридично значущих процедурах. Візуалізація інформативних ділянок кадру дає змогу операторам підтвердити або спростувати факт порушення, а також коригувати роботу моделі за рахунок аналізу помилкових класифікацій.

Таким чином, застосування комп'ютерного зору та CNN у задачі виявлення тютюнопаління формує технологічну основу для створення масштабованих, стійких і пояснюваних систем контролю поведінки в публічних місцях. У поєднанні з інфраструктурою «розумного міста» такі системи можуть стати ключовим інструментом у реалізації політик громадського здоров'я, а також у підвищенні ефективності міських сервісів безпеки та превентивного моніторингу.

Нейромережева система автоматизованого контролю за тютюнопалінням у публічних місцях розглядається як складний програмно-апаратний комплекс, що поєднує технології комп'ютерного зору, глибокого навчання та інструменти пояснюваного штучного інтелекту для підтримки реалізації антитютюнової політики в умовах сучасного міського середовища. Її призначення полягає у безперервному аналізі відеопотоків із камер спостереження, виявленні ознак

тютюнопаління в реальному часі, формуванні машинних рішень щодо факту порушення та наданні оператору інтерпретованих візуальних доказів, придатних для подальших адміністративних дій. Концепція такої системи спирається на попередньо розроблений метод автоматизованого контролю за тютюнопалінням з використанням архітектури Vision Transformer та Grad-CAM-візуалізацій, удосконалюючи його до рівня повноцінної прикладної інфраструктури відеоаналітики.

Проблематика тютюнопаління в публічних місцях має комплексний характер і виходить за межі суто медичного виміру. Вона охоплює аспекти громадського здоров'я, правозастосування, міського планування та цифрової трансформації сервісів безпеки. Попри багаторічну практику нормативного обмеження куріння, більшість держав, у тому числі Україна, стикається із систематичними порушеннями заборони на використання тютюнових виробів, електронних сигарет та пристроїв нагрівання тютюну у місцях масового скупчення людей. Пасивне куріння, яке неминуче супроводжує такі порушення, асоціюється з підвищеним ризиком серцево-судинних, онкологічних та респіраторних захворювань, причому особливо вразливими є діти, літні люди та особи з хронічними хворобами дихальної системи. За умов інтенсивної урбанізації та збільшення пасажиропотоків у громадському транспорті, торговельно-розважальних центрах, на транспортних вузлах та територіях освітніх закладів навіть епізодичні випадки куріння створюють значний сукупний ризик для населення.

Традиційна модель контролю за дотриманням антитютюнового законодавства ґрунтується на чергуванні працівників поліції, інспекторів муніципальних служб чи локального персоналу безпеки. Такий підхід демонструє обмежену ефективність у масштабі сучасного міста, оскільки фізична присутність контролюючих осіб у кожній потенційно проблемній точці є економічно недоцільною, а людський фактор неминуче призводить до пропуску значної частки порушень. Розгортання мереж відеоспостереження формує технічну основу для переходу до автоматизованих стратегій моніторингу поведінки людей, проте без інтелектуальної обробки відеоданих такі системи залишаються пасивним засобом фіксації подій, а не інструментом активного запобігання.

Нейромережева система автоматизованого контролю за тютюнопалінням пропонує якісно інший рівень функціонування інфраструктури відеоспостереження. Вона перетворює камери з традиційних сенсорів зображення на активні вузли мережі штучного інтелекту, що здатні самостійно розпізнавати ситуації куріння на основі аналізу просторово-візуальних патернів. Відповідно, навантаження на персонал зміщується від ручного перегляду багатогодинних відеозаписів до вибіркової роботи з уже попередньо відфільтрованими та інтерпретованими сповіщеннями, що містять кадри з високою ймовірністю виявленого порушення. Це не лише підвищує оперативність реагування, але й створює прозорий, задокументований механізм фіксації інцидентів, який знижує суб'єктивність оцінок.

З науково-технічної точки зору, завдання розпізнавання фактів тютюнопаління має низку особливостей, які відрізняють його від класичних задач комп'ютерного зору. По-перше, об'єкти інтересу є дрібними, часто частково перекритими і візуально подібними до фонового шуму: сигарета має невеликі розміри, а дим може маскуватися під атмосферні ефекти, відблиски чи шуми сенсора. По-друге, ключовими індикаторами є не лише самі об'єкти, а й поведінкові жести – характерне положення руки, піднесення її до рота, певна конфігурація обличчя. По-третє, середовище спостереження характеризується значною варіативністю: різкі зміни освітлення, контрасту, ракурсу, типу камери, щільності навігпу. Ці фактори обумовлюють необхідність застосування архітектур глибокого навчання, здатних моделювати глобальний контекст сцени та вловлювати високорівневі залежності між просторово рознесеними ознаками.

Класичні згорткові нейронні мережі, які домінували в комп'ютерному зорі протягом останнього десятиліття, демонструють високу ефективність у задачах класифікації та детекції об'єктів, однак їхня локальна природа обробки поступово виявляє обмеження в подібних задачах. Згортки будують подання на основі локальних рецептивних полів, і хоча використання глибоких архітектур, залишкових зв'язків та багатомасштабних блоків частково компенсує цей недолік, глобальний контекст сцени все ще відновлюється опосередковано. На противагу цьому трансформерні підходи, такі як Vision Transformer, безпосередньо моделюють взаємодію між усіма фрагментами зображення через механізм самоуваги, що особливо важливо для ситуацій, коли вирішальними є відносні взаєморозташування об'єктів та поведінкові патерни.

У запропонованій нейромережевій системі центральне місце посідає модель на основі Vision Transformer, попередньо навчена на великомасштабному наборі ImageNet та донавчена за допомогою трансферного навчання на спеціалізованому корпусі зображень із курцями та некурцями. Вхідний кадр з відеопотоку перетворюється у нормалізоване зображення фіксованого розміру, після чого розбивається на рівновеликі патчі, які проєктуються у векторний простір ознак. Послідовність цих векторів доповнюється позиційними кодуваннями, що зберігають інформацію про розташування фрагментів у вихідному кадрі, а також спеціальним класифікаційним токеном, який акумулює глобальну інформацію. Далі послідовність проходить через багат шаровий енкодер із багатоголовою самоувагою та блоками багат шарового перцептрона, де формується високорівневе подання сцени.

Стратегія трансферного навчання, покладена в основу системи, орієнтована на ефективну роботу з відносно невеликими доменно-специфічними датасетами. Основні параметри трансформерного енкодера залишаються замороженими, що дозволяє зберегти узагальнюючу здатність моделі, накопичену на базовому наборі даних, тоді як донавчання зосереджується на фінальному класифікаційному шарі, адаптуючи його до дихотомії «куріння / відсутність куріння». Такий підхід мінімізує ризик перенавчання, зменшує обчислювальні витрати та дає змогу

впроваджувати систему на обладнанні з обмеженими ресурсами, зокрема на вбудованих рішеннях у мережесх відеореєстраторах або edge-пристроях.

Важливим концептуальним компонентом нейромережесх системи є пояснюваність прийнятих рішень. Оскільки результати автоматизованого контролю можуть бути підставою для адміністративних стягнень, оператори та уповноважені органи мають отримувати не лише бінарний висновок моделі, а й наочне обґрунтування. Для цього в систему інтегровано модифікований підхід Grad-CAM, адаптований до трансформерної архітектури. Після отримання класифікаційного результату алгоритм обчислює градієнти за відношенням до проміжних представлень патчів, агрегує їх та формує теплову карту важливості, яка накладається на оригінальний кадр. Таким чином, оператор бачить, які області зображення стали вирішальними: це може бути зона в руках людини, обличчя, згусток диму або комбінація кількох ділянок. Така візуалізація підвищує довіру до системи, спрощує виявлення помилкових спрацювань та сприяє аналізу граничних випадків. Діаграма класів розробленої інтелектуальної системи наведено на рисунку 1.

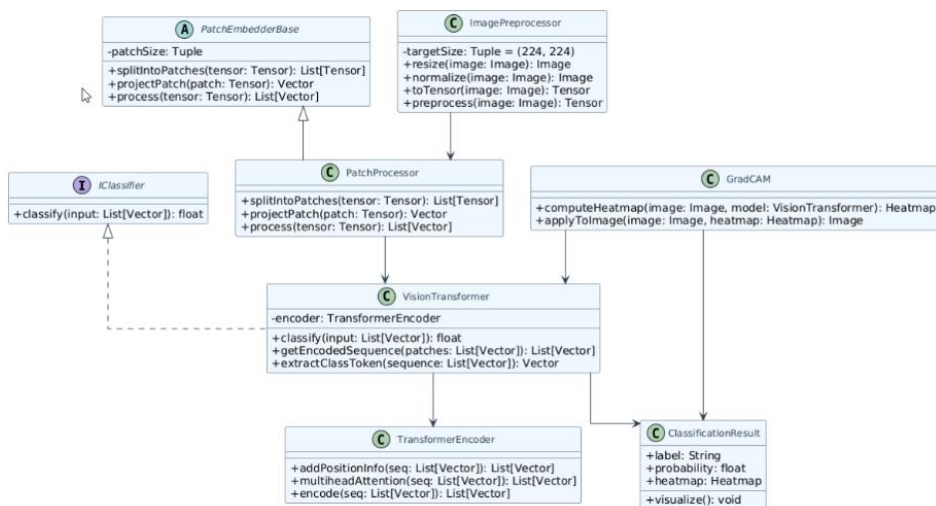


Рисунок 1 – Діаграми класів

Система функціонує в кількох логічно пов'язаних режимах. У режимі безперервного моніторингу відеопотік із камер розщеплюється на окремі кадри із заданою періодичністю або подією (наприклад, за зміни сцени чи виявлення людей зовнішніми детекторами). Кожен кадр або серія ключових кадрів передається до модуля попередньої обробки, де виконується масштабування, колірна нормалізація, при потребі – стабілізація та усунення артефактів стиснення. Після цього

зображення потрапляє до нейромережевого ядра, яке повертає ймовірність наявності тютюнопаління. Якщо ця ймовірність перевищує наперед визначений поріг, модуль прийняття рішень створює об'єкт події, до якого включаються кадр-джерело, теплові карти, часові мітки та ідентифікатор камери. Подальші дії залежать від політики експлуатації: система може автоматично формувати сповіщення оператору, зберігати фрагмент відео у спеціальному сховищі, інтегруватися з міськими центрами обробки даних або інформаційними системами правоохоронних органів.

Другий важливий режим – аналітико-дослідницький. Він призначений для розробників, адміністраторів та експертів у сфері громадського здоров'я і дозволяє працювати з архівними даними, оцінювати динаміку порушень у певних локаціях, час доби чи днях тижня, а також аналізувати помилки нейромережі. У рамках цього режиму забезпечується розширена візуалізація результатів, можливість переглядати серії кадрів до і після події, а також побудова статистичних звітів. Така функціональність відкриває перспективи інтеграції нейромережевої системи контролю за тютюнопалінням у ширші платформи «розумного міста», де дані про куріння розглядаються поряд з іншими індикаторами безпеки та поведінки населення.

Формування навчального і тестового корпусу є критичним етапом, що визначає якість роботи системи. Для початкового навчання використовується відкритий збалансований датасет зображень, у якому категорії курців та некурців представлені приблизно в рівних пропорціях. У класі «курців» переважають сцени з чітко видимими сигаретами або пристроями для вейпінгу, у той час як клас «некурців» включає як нейтральні зображення, так і кадри з подібними до куріння жестами, але без фактичної наявності тютюнових виробів. Цей прийом ускладнює задачу й змушує модель шукати тонкі відмінності, не спираючись лише на грубі контури руки біля обличчя. Після базового навчання система може донаводитися на локальних даних з конкретних камер або інфраструктурних об'єктів, що дає змогу враховувати особливості реального середовища – типові ракурси, освітлення, локальні культурні патерни поведінки.

Експериментальне дослідження нейромережевої системи проводиться на основі розділення корпусу зображень на навчальну, валідаційну та тестову підмножини. У процесі тренування відстежуються такі метрики, як точність класифікації, повнота, точність у вузькому розумінні, F1-міря та площа під ROC-кривою. Аналіз кривих навчання й валідації дозволяє своєчасно зупиняти навчання при досягненні плато, запобігаючи перенавчанню. За результатами тестування на відкладеній вибірці можна зробити висновок про здатність моделі узагальнювати знання на нових сценах. Особливу увагу приділяють аналізу помилкових позитивних та помилкових негативних спрацювань, оскільки перші створюють надлишкове навантаження на операторів, а другі безпосередньо знижують ефективність контролю.

З погляду системної інтеграції важливою характеристикою є масштабованість нейромережевої системи. Вона повинна коректно працювати як у форматі пілотного проекту на декількох камерах, так і в умовах міської інфраструктури з сотнями чи тисячами джерел відео. Для цього передбачається модульна мікросервісна архітектура, у якій окремі вузли відповідають за отримання відеоданих, буферизацію, розподіл кадрів між інференс-модулями, зберігання результатів та візуалізацію. За наявності графічних прискорювачів або спеціалізованих нейропроцесорів система може виконувати обробку в режимі, близькому до реального часу, що дозволяє оперативно реагувати на порушення в публічних місцях. Рисунок 2 наводить приклад роботи розробленої системи.

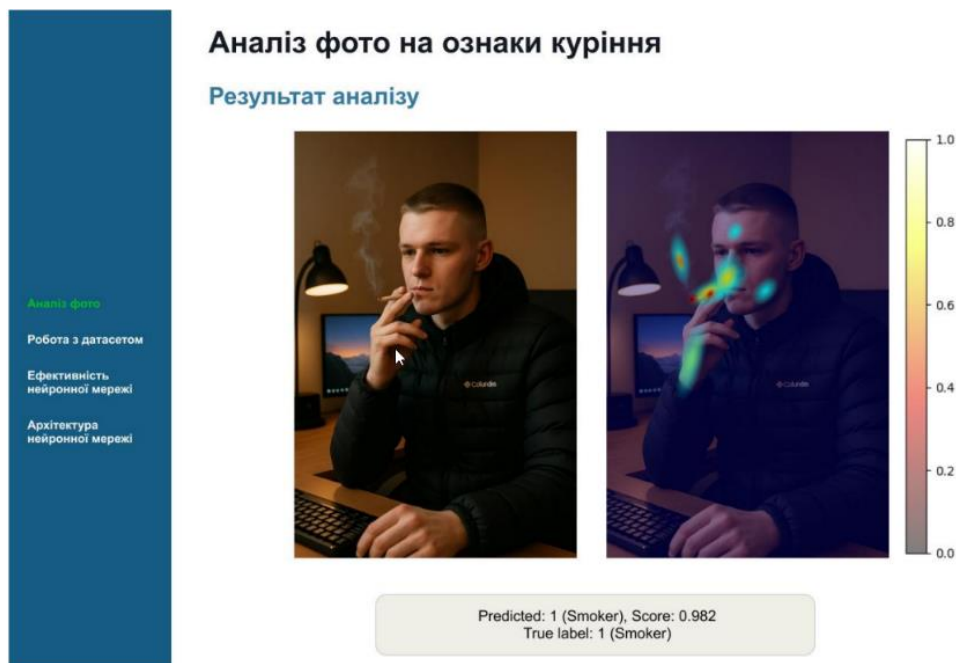


Рисунок 2 – Результат виявлення тютюнопаління

Разом з технічними аспектами не можна ігнорувати питання етики та захисту персональних даних. Нейромережева система автоматизованого контролю за тютюнопалінням працює з відеозображеннями людей, а отже повинна відповідати вимогам законодавства щодо обробки персональних даних і принципам мінімізації втручання в приватність. Це передбачає обмеження доступу до повних відеозаписів, використання ролей та прав доступу, протоколювання дій операторів, а також, за можливості, застосування технологій деперсоналізації або розмиття

облич у тих сценаріях, де ідентифікація конкретної особи не є необхідною. Технічні рішення мають бути доповнені організаційними регламентами, що визначають, хто, скільки часу та з якою метою може працювати з даними системи.

Незважаючи на перспективність запропонованого підходу, нейромережева система має низку обмежень, які визначають напрями подальших досліджень. Одним із ключових є залежність від якості та репрезентативності даних: якщо у навчальному наборі недостатньо прикладів певних сценаріїв, система може демонструвати нестабільну поведінку в реальних умовах. Ще одним викликом є адаптація до нових форм курильних пристроїв, дизайни яких швидко змінюються під впливом ринку. Це вимагає регулярного оновлення корпусу зображень та періодичного донавчання моделі. Окремою лінією розвитку є перехід від класифікації на рівні кадру до повноцінної просторово-часової детекції, коли система здатна враховувати динаміку жестів у коротких відеофрагментах, а не лише статичні зображення.

Перспективним напрямом є також використання мультимодальних моделей, які поєднують аналіз відео з іншими каналами даних. Наприклад, у закритих приміщеннях система може доповнюватися сенсорами якості повітря, що фіксують концентрації продуктів згоряння, а на відкритих майданчиках – даними з соціальних сервісів або платформи «розумне місто», які вказують на масові заходи чи аномальні скупчення людей. Інтеграція таких сигналів із нейромережею дозволить формувати більш надійні композитні рішення, зменшуючи кількість хибних спрацювань.

Підсумовуючи, нейромережева система автоматизованого контролю за тютюнопалінням у публічних місцях поєднає низку сучасних технологічних складових: архітектуру Vision Transformer для високоточного розпізнавання візуальних ознак куріння, методи трансферного навчання для роботи з обмеженими датасетами, Grad-CAM-інструменти пояснюваності, модульну інфраструктуру для обробки відеопотоків та аналітичні засоби для підтримки прийняття управлінських рішень. Її впровадження здатне підвищити ефективність виконання антитютюнового законодавства, зменшити ризики, пов'язані з пасивним курінням, та сприяти побудові більш безпечного й здорового міського середовища. Одночасно система створює підґрунтя для подальших досліджень на стику глибокого навчання, комп'ютерного зору, цифрової безпеки та політики громадського здоров'я, де кожне нове покоління моделей може забезпечувати ще більш точний, стійкий і прозорий контроль за поведінковими порушеннями у публічному просторі.

Перелік посилань

1. Куріння, що повільно вбиває. До Всесвітнього дня без тютюну. НАМН України. НАМН України. URL: <https://amnu.gov.ua/kurinnya-shho-povilno-vbyvaye/>
2. Аналіз ринку цигарок в Україні. Інвестиції в Україні. InVenture. URL: <https://inventure.com.ua/uk/analytics/investments/analiz-rinku-cigarok-v-ukrayini>

3. Vezha Smoking Detection module allows to identify a smoker with a cigarette. Milestone Systems. URL: <http://www.milestonesys.com/technology-partner-finder/incoresoft-llc/vezha-smoking-detection/>
4. Didur V., Molchanova M., Mazurets O. Research on the effectiveness of neural network detection of plots with the destroyed buildings remains. Modern technologies and science: problems, new and relevant developments. Proceedings XXI International Scientific and Practical Conference. May 26, 2025. Zaragoza, Spain. Pp. 245-251.
5. Bas I.S., Kadyńska V.D., Klimenko V.I., Mazurets O.V. Convolutional Neural Network Transfer Learning Method for Aircraft Image Classification. Scientific method: reality and future trends of researching. Proceedings of VI International Scientific and Theoretical Conference. June 6, 2025. Montreal, Canada. Pp. 147-155.
6. Mushtyn O., Sobko O., Molchanova M., Mazurets O. Convolutional Neural Network Architecture for Image-Based Architectural Style Recognition. Evolving Science: Theories, Discoveries and Practical Outcomes. Proceedings of 4th International Scientific and Practical Conference. June 9-11, 2025. Zurich, Switzerland. Pp. 130-143.
7. Malaydakh V., Molchanova M., Shevchuk P., Mazurets O. Deep learning neural network architecture for determining sunflower growth stage from visual data. Modern Scientific Research: Theoretical and Practical Aspects. Proceedings II International Scientific and Practical Conference. May 26-28, 2025. Riga, Latvia. Pp. 143-148.
8. Hladun O.V., Molchanova M.O., Zalutskia O.O., Mazurets O.V. Effectiveness research of using ViT neural network architecture for classifying the destroyed buildings remains. Achievements of Science and Applied Research. Proceedings of 2nd International Scientific and Theoretical Conference. May 19-21, 2025. Dublin, Ireland. Pp. 96-100.
9. Krak I., Mazurets O., Zalutskia O., Molchanova M., Barmak O., Approach for Postural Disorders Recognizing from Visual Data Using Deep Neural Network, CEUR Workshop Proceedings. 4049. 2025. Pp. 244-255.
10. Кок І.А., Мазурець О.В., Кліменко В.І., Петровський С.С. Метод автоматизованого визначення оцінки ступеня співвіднесення графічних зображень до актуальних категорій із застосуванням згорткової нейронної мережі. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». 15-16 листопада 2024. Хмельницький, 2024. с. 277-281.
11. Kok I.A., Kadyńska V.D., Zalutskia O.O., Mazurets O.V. Object-Oriented Intelligent System for Automated Control of Smoking by Video Data. Current scientific goals, approaches and challenges. Proceedings of IV International Scientific and Theoretical Conference. June 13, 2025. Dresden, Federal Republic of Germany. Pp. 156-164.
12. Кок І.А., Мазурець О.В., Молчанова М.О. Пояснений підхід на основі трансферного навчання Vision Transformers до виявлення куріння у публічних просторах. Матеріали XIII Міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології ІУСТ-ОДЕСА-2025». 24-26.09.2025. Одеса. 2025. С.147-149.

УДК 004.4

Колесніков В.Р., Капустян М.В.

Хмельницький національний університет

ПОРІВНЯЛЬНИЙ АНАЛІЗ РІВНІВ ОБФУСКАЦІЇ .NET-КОДУ

У роботі проведено порівняльний аналіз ефективності різних рівнів обфускації .NET-додатків. Досліджено три стандартні профілі захисту в інструменті ConfuserEx. Було проаналізовано ключові техніки та методи, що застосовуються на кожному рівні обфускації, та їхній вплив на характеристики файлу, а саме порівнюється ступінь ускладнення статичного аналізу (читабельність) та розмір обфускованих файлів. Запропоновано рекомендації щодо вибору оптимального рівня захисту залежно від завдань проекту.

The paper carries out a comparative analysis of the effectiveness of different levels of obfuscation .NET applications. Three standard protection profiles in the ConfuserEx tool were studied. Key techniques and methods applied at each obfuscation level and their impact on file characteristics were analyzed, namely comparison between the degrees of complexity of static analysis and readability, comparison of the size of obfuscated files. Recommendations for choosing the optimal level of protection depending on the tasks of the project are offered.

Скомпільовані .NET-додатки містять проміжний код, який легко декомпілюється у вихідний код, практично ідентичний оригінальному, за допомогою таких інструментів, як dnSpyEx [1]. Це створює загрозу крадіжки інтелектуальної власності, комерційних таємниць та полегшує зловмисникам пошук вразливостей, що є ризиком, визнаним у стандартах безпеки [2].

На ринку присутні як безкоштовні, так і комерційні програмні забезпечення для обфускації, у даному дослідженні використаний інструмент ConfuserEx [3], який пропонує гнучке налаштування параметрів обфускації, що дозволяє обирати між потрібним рівнем захисту та продуктивністю. Виділяють ключові методи перешкоджання статичному аналізу [4], а саме: перейменування, шифрування рядків та заплутування потоку керування (Control Flow Obfuscation).

Метою є дослідження та порівняння ефективності трьох стандартних профілів обфускації (Minimum, Normal, Maximum). Завданням є проаналізувати їхній конкретний вплив на розмір файлу, читабельність коду та складність статичного аналізу.

Для експерименту було створено тестовий додаток на .NET 6 з оригінальним розміром .dll збірки 6 КБ. Декомпіляція оригінального файлу на рисунку 1 показує повну відповідність вихідному коду.

```

1  using System;
2  using System.Runtime.CompilerServices;
3
4  namespace TestApp
5  {
6      // Token: 0x02000005 RID: 5
7      [NullableContext(1)]
8      [Nullable(0)]
9      internal class Program
10     {
11         // Token: 0x06000006 RID: 6 RVA: 0x00002090 File Offset: 0x00000290
12         private static void Main(string[] args)
13         {
14             new Program.SecureManager().ValidateUser("admin", "pa$$w0rd");
15             Console.WriteLine("Press any key to exit...");
16             Console.ReadKey();
17         }
18     }
19
20     // Token: 0x02000006 RID: 6
21     [Nullable(0)]
22     public class SecureManager
23     {
24         // Token: 0x06000008 RID: 8 RVA: 0x000020C0 File Offset: 0x000002C0
25         public bool ValidateUser(string username, string password)
26         {
27             if (string.IsNullOrEmpty(password))
28             {
29                 return false;
30             }
31             if (password.Length < 8)
32             {
33                 Console.WriteLine("Password is too short!");
34                 return false;
35             }
36             Console.WriteLine("API Key is: my_secret_api_key_12345");
37             return username == "admin" && password == "pa$$w0rd";
38         }
39
40         // Token: 0x04000003 RID: 3
41         private const string ApiKey = "my_secret_api_key_12345";
42     }
43 }
44

```

Рисунок 1 – Декомпільований код додатка до обфускації

Далі, оригінальна збірка була послідовно оброблена з трьома різними профілями захисту.

Профіль Minimum: Цей рівень застосовує лише найбазовіший захист, переважно агресивне перейменування. Усі змістовні імена класів (SecureManager), методів (ValidateUser) та просторів імен (TestApp) замінюються на нечитабельні символи. Однак логіка самих методів залишається практично незмінною. Розмір файлу збільшився незначно. Розмір опрацьованого файлу 8 кілобайт. Результат обфускованого коду зображено на рисунку 2.

```

1 using System;
2
3 // Token: 0x02000005 RID: 5
4 ["B-DBodvrrn9%9ya&'8Uo8dKJ](1)]
5 ["0;;M\JtV\9J0k2=CJEmd(v0(0)]
6 internal class \u200D\u200B\u2008\u200E\u2008\u2008\u200A\u206A\u206A\u202D\u200F\u206D\u200B\u206F\u206C\u200C\u206C\u206F\u202D
  \u206E\u200B\u202B\u206A\u200B\u206F\u206F\u206E\u202A\u202C\u206D\u202A\u200B\u200D\u206E\u206E\u206F\u206F\u202A\u200B
  \u200B\u202E\u206F\u206D\u202E
7 {
8 // Token: 0x06000007 RID: 7 RVA: 0x0000208E File Offset: 0x0000208E
9 private static void \u202B\u202D\u200C\u200D\u206D\u200B\u200F\u206F\u206F\u206A\u200E\u202B\u206D\u206F\u206E\u206E\u200C
  \u206A\u206E\u200F\u200F\u200D\u200C\u200C\u202E\u200B\u200E\u200E\u200C\u206C\u200B\u202C\u206E\u206F\u200C\u202D\u206C\u202E
  \u200E\u206A\u206E\u206E\u202E\u202E(string[] A_0)
10 {
11     new \u200D\u200B\u2008\u200E\u2008\u2008\u200A\u206A\u206A\u202D\u200F\u206D\u200B\u206F\u206C\u200C\u206C\u206F\u202D\u206E
      \u200B\u202B\u206A\u200B\u206F\u200F\u206E\u202A\u202C\u206D\u202A\u200B\u200D\u206E\u206E\u206F\u202A\u200B
      \u200B\u202E\u206F\u206D\u206D\u202E. \u206D\u206E\u206E\u206E\u202B\u202C\u206F\u206F\u202C\u202A\u206E\u202A\u206D\u206D\u200D
      \u202D\u206B\u200E\u206F\u206F\u206C\u206B\u206B\u202C\u206D\u206D\u206B\u202C\u206A\u202A\u200B\u200E\u200F\u206B\u202C
      \u202A\u202C\u206C\u200E\u200E\u200C\u200C\u202C\u200D\u206F\u206F\u202E(). \u206D\u202C\u202C\u202B\u200B\u202A\u202C\u202C\u206E
      \u202C\u206A\u200C\u202B\u206D\u206D\u200D\u202B\u200F\u202B\u206B\u206C\u206F\u202D\u200B\u202D\u200F\u202D\u206C\u206B
      \u206F\u202D\u200E\u200B\u200D\u206B\u206C\u206C\u200D\u206C\u202E\u206A\u206B\u206F\u202E("admin", "pa$
      $w0rd");
12     Console.WriteLine("Press any key to exit...");
13     Console.ReadKey();
14 }
15
16 // Token: 0x02000006 RID: 6
17 ["0;;M\JtV\9J0k2=CJEmd(v0(0)]
18 public class \u206D\u206E\u202B\u202C\u206F\u206F\u202C\u202A\u206E\u202A\u206D\u206D\u200D\u202D\u206B\u200E\u206F
  \u206C\u206B\u206B\u202C\u206D\u206D\u206B\u206C\u202C\u206A\u202A\u200B\u200E\u200F\u206B\u206B\u202C\u202A\u206C\u200E\u200E\u200C
  \u202C\u200D\u206F\u200F\u202E
19 {
20 // Token: 0x06000009 RID: 9 RVA: 0x000021B4 File Offset: 0x000021B4
21 public bool \u206D\u202C\u202B\u200B\u200B\u200B\u202C\u206E\u202C\u206A\u200C\u202B\u206D\u200D\u202B\u200F\u202B
  \u206C\u206B\u206B\u206F\u202D\u200B\u202D\u200F\u206C\u206B\u206B\u206F\u202D\u200E\u200B\u200D\u206B\u206C\u200D\u206C
  \u206D\u202E\u206A\u206B\u206F\u202E(string A_1, string A_2)
22 {
23     if (string.IsNullOrEmpty(A_2))
24     {
25         return false;
26     }
27     if (A_2.Length < 8)
28     {
29         Console.WriteLine("Password is too short!");
30         return false;
31     }
32     Console.WriteLine("API Key is: my_secret_api_key_12345");
33     return A_1 == "admin" && A_2 == "pa$w0rd";
34 }
35
36 // Token: 0x04000003 RID: 3
37 private const string \u200D\u200F\u206A\u206C\u200D\u206B\u200D\u202A\u200D\u206F\u200C\u206F\u202D\u200C\u202D
  \u202C\u206B\u200F\u202A\u202A\u200E\u200E\u206D\u200C\u206A\u206E\u200E\u200F\u206D\u206D\u206F\u202C\u206F\u200F\u206F
  \u206F\u202E\u200E\u200B\u200C\u206F\u206E\u202E = "my_secret_api_key_12345";
38 }
39
40

```

Рисунок 2 – Декомпільований код додатка після обфускації профілем Minipit

Профіль Normal: Цей профіль включає агресивне перейменування, шифрування рядків та помірне заплутування потоку керування. Логіка методів вже стає важкою для аналізу, але ще не перетворюється на повний "спагеті-код". Розмір вихідного файлу 41 кілобайт. Кількість рядків у файлі «Program» 3622 рядки, відобразити повністю файл недоцільно, тому буде зображений обфускований код класу SecureManager на рисунку 3.

```

1 using System;
2 using System.Runtime.CompilerServices;
3
4 // Token: 0x0200000F RID: 15
5 [CompilerGenerated]
6 [Px^Em-02pD^v$R_.,@dl1,!KE]
7 [AttributeUsage(AttributeTargets.Class | AttributeTargets.Struct | AttributeTargets.Method | AttributeTargets.Interface
  | AttributeTargets.Delegate, AllowMultiple = false, Inherited = false)]
8 internal sealed class a&h+k"R,nJ6 : Attribute
9 {
10     // Token: 0x0600003E RID: 62 RVA: 0x000063B8 File Offset: 0x000045B8
11     public a&h+k"R,nJ6(byte A_1)
12     {
13         for (;;)
14         {
15             IL_06:
16             uint num = 475066144U;
17             for (;;)
18             {
19                 uint num2;
20                 switch ((num2 = (num ^ 2124479475U)) % 3U)
21                 {
22                     case 0U:
23                         goto IL_06;
24                     case 2U:
25                         this.\u200C\u200D\u200D\u200D\u202A\u202B\u200C\u202A\u200E\u200D\u206B\u202E\u200F\u206B\u200F
\u202A\u202B\u206B\u202E\u200B\u206E\u202C\u202A\u200E\u200C\u202D\u202C\u206B\u200B\u206C\u206B
\u202D\u206B\u206A\u202C\u206A\u200E\u200B\u202E\u206E\u202E = A_1;
26                         num = (num2 * 2490827180U ^ 363061864U);
27                         continue;
28                     }
29                 }
30                 return;
31             }
32         }
33     }
34
35     // Token: 0x0400002F RID: 47
36     public readonly byte \u200C\u200D\u200D\u200D\u202A\u202B\u200C\u202A\u200E\u200D\u206B\u202E\u200F\u206B\u200F
\u202A\u202B\u206B\u202E\u200B\u206E\u202C\u202A\u200E\u200C\u202D\u202C\u206B\u200B\u206C\u206B\u202D\u206B\u206A
\u202C\u206A\u200E\u200B\u202E\u206E\u202E;
37

```

Рисунок 3 – Декомпільований код додатка після обфускації профілем Normal

Профіль Maximum включає всі захисти Normal плюс агресивне заплутування потоку керування. Прості умовні оператори перетворюються на тисячі надлишкових інструкцій, з використанням switch та goto. Це забезпечує найвищий рівень захисту від статичного аналізу, але ціною значного збільшення файлу. Розмір файлу 51 кілобайт. При використанні інструменту декомпіляції нічого не зрозуміло де знаходиться який файл, також можна побачити значну кількість надлишковості, тобто код який був незрозумілий уже при використанні профілю Normal є ще більш заплутаним, тому зображення коду цього профілю не буде продемонстровано.

Отже, проведений аналіз доводить, що обфускація є гнучким інструментом. Профіль Minimum забезпечує базовий захист від аматорського аналізу, практично не збільшуючи розмір. Профіль Normal пропонує гарний результат, надійно ховаючи логіку та рядки. Профіль Maximum забезпечує найвищий рівень статичного захисту ціною значного збільшення розміру файлу а саме на 750%, що може бути виправдано для захисту критично важливих комерційних алгоритмів.

Таблиця 1 – Порівняльний аналіз профілів обфускації

Конфіг.	Використані техніки	Розм. файл.	Збільш.	Складн. аналізу
Orig.	Відсутні	6 кб.	-	Дуже легка
Min.	Тільки перейменування	8 кб.	33%	Легка
	Перейменування, Шифр. рядків, Заплутування (Середнє)	41 кб.	583%	Складна
Max.	Все + Агресивне заплутування	51 кб.	750%	Дуже складна

Згідно наведеної вище інформації можна надати певні рекомендації. Для внутрішніх інструментів або бібліотек можна використати профіль Minimum, оскільки може бути потреба у приховуванні структури коду. Оптимальним рішенням для бізнес логіки комерційних додатків буде профіль Normal, у нього найкраще співвідношення розміру файлу та складності аналізу. Для специфічних випадків залишається профіль Maximum, він може використовуватись для програм, які зосереджуються на безпеці, або на критичних алгоритмах, де можна знехтувати розміром файлів заради захисту від статичного аналізу.

Перелік посилань

1. Проект dnSpyEx. dnSpyEx: .NET debugger and assembly editor. URL: <https://github.com/dnSpyEx/dnSpy>
2. Thakur M. S., Mesbahi A., Atul K., Benchikh M. OWASP Mobile Top 10. URL: <https://owasp.org/www-project-mobile-top-10/>
3. Yck1509. ConfuserEx: An open-source, free protector for .NET applications. URL: <https://yck1509.github.io/ConfuserEx/>
4. Iterasec. Understanding ConfuserEx2: .NET Obfuscation and Deobfuscation Techniques. URL: <https://iterasec.com/blog/understanding-confuserex2-net-obfuscation-and-deobfuscation-techniques/>

УДК 004.8

Коркунда Н.С., Манзюк Е.А., Скрипник Т.К.

Хмельницький національний університет

МЕТОД КЛАСИФІКАЦІЇ РЕЗЮМЕ ЗА ПРОФЕСІЙНИМИ КАТЕГОРІЯМИ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

Розглянуто метод автоматизованої класифікації резюме за професійними категоріями з використанням нейронних мереж та обробки природної мови. Запропонована архітектура поєднує векторизацію TF-IDF з біграмами та нейронну мережу, що забезпечує точність класифікації 87.3%.

A method for automated resume classification by professional categories using neural networks and natural language processing is considered. The proposed architecture combines TF-IDF vectorization with bigrams and neural network, achieving classification accuracy of 87.3%.

Автоматизація класифікації резюме є актуальною задачею для компаній, які обробляють велику кількість заявок від кандидатів [1-3]. Використання методів машинного навчання дозволяє підвищити ефективність процесу підбору персоналу та скоротити час обробки заявок на 75-80%. Сучасні підходи до обробки природної мови та машинного навчання демонструють високу ефективність у різноманітних застосуваннях [4,10], включаючи класифікацію текстових даних, розпізнавання візуальних патернів та пояснюване глибоке навчання в медичній діагностиці [6, 8]. Зокрема, методи глибокого навчання успішно застосовуються для інтерпретації складних даних [6], інтеграції контекстних дескрипторів [7] та вирішення задач класифікації в різних предметних областях [4, 5, 9].

Метою роботи є розробка методу класифікації резюме за професійними категоріями, який забезпечує високу точність при швидкій обробці.

Розроблений метод складається з трьох послідовних етапів: препроцесинг тексту, витягування ознак та класифікація. На першому етапі виконується очищення та нормалізація текстових даних. Другий етап формує числове векторне представлення тексту з використанням TF-IDF та біграм. Третій етап здійснює класифікацію за допомогою нейронної мережі.

Препроцесинг включає п'ять послідовних кроків: приведення до нижнього регістру, видалення спеціальних символів та цифр, токенизацію за допомогою NLTK, видалення стоп-слів англійської мови та лематизацію з використанням WordNet Lemmatizer. Такий підхід дозволяє зменшити розмірність словника на 35% та підвищити якість ознак. Ключовою особливістю є використання комбінованого векторного представлення методом TF-IDF. Словник розміром 5000 елементів містить 4000 уніграм (окремих слів) та 1000 біграм (пар послідовних слів),

відібраних за метрикою pointwise mutual information (PMI). Біграми дозволяють захоплювати контекст професійних термінів та розрізняти схожі категорії (таблиця 1). Архітектура нейронної мережі побудована за принципом послідовного зменшення розмірності. Вхідний шар приймає вектор з 5000 TF-IDF ознак. Перший прихований шар містить 256 нейронів з функцією активації ReLU. Другий прихований шар має 128 нейронів також з ReLU.

Таблиця 1 – Компоненти векторного представлення та їх вплив

Тип ознак	Приклади	Вплив на точність
Тільки уніграми	software, development, management	82.1%
Уніграми + біграми	machine learning, data science, project management	87.3%

Після кожного прихованого шару застосовується dropout-регуляризація з коефіцієнтом 0.3. Вихідний шар складається з 24 нейронів з функцією активації softmax для визначення ймовірності належності до кожної професійної категорії.

Для навчання та тестування використовується датасет Resume Dataset, який містить 2400+ резюме в 24 професійних категоріях: IT, Healthcare, Sales, Marketing, Finance, Engineering та інші. Датасет розділяється на навчальну (1680 резюме, 70%), валідаційну (360 резюме, 15%) та тестову (360 резюме, 15%) вибірки зі збереженням пропорцій категорій.

Навчання виконується з використанням функції втрат та оптимізатора Adam з початковою швидкістю навчання 0.001. Модель навчалася протягом 50 епох з розміром батчу 32. Для запобігання перенавчанню використовувалася рання зупинка при відсутності покращення на валідаційній вибірці протягом 10 епох. Аналіз матриці плутанини виявив характерні особливості роботи методу. Найвища точність досягнута для технічних категорій: Information Technology (92.4%), Data Science (91.8%), Engineering (90.6%). Найчастіше плутаються категорії Sales та Business Development (12% перекресних помилок) через схожість термінології, а також Marketing та Digital Media (9% помилок).

Порівняльний аналіз показав переваги запропонованого методу. Базова модель з уніграмами без нейронної мережі досягла точності 72.6%. Модель з уніграмами та нейронною мережею показала 82.1%. Запропонований метод з біграмами досяг 87.3%, що на 5.2% краще попередньої версії при збільшенні часу обробки лише на 0.08 секунди. Використання регуляризації зменшило різницю між точністю на навчальній (89.1%) та тестовій (87.3%) вибірках до 1.8%, що свідчить про узагальнювальну здатність моделі та відсутність значного перенавчання.

Отже, розроблений метод класифікації резюме забезпечує точність 87.3%. Додавання біграм до векторного представлення покращило точність на 5.2% порівняно з базовою моделлю. Метод є практично придатним для систем автоматизованого рекрутингу. Подальші дослідження спрямовані на використання

трансформерних моделей типу BERT для досягнення точності понад 90% та розширення методу на багатомовні резюме.

Перелік посилань

1. Pal R., Shaikh S., Satpute S., Bhagwat S. Resume Classification using various Machine Learning Algorithms. ITM Web of Conferences. 2022. Vol. 44. Pp. 03011. URL: <https://doi.org/10.1051/itmconf/20224403011>.
2. Upadhye A. Automating Resume Classification: Leveraging NLP and AI for Efficient Candidate Screening. International Journal of Computer Applications. 2023. Vol. 185, No. 40. Pp. 46–50. URL: <https://doi.org/10.5120/ijca2023923208>.
3. Heakl A., Mohamed Y., Mohamed N., Elsharkawy A., Zaky A. ResumeAtlas: Revisiting Resume Classification with Large-Scale Datasets and Large Language Models. arXiv, 2024. URL: <https://doi.org/10.48550/arXiv.2406.18125>.
4. Прийма А., Манзюк Е., Пасічник О., Скрипник Т. Метод генерації багатотрекових символічних композицій за допомогою генеративного штучного інтелекту. Herald of Khmelnytskyi National University. Technical sciences. 2025. Vol. 357, No. 5.1. Pp. 114–119. URL: [HYPERLINK "https://doi.org/10.31891/2307-5732-2025-357-59"](https://doi.org/10.31891/2307-5732-2025-357-59)<https://doi.org/10.31891/2307-5732-2025-357-59>.
5. Манчур О., Манзюк Е., Скрипник Т., Пасічник О., Петровський С. Метод визначення навантаження тренування атлетів з використанням машинного навчання. Herald of Khmelnytskyi National University. Technical sciences. 2025. Vol. 353, No. 3.2. Pp. 342–348. URL: [HYPERLINK "https://doi.org/10.31891/2307-5732-2025-353-48"](https://doi.org/10.31891/2307-5732-2025-353-48)<https://doi.org/10.31891/2307-5732-2025-353-48>.
6. Manziuk E., Barmak O., Krak I., Petliak N., Jin Z., Radiuk P. Explainable Deep Learning for Interpretable Brain Tumor Diagnosis from MRI Images / Lecture Notes in Data Engineering, Computational Intelligence, and Decision-Making, Volume 1, Cham, Springer Nature Switzerland, 2024. Pp. 326–348. URL: https://doi.org/10.1007/978-3-031-70959-3_17.
7. Manziuk E., Barmak O., Krak I., Petliak N., Jin Z., Radiuk P. Interpretable deep learning method for medical image diagnosis ФОП Вишемирський В.С. 2024.
8. Manziuk E., Barmak O., Radiuk P., Kuznetsov V., Krak I., Yakovlev S. Integration of Contextual Descriptors in Ontology Alignment for Enrichment of Semantic Correspondence. arXiv, 2024. URL: [HYPERLINK "https://doi.org/10.48550/arXiv.2411.19113"](https://doi.org/10.48550/arXiv.2411.19113)<https://doi.org/10.48550/arXiv.2411.19113>.
9. Barmak O., Krak I., Yakovlev S., Manziuk E., Radiuk P., Kuznetsov V. Toward explainable deep learning in healthcare through transition matrix and user-friendly features. Frontiers in Artificial Intelligence. 2024. Vol. 7. Pp. 1482141. URL: [HYPERLINK "https://doi.org/10.3389/frai.2024.1482141"](https://doi.org/10.3389/frai.2024.1482141)<https://doi.org/10.3389/frai.2024.1482141>.
10. Яворський К., Манзюк Е., Скрипник Т., Пасічник О. Визначення обсягу даних для ефективної класифікації номерів автомобілів. Herald of Khmelnytskyi National University. Technical sciences. 2024. Vol. 343, No. 6(1). Pp. 406–411. URL: [HYPERLINK "https://doi.org/10.31891/2307-5732-2024-343-6-60"](https://doi.org/10.31891/2307-5732-2024-343-6-60)<https://doi.org/10.31891/2307-5732-2024-343-6-60>.
11. Ryzhanskyi O., Pavlyshyn V., Radiuk P., Manziuk E., Barmak O., Krak I. AI Driven Traffic Signal Control System to Reduce CO2 Emissions / CEUR Workshop Proc., CEUR-WS, 2025. Pp. 18–27. URL: <https://ceur-ws.org/Vol-3974/paper02.pdf>

УДК 004.4

Красникова Д.П.

Кам'янський енергетичний фаховий коледж

ЗАХИСТ ДАНИХ У ХМАРНИХ ОБЧИСЛЕННЯХ

Хмарні обчислення (cloud computing) є однією з найдинамічніших технологій сучасності. Вони забезпечують зручний доступ до обчислювальних ресурсів, програмного забезпечення та сховищ даних через інтернет, що дозволяє організаціям зменшувати витрати на IT-інфраструктуру та підвищувати гнучкість бізнес-процесів. Однак разом із перевагами виникають і серйозні проблеми – ризики для безпеки даних. Інформація, яка раніше зберігалася локально, тепер розміщується на віддалених серверах, що підконтрольні стороннім компаніям-провайдерам. Це створює нові вектори атак, зокрема несанкціонований доступ, витік конфіденційної інформації та порушення цілісності даних.

Cloud computing is one of the most dynamic technologies of today. They provide convenient access to computing resources, software and data storage over the Internet, which allows organizations to reduce IT infrastructure costs and increase the flexibility of business processes. However, along with the advantages, there are also serious problems - data security risks. Information that was previously stored locally is now hosted on remote servers controlled by third-party provider companies. This creates new attack vectors, including unauthorized access, leakage of confidential information, and data integrity violations.

Метою даної доповіді є дослідження методів і технологій забезпечення безпеки даних у хмарних обчисленнях, аналіз основних загроз і способів їх нейтралізації.

Хмарні обчислення базуються на моделі «Інфраструктура як послуга» (IaaS), «Платформа як послуга» (PaaS) і «Програмне забезпечення як послуга» (SaaS). Усі три рівні мають власні ризики безпеки, оскільки різні сторони (користувач, провайдер, розробник) відповідають за різні компоненти системи.

Основні вимоги до безпеки в хмарі включають:

– Конфіденційність – забезпечення доступу лише уповноваженим користувачам.

– Цілісність – гарантування, що дані не змінені чи пошкоджені.

– Доступність – забезпечення безперервного доступу до ресурсів.

– Відповідальність – контроль дій користувачів і адміністраторів.

Для виконання цих вимог провайдери впроваджують багаторівневі системи безпеки, що поєднують криптографічні, організаційні та апаратні механізми захисту.

Основні загрози безпеці у хмарних середовищах:

– Несанкціонований доступ до даних. Через слабкі паролі, фішинг або викрадення облікових записів користувачі можуть втратити контроль над своїми обліковими записами.

– Витік конфіденційної інформації. Внаслідок помилок налаштування хмарних сервісів (наприклад, відкриті S3-бакети в AWS) дані можуть стати публічними.

– Атаки з боку внутрішніх користувачів. Працівники компанії або адміністратори провайдера мають потенційний доступ до даних клієнтів.

– DDoS-атаки. Перевантаження хмарної інфраструктури може призвести до тимчасової недоступності сервісів.

– Порушення ізоляції даних. У мультикористувачьких середовищах можливі атаки між віртуальними машинами.

Методи захисту даних у хмарних обчисленнях:

1. Криптографічний захист

Найбільш ефективним способом забезпечення конфіденційності даних є шифрування:

Під час передачі (протоколи SSL/TLS) – захист від перехоплення в мережі.

Під час зберігання (AES, RSA, ECC) – шифрування файлів та баз даних у хмарі.

Гомоморфне шифрування – дозволяє виконувати обчислення над зашифрованими даними без їх розшифрування, що підвищує рівень безпеки.

2. Управління доступом і автентифікація

Використовуються моделі контролю доступу:

– RBAC (Role-Based Access Control) – права призначаються відповідно до ролей користувачів.

– ABAC (Attribute-Based Access Control) – рішення про доступ базується на атрибутах користувача, дії та середовища.

– Мультифакторна автентифікація (MFA) – комбінація пароля, біометрії або одноразового коду для підвищення безпеки.

3. Безпечне управління ключами

Зберігання ключів шифрування у хмарі є вразливим місцем. Використання сервісів типу AWS KMS (Key Management Service) або Azure Key Vault забезпечує централізоване й контрольоване управління криптографічними ключами.

4. Моніторинг і виявлення загроз

Системи Cloud Security Posture Management (CSPM) та Cloud Access Security Broker (CASB) аналізують події, журнали доступу й налаштування, попереджаючи про потенційні вразливості.

5. Анонімізація та токенизація даних

Ці методи дозволяють замінювати конфіденційні дані (наприклад, номери карток) на унікальні токени, що не розкривають справжню інформацію користувачів.

6. Організаційні аспекти безпеки

Крім технічних засобів, важливе значення має інформаційна політика безпеки, яка передбачає:

- аудит хмарних сервісів перед використанням;
- укладення договорів SLA із чітко прописаними вимогами до безпеки;
- навчання персоналу основам кібергігієни;
- резервне копіювання даних для запобігання втраті у разі інцидентів.

Сучасні тенденції у сфері хмарної безпеки:

1. Використання штучного інтелекту для автоматичного виявлення загроз і аномалій у хмарному трафіку.

2. Zero Trust Architecture – модель, за якої жоден користувач або пристрій не вважається безпечним за замовчуванням.

3. Постквантова криптографія – нові алгоритми, стійкі до атак квантових комп'ютерів.

4. Хмарна ізоляція контейнерів – покращення захисту мікросервісів у середовищах Docker і Kubernetes.

Хмарні технології радикально змінюють спосіб зберігання та обробки інформації, забезпечуючи масштабованість і економічність. Проте саме передача контролю над даними сторонньому провайдеру створює значні ризики безпеки.

Ефективний захист інформації у хмарних середовищах потребує комплексного підходу, який поєднує криптографію, багаторівневу автентифікацію, моніторинг подій безпеки та політики управління доступом.

У майбутньому ключову роль відіграватиме інтеграція ШІ у процеси кіберзахисту, а також розвиток постквантових методів шифрування, що дозволять зберегти конфіденційність навіть у нову еру квантових обчислень.

Перелік посилань

1. Stallings W. Network Security Essentials: Applications and Standards. – 7th ed. – Pearson, 2023.
2. Subashini S., Kavitha V. A Survey on Security Issues in Service Delivery Models of Cloud Computing. – Journal of Network and Computer Applications, 2022.
3. NIST Special Publication 800-210. General Access Control Guidance for Cloud Systems. – 2021.
4. Мельник А.І. Захист інформації у хмарних технологіях: навчальний посібник. – Київ: КПП ім. І. Сікорського, 2022.
5. Microsoft Azure Security Documentation. – <https://learn.microsoft.com/azure/security>

УДК 004.4

Красюк В.К., Резнікова М.А., Бойцун Д.О., Тімош В.Л.

Хмельницький національний університет

ФОРМАЛІЗАЦІЯ СТРУКТУРИ ZIGBEE-МЕРЕЖ ТА АТАК ГРАФОВИМИ МНОЖИНАМИ

Запропоновано представити топологію ZigBee-мережі та множини можливих атак у вигляді формалізованих графових структур. Мережа описується як сукупність множин вузлів (кінцевих пристроїв, маршрутизаторів, координаторів), каналів зв'язку та функціональних залежностей, що визначають її поведінку. Атаки моделюються як впливи на підмножини елементів графа із заданими інтенсивністю, тривалістю та критичністю. Такий підхід дозволяє уніфікувати опис сценаріїв порушення цілісності та сформувати основу для подальшого виявлення аномалій і автоматизованої реакції на них.

It is proposed to represent the topology of ZigBee networks and associated attack scenarios as formal graph-based structures. The network is modelled as sets of nodes (end devices, routers, coordinator), communication channels, and functional dependencies. Attacks are defined as directed impacts on node subsets with given intensity, duration, and criticality. This representation unifies threat scenarios and lays the foundation for anomaly detection and automated response mechanisms.

Широке впровадження бездротових IoT-мереж на базі протоколу ZigBee супроводжується зростанням кількості атак, які спрямовані як на окремі вузли, так і на цілі фрагменти топології.[1] Уразливості поділяються на два ключові класи: реалізаційні (наприклад, витік ключів, CVE-2015-3974) і протокольні (статичні ключі, jamming, CVE-2019-18984), а атаки – на локальні (DoS, spoofing) та системні (перехоплення координатора, отруєння маршрутів). Типові наслідки включають втрату зв'язку, структурну деградацію та глобальну нестабільність мережі. З огляду на це, у роботі запропоновано формалізувати ZigBee-інфраструктуру у вигляді множинно-графової моделі, де вузли (кінцеві пристрої, маршрутизатори, координатор), канали, функціональні залежності та сценарії активності описуються як підмножини зв'язного орієнтованого графа. Атаки моделюються як множини впливу з параметрами інтенсивності, тривалості, критичності та функцією деградації [2, 3]. Це дозволяє уніфіковано описати широкий спектр впливів — від короточасного перенавантаження окремих вузлів до багатофазної дестабілізації маршрутизації. Таким чином, графова модель виступає не лише як формальний

опис мережі, а як основа для побудови математично обґрунтованих засобів аналізу, локалізації та подальшої автоматизованої реакції.

Таблиця 1 – Класифікація загроз у ZigBee мережах

Категорія	Типові проблеми	Приклади атак	Цільові елементи	Потенційний вплив
Реалізаційного рівня	Витік ключів, слабка конфігурація	CVE-2015-3974, CVE-2020-6007	Кінцеві пристрої, шлюзи	Несанкціонований доступ, нестабільність
Протокольного рівня	Статичні ключі, ACK, недоліки CSMA/CA	CVE-2019-18984, jamming	Канали, маршрутизатори	Втрата зв'язку, порушення маршрутизації
Локальні атаки	Flooding, spoofing	DoS, повтор ідентифікаторів	Окремий вузол або лінія	Тимчасове погіршення обслуговування

Дана класифікація дозволяє отримати єдине розуміння типів загроз і слугувати основою для формальної моделі атаки та механізмів реагування.

Атаки на бездротові IoT-мережі, зокрема на базі протоколу ZigBee, демонструють стійке зростання складності та різноманітності. Зловмисники дедалі частіше застосовують багатоступеневі стратегії, спрямовані на дестабілізацію мережі або отримання контролю над її окремими компонентами.[4] На основі класичних моделей вторгнення сформовано адаптовану структуру атак, яка враховує особливості ZigBee-інфраструктур. Як і в традиційних схемах компрометації, тут атаки реалізуються поетапно – з впливом на кінцеві пристрої, маршрутизатори, канали зв'язку або координатор мережі. У межах цієї моделі атака реалізується як цілеспрямований вплив на окремий фрагмент мережі. Зловмисник може здійснити компрометацію координатора чи маршрутизатора, перехопити канал зв'язку або імітувати легітимний вузол. Результатом таких дій можуть стати порушення маршрутів, втрата зв'язку, зміни топології, перевантаження окремих вузлів або каналів, а також зупинка критичних функцій. Запропонована модель дозволяє розділити атаки за масштабом впливу. До локальних належать ті, що спрямовані на окремі вузли або канали :DoS, spoofing, flooding, тощо.[5] До глобальних – ті, що змінюють структуру всієї мережі або провокують каскадні збої.

Для забезпечення стійкості ZigBee-мережі до атак під час її функціонування запропоновано формалізувати її у вигляді координованої сукупності логічно взаємопов'язаних компонентів, кожен з яких виконує спеціалізовану роль у загальній структурі IoT-системи.

Такий підхід дає змогу не лише описати поведінку елементів мережі за нормальних умов, а й визначити сценарії порушення її цілісності внаслідок цілеспрямованого зовнішнього впливу.

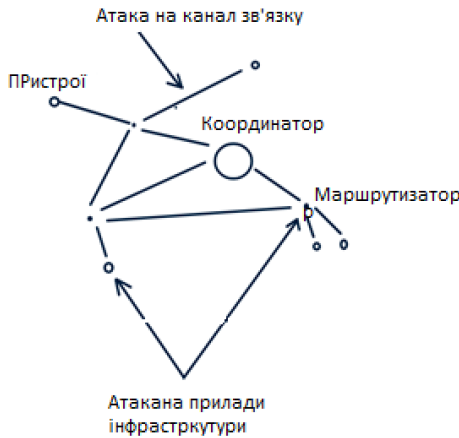


Рисунок 1 – Представлення схеми атак на інфраструктуру ZigBee мережу

У межах запропонованої моделі ZigBee-мережа розглядається як функціонально розподілена система, структура якої описується через множину компонентів, що взаємодіють у межах єдиного середовища :

$$M_{zb} = \{C, D, R, Z, F_{zb}, A_{zb}\} \quad (1)$$

Де $C = \{ch_1, ch_2, \dots, ch_n\}$ – множина каналів зв'язку, які реалізують фізичну або логічну маршрутизацію між вузлами, $D = \{d_1, d_2, \dots, d_n\}$ – множина кінцевих пристроїв, що збирають, генерують або отримують дані. $R = \{r_1, r_2, \dots, r_n\}$ – множина маршрутизаторів, відповідальних за ретрансляцію, побудову та підтримку маршрутів, $Z = \{z\}$ – координатор мережі, елемент управління і ініціалізації, $F_{zb} = \{f_0, f_1, \dots, f_n\}$ – множина функціональних ролей і сервісів, які забезпечують роботу ZigBee-мережі: адресація, маршрутизація, захист, синхронізація, $A_{zb} = \{a_0, a_1, \dots, a_n\}$ – множина умов активації, що визначають залежність роботи елементів від подій, запитів або змін топології.

Оскільки ZigBee-мережа зазвичай є географічно або логічно розподіленою, її компоненти можуть бути розміщені на різних фізичних пристроях або в різних зонах. Кожен компонент моделі подається як комбінація елементів відповідних підмереж (або груп вузлів), які функціонують автономно, але виконують роль у межах загальної інфраструктури:

$$M_{zb} = \begin{cases} C = U_{i=1}^N C_i \\ D = U_{i=1}^N D_i \\ R = U_{i=1}^N R_i \\ Z = U_{i=1}^N Z_i \\ F_{zb} = U_{i=1}^N F_{zb,i} \\ A_{zb} = U_{i=1}^N A_{zb,i} \end{cases} \quad (2)$$

Зважаючи на те, що ZigBee-мережі зазвичай мають географічно або логічно розподілену структуру (наприклад, кімнати, поверхи, сегменти), кожна частина може відрізнятися критичністю, відмовостійкістю та ступенем впливу на цілісність мережі. Для цього вводиться поняття вагових коефіцієнтів для різних типів елементів. Координатор вважається критичною точкою відмови, тому йому надається максимальна вага. Маршрутизатори мають високу важливість для підтримки топології, канали — вразливі до навмисного перевантаження, а кінцеві пристрої — локальні за впливом. Таким чином, мережа описується не лише структурно, а й з урахуванням ролі кожного елемента в її загальній стабільності. Для побудови ефективної системи виявлення та протидії атакам також необхідно формалізувати сам вплив як набір параметрів, що описують тип атаки, її динаміку у часі, цільову область і очікувані наслідки.[6] У загальному вигляді атака подається як структура з п'яти компонентів: тип загрози, цільові елементи (наприклад, вузли або канали), функція інтенсивності у часі, функція деградації, яка показує, за яких умов елемент вийде з ладу, та функція оцінки критичності.[7] Модель дозволяє визначити, які компоненти мережі з найбільшою ймовірністю зазнають впливу в певний момент часу, враховуючи силу атаки та стійкість елементів. Додатково, для кожного елемента оцінюється критичність наслідків, яка залежить від його ваги в структурі мережі. Загальний ефект атаки на мережу в певний момент часу обчислюється як сума критичностей усіх уражених елементів. Це дозволяє оцінити рівень деградації мережі в конкретному сценарії та відрізнити атаки за типом — руйнівні (наприклад, фізичне знищення або блокування) або пасивні (перехоплення, підміна, прослуховування). Такий формалізований підхід дозволяє уніфікувати опис атак, аналізувати їх у динаміці та виявляти, які елементи найбільш вразливі до конкретних типів впливів. Це створює основу для побудови реактивних або адаптивних механізмів захисту.

Перелік посилань

1. Іваненко, П.В. Виявлення аномалій у системах Інтернету речей: Навчальний посібник. / П.В. Іваненко. — Київ: Державний університет телекомунікацій, 2021. — 312 с.
2. Сидоренко, О.М. Безпека Інтернету речей. / О.М. Сидоренко. — Харків: ХНУРЕ, 2020. — 278 с.
3. Петренко, Л.О. Вступ до IoT та аналіз аномалій: Підхід на основі статистичних методів. / Л.О. Петренко. — Львів: Видавництво Львівської політехніки, 2019. — 345 с.
4. Мартинюк, Д.В. Статистичні методи виявлення аномалій у IoT: Практичний посібник. / Д.В. Мартинюк. — Одеса: ОНПУ, 2022. — 256 с.
5. F. Ahmed, M. Hafeez, S. Hussain, Blockchain-Based Intrusion Detection System for IoT-Enabled Smart Homes Using ZigBee Protocol, IEEE Access 11 (2023) 78415–78429. DOI: 10.1109/ACCESS.2023.3298745.
6. A. Nicheporuk, O. Dariychuk, S. Danchuk, Model of Process for Ensuring Fault Tolerance in Internet of Things Networks, Computer Systems and Information Technologies 2 (2024) 14–20. DOI: 10.31891/csit-2024-2-2
7. Павленко, Т.М. Основи обробки даних для виявлення аномалій в IoT. / Т.М. Павленко. — Київ: Університет ім. Т. Шевченка, 2018. — 189 с.

УДК 004.8

Крива Д.О., Кліменко В.І.

Хмельницький національний університет

МЕТОДОЛОГІЯ СТВОРЕННЯ НАБОРУ ТЕГІВ ДЛЯ ФОРМАЛІЗОВАНОГО ОПИСУ МОДЕЛЕЙ ФОРМУВАННЯ ТЕСТОВИХ ЗАВДАНЬ

У роботі запропоновано методологію створення набору тегів для формалізованого опису моделей формування тестових завдань на основі понятійно-тезової структури навчального матеріалу. Теги розглядаються як елементи предметноорієнтованої псевдомови, що поєднує етапи ідентифікації релевантних фрагментів тексту та побудови тестів у форматі GIFT для середовища Moodle. Виділено дві групи тегів: ідентифікаційні, орієнтовані на терміни, тези та службові конструкції, і формувальні, які задають ролі основи питання, правильної відповіді та дистракторів у шаблонах завдань різних типів. Показано ітераційний характер побудови та уточнення набору тегів, його предметну незалежність і сумісність із внутрішніми структурами інформаційної технології. Практичну реалізацію методології здійснено у вигляді програмного модуля TestGenerator мовою C#, який забезпечує вибір термінів, конфігурацію типів питань та автоматичну генерацію GIFT-файлів для імпорту до Moodle.

The paper proposes a methodology for designing a tag set used for the formalized description of test-item generation models based on the concept–thesis structure of educational texts. Tags are treated as elements of a domain-specific pseudolanguage that integrates two stages: identification of relevant text fragments and construction of test items in the GIFT format for the Moodle environment. Two tag groups are distinguished: identification tags, focused on terms, theses and auxiliary constructions, and generation tags, which define the roles of question stem, correct answer and distractors in templates for different item types. The iterative nature of tag-set refinement, its domain independence and compatibility with the internal structures of the information technology are shown. The methodology is implemented in the C#-based TestGenerator module, which supports term selection, configuration of question types and automatic GIFT file generation for subsequent import into Moodle.

Сучасний стан використання технологій тестування характеризується зростаючою потребою в автоматизованому генеруванні якісних тестових завдань для адаптивних систем контролю знань [1]. Сучасні освітні платформи дедалі частіше переходять до адаптивного тестування, у якому рівень складності, тип завдання та траєкторія оцінювання змінюються динамічно відповідно до відповіді користувача [2, 3]. Для коректної роботи таких систем потрібні великі, структурно узгоджені, семантично марковані набори тестових завдань, здатні підтримувати різні когнітивні рівні, варіативність дистракторів та багатоваріантність формулювань [4]. Ручне створення подібних банків тестів є трудомістким,

повільним і слабо масштабованим, що унеможливує оперативне оновлення завдань відповідно до змін навчального контенту.

Сучасні моделі мовної обробки забезпечують здатність до семантичного аналізу навчальних матеріалів [5, 6], автоматичного виділення ключових понять і релевантних фрагментів тексту [7], а також переформулювання змісту з урахуванням заданих дидактичних вимог [8, 9]. Поєднання тегової псевдомови з інструментами NLP дозволяє не лише структурувати дані для генератора завдань, а й автоматично знаходити потенційні основи питань, генерувати варіанти відповідей і контролювати їхню лінгвістичну коректність та однозначність.

Особливе значення це має для адаптивного тестування, де якість і спрямованість кожного наступного завдання суттєво впливають на точність оцінювання [10]. NLP-моделі можуть підтримувати автоматизоване визначення складності текстових формулювань і забезпечувати стилістичну узгодженість великої кількості згенерованих питань [11]. Інтеграція семантичного аналізу з формалізованою системою тегів дає змогу створювати тестові завдання з чітко визначеною когнітивною метою, а також контролювати ризики надмірної схожості, двозначності чи змістових перекоручень, що є критичним для адаптивних систем.

Запропонована методологія формалізованого опису моделей формування тестових завдань на основі системи тегів забезпечує узгоджену структуру даних, яка дозволяє автоматично генерувати GIFT-файли для Moodle, адаптувати зміст під конкретний рівень складності та оперативно формувати нові варіанти завдань [12, 13]. Використання тегів як елементів предметноорієнтованої псевдомови створює основу для масштабованого, керованого та відтворюваного процесу побудови тестів, що є критично важливим для адаптивних систем [14]. Такий підхід не лише зменшує витрати часу на формування банку завдань, а й підвищує якість адаптації тестування, дозволяючи гнучко поєднувати глибину опрацювання навчального матеріалу зі структурованою автоматизованою генерацією контенту.

Крім того, адаптивні системи оцінювання вимагають не лише великих обсягів тестового контенту [15], а й чіткої керованості його параметрами – рівнем складності [16], типом когнітивної операції [17], структурою відповіді [18] та ступенем варіативності [19]. Формалізований набір тегів дозволяє явно кодувати ці характеристики у процесі побудови завдання, що забезпечує можливість їхньої подальшої автоматичної інтерпретації алгоритмами адаптації [20]. Завдяки такому підходу тестові моделі можуть бути узгоджені з алгоритмами комп'ютеризованого адаптивного тестування, які призначають наступне питання, ґрунтуючись на оціненому рівні знань здобувача та статистичних властивостях завдання.

Використання тегів як універсального інтерфейсу між моделлю навчального матеріалу та механізмами автоматизованого формування завдань сприяє підвищенню точності діагностики навчальних результатів. Теги забезпечують можливість чіткого позначення структурних і семантичних елементів змісту, що дозволяє формувати питання різних типів – від базових на відтворення термінів до аналітичних, спрямованих на інтерпретацію, порівняння чи

узагальнення [21]. Це створює основу для побудови адаптивних тестів, які не лише коригують складність, а й адаптують когнітивний формат завдань під індивідуальні характеристики здобувача.

Таким чином, формалізована система тегів є ключовим інструментом для забезпечення масштабованості, узгодженості та якості автоматизованого генерування контенту, необхідного для сучасного адаптивного тестування. Вона спрощує підтримку актуальності тестових банків, підвищує гнучкість побудови траєкторій оцінювання та зменшує залежність процесу розроблення завдань від ручної праці експертів. У підсумку це сприяє формуванню ефективних, динамічних і методично обґрунтованих систем оцінювання знань.

Методологія створення набору тегів для формалізованого опису моделей формування тестових завдань ґрунтується на уявленні про формування тесту як про послідовність перетворень над текстовим контентом, які можуть бути описані у вигляді правил конвертації. Кожне таке правило працює з вхідним фрагментом навчального матеріалу, виокремлює в ньому релевантні семантичні елементи та послідовно відтворює структуру тестового завдання, що відповідає цим елементам. Для того щоб правила конвертації могли бути реалізовані програмними засобами, необхідно задати формальний словник елементарних конструкцій, які використовуються і на етапі ідентифікації змістових компонентів, і на етапі побудови вихідного тесту. Цю роль і відіграє набір тегів, що виступає проміжною мовою між природною мовою навчального тексту, внутрішніми структурами інформаційної технології та форматом представлення тестів у середовищі Moodle, зокрема GIFT.

Вихідним положенням методології є виділення двох взаємопов'язаних, але функціонально різних груп тегів: тегів для ідентифікації елементів контенту та тегів для формування тестових завдань. Такий поділ безпосередньо витікає із структури правил конвертації, яка включає маску ідентифікації, правило перетворення та маску формування тесту. У масці ідентифікації теги позначають фрагменти навчального тексту, що мають семантичне значення з точки зору майбутнього тесту (терміни, тези, допоміжні конструкції, межі речень тощо), тоді як у масці формування вони окреслюють структурні складові тестового завдання (основа запитання, правильний варіант відповіді, дистрактори, службові елементи синтаксису цільового формату). У вихідній роботі підкреслюється, що такі теги фактично є елементами псевдокоду або змінними, значення яких під час роботи алгоритму визначаються конкретними фрагментами контенту навчального матеріалу.

Методологічно процес побудови набору тегів починається з аналізу об'єкта формалізації, яким виступають моделі формування тестових завдань, уже визначені за результатами попередніх етапів роботи. Для кожної моделі встановлюється, які саме фрагменти тексту необхідні, щоб побудувати змістовно коректне тестове завдання заданого типу. На цьому етапі ключовим є семантичний аналіз понятійно-тезової структури навчального матеріалу: терміни розглядаються як вузли

семантичної мережі, а тези – як текстові фрагменти, що задають визначення, властивості, відношення або приклади, достатні для побудови тестового завдання. Власне на стику між семантичною моделлю навчального матеріалу та формальною моделлю тестового завдання і виникає потреба у спеціальних маркерах, здатних одночасно «бачити» обидві сторони цього відображення.

Далі формується концептуальна класифікація потенційних тегів. У межах ідентифікаційного шару виділяються теги, що позначають групи слів, які виконують роль терміна, та фрагменти, які виконують роль тези, що пояснює цей термін. У роботі описано теги типу [TermGroup] для позначення фрагмента тексту, який являє собою термін, що складається з одного або кількох слів, та [ThesisGroup] для позначення фрагмента, який виконує функцію тези – визначення або формулювання змістовно завершеної характеристики терміна.

Наявність таких тегів дозволяє алгоритму формування тестових завдань спиратися не на сирий текст, а на попередньо виділені семантичні одиниці, які відповідають уявленню про понятійно-тезову модель навчального фрагмента.

Окремим кроком є введення тегів, пов'язаних із випадковим вибором альтернативних елементів контенту, що необхідно для автоматичного формування дистракторів. У базовій моделі пропонуються теги на кшталт [RandomTermGroup] та [RandomThesisGroup], які інтерпретуються як вказівка алгоритму вибрати інший термін або інше визначення з множини доступних.

Таке рішення методологічно важливе з двох причин. По-перше, воно дозволяє відокремити логіку побудови тесту (де саме мають з'являтися альтернативні варіанти) від механізмів вибірки і комбінування дистракторів. По-друге, воно забезпечує можливість подальшого розширення стратегії вибору – наприклад, від простого випадкового вибору до складніших схем, які враховують близькість термінів за тематикою, частотні характеристики або рівень складності.

До групи ідентифікаційних тегів також належать маркери, що позначають структурні елементи тексту, які не є носіями основного змісту, але виступають сигнальними елементами для алгоритму. У роботі згадується тег [Connector], що позначає слово або символ, який поєднує термін і тезу (наприклад, «–», «– це», «є», «називається»).

Введення такого тегу дозволяє явно відділити змістові компоненти від службових, а також використовувати регулярні конструкції масок для виявлення типових патернів формулювання визначень у навчальних текстах. Додаткові теги на кшталт [BeginSentence] або аналогічних маркерів межі речення забезпечують можливість контролю контексту: модель може, наприклад, відсікати занадто протяжні фрагменти або обмежувати пошук відповідних тез межами одного чи кількох речень.

Наступним методологічним блоком є побудова тегів, орієнтованих безпосередньо на формування тестових завдань. Якщо ідентифікаційні теги відповідають «що знайти в навчальному тексті», то теги формування відповідають «як саме представити знайдене у форматі тесту». На цьому етапі враховуються

вимоги середовища Moodle і, зокрема, формату GIFT, який задає синтаксис представлення основи питання, переліку відповідей, маркерів правильності, вагових коефіцієнтів, коментарів тощо. У методології виходять із того, що кожна модель формування тесту складається з певної схеми «підстановки» відібраних елементів контенту у шаблон, де відповідні позиції також позначаються тегами. Таким чином, для кожного типу тестових завдань вибудовується відповідний шаблон, який поєднає жорстко задані елементи синтаксису GIFT і параметризовані місця, на які підставляються фрагменти з [TermGroup], [ThesisGroup] та інших ідентифікаційних структур.

Важливим принципом у побудові такого набору тегів є предметна незалежність. Теги не повинні кодувати конкретні терміни, галузь знань або змістові нюанси окремого курсу. Натомість вони задають ролі у процесі перетворення: «фрагмент, що містить визначення», «фрагмент, який слугує дистрактором», «слово-зв'язка між терміном і тезою», «позиція для правильної відповіді у форматі GIFT» тощо. Такий підхід робить набір тегів універсальним і придатним для багаторазового використання в інформаційній технології, орієнтованій на різні навчальні дисципліни, які подаються у вигляді текстових матеріалів єдиного формату.

Методологія побудови набору тегів включає також етап формалізації їх синтаксису та семантики. Для кожного тегу задається область його допустимого використання (наприклад, лише в масках ідентифікації або лише в масках формування), очікуваний тип даних, що з ним асоціюється (фрагмент тексту, окрема лексема, посилання на елемент іншої множини), а також правила взаємодії з іншими тегами. Семантика тегу визначає, яку саме роль він відіграє у процесі перетворення: чи є він джерелом даних, проміжним контейнером, керувальним маркером або службовим елементом, що відповідає за коректний синтаксис вихідного тесту. Чітка специфікація цих властивостей дає можливість трактувати набір тегів як легковагу предметно-орієнтовану мову опису моделей формування тестових завдань.

Подальшим кроком виступає узгодження тегів із внутрішніми структурами інформаційної технології. Оскільки розроблена технологія уже містить механізми формування вихідних множин термінів, обробки текстового контенту та застосування правил конвертації, кожен тег має бути відображений у відповідні програмні сутності. На рівні реалізації це означає побудову об'єктних структур, які інкапсулюють логіку роботи з тегами, забезпечують перевірку коректності їх використання, підтримують операції пошуку, підстановки, комбінування та серіалізації до формату GIFT. Окремо розв'язується задача сумісності зі схемою даних інформаційної системи, у якій результати роботи алгоритму мають зберігатися та повторно використовуватися у подальших сесіях формування тестів.

Критично важливо, що методологія розробки набору тегів передбачає ітераційний характер його формування. Початковий варіант набору створюється на основі теоретичного аналізу моделей тестових завдань та можливостей формату

GIFT, але надалі уточнюється за результатами експериментів із реальними навчальними матеріалами. У процесі апробації виявляються типові ситуації, коли наявних тегів недостатньо для адекватного відображення того чи іншого способу викладу матеріалу, коли деякі теги використовуються надто рідко або, навпаки, виявляються надмірно універсальними й потребують поділу на більш спеціалізовані. Такі спостереження призводять до послідовного розширення, узагальнення або реструктуризації набору тегів, при цьому зберігається сумісність із уже розробленими моделями формування тестових завдань.

Ще одним компонентом методології є забезпечення прозорості та інтерпретованості побудованого набору тегів для розробника навчальних курсів та експерта з тестування. Хоча теги спочатку орієнтовані на машинну обробку, важливо, щоб їхні позначення і вербальні описи залишалися зрозумілими для людини, яка аналізує або модифікує моделі формування тестових завдань. Це досягається через вибір інтуїтивно зрозумілих позначень, узгодження термінології з педагогічною та тестологічною літературою, а також через надання текстових описів кожного тегу.

Така «людино-читабельність» псевдокоду сприяє перевірці коректності моделей, спільній роботі над їх удосконаленням і можливості адаптації інформаційної технології у нових контекстах.

Нарешті, методологія створення набору тегів тісно пов'язана з вимогами до масштабованості інформаційної технології. Набір тегів має бути достатньо повним, щоб описати весь спектр моделей формування тестових завдань, передбачених у системі (логічного типу, одиничного та множинного вибору, завдань із введенням тексту тощо), і водночас достатньо компактним, щоб не ускладнювати розробку та супровід нових правил конвертації. У цьому сенсі теги виступають точкою балансування між формальною потужністю мови опису моделей і практичною керованістю технології. Вдале конструювання такого набору створює підґрунтя для подальшого розвитку системи, зокрема для інтеграції з іншими форматами представлення тестів, розширення спектру типів завдань та застосування більш складних алгоритмів семантичного аналізу навчальних матеріалів.

Практичну реалізацію запропонованої методології формалізованого опису моделей формування тестових завдань здійснено у вигляді програмного модуля TestGenerator, розробленого мовою C#. Інтерфейс модуля (рисунок 1) відображає ключові етапи технологічного процесу, закладеного в моделях і системі тегів. Ліва частина головного вікна орієнтована на роботу з понятійно-тезовою структурою навчального матеріалу: таблиця термінів містить перелік відібраних термінологічних одиниць, пов'язаних з ними тез та службових параметрів, що фіксують результати попереднього етапу автоматизованої обробки тексту. Користувач має змогу уточнити множину базових термінів для тестування шляхом інтерактивного відбору записів у стовпці «Select», що фактично задає підмножину елементів, до яких будуть застосовані правила конвертації та відповідні моделі формування завдань.

Права частина вікна реалізує шар конфігурації тесту і безпосередньо відображає формалізовані моделі побудови завдань. Для кожного підтримуваного типу питання (зокрема, YES/NO, Single Choice, Multiple Choice, Matching) задаються параметри активності та кількості генерованих завдань. Перемикачі типів відображають вибір конкретних моделей формування, тоді як числові поля «Count» дозволяють регламентувати питомі частки різних типів завдань у сформованому тесті. Така організація інтерфейсу узгоджується з розробленим набором тегів: вибір термів на рівні таблиці визначає множину значень для тегів, пов'язаних із поняттєвими одиницями, тоді як конфігурація типів питань активує відповідні шаблони формування тестових конструкцій у форматі GIFT.

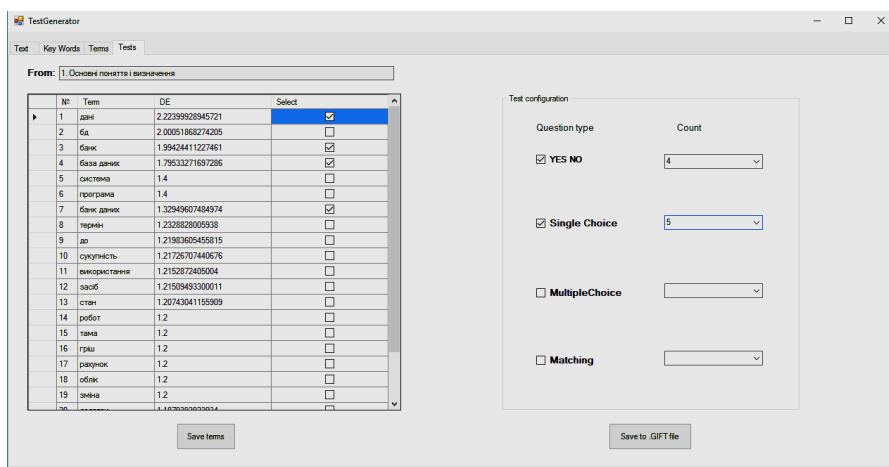


Рисунок 1 – Вікно програмного модуля TestGenerator

Після узгодження множини термінів і параметрів тесту система застосовує описані правила конвертації, підставляє в шаблони значення, пов'язані з тегами, та генерує вихідний файл у форматі GIFT, придатний для імпорту до середовища Moodle. Таким чином, програмний модуль TestGenerator демонструє практичну реалізацію запропонованого підходу: починаючи від формалізованого виділення термінів і тез та закінчуючи автоматизованим утворенням структурованого тесту, він забезпечує технологічну спадкоємність між теоретичною моделлю системи тегів і реальним інструментом підтримки тестування у навчальному процесі.

Узагальнюючи, методологія побудови набору тегів для формалізованого опису моделей формування тестових завдань спирається на три ключові ідеї. По-перше, тестове завдання розглядається як результат застосування правил конвертації до семантично структурованого текстового контенту, а теги – як елементи предметно-орієнтованої мови опису цих правил. По-друге, вводиться чіткий поділ тегів на ідентифікаційні та формувальні, що відповідає двом фазам

роботи алгоритму: пошуку релевантних фрагментів тексту та побудови структурованого тесту у форматі GIFT. По-третє, наголошується на предметній незалежності, розширюваності й інтерпретованості набору тегів, що забезпечує його застосовність у різних навчальних дисциплінах та створює основу для подальшого розвитку інформаційної технології автоматизованого формування тестових завдань.

Перелік посилань

1. Використання тестів в освітньому процесі. Vseosvita. URL: <https://vseosvita.ua/library/vikoristanna-testiv-v-osvitnomu-procesi-487976.html>
2. Multiple Choice Questions Types With Examples. SurveySparrow. URL: <https://surveysparrow.com/blog/multiple-choice-questions/>
3. Методика використання тестової перевірки знань. Vseosvita. URL: <https://vseosvita.ua/library/metodika-vikoristanna-testovoi-perevirki-znan-204638.html>
4. Класифікація тестів. Форми тестових завдань. StudFiles. URL: <https://studfile.net/preview/8839472/page:72/>
5. Hardysh D., Mazurets O., Tyschenko O. Datalogic Relation Model for Automated Evaluating the Semantic Integrity of Test Tasks Sets by Machine Learning Means. Innovative Solutions in Science: Balancing Theory and Practice. Proceedings 2nd International Scientific and Practical Conference. December 23–25, 2024. San Francisco, USA, 2024. P. 114–125.
6. Murava V., Zalutska O., Didur V., Mazurets O. Software architecture of information system for exchanging LLM thematic prompts. Global Trends in the Development of Information Technology and Science. Proceedings IV International Scientific and Practical Conference. June 25–27, 2025. Stockholm, Sweden. Pp. 121–127.
7. Mazurets O., Vit R. Practical Application of Method of Thematic Classification of Text Information Using LDA. Information Technology and Implementation (Satellite). Proceedings 11th International Conference. November 21, 2024. Kyiv, Ukraine. 2024. Pp. 151–152.
8. Yurchenko D., Mazurets O., Didur V., Molchanova M. Approach to Using Cloud Services for Visual Analytics of Neural Network Analysis of Texts Emotional Tonality. The Future of Scientific Discoveries: New Trends and Technologies. Proceedings of the XLVII International scientific and practical conference. November 13–15, 2024. Marseille, France. 2024. Pp. 108–113.
9. Mazurets O., Molchanova M., Klimenko V., Prosvitliuk M Practice Implementation of Neural Network Model BART-Large-CNN for Text Annotation. Prospects of Scientific Research in the Conditions of the Modern World. Proceedings of XXVII International scientific and practical conference. June 12–14, 2024. Rotterdam, Netherlands. 2024. Pp. 97–102.
10. Blazhuk V., Mazurets O., Zalutska O. An Approach to Using the mBERT Deep Learning Neural Network Model for Identifying Emotional Components and Communication Intentions. The Impact of Scientific Research on the Development of the Modern World. Proceedings of the XLIV International scientific and practical conference. October 23–25, 2024. Dubrovnik, Croatia. 2024. Pp. 79–84.
11. Shevchuk P., Molchanova M., Mazurets O. Software for Text Messages Reliability Analysis Based on the Machine Learning Models Ensemble. Proceedings of IV International Scientific and Practical Conference «Innovative research and perspectives of the development of science and technology». January 29–31, 2024. Stockholm, Sweden. 2024. Pp. 347–354.
12. Hardysh D., Tyschenko O., Mazurets O. Intelligent System for Automated Assessment of Test Tasks Sets Conformity to Semantic Structure of Educational Materials. The Role of Science and

Technology in Solving Global Problems of Humanity. Proceedings LIII International Scientific and Practical Conference. December 25–27, 2024. Vienna, Austria, 2024. P. 110–115.

13. Мазурець О.В., Тищенко О.О., Гардиш Д.О. Реляційна даталогічна модель для прикладного аналізу репрезентативності навчальних тестів засобами обробки природної мови. Наука і техніка сьогодні. 2025. № 13(41). С. 1129–1142.

14. Мазурець О.В., Собко О.В., Гардиш Д.О. Прикладні аспекти оцінювання релевантності бази тестових завдань семантичній структурі навчальних матеріалів засобами штучного інтелекту. Інформаційні технології і автоматизація. Матеріали XVII міжнародної науково-практичної конференції. Одеса, ОНТУ, 2024. С. 381–383.

15. Гардиш Д.О., Мазурець О.В. Метод автоматизованого оцінювання відповідності тестових завдань семантичній складовій навчальних матеріалів за інтелектуальним аналізом їх текстового контенту. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». Хмельницький, 2024. С. 121–139.

16. Шебетко О.В., Кліменко В.І., Мазурець О.В. Метод адаптивного тестування з використанням продукційних правил. Збірник наукових праць за матеріалами XV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2023». Хмельницький, 2023. с. 311–322.

17. Бармак О.В., Крак Ю.В., Мазурець О.В., Манзюк Е.А. Ментально-формальні рішення машинного навчання для інформаційної технології автоматизованого створення тестів у сфері безпеки та медицини. Матеріали X Міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології ICST-ODESSA-2021». Одеса – 2021. – С.105–107.

18. Гардиш Д.О., Мазурець О.В. Метод автоматизованого аналізу відповідності множин тестових завдань семантичній структурі навчальних матеріалів засобами штучного інтелекту. Сучасні інформаційні технології в освіті і науці. Збірник матеріалів VI Всеукраїнської науково-практичної конференції. 14–15 листопада 2024. Умань, 2024. С. 43–48.

19. Гардиш Д.О., Кліменко В.І., Мазурець О.В. Підхід до аналізу відповідності множини тестових завдань семантичній структурі навчальних матеріалів засобами обробки природної мови. Тези доповідей XII Міжнародної науково-практичної конференції «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій». 10–12 грудня 2024. Запоріжжя, Національний університет «Запорізька політехніка», 2024. С. 344–348.

20. Крива Д.О., Мазурець О.В., Кліменко В.І., Тищенко О.О. Підхід до автоматизованого визначення рівня емпатії з використанням нелінійного тестування. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». 15–16 листопада 2024. Хмельницький, 2024. с. 316–324. URL: <https://kn.khmnu.edu.ua/wp-content/uploads/sites/18/apkn-2024-corpuspaper.pdf>

УДК 004.8

Кузь М.М.

Хмельницький національний університет

АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ЗАХИСТУ КОРИСТУВАЧІВ WI-FI-МЕРЕЖ ВІД ПІДРОБЛЕНИХ ТОЧОК ДОСТУПУ

У роботі розглянуто проблему безпеки користувачів бездротових Wi-Fi-мереж, зокрема загрозу, пов'язану з підробленими точками доступу. Проведено огляд сучасних підходів до їх виявлення та запобігання атакам. Визначено напрями подальших досліджень, спрямованих на підвищення захищеності користувачів у публічних і корпоративних мережах.

The paper examines the security problem of users of wireless Wi-Fi networks, in particular the threat associated with fake access points. A review of modern approaches to their detection and prevention of attacks is conducted. Directions for further research aimed at increasing user security in public and corporate networks are identified.

У сучасному середовищі бездротові мережі Wi-Fi стали невід'ємною складовою інфраструктури інформаційного обміну як у приватних домогосподарствах, так і в організаціях різного масштабу. Зростання кількості публічних точок доступу в громадських місцях, транспорті та навчальних закладах призвело до істотного підвищення ризиків, пов'язаних із несанкціонованим перехопленням даних користувачів. Однією з найпоширеніших і водночас найбільш небезпечних форм кіберзагроз у Wi-Fi-мережах є підроблені точки доступу, створені зловмисниками з метою перехоплення трафіку, отримання облікових даних або здійснення фішингових атак.

Проблема полягає в тому, що користувач, підключаючись до знайомої або нібито легітимної мережі, не має технічної можливості швидко перевірити автентичність точки доступу. Такі атаки ускладнюються тим, що підроблені точки можуть мати ті самі SSID, MAC-адреси та параметри шифрування, що й справжні мережі. З огляду на це, питання виявлення та нейтралізації фальшивих точок доступу є одним із напрямів інформаційної безпеки бездротових технологій. Практичне значення проблеми визначається необхідністю забезпечення конфіденційності, цілісності та доступності даних користувачів.

За останні роки було опубліковано значну кількість робіт, присвячених проблематиці виявлення підроблених точок доступу. У працях міжнародних дослідників розглянуто методи аналізу поведінкових характеристик точок доступу, зокрема часових затримок, інтенсивності пакетів і відмінностей у рівнях сигналу. Українські науковці досліджували питання побудови систем моніторингу Wi-Fi-простору для виявлення аномалій та розробки засобів активного захисту на основі аналізу радіочастотних параметрів.

Існуючі рішення можна умовно поділити на три групи: програмні методи, апаратні системи виявлення та гібридні підходи. Програмні методи передбачають використання клієнтських або серверних додатків, які здійснюють перевірку параметрів з'єднання, сертифікатів або відбитків точок доступу. Апаратні системи базуються на аналізі радіочастотних сигналів і можуть ідентифікувати джерела передавання за унікальними фізичними характеристиками, що дозволяє точніше визначати підроблені пристрої. Гібридні рішення поєднують переваги обох підходів, інтегруючи аналіз на рівні сигналу з програмними перевірками автентичності.

Попри значний прогрес у цій сфері, більшість рішень мають обмеження щодо масштабованості, вартості реалізації або рівня автоматизації. Зокрема, системи моніторингу Wi-Fi середовища у великих корпоративних мережах потребують значних ресурсів для оброблення даних, тоді як користувацькі додатки часто не мають доступу до низькорівневих параметрів адаптерів і не забезпечують повноцінний захист. Таким чином, залишаються невирішеними питання оптимізації точності виявлення при збереженні продуктивності системи, а також підвищення рівня адаптивності алгоритмів до нових типів атак.

Метою даної роботи є проведення системного аналізу сучасних методів виявлення та запобігання підробленим точкам доступу у Wi-Fi-мережах, визначення їхніх переваг і недоліків, а також обґрунтування напрямів подальшого вдосконалення механізмів захисту користувачів. Завдання дослідження полягає в узагальненні існуючих підходів, оцінці ефективності наявних алгоритмів і визначенні вимог до перспективних систем захисту, здатних функціонувати в умовах динамічного радіочастотного середовища.

У процесі дослідження було встановлено, що основні методи виявлення підроблених точок доступу поділяються за принципом дії на три групи: сигнатурні, поведінкові та контекстно-аналітичні. Сигнатурні методи базуються на порівнянні характеристик точки доступу з базою даних відомих легітимних пристроїв. Цей підхід ефективний у стабільних середовищах, проте вразливий до нових або змінених фальшивих точок. Поведінкові методи аналізують особливості обміну пакетами, рівень сигналу, швидкість автентифікації та інші динамічні параметри, що дозволяє виявляти аномалії, але вимагає значних обчислювальних ресурсів. Контекстно-аналітичні системи поєднують дані з різних джерел — зокрема GPS-координати, інформацію про довірені мережі та часові шаблони підключення — створюючи профіль користувацької поведінки.

Сучасні дослідження показують, що використання методів машинного навчання дозволяє підвищити точність і адаптивність таких систем. Наприклад, моделі на основі класифікації дерев рішень або нейронних мереж можуть автоматично визначати фальшиві точки за статистичними ознаками, навіть якщо ті змінюють свої параметри. Водночас необхідність великої кількості навчальних даних і обмеження мобільних пристроїв знижують ефективність практичної реалізації цих підходів.

Особливу увагу привертає концепція побудови довірених мереж (Trusted Wi-Fi Frameworks), у яких автентифікація здійснюється не лише за SSID і паролем,

а й за цифровими сертифікатами або криптографічними ключами, пов'язаними з конкретним пристроєм. Така модель дозволяє значно зменшити ризик перехоплення сесії, однак її впровадження потребує централізованого управління й підтримки інфраструктури публічних ключів.

Водночас у контексті публічних мереж перспективними є методи колективного моніторингу, коли пристрої користувачів спільно формують базу довірених точок доступу, обмінюючись даними про спостережувані аномалії. Це дозволяє створювати децентралізовані системи виявлення, які не залежать від одного адміністратора.

Результати проведеного аналізу свідчать, що жодне з існуючих рішень не забезпечує універсального захисту в усіх сценаріях використання Wi-Fi. Тому доцільним є поєднання декількох методів — наприклад, сигнатурного аналізу для попереднього фільтрування і поведінкового моніторингу для глибокої перевірки. Перспективним напрямом є впровадження інтегрованих систем, які використовують машинне навчання в поєднанні з апаратними засобами вимірювання параметрів сигналу.

Проведений аналіз показав, що проблема захисту користувачів Wi-Fi-мереж від підроблених точок доступу залишається надзвичайно актуальною через стрімкий розвиток технологій бездротового зв'язку та зростання кількості мобільних користувачів. Існуючі рішення забезпечують частковий рівень захисту, але потребують подальшої адаптації до умов реального середовища. Основними напрямками вдосконалення є інтеграція методів штучного інтелекту для автоматизованого виявлення аномалій, створення гібридних архітектур безпеки, що поєднують програмні та апаратні підходи, а також розробка стандартів обміну даними між системами моніторингу різних постачальників.

Подальші дослідження мають бути спрямовані на створення уніфікованої системи оцінювання довіри до точок доступу, яка могла б функціонувати як у корпоративному, так і у відкритому середовищі. Важливим завданням є підвищення рівня обізнаності користувачів щодо ризиків підключення до невідомих мереж та впровадження освітніх програм із кібергігієни. Отже, розвиток технологій захисту Wi-Fi не може розглядатися лише з технічного боку — він має супроводжуватися соціально-освітніми заходами, спрямованими на формування культури безпечного користування цифровими ресурсами.

Перелік посилань

1. Наталія Лукова-Чуйко, Тетяна Лаптева. Удосконалення методу виявлення та локалізації нелегальних точок доступу до бездротової мережі об'єктів інформаційної діяльності. Безпека інформаційних систем і технологій. Вип. 1, с. 21-27. DOI:10.17721/STS.2023.1.21-27.
2. Яровий, Р. О., Подвиженко, А. В., Переверзєв, А. М., Левченко, С. В. Публічні WI-FI мережі: захист особистої інформації. Науковий вісник Таврійського державного агротехнологічного університету. 2025. Вип. 15, с. 245-250. DOI: 10.32782/2220-8674-2025-25-1-29

УДК 004.855:519.85

Кутній М.С., Литвинова Є.І.

Харківський національний університет радіоелектроніки

ШУМОЧУТЛИВИЙ АДАМ ДЛЯ ГІБРИДНИХ КВАНТОВИХ МОДЕЛЕЙ

Запропоновано шумо-обізнаний метод оптимізації для навчання гібридних квантово-класичних нейронних мереж. Крок навчання адаптується до дисперсії оцінених градієнтів із повторним використанням тих самих вимірювань для градієнта та шуму. Показано підвищення стабільності й зменшення чутливості до вимірювального шуму в режимах із малою кількістю вимірювань порівняно з градієнтним спуском і Adam. Метод сумісний із правилом параметр-зсуву та не потребує додаткових квантових ресурсів.

A noise-aware optimization method for training hybrid quantum-classical neural networks is proposed. The learning rate adapts to the variance of gradient estimates while reusing the same measurements for both gradient and noise. Improved training stability and reduced sensitivity to measurement noise are demonstrated in low-shot regimes versus gradient descent and Adam. The method is compatible with the parameter-shift rule and requires no additional quantum resources.

Основну складність навчання гібридних квантово-класичних моделей становить вимірювальний шум, зумовлений скінченною кількістю вимірювань (shots — кількістю повторів), який підвищує дисперсію оцінок градієнтів і призводить до нестабільних оновлень параметрів [1–3]. Типові оптимізатори з фіксованими або емпірично підібраними гіперпараметрами не враховують поточний рівень шуму, що знижує ефективність оптимізації в низькошотових режимах. На тлі активних досліджень варіаційних квантових алгоритмів (VQA, Variational Quantum Algorithms — параметризовані квантові ланцюги, які навчаються класичним оптимізатором) і квантовому машинному навчанні сформовано інструменти для обчислення аналітичних градієнтів на квантовому обладнанні [1–4], а геометричні підходи на кшталт квантового натурального градієнта пропонують альтернативні схеми керування кроком у просторі параметрів [5].

Водночас лишається відкрите практичне завдання безресурсної (тобто такої, що обійдеться без додаткових вимірювань) адаптації кроку навчання до рівня квантового шуму, коли статистики для оцінювання градієнта та його дисперсії отримуються з одних і тих самих вимірювань у межах стандартної процедури parameter-shift [4].

Запропоновано масштабувати крок за оціненою дисперсією градієнта. Нехай α — базова швидкість навчання, $\lambda > 0$ — коефіцієнт чутливості, $\widehat{\text{Var}}[g_t]$ — оцінка дисперсії градієнта на кроці t , отримана з тих самих шотів, що й $\hat{g}_t$. Визначаємо:

$$\alpha_t = \frac{\alpha}{1 + \lambda \widehat{\text{Var}}[g_t]}, \quad \theta_{t+1} = \theta_t - \alpha_t \hat{g}_t. \quad (1)$$

Форма (1) зменшує крок за підвищеного шуму та відновлює його за низького.

Експериментальна схема узгоджена зі стандартною практикою VQA [1–3]. Вихідні дані MNIST попередньо зменшуються методом головних компонент до розмірності, що дорівнює кількості кубітів, і стандартизуються. Кодування ознак здійснюється обертаннями R_y з повторним завантаженням (recycling; параметр k визначає кількість повторів кодування у варіаційному ланцюгу). Анзац — апаратно-ефективний (HEA) із двома шарами ($L = 2$) та кільцевою топологією переплутування (ring) у поєднанні з локальними обертаннями. Математичні сподівання (expectation values) вимірюються в базисах Z та X і подаються на лінійний класифікатор з багатокласовою крос-ентропією як функцією втрат $L(\theta)$; якість моделі оцінюється точністю на валідації. Ми мінімізуємо функцію втрат $L(\theta)$ (багатокласова крос-ентропія) на тренувальній вибірці за допомогою базового Adam та запропонованого шумо-обізнаного Adam (масштабування кроку за (1)); якість моделі оцінюємо за точністю (accuracy) на валідаційній вибірці. Градієнти та їх дисперсія обчислюються правилом parameter-shift на тих самих shots, що унеможлиблює «витік» додаткового бюджету вимірювань. Для базового порівняння використовується Adam із фіксованими гіперпараметрами; шумо-обізнаний варіант застосовується в ідентичній конфігурації вимірювань. За потреби дозволено лінійно змінювати кількість shots упродовж епох (shot-annealing) і використовувати окремий бюджет shots на валідації для аналізу. У низькошотових режимах очікується зменшення коливань втрат і підвищення відтворюваності; зі зростанням shots — зближення з поведінкою базових оптимізаторів. Запропоноване шумо-обізнане масштабування кроку повністю сумісне з parameter-shift і типовими VQA, не потребує додаткових квантових ресурсів і орієнтоване на стабілізацію навчання за малих shots; подальші роботи передбачають ширший діапазон shots, інші анзаці та задачі, а також порівняння з геометричними методами оптимізації.

Для відтворюваності фіксуються сіди генераторів, єдині гіперпараметри анзацу/кодування для всіх оптимізаторів та логування метрик (втрати, точність,

норми градієнта, оцінена дисперсія, масштабувальний коефіцієнт) у CSV; порівняння проводиться в однакових умовах вимірювань.

Отже, запропоноване шумо-обізнане масштабування кроку є сумісним із parameter-shift і типовими VQA, не потребує додаткових ресурсів та орієнтоване на стабілізацію навчання за малих шотів. Перспективи подальших робіт включають розширені експерименти на діапазоні шотів, дослідження інших анзаців і задач, а також порівняння з геометричними методами оптимізації.

Перелік посилань

1. Cerezo M., Arrasmith A., et al. Variational quantum algorithms. *Nature Reviews Physics*. 2021;3(9):625–644.
2. Biamonte J., Wittek P., et al. Quantum machine learning. *Nature*. 2017;549:195–202.
3. Preskill J. Quantum computing in the NISQ era and beyond. *Quantum*. 2018;2:79.
4. Schuld M., Sweke R., Petruccione F. Evaluating analytic gradients on quantum hardware. *Phys. Rev. A*. 2019;99(3):032331.
5. Stokes J., Izaac J., et al. Quantum natural gradient. *Quantum*. 2020;4:269.

УДК 004.8

Кухар Т.Г.¹, Собко О.В.²

¹ Комунальний заклад загальної середньої освіти

«Лицей №17 Хмельницької міської ради»

² Хмельницький національний університет

РОЗРОБКА ЧАТБОТУ ДЛЯ САМООЦІНКИ СОЦІАЛЬНОЇ ТРИВОЖНОСТІ З ВИКОРИСТАННЯМ ЗАСОБІВ МАШИННОГО НАВЧАННЯ

Робота присвячена розробленню чатбота для самооцінки соціальної тривожності із застосуванням методів машинного навчання. На основі класифікаційної моделі, створено прототип, що аналізує поведінкові та самооцінні параметри користувача й формує орієнтовну оцінку рівня соціальної тривожності. Інтеграція у Telegram забезпечує високу доступність, мобільність та швидкість взаємодії, що підвищує практичну цінність інструмента. У роботі враховано етичні вимоги щодо конфіденційності, добровільної участі та недіагностичного характеру сервісу, відповідно до рекомендацій ВООЗ та ЮНЕСКО. Запропоноване рішення має потенціал для використання як допоміжний засіб самоспостереження й первинної орієнтації користувачів у власному психологічному стані.

The work is devoted to the development of a chatbot for self-assessment of social anxiety using machine learning methods. Based on the classification model, a prototype was created that analyzes the behavioral and self-assessment parameters of the user and forms an approximate assessment of the level of social anxiety. Integration into Telegram provides high accessibility, mobility and speed of interaction, which increases the practical value of the tool. The work takes into account ethical requirements for confidentiality, voluntary participation and non-diagnostic nature of the service, in accordance with the recommendations of WHO and UNESCO. The proposed solution has the potential to be used as an auxiliary tool for self-monitoring and primary orientation of users in their own psychological state.

Поширеність тривожних розладів у світі та в Україні стабільно зростає, що пов'язано з впливом пандемії COVID-19, воєнних подій, економічної нестабільності та зростаючої соціальної напруги [1]. За даними ВООЗ, тривожні розлади входять до провідних причин погіршення психічного здоров'я населення, а в Україні їх рівень істотно підвищився у 2022–2024 роках [2]. Зростання потреби в індивідуальній психологічній підтримці та брак доступних фахівців зумовлюють актуальність цифрових інструментів попередньої самооцінки емоційного стану.

Зростання рівня соціальної тривожності серед різних вікових груп [3], а також обмежений доступ частини населення до психологічної підтримки

підсилюють потребу у створенні інструментів ранньої самооцінки психоемоційного стану. У цьому контексті чатботи, здатні аналізувати мовлення користувача, набувають особливої актуальності [4, 5]. Вони можуть забезпечити анонімність, доступність і миттєвий зворотний зв'язок, що робить їх ефективним доповненням до традиційних методів психологічної діагностики. Застосування сучасних методів обробки природної мови [6] дає змогу виявляти ознаки соціальної тривожності на основі текстових повідомлень шляхом автоматичного аналізу лінгвістичних, семантичних та прагматичних характеристик висловлювань [7, 8].

Можливості NLP у цьому напрямку значно розширилися завдяки появі трансформерних архітектур [9], які забезпечують контекстне моделювання висловлювань та здатні виявляти приховані психоемоційні маркери [10], що не піддаються простому частотному чи лексичному аналізу. Нейромережеві моделі можуть розпізнавати лексеми, пов'язані з униканням, невпевненістю чи страхом соціальних взаємодій [11], а також аналізувати стилістичні особливості мовлення, такі як ступінь конкретності, варіативність словника та наявність емоційно забарвлених конструкцій [12]. Крім того, інтеграція моделей сентимент-аналізу, детекторів когнітивних викривлень та класифікаторів психоемоційних станів забезпечує комплексний підхід до оцінювання соціальної тривожності [13, 14].

Метою роботи є розроблення та апробація чатбота для самооцінки соціальної тривожності на основі класифікаційної моделі машинного навчання, інтегрованої у середовище Telegram, з орієнтацією на доступність, швидкість отримання зворотного зв'язку та коректність інтерпретації результатів.

У межах дослідження було реалізовано прототип чатбота, який використовує параметри способу життя та самооцінні показники, оброблені класифікаційною моделлю. Алгоритм передбачає попередню обробку відповідей користувача, подальшу оцінку ймовірності проявів соціальної тривожності та формування узагальненої рекомендації. Інтеграція в Telegram дає змогу забезпечити миттєву взаємодію, мобільність, асинхронність комунікації та низький поріг входження для користувача.

Перевагами розробленого рішення є висока доступність сервісу, можливість використання без спеціальної підготовки, швидке отримання первинної оцінки та потенціал масштабування функціональності. Модель машинного навчання дозволяє індивідуалізувати результати на основі поведінкових даних користувача, а інтеграція в месенджер підвищує зручність та мотивацію до регулярного самоспостереження.

Етичні аспекти проекту охоплюють добровільність участі користувача, прозоре пояснення мети та обмежень роботи моделі, дотримання принципів конфіденційності та мінімізації збору даних. Чатбот не виконує діагностики й не

замінює фахівця, а слугує лише допоміжним засобом попередньої самооцінки. Система передбачає нейтральну, недискримінаційну комунікацію, а також перенаправлення до професійної допомоги у разі виявлення ознак вираженого емоційного дистресу. Такі підходи узгоджуються з рекомендаціями ВООЗ, ЮНЕСКО та OECD щодо етичного застосування ШІ у сфері здоров'я.

Узагальнюючи, запропоноване рішення демонструє наукову новизну у поєднанні методів машинного навчання з інтерактивними технологіями месенджерів для підтримки психічного здоров'я. Практична значущість полягає у можливості застосування чатбота як доступного інструменту самооцінки, що може слугувати першим кроком до своєчасного звернення по фахову допомогу та підвищення цифрової психологічної грамотності населення.

Перелік посилань

1. WHO Report: Pandemic triggers 25% spike in depression and anxiety. URL: <https://strongminds.org/who-report-pandemic-triggers-25-spike-in-depression-and-anxiety/>
2. Anxiety disorders. URL: <https://www.who.int/news-room/fact-sheets/detail/anxiety-disorders>.
3. Hladun O., Mazurets O., Molchanova M., Sobko O. Real Time Detection the Person Emotion State Using Neural Network. Scientific Research: Modern Innovations and Future Perspectives. Proceedings of the 2 International scientific and practical conference. November 25-27, 2024. Montreal, Canada. 2024. Pp. 119-123.
4. Sobko O., Mazurets O., Didur V., Chervonchuk I. Recurrent Neural Network Model Architecture for Detecting a Tendency to Atypical Behavior Of Individuals by Text Posts. Theoretical and Practical Aspects of Modern Research. Proceedings of XXVI International scientific and practical conference. June 5-7, 2024. International Scientific Unity. Ottawa, Canada. 2024. Pp. 113-117.
5. Mazurets O., Sobko O., Vit R., Pasternak V. Practical Approach for Detection by Deep Learning of Target Objects of Subject Area Based on Semantic Connectivity Indicators in Audio Database. Proceedings of XXIV International Scientific and Practical Conference «Modern Scientific Challenges are the Driving Force of the Development of Scientific Research». May 22-24, 2024. Bruges, Belgium. International Scientific Unity. 2024. Pp. 91-96.
6. Овчарук О.М., Мазурець О.В. Нейромережевий метод діагностування психологічних розладів за аналізом повідомлень на основі роздільного підходу до класифікації. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». № 1, 2025. с. 210-216.
7. Murava V., Zalutska O., Didur V., Mazurets O. Software architecture of information system for exchanging LLM thematic prompts. Global Trends in the Development of Information Technology and Science. Proceedings IV International Scientific and Practical Conference. June 25-27, 2025. Stockholm, Sweden. Pp. 121-127.
8. Юрченко Д.Ю., Овчарук О.М., Мазурець О.В., Шевчук П.О. Метод використання нейромережі гібридної архітектури для визначення емоційної тональності текстових

повідомлень. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». № 2, 2025. с. 136-141.

9. Біт Р.В., Мазурець О.В. Метод виявлення психологічного цифрового перевантаження за аналізом текстових даних нейромережевими моделями глибокого навчання. Науковий журнал «Вісник Херсонського національного технічного університету». 2025. №2 (93). Т. 2. С. 107-114.

10. Mazurets O.V., Sobko O.V., Molchanova M.O., Zalutska O.O., Yurchak A.V. Practical Implementation of Neural Network Method for Stress Features Detection by Social Internet Networks Posts. Global Science: Prospects and Innovations. Proceedings of the II International Scientific and Theoretical Conference «Scientific Review of the Actual Events, Achievements and Problems». May 31, 2024. Berlin, Federal Republic of Germany: International Center of Scientific Research. 2024. Pp. 160-167.

11. Мазурець О.В., Козенко О.В., Собко О.В. Метод автоматизованого підбору відповідей на користувацькі запитання за семантичною подібністю. Матеріали XII Всеукраїнської науково-практичної конференції «Глушковські читання». Київ – 2023. с. 106-109.

12. E. A. Manziuk, O. V. Sobko, I. O. Podhorniuk, M. O. Molchanova, O. V. Mazurets, Multifactorial analysis of mobbing behavioral signs in educational environments posts by NLP means, Journal of Physics Conference Series 3105(1) (2025) 012025.

13. Molchanova M., Didur V., Sobko O., Mazurets O. Detection of Web Propaganda Patterns by Transformer Neural Networks: Improving Efficiency via Dataset Balancing, CEUR Workshop Proceedings, 2025, vol. 3988, pp. 112-126.

14. O. Mazurets, R. Vit, M. Molchanova, I. Tymofiiiev, O. Sobko, Context-enriched approach to students depression monitoring in education using BERT-GPT hybrid model, CEUR Workshop Proceedings 4096 (2025) 167-176.

УДК 004.4

Куцький А.С., Павлова О.О.

Хмельницький національний університет

АНАЛІЗ СУЧАСНИХ НАПРЯМКІВ ДОСЛІДЖЕНЬ У СФЕРІ ПЕРИФЕРІЙНИХ ОБЧИСЛЕНЬ

Розглянуто ключові напрямки сучасних наукових досліджень у галузі периферійних обчислень за період 2022–2024 років. Проаналізовано публікації, присвячені архітектурі безпеки, застосуванню штучного інтелекту на краю мережі, методам оптимізації розподілу ресурсів та відвантаження завдань. Систематизовано основні виклики та визначено перспективні «прогалини» для подальших наукових розвідок, зокрема у сферах надійності, прозорості та стійкості інтелектуальних периферійних систем

The key directions of modern scientific research in the field of edge computing for the period 2022–2024 are considered. Publications on security architectures, the application of artificial intelligence at the edge of the network, methods for optimizing resource allocation, and task offloading are analyzed. The main challenges are systematized, and promising "gaps" for further scientific exploration are identified, particularly in the areas of trustworthiness, transparency, and sustainability of intelligent edge systems.

Зі стрімким розвитком Інтернету речей та вимог до обробки даних у реальному часі, традиційні хмарні архітектури стикаються з проблемами затримок, пропускнуої здатності та приватності. Технологія периферійних обчислень, що передбачає перенесення обчислювальних ресурсів ближче до джерела даних, стала ключовим рішенням цих проблем. Однак ефективне впровадження edge-систем вимагає розв'язання низки наукових і практичних завдань, пов'язаних із безпекою, управлінням ресурсами та інтеграцією зі штучним інтелектом.

Метою дослідження є розробка алгоритму розподілу ресурсів в периферійних системах, яка б враховувала не лише критерії продуктивності, але й показники енергоефективності та надійності для завдань машинного навчання.

Аналіз наукових праць дозволяє виділити кілька домінантних напрямків досліджень у сфері периферійних обчислень.

Першим і одним із найбільш критичних є питання безпеки. Розподілена природа периферійних систем створює нові вектори атак. У роботі представлено детальний огляд архітектури безпеки спеціально для систем Edge-IoT. Більш широкий контекст надається у дослідженні, де автори проводять систематичний аналіз безпеки в трьох парадигмах: хмарних, туманних та периферійних обчисленнях.



Рисунок 1 – Захищена архітектура периферійних обчислень на базі IoT[1]

Другий важливий напрямок – це загальні огляди та практичні аспекти впровадження технології. Якісне дослідження допомагає зрозуміти реальні проблеми та переваги периферійних обчислень. У свою чергу, робота пропонує широкий огляд дослідницьких тенденцій та конкретних випадків використання.

Третій, і наразі найпопулярніший, напрямок – інтеграція периферійних обчислень зі штучним інтелектом, що отримало назву Edge AI. Інженерний аспект цього напрямку розкрито в роботі, де аналізуються апаратні можливості та обмеження сучасних пристроїв для розгортання вбудованого ШІ.

Четвертий блок досліджень присвячений технічним питанням оптимізації та управління ресурсами. Ефективне відвантаження завдань та розподіл ресурсів є ключовими для продуктивності edge-систем.

Суть проблеми відвантаження полягає у прийнятті рішення: виконувати завдання локально на пристрої чи передати його на потужніший периферійний вузол.

Модель прийняття рішення щодо відвантаження завдання

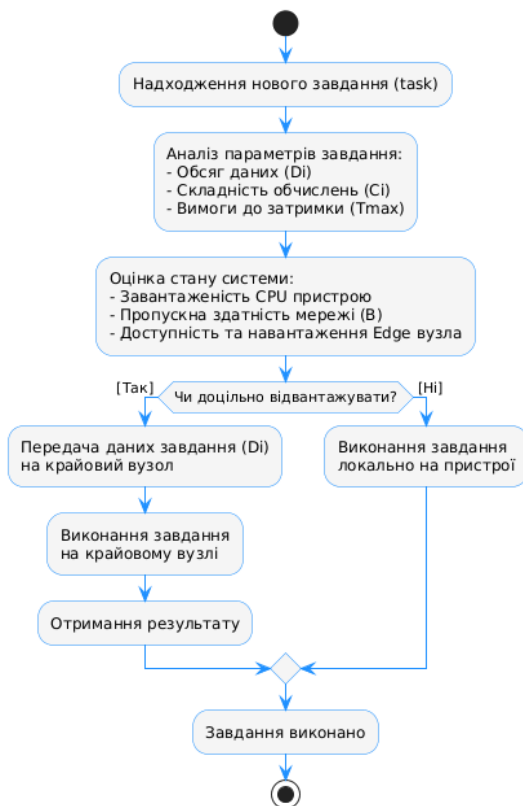


Рисунок 2 – Модель прийняття рішення щодо відвантаження завдання

Це рішення часто формалізується як оптимізаційна задача. Наприклад, для мінімізації загальної затримки виконання завдання i (T_{total}^i), необхідно зробити вибір, що описується бінарної змінною $a_i \in \{0,1\}$, де 1 означає відвантаження на край, а 0 — локальне виконання:

$$\min \sum_{i=1}^N (a_i * T_{edge}^i + (1 - a_i) * T_{local}^i) \quad (1)$$

де, T_{local}^i — час локального виконання, T_{edge}^i — сумарний час для відвантаження, який включає передачу даних та обчислення на периферійному сервері:

$$T_{edge}^i = T_{trans}^i + T_{proc}^i = \frac{D_i}{B} + \frac{C_i}{F_{edge}} \quad (2)$$

де D_i – обсяг даних завдання, B – пропускна здатність каналу, C_i – обчислювальна складність завдання, F_{edge} – обчислювальна здатність периферійного вузла.

Така оптимізація повинна виконуватись з урахуванням обмежень ресурсів периферійного вузла, наприклад, навантаження на процесор:

$$\sum_{i=1}^N a_i * C_i \leq C_{max} \quad (3)$$

Аналіз останніх досліджень показує, що хоча окремі аспекти периферійних обчислень, такі як оптимізація затримки та базова безпека, добре вивчені, бракує комплексних підходів.

Існує «прогалина» у створенні адаптивних фреймворків, які б динамічно керували ресурсами, враховуючи одночасно декілька критеріїв: продуктивність, енергоефективність та безпекові вимоги.

Більшість моделей оптимізації є статичними і не реагують на зміни в мережевому оточенні чи появу нових загроз.

Нарешті, залишаються відкритими питання життєвого циклу моделей III на краю: автоматизоване розгортання, моніторинг деградації продуктивності та безпечне оновлення моделей на тисячах гетерогенних пристроїв без втручання людини.

Отже, проведений аналіз сучасної наукової літератури засвідчив, що попри значну увагу до проблем оптимізації та безпеки в периферійних обчисленнях, існуючі рішення часто є вузькоспеціалізованими та статичними. Сформульована мета дослідження безпосередньо спрямована на подолання цієї прогалини шляхом створення адаптивного алгоритму, що динамічно балансує між критеріями продуктивності, енергоефективності та надійності. Розробка такого підходу дозволить створювати більш інтелектуальні, стійкі та ефективні периферійні системи для виконання завдань машинного навчання.

Перелік посилань

1. Elane F, Tor-Morten G. A Survey of Security Architectures for Edge Computing-Based IoT. 2022. MDPI.
2. Pérez, J., Díaz, J., Berrocal, J. et al. Edge computing. Computing 104. 2022. p. 2711–2747.
3. Raghbir Singh, Sukhpal Singh Gill. Internet of Things and Cyber-Physical Systems. 2023

УДК 004.8

Левченко А.С., Кліменко В.І.

Хмельницький національний університет

МЕТОД ФОРМУВАННЯ GIFT-ФАЙЛІВ ДЛЯ СЕРЕДОВИЩА MOODLE ДЛЯ АВТОМАТИЗОВАНОГО ФОРМУВАННЯ ТЕСТОВИХ ЗАВДАНЬ

Подано метод формування GIFT-файлів у складі інформаційної технології автоматизованого створення тестових завдань для середовища Moodle. Тестове завдання розглядається як об'єкт із внутрішньою об'єктною моделлю та зовнішнім текстовим представленням у форматі GIFT, між якими побудовано уніфіковане відображення. Запропоновано ієрархію викликів, у якій генерація змісту завдання здійснюється моделями типу BaseModel, а серіалізація до GIFT-файлу – спеціалізованим методом WriteTestCase. Показано інтеграцію методу з понятійно-тезовою моделлю навчального матеріалу, підтримку різних типів тестових завдань і використання випадкового вибору для формування варіативних тестів. Зазначено переваги методу щодо масштабованості, сумісності з Moodle та зручності експлуатації сформованих GIFT-файлів у навчальному процесі.

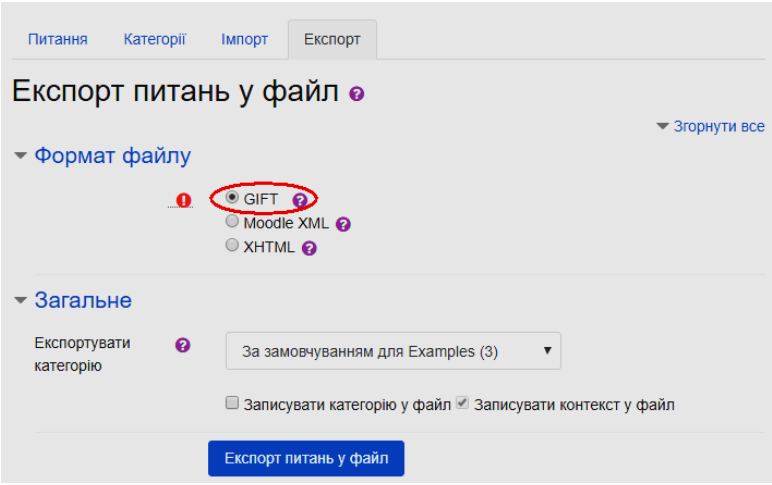
The paper presents a method for generating GIFT files within an information technology for automated test item creation in the Moodle environment. A test item is treated as an object with an internal model and an external text representation in GIFT format, and a unified mapping between these two levels is defined. The proposed call hierarchy separates content generation, implemented by BaseModel-derived item models, from serialization to a GIFT file performed by the WriteTestCase method. The method is integrated with the concept-thesis model of instructional texts, supports multiple item types and employs random selection to produce variable test versions. Its advantages in terms of scalability, compatibility with Moodle and practical usability of the resulting GIFT files in educational practice are outlined.

Актуальність дослідження зумовлена зростаючою потребою у високоефективних інструментах автоматизованого формування тестових завдань, які можуть підтримувати індивідуальні освітні траєкторії та адаптивні сценарії контролю знань [1, 2]. Традиційні підходи до створення тестів у Moodle вимагають значних часових і кадрових ресурсів [3], особливо коли йдеться про масштабні курси або системи, що повинні динамічно змінювати складність і зміст завдань залежно від рівня підготовки студента [4, 5]. У цьому контексті формати автоматизованої генерації, зокрема GIFT, виступають ключовим інструментом для забезпечення гнучкого та швидкого оновлення банку тестових завдань [6, 7].

Завдяки можливості алгоритмічного формування змісту питання [8], а також програмної варіації параметрів і структур [9], автоматизація дозволяє створювати великі набори тестів зі збереженням педагогічної валідності [10, 11]. Для адаптивного тестування це має особливе значення, оскільки система потребує великої кількості еквівалентних за змістом [12], але різних за формою завдань [13], щоб забезпечити коректне визначення рівня знань студента та мінімізувати ефект запам'ятовування [14, 15, 16]. Використання уніфікованих моделей представлення тестового завдання й автоматизованої серіалізації у формат GIFT забезпечує можливість швидкого масштабування, централізованого оновлення та автоматичного формування різнорівневих тестових наборів.

Таким чином, розробка методу формування GIFT-файлів для автоматизованого створення тестових завдань не лише підвищує ефективність розробки систем тестового контролю, але й створює основу для побудови адаптивних освітніх систем, здатних гнучко реагувати на індивідуальні особливості користувача та вимоги сучасного цифрового навчального середовища.

Метод формування GIFT-файлів для середовища Moodle у розробленій інформаційній технології ґрунтується на поданні тестового завдання як об'єкта, що має чітко визначену внутрішню структуру [17] та однозначне текстове відображення у форматі розмітки GIFT. Формат GIFT розглядається як цільова мова подання результатів роботи системи, що забезпечує сумісність із механізмами імпорту тестів у Moodle (рисунок 1) та не вимагає від користувача додаткових знань мов розмітки або спеціалізованих інструментів редагування [18].



The screenshot displays the 'Export questions to file' interface in Moodle. At the top, there are tabs for 'Питання' (Questions), 'Категорії' (Categories), 'Імпорт' (Import), and 'Експорт' (Export). The main heading is 'Експорт питань у файл'. Below this, there is a section 'Формат файлу' (File format) with three radio button options: 'GIFT' (selected and circled in red), 'Moodle XML', and 'XHTML'. To the right of this section is a link 'Згорнути все' (Collapse all). Below the format section is a 'Загальне' (General) section. It contains a dropdown menu for 'Експортувати категорію' (Export category) set to 'За замовчуванням для Examples (3)'. There are two checkboxes: 'Записувати категорію у файл' (Save category to file) which is unchecked, and 'Записувати контекст у файл' (Save context to file) which is checked. At the bottom is a blue button labeled 'Експорт питань у файл' (Export questions to file).

Рисунок 1 – Експорт питань у файл

У вихідному тексті підкреслено, що GIFT є простим текстовим форматом, здатним у межах одного файлу акумулювати велику кількість тестових завдань різних типів [19], підтримує запитання закритої та відкритої форми і допускає опис назви завдання, коментарів, вагових коефіцієнтів та інших параметрів, необхідних для організації тестування у Moodle.

На концептуальному рівні метод формування GIFT-файлів спирається на уявлення про дві взаємопов'язані площини подання тестового завдання – внутрішню об'єктну модель, яка використовується у програмному модулі TestGenerator, та зовнішнє текстове представлення, що відповідає формату GIFT. Внутрішня модель репрезентує завдання у вигляді екземпляра абстрактного класу BaseModel із заданими полями заголовка питання, множини варіантів відповідей, ознак правильності та, за потреби, додаткових параметрів [20]. Зовнішня форма задається через рядки текстового файлу, де питання починається з заголовка, далі в дужках фіксується перелік варіантів, кожен з яких маркується символом «=» для правильної відповіді або «~» для дистракторів, а структура файлу допускає також використання службових коментарів, які у розробленій системі позначають початок нового тестового завдання.

Ключовим завданням методу є побудова відображення між цими двома представленнями, яке забезпечує коректну і повну передачу інформації про форму і зміст тестового завдання. Для цього в базовому класі моделей формування завдань реалізовано уніфікований метод запису питання у файл WriteTestCase. Саме він інкапсулює конкретний синтаксис GIFT та приховує його від інших компонентів системи. Під час виклику цього методу модуль послідовно додає до вихідного потоку службовий коментар, що фіксує початок питання, текст заголовка з відповідним форматом, а потім у циклі обробляє всі елементи колекції відповідей, кожен з яких представлено об'єктом із полями «текст відповіді» та «ознака правильності». Для кожного варіанта за ознакою правильності обирається маркер «=» або «~», який у GIFT визначає, чи є відповідь правильною, після чого формується текстовий рядок, що містить цей маркер і власне текст відповіді. Завершальним кроком є запис закриваючої дужки і порожнього рядка, що відокремлює поточне питання від наступного.

Такий підхід має кілька методологічних наслідків. По-перше, задається чітка межа між логікою побудови змісту завдання та механізмом його текстового подання. Моделі формування завдань концентруються на виборі термінів, тез, дистракторів, побудові формулювання питання та комбінуванні відповідей, тоді як метод WriteTestCase відповідає виключно за коректну упаковку отриманого змісту у формат GIFT. Це суттєво спрощує розширення системи: додавання нового типу тестового завдання потребує розроблення лише спеціалізованого підкласу

BaseModel із власною реалізацією побудови питання, але не вимагає змін у механізмі запису у файл [21]. По-друге, уніфікована процедура запису гарантує однорідність вихідних GIFT-файлів незалежно від конкретної моделі, що підвищує надійність імпорту до Moodle та мінімізує ризики синтаксичних помилок.

Центральну роль у реалізації методу формування GIFT-файлів відіграє метод `GenerateTests` класу `TestGenerator`, який організовує послідовність викликів моделей формування завдань. У вихідному коді цей метод приймає на вхід тип тестового завдання, кількість питань, що мають бути сформовані, та засіб запису у файл. Перед генерацією система коригує бажану кількість питань з урахуванням розміру доступної множини термінів, щоб уникнути ситуацій, коли запитується більше завдань, ніж дозволяє інформаційний ресурс. Використовуючи список уже використаних індексів, метод забезпечує невідтворення однакових термінів у межах однієї сесії генерації, що підвищує різноманітність сформованого тесту. Для кожного нового завдання випадково обирається термін, на основі якого, через фабричний метод `ModelFactory`, створюється відповідна модель `BaseModel`. Далі послідовно викликаються методи `BuildTestCase`, який формує питання і набір відповідей відповідно до обраної моделі, та `WriteTestCase`, який записує результат у GIFT-файл.

Таким чином формується ієрархія викликів, де `GenerateTests` відповідає за стратегічну організацію процесу (вибір терміну, типу завдання, кількості питань), моделі типу `BaseModel` – за побудову змісту конкретного завдання, а метод `WriteTestCase` – за текстову реалізацію сформованого завдання у форматі GIFT. Важливо, що всі ці рівні взаємодіють через чітко визначені інтерфейси, що дає змогу розглядати метод формування GIFT-файлів як окремий компонент в архітектурі інформаційної технології, який може бути використаний повторно в інших системах, орієнтованих на Moodle.

Метод формування GIFT-файлів інтегровано з попередніми етапами обробки навчальних текстів та побудови моделей формування завдань. На вході методу перебуває множина термінів і тез, структурована відповідно до понятійно-тезової моделі навчального матеріалу та описана набором тегів, що використовуються в правилах конвертації.

Для кожного обраного терміна моделі формування завдань, спираючись на ці теги, генерують основу питання, коректну відповідь і один або декілька дистракторів. Метод `GenerateTests` забезпечує послідовне застосування цих моделей до елементів вхідної множини, тоді як запис у файл реалізує перехід від внутрішнього подання завдання до зовнішнього текстового представлення. Це дозволяє розглядати формування GIFT-файлу як завершальний етап конвеєра, що починається з аналізу лекційного тексту, виділення термінів, побудови тегованої

структури і завершується готовим набором завдань, доступним для імпорту у Moodle.

Особливе значення для практичної придатності методу має підтримка різних типів тестових завдань, передбачених форматом GIFT. У вихідному тексті відзначено, що GIFT дозволяє описувати завдання типу вибір з множини, вірно–невірно, коротка відповідь, вибір відповідності, числова відповідь, доповнювати їх коментарями та ваговими коефіцієнтами, а також акумулювати в одному файлі всі завдання незалежно від типу.

У розробленій інформаційній технології це реалізується через окремі моделі для кожного типу завдання, які успадковуються від BaseModel і перевизначають логіку побудови колекції відповідей. Метод WriteTestCase при цьому залишається спільним, оскільки формат подання варіантів відповідей у GIFT уніфіковано через маркери «=» і «~» та фігурні дужки, що обрамляють перелік відповідей. Така організація коду дозволяє надалі розширювати спектр підтримуваних типів завдань, зберігаючи загальний механізм формування GIFT-файлу незмінним.

Метод формування GIFT-файлів має також експлуатаційні переваги, пов'язані з простотою зберігання і перенесення сформованих тестів. Оскільки результати роботи системи подаються у вигляді звичайного текстового файлу з розширенням, що інтерпретується Moodle як GIFT, користувач може архівувати, копіювати, версійно контролювати та редагувати цей файл без спеціалізованих засобів. При необхідності вручну виправити окремі формулювання або додати коментарі достатньо відкрити GIFT-файл у текстовому редакторі, що знижує вхідний поріг для викладача й робить систему більш прозорою. У той же час завдяки суворому дотриманню синтаксису GIFT, яке забезпечується методом WriteTestCase, зберігається гарантія коректного імпорту тестів у Moodle без додаткової ручної адаптації (рисунк 2).

З точки зору архітектури інформаційної системи, описаний метод формування GIFT-файлів функціонує як модуль вихідної серіалізації, який використовує абстракції вищих рівнів, не впливаючи на них. Розробник може модифікувати або розширювати моделі формування завдань, змінювати правила конвертації, вводити нові теги, не змінюючи базовий механізм запису у формат GIFT. У граничному випадку можливо навіть реалізувати альтернативні модулі серіалізації для інших форматів, наприклад, Moodle XML або QTI, залишивши незмінними алгоритми формування змісту тестових завдань. Така модульність є важливою передумовою масштабованості та довготривалої підтримки системи.

Окремим аспектом методу є використання механізмів випадкового вибору при формуванні набору завдань. У фрагментах коду, наведених у роботі, показано

використання генератора псевдовипадкових чисел та структур спискового контролю вже використаних індексів, що забезпечує нерівномірність розподілу термінів і запобігає повторенню однакових завдань у межах одного тесту.

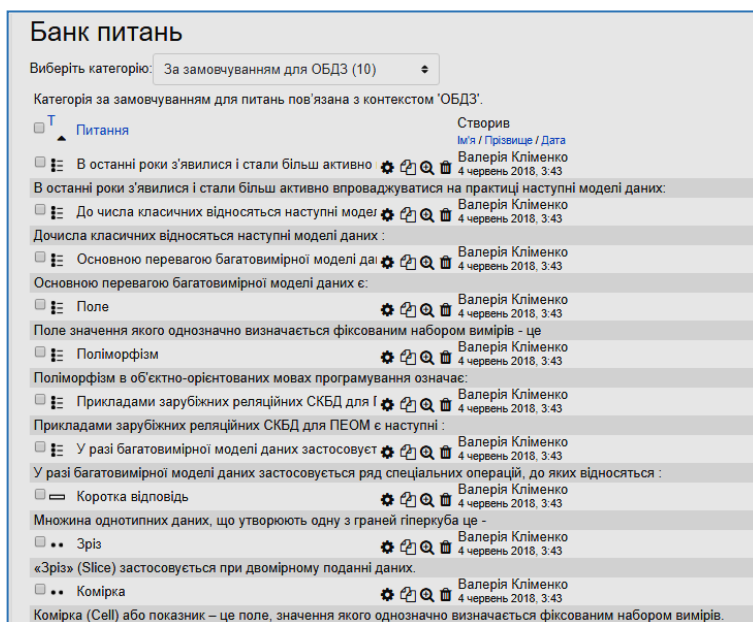


Рисунок 2 – Сформовані тестові завдання після імпорту до середовища Moodle

Це дозволяє на основі однієї й тієї самої множини термінів створювати різні варіанти тестів, що є важливим для організації поточного та підсумкового контролю знань. У поєднанні з можливостями GIFT щодо вагових коефіцієнтів та коментарів це створює підґрунтя для адаптивних сценаріїв тестування, де складність і структура тесту можуть змінюватися залежно від педагогічних цілей.

Узагальнюючи, метод формування GIFT-файлів для середовища Moodle у рамках розробленої інформаційної технології являє собою формалізований процес переходу від внутрішніх моделей тестових завдань до текстового представлення, стандартизованого у форматі GIFT. Він базується на чіткій об'єктній моделі завдання, уніфікованому механізмі серіалізації, використанні фабричних методів для побудови завдань різних типів, механізмах випадкового вибору термінів і надійній інтеграції з теґованим поданням навчального матеріалу. Така організація забезпечує сумісність із Moodle, підтримку широкого спектра типів завдань,

можливість масштабування та розширення системи, а також практичну зручність використання сформованих GIFT-файлів у навчальному процесі.

Перелік посилань

1. Як школи впроваджують технології в освіту. News IO. URL: <https://io.ua/yak-shkoly-integruyutsya-v-tsyfrovyj-svit/>
2. Методика використання тестової перевірки знань. Vseosvita. URL: <https://vseosvita.ua/library/metodika-vikoristanna-testovoi-perevirki-znan-204638.html>
3. Використання тестів в освітньому процесі. Vseosvita. URL: <https://vseosvita.ua/library/vikoristanna-testiv-v-osvitnomu-procesi-487976.html>
4. Multiple Choice Questions Types With Examples. SurveySparrow. URL: <https://surveysparrow.com/blog/multiple-choice-questions/>
5. Класифікація тестів. Форми тестових завдань. StudFiles. URL: <https://studfile.net/preview/8839472/page:72/>
6. Murava V., Zalutska O., Didur V., Mazurets O. Software architecture of information system for exchanging LLM thematic prompts. Global Trends in the Development of Information Technology and Science. Proceedings IV International Scientific and Practical Conference. June 25-27, 2025. Stockholm, Sweden. Pp. 121-127.
7. Mazurets O., Vit R. Practical Application of Method of Thematic Classification of Text Information Using LDA. Information Technology and Implementation (Satellite). Proceedings 11th International Conference. November 21, 2024. Kyiv, Ukraine. 2024. Pp. 151-152.
8. Yurchenko D., Mazurets O., Didur V., Molchanova M. Approach to Using Cloud Services for Visual Analytics of Neural Network Analysis of Texts Emotional Tonality. The Future of Scientific Discoveries: New Trends and Technologies. Proceedings of the XLVII International scientific and practical conference. November 13-15, 2024. Marseille, France. 2024. Pp. 108-113.
9. Blazhuk V., Mazurets O., Zalutska O. An Approach to Using the mBERT Deep Learning Neural Network Model for Identifying Emotional Components and Communication Intentions. The Impact of Scientific Research on the Development of the Modern World. Proceedings of the XLIV International scientific and practical conference. October 23-25, 2024. Dubrovnik, Croatia. 2024. Pp. 79-84.
10. Mazurets O., Molchanova M., Klimenko V., Prosvitliuk M Practice Implementation of Neural Network Model BART-Large-CNN for Text Annotation. Prospects of Scientific Research in the Conditions of the Modern World. Proceedings of XXVII International scientific and practical conference. June 12-14, 2024. Rotterdam, Netherlands. 2024. Pp. 97-102.
11. Shevchuk P., Molchanova M., Mazurets O. Software for Text Messages Reliability Analysis Based on the Machine Learning Models Ensemble. Proceedings of IV International Scientific and Practical Conference «Innovative research and perspectives of the development of science and technology». January 29-31, 2024. Stockholm, Sweden. 2024. Pp. 347-354.
12. Мазурець О.В., Тищенко О.О., Гардиш Д.О. Реляційна даталогічна модель для прикладного аналізу репрезентативності навчальних тестів засобами обробки природної мови. Наука і техніка сьогодні. 2025. № 13(41). С. 1129-1142.

13. Мазурець О.В., Собко О.В., Гардиш Д.О. Прикладні аспекти оцінювання релевантності бази тестових завдань семантичній структурі навчальних матеріалів засобами штучного інтелекту. Інформаційні технології і автоматизація. Матеріали XVII міжнародної науково-практичної конференції. Одеса, ОНТУ, 2024. С. 381–383.
14. Гардиш Д.О., Мазурець О.В. Метод автоматизованого оцінювання відповідності тестових завдань семантичній складовій навчальних матеріалів за інтелектуальним аналізом їх текстового контенту. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». Хмельницький, 2024. С. 121–139.
15. Hardysh D., Mazurets O., Tyschenko O. Datalogic Relation Model for Automated Evaluating the Semantic Integrity of Test Tasks Sets by Machine Learning Means. Innovative Solutions in Science: Balancing Theory and Practice. Proceedings 2nd International Scientific and Practical Conference. December 23–25, 2024. San Francisco, USA, 2024. P. 114–125.
16. Hardysh D., Tyschenko O., Mazurets O. Intelligent System for Automated Assessment of Test Tasks Sets Conformity to Semantic Structure of Educational Materials. The Role of Science and Technology in Solving Global Problems of Humanity. Proceedings LIII International Scientific and Practical Conference. December 25–27, 2024. Vienna, Austria, 2024. P. 110–115.
17. Гардиш Д.О., Мазурець О.В. Метод автоматизованого аналізу відповідності множин тестових завдань семантичній структурі навчальних матеріалів засобами штучного інтелекту. Сучасні інформаційні технології в освіті і науці. Збірник матеріалів VI Всеукраїнської науково-практичної конференції. 14–15 листопада 2024. Умань, 2024. С. 43–48.
18. Гардиш Д.О., Кліменко В.І., Мазурець О.В. Підхід до аналізу відповідності множини тестових завдань семантичній структурі навчальних матеріалів засобами обробки природної мови. Тези доповідей XII Міжнародної науково-практичної конференції «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій». 10–12 грудня 2024. Запоріжжя, Національний університет «Запорізька політехніка», 2024. С. 344–348.
19. Крива Д.О., Мазурець О.В., Кліменко В.І., Тищенко О.О. Підхід до автоматизованого визначення рівня емпатії з використанням нелінійного тестування. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». 15-16 листопада 2024. Хмельницький, 2024. с. 316-324. URL: <https://kn.khmn.u.edu.ua/wp-content/uploads/sites/18/apkn-2024-corpuspaper.pdf>
20. Шебетко О.В., Кліменко В.І., Мазурець О.В. Метод адаптивного тестування з використанням продукційних правил. Збірник наукових праць за матеріалами XV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2023». Хмельницький, 2023. с. 311-322.
21. Бармак О.В., Крак Ю.В., Мазурець О.В., Манзюк Е.А. Ментально-формальні рішення машинного навчання для інформаційної технології автоматизованого створення тестів у сфері безпеки та медицини. Матеріали X Міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології ICST-ODESSA-2021». Одеса – 2021. – С.105-107.

УДК 004.4

Лисенко С.М., Качур А.В.

*Хмельницький національний університет***МЕТОД СИНТЕЗУ РЕЗИЛЬЄНТНИХ АРХІТЕКТУР СИСТЕМ
ВІРТУАЛЬНОЇ ТА ДОДАНОЇ РЕАЛЬНОСТІ**

Запропоновано підхід, що поєднує формальні критерії резильєнтності з кількісною оптимізацією для підвищення стійкості систем на рівнях апаратного та програмного забезпечення, даних і користувача. Визначено ключові показники – надійність, доступність, цілісність, відмовостійкість, час відновлення, стабільність продуктивності та безпеку користувача – і показано, як вони формують єдину систему оцінки здатності AR/VR-середовищ підтримувати роботу за змінних умов. Метод передбачає перевірку вхідних параметрів, побудову моделей надійності та застосування стратегій мінімізації впливу мережевих, середовищних, поведінкових, системних і апаратних факторів. Результатом є узгоджена модель забезпечення резильєнтності, що дозволяє оптимізувати архітектури AR/VR за вимірюваними показниками продуктивності й безпеки. Запропонований підхід створює основу для числової оптимізації та практичного проектування резильєнтних систем занурення, здатних стабільно функціонувати навіть за дії зовнішніх факторів.

A method is proposed that combines formal resilience criteria with quantitative optimisation to enhance system stability across hardware, software, data, and user levels. Key indicators – reliability, availability, integrity, fault tolerance, recovery time, performance stability, and user safety – are defined and shown to form a unified framework for assessing the capability of AR/VR environments to maintain operation under variable conditions. The method includes verification of input parameters, construction of reliability models, and application of strategies to minimise the impact of network, environmental, behavioural, system, and hardware factors. The result is a coherent resilience assurance model that enables optimisation of AR/VR architectures according to measurable performance and safety criteria. The proposed approach provides a foundation for numerical optimisation and practical design of resilient immersive systems capable of stable functioning even under external disturbances.

Резильєнтність розглядається як здатність системи підтримувати прийнятний рівень продуктивності, попри збої, деградацію чи зовнішні впливи. Для її оцінювання визначено сукупність кількісних критеріїв: надійність, доступність, відмовостійкість, цілісність, час відновлення, стабільність продуктивності та безпека користувача [1]. Надійність системи:

$$R(t) = e^{-\lambda t}, \quad (1)$$

де λ – інтенсивність відмов.

Доступність визначається як:

$$A = \frac{MTTF}{MTTF + MTTR}, \quad (2)$$

де MTTF – середній час до відмови, MTTR – середній час відновлення. Відмовостійкість для k-із-n систем:

$$FT(k, n, t) = \sum_{i=k}^n \binom{n}{i} R(t)^i [1 - R(t)]^{n-i} \quad (3)$$

Цілісність відображає стійкість до пошкодження даних під час передачі та зберігання. З урахуванням знайдених та виправлених помилок:

$$I = 1 - \frac{E_d - E_c}{E_d} \quad (4)$$

Час відновлення – затрачений час від виникнення збою до повного відновлення, прив'язаний до середнього часу відновлення:

$$MTTR = \frac{1}{N} \sum_{i=1}^N (t_{\text{restore},i} - t_{\text{fail},i}) \quad (5)$$

Стабільність продуктивності показує відхилення від номінальних показників продуктивності:

$$PS = 1 - \frac{|P(t) - P_0|}{P_0} \quad (6)$$

Параметр безпеки користувача – це ймовірність того, що небезпечна ситуація не станеться:

$$US = 1 - P_{\text{hazard}} = 1 - \rho(1 - R_{\text{sys}}) \quad (7)$$

Кожен показник відображає окремий аспект поведінки системи й вимагає спеціалізованих стратегій покращення. Апаратна резильєнтність підвищується за рахунок надлишковості, теплового контролю та адаптивного енергокерування; програмна – завдяки механізмам самовідновлення та контрольним точкам; резильєнтність даних забезпечується надмірністю каналів зв'язку та корекцією помилок; користувацька – ергономічним дизайном і безпековими обмеженнями, що мінімізують вплив збоїв на сприйняття.

Методологічна схема розглядає ці критерії як взаємопов'язані цілі оптимізації. Поліпшення одного параметра часто покращує інші – наприклад, скорочення часу відновлення підвищує доступність, а зниження частоти помилок зміцнює цілісність і стабільність продуктивності. Отже, синтез спрямований на пошук багатовимірного оптимуму, де поєднання архітектурних рішень для апаратних, програмних, комунікаційних і користувацьких підсистем забезпечує найвищу стійкість системи за заданих умов експлуатації.

Метод передбачає максимізацію кожного критерію окремо при одночасній мінімізації часу відновлення. Конфігураційні параметри (рівень резервування,

політика DVFS, частота контрольних точок, рівень FEC, режим безпеки [2]-[5]) оцінюються відносно вимірюваних метрик.

Етап 1 – верифікація та базова оцінка.

Перед застосуванням методів пом'якшення система проходить структурну перевірку: уточнюються параметри, моделі та вимірювання. Визначається час місії й робочі режими (idle/normal/peak), створюється Reliability Block Diagram (RBD) для основних компонентів, а для блоків із відновленням – мінімальна СТМС-модель, що описує часову динаміку. Розраховуються інтенсивності відмов λ і відновлення μ перевіряються затримки і граничні механізми безпеки (guardian boundaries, freeze-on-fault). Для кожного критерію задаються мінімальні прийнятні значення, нижчі конфігурації відсіюються до етапу синтезу.

Етап 2 – застосування стратегій пом'якшення впливу.

Для підвищення загальної стійкості застосовуються цільові заходи проти основних збурювальних факторів: мережних умов, параметрів середовища, поведінки користувача, системного навантаження та апаратних обмежень. Ці фактори по-різному впливають на апаратні (H), програмні (S), комунікаційні (D) й користувацькі (U) підсистеми. Для кожного рівня передбачено конкретні методи – адаптивне потокове передавання, прогнозне керування температурою, самовідновлення процесів, багатоканальне з'єднання, динамічну зміну рівня деталізації, а також механізми, що підвищують комфорт і безпеку користувача.

Застосування методу може бути промодельоване в Simulink (рисунок 1)

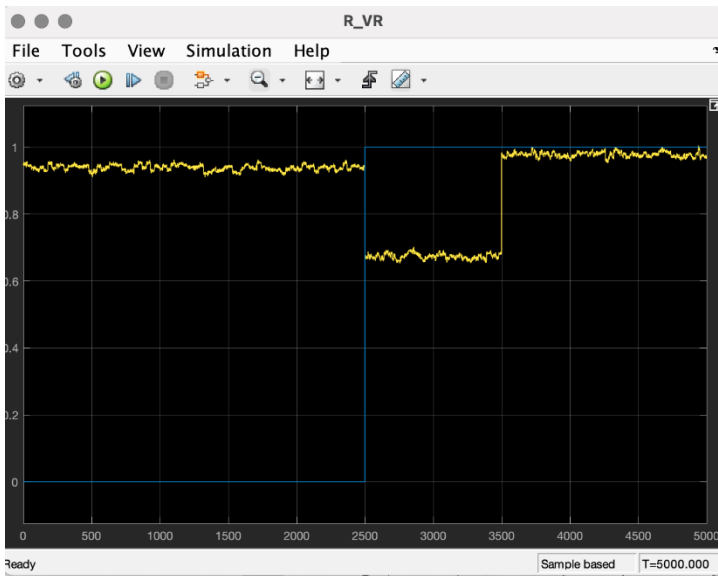


Рисунок 1 – Відновлення системи після збою

У результаті формується уніфікована модель синтезу, яка перетворює ці стратегії на параметризовані змінні, що можуть бути оптимізовані аналітично або шляхом чисельного моделювання для досягнення максимальної резильєнтності AR/VR-систем.

Перелік посилань

1. S. Lysenko and A. Kachur, "A Resilience Assurance Process Model for Enhancing Virtual Reality Architectural Design," 2024 14th International Conference on Dependable Systems, Services and Technologies (DESSERT), Athens, Greece, 2024, pp. 1–9, doi: 10.1109/DESSERT65323.2024.11122129.
2. Y. Sun, Z. Jiang, C. Xu, S. Zhou, and Z. Niu, "Communication, Computing and Caching for Mobile VR Delivery: Modeling and Trade-off," arXiv preprint arXiv:1804.10335, 2018. [Online]. Available: <https://arxiv.org/abs/1804.10335>
3. X. Zhang, Y. Xia, and M. Ali, "A Smartphone Thermal Temperature Analysis for Virtual and Augmented Reality," National Science Foundation Technical Report, 2020. [Online]. Available: <https://par.nsf.gov/servlets/purl/10219090>
4. J. Gomez, S. Raghunathan, and K. Chowdhury, "Distributed On-Sensor Compute System for AR/VR Devices: A Semi-Analytical Simulation Framework for Power Estimation," arXiv preprint arXiv:2203.07474, 2022. [Online]. Available: <https://arxiv.org/abs/2203.07474>
5. J. Xiong, Y. Li, K. Liu, X. Liu, and Z. Liu, "Augmented Reality and Virtual Reality Displays: Emerging Technologies and Future Perspectives," *Light: Science & Applications*, vol. 10, no. 1, 2021. [Online]. Available: <https://www.nature.com/articles/s41377-021-00658-8>

УДК 004.738.5

Лісовий В.В., Мішан В.В.

Хмельницький національний університет

МЕРЕЖЕВА АРХІТЕКТУРА РОЗУМНОГО МІСТА З ВИКОРИСТАННЯМ ІОТ-РІШЕНЬ

Розглянуто принципи побудови мережевої архітектури розумного міста із застосуванням технологій Інтернету речей (IoT). Проаналізовано сучасні підходи до інтеграції сенсорних систем, передачі даних та управління міською інфраструктурою. Запропоновано модель архітектури, яка забезпечує ефективну взаємодію підсистем, масштабованість і підвищену безпеку інформаційного обміну.

The principles of building a smart city network architecture using Internet of Things (IoT) technologies are considered. Modern approaches to the integration of sensor systems, data transmission, and urban infrastructure management are analyzed. A model of architecture that ensures efficient subsystem interaction, scalability, and increased data security is proposed.

Згідно зі звітами ITU-T (2024) та Cisco Smart Cities Report (2023), понад 60% міст світу вже використовують елементи IoT для управління транспортом, енергетикою та комунальними послугами. Зі зростанням кількості підключених пристроїв виникає потреба у побудові надійної та уніфікованої мережевої інфраструктури, здатної обробляти великі обсяги даних у реальному часі.

Метою роботи є аналіз і проектування мережевої архітектури розумного міста з використанням IoT-рішень, що забезпечують безпечний обмін даними, гнучке масштабування системи та можливість централізованого управління міськими ресурсами.

Проблема ефективного функціонування розумного міста пов'язана із сумісністю великої кількості сенсорів і протоколів, оптимізацією передачі даних та забезпеченням кібербезпеки. Традиційні централізовані моделі не завжди здатні обробляти інформаційні потоки від тисяч пристроїв, тому актуальним є використання гібридної архітектури – Edge-Fog-Cloud.

На периферійному рівні (Edge) розташовуються сенсори, контролери та мікропристрої, які збирають дані про довкілля, транспорт, енергоспоживання тощо. Проміжний рівень (Fog) виконує попередню обробку даних, фільтрацію та маршрутизацію, зменшуючи навантаження на хмару. Хмарний рівень (Cloud)

забезпечує аналітику, зберігання великих даних (Big Data) та управління міськими сервісами через API.

Передача даних здійснюється з використанням протоколів MQTT, CoAP та LoRaWAN, які оптимізовані для пристроїв з обмеженими ресурсами. Для побудови транспортної мережі пропонується застосування принципів SDN (Software-Defined Networking), що дає змогу централізовано керувати потоками трафіку та підвищувати ефективність маршрутизації.

Безпека інформаційного обміну реалізується через TLS-шифрування, автентифікацію пристроїв на основі сертифікатів X.509 та сегментацію мережі за рівнями доступу. Ключовими показниками ефективності системи є затримка передачі даних (latency), енергоспоживання вузлів, рівень доступності (uptime) та стійкість до відмов.

При розробленні моделі враховано перспективу впровадження штучного інтелекту для адаптивного керування міськими ресурсами. Така система дозволить автоматично змінювати режими роботи освітлення, транспорту та енергопостачання залежно від поточних даних сенсорів.

Отже, запропонована мережева архітектура розумного міста з використанням IoT-рішень забезпечує гнучку інтеграцію підсистем, підвищення енергоефективності та зниження експлуатаційних витрат. Подальші дослідження доцільно спрямувати на моделювання навантажень у реальному часі, розроблення системи пріоритетизації трафіку та вдосконалення методів кіберзахисту.

Перелік посилань

1. Cisco Systems. Smart Cities Architecture Guide. – 2023. – URL: <https://www.cisco.com/smartcity>.
2. ITU-T Y.4900. Smart Sustainable Cities – Overview and Definitions. – International Telecommunication Union, 2024.
3. Li, Y., Chen, M. Internet of Things for Smart City: Architecture and Security Issues. – IEEE Internet of Things Journal, 2024, Vol. 11(3), pp. 2214–2228.
4. Juniper Research. Smart City Market Outlook 2025. – 2024. – URL: <https://www.juniperresearch.com>.
5. ISO/IEC 30182:2023. Smart city concept model – Guidance for establishing a model for data interoperability.

УДК 004.8

Лянськорунський К.О., Молчанова М.О.

Хмельницький національний університет

АЛГОРИТМ СЕГМЕНТАЦІЇ ПРИНТІВ ЗАСОБАМИ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ШОВКОГРАФІЇ

Описано нейромережевий алгоритм сегментації принтів для шовкографського друку, спрямований на автоматичне відокремлення зображення принта від фону тканини, складок, тіней та сторонніх артефактів. Запропонований каскадний підхід поєднує попереднє грубе виділення області «принт/фон» на основі моделей SAM-подібного класу з подальшою деталізованою багатокласовою сегментацією елементів принта з орієнтацією на цілісність контурів. Навчання здійснюється на спеціалізованому датасеті з полігональною розміткою ключових елементів із використанням аугментацій та функції втрат, чутливої до розривів контурів. Експериментальні результати показали зменшення обсягу ручної дорисовки масок та підвищення стабільності виділення дрібних деталей і якості подальшого кольороподілу й масштабування, що створює основу для побудови повністю цифрового препрес-конвеєра «фото принта – набір трафаретів».

This paper presents a neural network-based segmentation algorithm for screen-print artwork, aimed at automatically separating the print from the fabric background, folds, shadows and other artefacts. The proposed cascaded approach combines an initial coarse «print/background» separation using SAM-like segmentation models with a subsequent detailed multi-class segmentation of print elements focused on contour integrity. Training is performed on a specialised dataset of print photographs with polygonal annotations of key elements, employing extensive data augmentation and a loss function penalising contour fragmentation. Experimental results demonstrate reduced manual mask editing, more stable extraction of fine details and improved quality of downstream colour separation and scaling, thus forming a foundation for a fully digital prepress pipeline from print photo to a set of screen-printing stencils.

Цифрова підготовка макетів до шовкографського друку потребує не лише високої роздільної здатності зображення, а й коректного відокремлення принта від фону тканини, складок, тіней та сторонніх об'єктів [1]. Ручна векторизація або маскування призводять до значних трудовитрат і суб'єктивних похибок, особливо для складних багатокольорових принтів із дрібними деталями [2]. Класичні порогові та контурні методи сегментації виявляються нестійкими до варіацій освітлення, текстури тканини, спотворень при фотографуванні та шумів. Це зумовлює потребу в спеціалізованому алгоритмі сегментації принтів, побудованому на моделях штучного інтелекту та орієнтованому на вимоги шовкографії: чіткі контурно-стабільні маски, узгоджені з подальшим кольороподілом і формуванням друкарських шарів [3].

Актуальність автоматизованої сегментації принтів для шовкографічного друку зумовлена стрімким переходом текстильного виробництва до цифрових робочих процесів [4], де ключовими вимогами є швидкість, висока точність та мінімізація ручної праці. Традиційні методи підготовки принтів передбачають значний обсяг ручної дорисовки контурів, ретушування фону та відокремлення дрібних графічних елементів, що істотно сповільнює препрес-етап і створює високу залежність від кваліфікації оператора. Оскільки цифрові принти часто знімаються без контрольованих умов освітлення, містять складки тканини, тіні, зміни фактури та сторонні артефакти, класичні алгоритми сегментації демонструють нестабільність і не забезпечують потрібного ступеня точності для подальшого кольороподілу й створення трафаретів. Це формує запит на застосування сучасних інструментів комп'ютерного зору [5], які здатні працювати з реальними неконтрольованими даними та адаптуватися до варіативності матеріалів і стилістики графічних композицій.

Застосування згорткових нейронних мереж [6] та похідних архітектур [7] у сфері текстильних технологій відкриває принципово нові можливості для побудови автоматизованих виробничих конвеєрів. CNN-моделі [8] та трансформерні сегментатори [9] демонструють високу здатність до узагальнення складних візуальних патернів, що робить їх ефективними для завдань, де межа між принтом і фоном може бути нечіткою, а контури елементів – тонкими або частково перекритими [10, 11]. Завдяки вбудованій інваріантності до афінних перетворень та здатності вловлювати просторові залежності між пікселями, такі моделі дозволяють долати проблеми нерівномірного освітлення, зміни фактури тканини й локальних деформацій [12], які традиційно є критичними для шовкографічної підготовки. Успішні результати застосування моделей сегментації у суміжних сферах – медичній візуалізації, аналізі сцен, об'єктному трекінгу [13, 14] – підтверджують їх потенціал для опрацювання текстильних зображень, де важливими є як точність контурів, так і структурна цілісність.

У контексті сегментації принтів для шовкографії особливої значущості набувають моделі, здатні працювати в каскадному режимі: від початкового грубого відокремлення принта від фону до високоточних процедур багатокласового розбиття на структурні компоненти [15]. Використання алгоритмів SAM-подібного класу на першому етапі забезпечує стійке виділення області інтересу навіть за наявності шумів та неоднорідного фону, що створює надійну основу для подальшої деталізації. Другий етап, заснований на CNN або гібридних архітектурах із трансформерами, дозволяє глибоко аналізувати взаємне розташування елементів принта, виявляти їхні межі та відновлювати тонкі лінії, які є критично важливими для коректної побудови трафаретів [16]. Такий підхід не лише скорочує потребу в ручному коригуванні масок, а й підвищує відтворюваність результатів, що має ключове значення для масштабного виробництва та стандартизованих робочих процесів [17].

Запровадження нейромережових методів у препрес-процеси текстильного дизайну дозволяє переосмислити традиційні практики та перейти від напівручних способів підготовки до повністю автоматизованих систем. Алгоритми глибинного навчання створюють передумови для побудови цифрового циклу «фото принта – сегментація – кольороподіл – набір трафаретів» без втручання оператора, що радикально зменшує часові та ресурсні витрати [18]. Більше того, адаптивність сучасних моделей уможливорює перенавчання на конкретні стилі, типи тканин або художні техніки, що розширює сферу застосування та забезпечує високу універсальність. Таким чином, комп'ютерний зір та методи глибинної сегментації становлять фундамент для нового покоління інструментів цифрової шовкографії, де точність, автоматизація та стабільність обробки є визначальними факторами технологічного прогресу.

Метою роботи є розроблення нейромережового алгоритму сегментації принтів для шовкографського друку, який забезпечує автоматичне формування контурно-стабільних масок принта, стійких до змін умов зйомки та властивостей тканини-носія. Алгоритм розглядається як базовий елемент препрес-конвеєра, що передусє масштабуванню, кольороподілу та генерації трафаретів, і повинен забезпечувати технологічно коректні границі, придатні для побудови окремих друкарських шарів.

Запропонований підхід поєднує каскадну схему сегментації з використанням глибинних нейромереж. На першому етапі виконується грубе відділення області принта від фону тканини за допомогою попередньо натренованих моделей сегментації, типу SAM-подібних архітектур, які працюють із зображеннями, отриманими в реалістичних умовах (змінне освітлення, складки, шум). Результатом є маска «принт/фон», що очищує сцену від зайвих елементів та обмежує подальшу обробку робочою областю. На другому етапі в межах цієї області застосовується деталізована сегментація елементів принта з орієнтацією на контури: використовується багатокласова або багатомаскова модель, яка виділяє основні кольорові області та структурні фрагменти, забезпечуючи цілісність замкнених контурів і коректне відокремлення дрібного штриха.

Навчання алгоритму базується на спеціалізованому наборі даних, що містить оригінальні фотографії принтів на тканині з розміткою «принт/фон» та детальними полігональними масками ключових елементів. Для підвищення стійкості до варіацій умов зйомки застосовуються аугментації (зміни яскравості, контрасту, колірних відтінків, перспективні спотворення, додавання шуму). Функція втрат поєднує піксельно-орієнтовані метрики з додатковими штрафами за фрагментацію контурів або розриви замкнених областей, що відповідає вимогам трафаретного друку до безперервності друкарських елементів.

На етапі інференсу реалізовано тайлування з перекриттям, що дає змогу обробляти великі зображення принтів без втрати локальної деталізації. Маски, отримані для окремих тайлів, агрегуються із згладжуванням у зонах перекриття; додатково застосовується контурно-орієнтована морфологічна постобробка для

усунення дрібних «дір» та шумових артефактів. За потреби формується скорочений набір масок: глобальна маска принта для подальшого масштабування та відокремлені маски основних кольорових шарів, придатні до прямого використання в модулі кольороподілу.

Експериментальна перевірка алгоритму на корпоративному наборі принтів засвідчила, що нейромережева сегментація забезпечує стабільніше виділення контурів та дрібних елементів порівняно з традиційними пороговими підходами, знижує частку ручної дорисовки та виправлення масок, а також покращує якість подальшого кольороподілу й масштабування. Розроблений алгоритм сегментації формує основу для побудови повністю цифрового конвеєра підготовки даних до шовкографії, зменшує людський фактор і трудомісткість препрес-процесів та створює передумови для подальшої автоматизації ланцюжка «фото принта – набір трафаретів».

Перелік посилань

1. Kumah, C., Raji, R. K., & Pan, R. (2020). Review of printed fabric pattern segmentation analysis and application. *Autex Research Journal*, 20(4), 530-538.
2. Kumah, C., Zhang, N., Raji, R. K., Li, Z., & Pan, R. (2022). Unsupervised segmentation of printed fabric patterns based on mean shift algorithm. *The Journal of The Textile Institute*, 113(1), 1-9.
3. Chakraborty, S., Moore, M., & Parrillo-Chapman, L. (2022). Automatic defect detection for fabric printing using a deep convolutional neural network. *International Journal of Fashion Design, Technology and Education*, 15(2), 142-157.
4. Molchanova M., Mazurets O., Klimenko V., Kuflevsky Ev. Object-oriented model for neural network damage detection of mail packages. *Proceedings of XIV International Scientific and Practical Conference «Solving Scientific Problems Using Innovative Concepts»*. March 13-15, 2024. Copenhagen, Denmark. 2024. Pp. 58-62.
5. Pokhytun A., Mazurets O., Molchanova M., Tyschenko O. Method for Neural Network Detecting Changed Images of People's Faces Using CNN. *New Horizons in Scientific Research: Challenges and Solutions. Proceedings of the 1st International scientific and practical conference*. October 21-23, 2024. Marseille, France. 2024. Pp. 35-40.
6. Kharysh I., Sobko O., Mazurets O. Designing CNN Neural Network Model for Detecting Fractures of Lower Extremities by X-ray Images. *The Impact of Scientific Research on the Development of the Modern World. Proceedings of the XLIV International scientific and practical conference*. October 23-25, 2024. Dubrovnik, Croatia. 2024. Pp. 91-96.
7. Zharnovskiy O., Mazurets O., Sobko O. Approach to Identification of Artificial Intelligence-Generated People Images by Means of Machine Learning. *Key Aspects of the Development of Scientific Research in Modern Conditions. Proceedings of the XLV International scientific and practical conference*. October 30 – November 1, 2024. Constanta, Romania. 2024. Pp. 69-73.
8. Mazurets O. V., Klimenko V. I., Molchanova M. O., Sultanov A. V. Object-Oriented Intelligent System for Neural Network Detection of Sugar Crystallization Zones. *Global Science: Prospects and Innovations. Proceedings of the 10th International scientific and practical conference*. Cognum Publishing House. Liverpool, United Kingdom. 2024. Pp. 198-207.
9. Novak Y., Mazurets O. Practical Application of Method of Automated Personal Identification by Fingerprints Using Convolution Neural Networks. *Proceedings of V International Scientific*

- and Practical Conference «Modern strategies of global scientific solutions». December 27-29, 2023. Stockholm, Sweden, International Scientific Unity. 2023. Pp. 136-140.
10. Mazurets O., Uspenska K., Vit R., Tyschenko O. Intelligent System for Determining the Object Attributes Values by Neural Networks Means by Graphic Images in Databases. Current Trends in the Development of Scientific Research in Today's Conditions. Proceedings of XXV International scientific and practical conference. May 29-31, 2024. International Scientific Unity. Florence, Italy. 2024. Pp. 86-91.
 11. Kok I.A., Kadyńska V.D., Zalutka O.O., Mazurets O.V. Object-Oriented Intelligent System for Automated Control of Smoking by Video Data. Current scientific goals, approaches and challenges. Proceedings of IV International Scientific and Theoretical Conference. June 13, 2025. Dresden, Federal Republic of Germany. Pp. 156-164.
 12. Bas I.S., Kadyńska V.D., Klimenko V.I., Mazurets O.V. Convolutional Neural Network Transfer Learning Method for Aircraft Image Classification. Scientific method: reality and future trends of researching. Proceedings of VI International Scientific and Theoretical Conference. June 6, 2025. Montreal, Canada. Pp. 147-155.
 13. Mazurets O., Zalutka O., Tyschenko O., Bohdanova A. An Approach to Using MobileNet CNN-model for Gesture Recognition. Proceedings of XXIII International Scientific and Practical Conference «Problems of Science and Technology: the Search for Innovative Solutions». May 15-17, 2024. Munich, Germany. 2024. Pp. 59-64.
 14. Bohdanova A., Mazurets O., Sobko O. Gesture recognition using a neural network in real time. Black Sea Science 2023: Proceedings of the International Competition of Student Scientific Works. Odesa National University of Technology. Odesa, ONUT, 2023. Pp. 556-566.
 15. Mushtyn O., Sobko O., Molchanova M., Mazurets O. Convolutional Neural Network Architecture for Image-Based Architectural Style Recognition. Evolving Science: Theories, Discoveries and Practical Outcomes. Proceedings of 4th International Scientific and Practical Conference. June 9-11, 2025. Zurich, Switzerland. Pp. 130-143.
 16. Malaydakh V., Molchanova M., Shevchuk P., Mazurets O. Deep learning neural network architecture for determining sunflower growth stage from visual data. Modern Scientific Research: Theoretical and Practical Aspects. Proceedings II International Scientific and Practical Conference. May 26-28, 2025. Riga, Latvia. Pp. 143-148.
 17. Ostapchenko N., Tyschenko O., Denysenko B., Mazurets O. Semantic search of relevant images using vector databases. Modern Scientific Research: Theoretical and Practical Aspects. Proceedings II International Scientific and Practical Conference. May 26-28, 2025. Riga, Latvia. Pp. 161-165.
 18. Mazurets O., Molchanova M., Klimenko V., Klopotovskiy D. Datalogic Model for Image Recognition by Convolutional Neural Network Using Cloud Services. Proceedings of XXII International Scientific and Practical Conference «Modern Scientific Research: Theoretical and Practical Aspects». May 8-10, 2024. Oslo, Norway. 2024. Pp. 64-68.

УДК 004.8

Мазурець О.В., Віт Р.В.

Хмельницький національний університет

МОДЕЛЬ ВИЯВЛЕННЯ ЦИФРОВОЇ ВТОМИ У ТЕКСТОВОМУ КОНТЕНТІ ЗАСОБАМИ ШТУЧНОГО ІНТЕЛЕКТУ

У роботі розглянуто проблему цифрової втоми, що виникає внаслідок тривалого перебування користувачів у цифрових середовищах, інформаційного перевантаження та емоційного виснаження. Метою є розроблення нейромережевої моделі виявлення цифрової втоми у текстовому контенті користувачів, здатної автоматично оцінювати рівень втоми для окремих повідомлень і формувати інтегральні показники для користувача за певний період. Запропоновано конвеєр, у якому контекстно-орієнтована трансформерна модель типу BERT формує векторні подання текстів, на основі яких навчається бінарний класифікатор «втома / відсутність втоми». Додатково використано тематичне моделювання та виділення цільових об'єктів предметної області, що дає змогу деталізувати цифрову втому за темами й ключовими поняттями та будувати інтерпретований профіль користувача.

The paper addresses the problem of digital fatigue that emerges from prolonged exposure to online environments, information overload and emotional exhaustion. The aim is to develop a neural network-based model for detecting digital fatigue in user text content, capable of automatically assessing fatigue levels for individual messages and deriving integral indicators for a user over a given time period. The proposed pipeline employs a context-aware transformer model of the BERT family to obtain vector representations of texts, on top of which a binary “fatigue / no fatigue” classifier is trained. Additionally, topic modelling and extraction of domain-specific target objects are used to break down digital fatigue by themes and key concepts, forming an interpretable user profile.

Інтенсивне зростання часу, який користувачі проводять у цифрових середовищах, поєднання дистанційної роботи, онлайн-навчання, новинних стрічок і постійної присутності в соціальних мережах призводять до накопичення явищ цифрової втоми [1, 2]. Вона проявляється у перевантаженні інформацією, зниженні концентрації, емоційному виснаженні та формальному, «механічному» стилі взаємодії з цифровим контентом [3]. Традиційні підходи до діагностики ґрунтуються на анкетуванні та самооцінці, потребують активної участі користувача й не масштабуються до великих потоків текстових даних [4]. В умовах зростання інформаційного тиску та потреби в ранньому виявленні негативних тенденцій стає актуальним перехід до автоматизованого аналізу текстового контенту із застосуванням сучасних моделей штучного інтелекту [5].

Мета роботи полягає в розробленні нейромережевої моделі виявлення цифрової втоми у текстовому контенті користувачів, яка забезпечує автоматичну оцінку рівня цифрової втоми для окремих текстів і інтегральних показників для

користувача за визначений період, а також дозволяє деталізувати структуру цієї втоми за тематичними сегментами та ключовими об'єктами предметної області.

Запропонована модель будується як конвеєр, що поєднує глибинний нейромережевий подання тексту [6], тематичне моделювання [7] й аналіз цільових об'єктів [8, 9]. Вхідними даними є тексти повідомлень користувача x (пости, коментарі, чат-репліки), виходом – оцінка рівня цифрової втоми $d(x)$ у діапазоні від 0 до 1 та її розклад за основними темами. Обчислювальне ядро становить контекстно-орієнтована трансформерна модель типу BERT [10], яка перетворює кожен текст x на векторну репрезентацію $h(x)$, чутливу до семантики, емоційного забарвлення та когнітивної складності мовлення. Вектор $h(x)$ інтерпретується як компактний числовий опис стану користувача, відображаючи лексичні, синтаксичні й стилістичні особливості тексту.

На основі вектора $h(x)$ будується бінарний детектор цифрової втоми. Для кожного тексту x модель повертає ймовірнісну оцінку $d(x) = P(\text{«цифрова втома»} | x)$ у межах $[0;1]$. Якщо $d(x) \geq \tau$, де τ – обраний поріг чутливості, текст інтерпретується як такий, що містить ознаки цифрової втоми; якщо $d(x) < \tau$, ознаки втоми вважаються відсутніми або недостатньо вираженими. Навчання моделі здійснюється на розміченому корпусі текстів з експертними мітками «втома / немає втоми» із використанням логістичної (крос-ентропійної) функції втрат, що мінімізує розбіжність між $d(x)$ та еталонною міткою.

Для семантичної деталізації стану цифрової втоми текст x додатково подається до модуля тематичного моделювання, який розкладає його на суміш тем $T = \{t_1, \dots, t_m\}$ з вагами $w_j(x)$ у діапазоні $[0;1]$, де сума всіх $w_j(x)$ дорівнює 1. Паралельно формується множина цільових об'єктів $O(x)$ – характерних слів, стійких словосполучень та іменованих сутностей, виділених за поєднанням TF-IDF, виявлення іменованих сутностей та статистичного аналізу. Таким чином, кожен текст описується трійкою $(h(x), T, O(x))$, що дає змогу пов'язати факт цифрової втоми не лише з загальним стилем, а й з конкретними темами та поняттями, у межах яких виникає перевантаження.

Індекс цифрової втоми деталізується за темами у вигляді набору $d_j(x) = d(x) w_j(x)$, $j = 1 \dots m$, де $d_j(x)$ показує, яку частку загальної втоми пов'язано з кожною темою t_j . Це дозволяє побудувати тематичний профіль цифрової втоми для одного тексту й візуалізувати «зони напруження» у вигляді карти, на якій для окремих речень або фрагментів відображаються локальні значення $d_j(x)$ та пов'язані з ними цільові об'єкти з $O(x)$. У такий спосіб модель забезпечує не лише числову оцінку $d(x)$, а й інтерпретацію того, «де» і «внаслідок чого» формується стан перевантаження.

Для оцінювання стану конкретного користувача u у динаміці розглядається множина його повідомлень $M(u, T)$ за період T . Інтегральний рівень цифрової втоми визначається як $D(u, T) = \text{середнє значення } d(x) \text{ для всіх } x \in M(u, T)$. Аналогічно, для кожної теми t_j обчислюється тематичний індекс $D_j(u, T) = \text{середнє значення } d_j(x) \text{ за період } T$. Сукупність показників $\Psi(u, T) = \{D(u, T), D_1(u, T), \dots, D_m(u, T)\}$ описує як загальну інтенсивність цифрової втоми, так і її розподіл за темами, формуючи придатний до інтерпретації профіль користувача.

З математичної точки зору, повний конвеєр можна описати як відображення від множини текстів до множини показників стану: потік повідомлень $M(u, T)$ спершу перетворюється нейромережею на послідовність векторів $h(x)$, далі через модуль класифікації – на значення $d(x)$, потім через тематичний модуль і аналіз цільових об'єктів – на $d_j(x)$ і набори $O(x)$, після чого всі ці величини агрегуються у вектор $\Psi(u, T)$. Така модель поєднає гнучкість сучасних трансформерних архітектур із прозорими цифровими індикаторами, придатними для інтеграції в системи моніторингу ментального стану, адаптивні інтерфейси та сервіси підтримки користувачів, не замінюючи професійної оцінки фахівців, але підсилюючи можливості раннього виявлення цифрової втоми.

Перелік посилань

1. Watkins J. Alleviating digital fatigue through embodied artistic practice and green space. *International Journal of Performance Arts and Digital Media*. 2024. P. 1–16.
1. Fatigue-Related Changes of Daily Function: Most Promising Measures for the Digital Age / W. Maetzler et al. *Digital Biomarkers*. 2024. P. 30–39.
2. Byrne M. Special Topic on Reducing Technology Related Stress and Burnout: Digital Compassion Fatigue as an Emerging Phenomenon for Registered Nurses Experiencing Technostress. *Applied Clinical Informatics*. 2025. URL: <https://doi.org/10.1055/a-2564-8809>
3. Expressions of pandemic fatigue on digital platforms: a thematic analysis of sentiment and narratives for infodemic insights / B. K. White et al. *BMC Public Health*. 2024. Vol. 24, no. 1. URL: <https://doi.org/10.1186/s12889-024-17718-4>
4. Віт Р.В., Мазурець О.В. Підхід до тематичної класифікації текстової інформації засобами обробки природної мови. *Науковий журнал «Наукові праці Донецького національного технічного університету», серія «Проблеми моделювання та автоматизації проектування»*. 2025. №1 (21). С. 94-99.
5. Мазурець О.В., Віт Р.В. Дослідження ефективності методу виявлення цільових об'єктів предметної області. *Інформаційні технології і автоматизація. Матеріали XVII міжнародної науково-практичної конференції*. 31 жовтня – 1 листопада 2024 р. Одеса, ОНТУ. 2024. С.650-653.
6. Віт Р.В., Мазурець О.В. Тематична класифікація текстової інформації засобами обробки природної мови. *Збірник наукових праць XXIII Міжнародної наукової конференції «Нейромережні технології та їх застосування НМТІЗ-2024»*. 11-12 грудня 2024. Краматорськ-Тернопіль, ДДМА. 2024. с. 63-66.
7. Мазурець О.В., Віт Р.В. Метод виявлення цільових об'єктів предметної області у текстовому контенті. *Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки*. Хмельницький, 2024. №6, Т.1 (343). С. 152-157.
8. Віт Р.В., Мазурець О.В. Метод формування множин цільових об'єктів предметних областей у цифрових текстах засобами машинного навчання. *Науковий журнал «Наука і техніка сьогодні»*. Київ, 2024. №13 (41). С. 926-937.
9. Віт Р.В., Мазурець О.В. Метод виявлення психологічного цифрового перевантаження за аналізом текстових даних нейромережевими моделями глибокого навчання. *Науковий журнал «Вісник Херсонського національного технічного університету»*. 2025. №2 (93). Т. 2. С. 107-114.

УДК 004.8

Малярчук Н.В.¹, Молчанова М.О.²

¹ Комунальний заклад загальної середньої освіти

«Лицей №17 Хмельницької міської ради»

² Хмельницький національний університет

ПІДХІД ДО НЕЙРОМЕРЕЖЕВОГО ВИЯВЛЕННЯ ОЗНАК НАСИЛЬСТВА ГЕНДЕРНОГО СПРЯМУВАННЯ ЗА ПОВІДОМЛЕННЯМИ СОЦІАЛЬНО- ОРІЄНТОВАНИХ СЕРВІСІВ

Робота присвячена нейромережевому виявленню ознак насильства гендерного спрямування за текстами повідомлень соціально-орієнтованих сервісів. Запропоновано підхід, у якому трансформерні моделі глибокого навчання аналізують лінгвістичні та контекстуальні патерни, що відображають вербальну агресію, приниження, погрози та контроль, пов'язані з гендерною нерівністю, з урахуванням багатозначності висловлювань і впливу контексту діалогу. Забезпечується можливість подальшої інтеграції модуля в системи моніторингу та підтримки постраждалих, що сприяє більш ранньому виявленню ризикованих ситуацій і підвищенню ефективності цифрових сервісів соціальної допомоги.

The paper focuses on a neural network-based approach to detecting signs of gender-based violence in messages from social-oriented online services. The proposed method employs transformer-based deep learning models to capture linguistic and contextual patterns that reflect verbal aggression, humiliation, threats, and controlling behaviour linked to gender inequality, while accounting for ambiguity and dialogue context. The resulting module can be integrated into monitoring and support systems for victims, enabling earlier detection of high-risk situations and improving the effectiveness of digital social assistance services.

Текстові звернення до соціально-орієнтованих сервісів, чат-ботів і онлайн-консультацій дедалі частіше містять опис ситуацій, пов'язаних з насильством гендерного спрямування, однак подаються у вигляді коротких, фрагментарних повідомлень [1]. У таких повідомленнях постраждалі нерідко уникають прямої кваліфікації пережитого як насильства, натомість описують окремі епізоди, емоційні стани, висловлювання партнера чи близького оточення [2]. Методи автоматизованого аналізу тексту, що спираються на ключові слова або прості статистичні моделі, виявляються недостатньо чутливими до завуальованих, контекстно насичених форм вербального насильства, приниження, контролю й погроз [3]. Це зумовлює потребу у нейромережевих підходах, здатних виявляти ознаки гендерно обумовленого насильства на рівні одного окремого повідомлення, без залучення повної історії діалогу.

Поширення онлайн-комунікацій та соціально-орієнтованих сервісів значно збільшило обсяг текстового контенту, у якому можуть проявлятися ознаки

насильства гендерного спрямування. Виявлення таких проявів є важливим для створення безпечного цифрового середовища, захисту прав користувачів та запобігання психологічній шкоді [4]. Традиційні підходи до модерації контенту, що покладаються на людську експертизу, часто є неефективними через швидкість поширення повідомлень, що робить актуальним застосування автоматизованих методів аналізу тексту [5].

Сучасні технології обробки природної мови дозволяють ефективно розпізнавати лексичні [6], синтаксичні [7] та семантичні [8] маркери насильницьких або дискримінаційних висловлювань щодо певної гендерної групи. Використання нейромережових моделей, зокрема трансформерних архітектур [9], забезпечує контекстне розуміння повідомлень [10], виявлення прихованих форм образ, погроз чи психологічного тиску [11], які можуть бути замасковані або виражені непрямыми конструкціями. Такі моделі дозволяють аналізувати великі обсяги даних у реальному часі та забезпечують масштабованість при роботі з соціальними платформами [12].

Метою роботи є розроблення нейромережевого підходу до автоматизованого виявлення ознак насильства гендерного спрямування за одним текстовим повідомленням користувача соціально-орієнтованих цифрових сервісів. Об'єктом дослідження є процес обробки індивідуальних текстових звернень у системах онлайн-підтримки, консультацій та сервісах соціальної допомоги. Предметом дослідження виступають моделі та методи нейромережевої класифікації тексту, орієнтовані на розпізнавання лінгвістичних маркерів гендерно обумовленого насильства у форматі одиначного повідомлення.

Запропонований підхід ґрунтується на донавчанні попередньо натренованої трансформерної мовної моделі на спеціалізованому корпусі текстів, у якому повідомлення позначені за наявністю або відсутністю ознак насильства гендерного спрямування, а за потреби – за підтипами проявів (вербальні образи, приниження, погрози, контроль доступу до ресурсів тощо). Текстове повідомлення проходить етапи нормалізації та токенизації, після чого перетворюється на контекстно-залежне векторне представлення, що подається на вхід класифікаційному шару нейромережі. Модель навчається відносити кожне окреме повідомлення до класу «містить ознаки гендерно обумовленого насильства» чи «не містить», спираючись на сукупність лексичних, синтаксичних і семантичних патернів, притаманних описам токсичних і небезпечних взаємодій.

Для підвищення практичної придатності розроблюваного рішення передбачається використання інтерпретованих виходів моделі на рівні важливості окремих слів та словосполучень, що формують підґрунтя для експертної верифікації спрацьовувань. Це дозволяє фахівцям соціальної та психологічної допомоги оцінювати не лише факт спрацювання класифікатора, а й ті текстові фрагменти, які стали вирішальними для віднесення повідомлення до категорії ризику. Очікується, що інтеграція такого нейромережевого модуля у цифрові сервіси соціальної підтримки сприятиме ранньому виявленню потенційно небезпечних ситуацій,

оперативному скеруванню постраждалих до відповідних служб та підвищенню ефективності моніторингу проявів насильства гендерного спрямування у цифровому середовищі.

Перелік посилань

1. García-Rojas, A. D., Gómez, A. H., Montero-Fernández, D., & Rodríguez-Vargas, S. (2024). Perception of University Students Regarding Gender-Based Violence: Identification, Analysis and Detection. *Sexes*, 5(4), 758-768.
2. Wagner, A., & Condello, A. (Eds.). (2025). (In) Visible Signs of Gender-Based Violence (Vol. 1). Springer Nature.
3. Bondestam, F. (2024). Addressing Gender-Based violence through the ERA policy framework: a systemic solution to dilemmas and contestations for institutions. *International Journal of Higher Education*, 13(2), 74.
4. Молчанова М.О., Мазурець О.В., Собко О.В., Віт Р.В., Назаров В.В. Алгоритм виявлення аб'юзивного вмісту в україномовному аудіоконтенті для імплементації в об'єктно-орієнтовану інформаційну систему. *Науковий журнал «Вісник Хмельницького національного університету»* серія: Технічні науки. Хмельницький, 2024. №1 (331). С. 101-106.
5. Денисенко Б.О., Молчанова М.О., Мазурець О.В. Інтелектуальна система виявлення дезінформації з застосуванням штучних нейронних мереж. *Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024»*. 15-16 листопада 2024. Хмельницький, 2024. с. 167-174.
6. Sobko O., Mazurets O., Didur V., Chervonchuk I. Recurrent Neural Network Model Architecture for Detecting a Tendency to Atypical Behavior Of Individuals by Text Posts. Theoretical and Practical Aspects of Modern Research. *Proceedings of XXVI International scientific and practical conference*. June 5-7, 2024. International Scientific Unity. Ottawa, Canada. 2024. Pp. 113-117.
7. Blazhuk V., Mazurets O., Zalutska O. An Approach to Using the mBERT Deep Learning Neural Network Model for Identifying Emotional Components and Communication Intentions. The Impact of Scientific Research on the Development of the Modern World. *Proceedings of the XLIV International scientific and practical conference*. October 23-25, 2024. Dubrovnik, Croatia. 2024. Pp. 79-84.
8. Yurchenko D., Mazurets O., Didur V., Molchanova M. Approach to Using Cloud Services for Visual Analytics of Neural Network Analysis of Texts Emotional Tonality. The Future of Scientific Discoveries: New Trends and Technologies. *Proceedings of the XLVII International scientific and practical conference*. November 13-15, 2024. Marseille, France. 2024. Pp. 108-113.
9. Молчанова М.О., Мазурець О.В., Собко О.В., Кліменко В.І., Андрощук В.І. Метод нейромережевого виявлення кібербулінгу з використанням хмарних сервісів та об'єктно-орієнтованої моделі. *Науковий журнал «Вісник Хмельницького національного університету»* серія: Технічні науки. Хмельницький, 2024. №2 (333). С. 200-206.
10. O. Mazurets, R. Vit, M. Molchanova, I. Tymofiiiev, O. Sobko, Context-enriched approach to students depression monitoring in education using BERT-GPT hybrid model, *CEUR Workshop Proceedings 4096* (2025) 167-176.
11. Molchanova M., Didur V., Sobko O., Mazurets O. Detection of Web Propaganda Patterns by Transformer Neural Networks: Improving Efficiency via Dataset Balancing, *CEUR Workshop Proceedings*, 2025, vol. 3988, pp. 112-126.
12. E. A. Manziuk, O. V. Sobko, I. O. Podhorniuk, M. O. Molchanova, O. V. Mazurets, Multifactorial analysis of mobbing behavioral signs in educational environments posts by NLP means, *Journal of Physics Conference Series* 3105(1) (2025) 012025.

УДК 004.891

Мараховський Р.К., Дарачюс Є.С, Джулії В.М.

Хмельницький національний університет

АЛГОРИТМ ВИЯВЛЕННЯ АТАК В БЕЗДРОТОВИХ МЕРЕЖАХ ПЕРЕДАЧІ ДАНИХ

Широке розповсюдження бездротових локальних мереж та їх застосування в корпоративних інформаційних системах призводить до необхідності приділяти активну увагу вирішенню притаманних їм проблем інформаційної безпеки. При цьому існуючі засоби захисту, в тому числі комерційні бездротові системи виявлення атак, не забезпечують повноцінного захисту від зловмисної активності.

Запропоновані алгоритми виявлення атак в бездротовій мережі на основі застосування класифікованої моделі з використанням технологій інтелектуального аналізу даних. Аналіз алгоритмів дозволяє зробити висновок про їх застосовності в складі системи виявлення атак.

The widespread use of wireless local area networks and their application in corporate information systems leads to the need to pay active attention to solving their inherent information security problems. At the same time, existing means of protection, including commercial wireless attack detection systems, do not provide full protection against malicious activity.

Algorithms for detecting attacks in a wireless network based on the application of a classified model using data mining technologies are proposed. Analysis of the algorithms allows us to conclude about their applicability as part of an attack detection system.

Бездротові мережі передачі даних схильні, в тому числі з причини недосконалості протоколів, до різних типів атак. Рядові користувачі і невеликі організації, як правило, обмежуються використанням антивірусного програмного забезпечення, яке на сучасному етапі розвитку має ряд додаткових модулів захисту. Великі підприємства змушені купувати дорогі системи виявлення та запобігання атакам [1,2].

Для вирішення зазначених проблем забезпечення безпеки інформації в бездротових мережах використовуються як технічні засоби захисту, так і організаційні заходи.

Як було відзначено, в доступній літературі відсутні роботи по застосуванню методів інтелектуального аналізу даних в задачах виявлення атак на локальні бездротові мережі. У зв'язку з цим виникає проблема вибору оптимального вектора ознак, специфічних для подій безпеки в бездротових мережах, які будуть використовуватися в ході класифікації даних подій [3,4]. Задача розробки алгоритмічного та програмного забезпечення системи, що дозволяє автоматизувати

процес виявлення бездротових атак на основі застосування сучасних методів інтелектуального аналізу параметрів мережевого трафіку, є актуальною.

Для організації безпечного функціонування корпоративної бездротової мережі необхідно вибудувати систему багаторівневого захисту. Дана система включає в себе наступні рубежі (заходи): захист периметра бездротової мережі: точок доступу і пристроїв користувачів; забезпечення безпеки сеансів зв'язку: застосування надійних методів аутентифікації, стійких алгоритмів шифрування і т. д.; постійний моніторинг радіоефіру, включаючи фізичний рівень, виявлення і аналіз підозрілої активності.

Умовою, що забезпечує можливість реалізації наведених загроз безпеки оброблюваної в системі інформації, можуть бути недоліки або слабкі місця в компонентах інформаційної системи, мережевих протоколах і програмному забезпеченні. Основою атак в бездротових мережах служить перехоплення мережевого трафіку від/до точки доступу або трафіку між двома підключеними станціями, а також впровадження додаткових (підроблених) даних в сеанс бездротової зв'язку. Атаки можуть бути спрямовані на різні об'єкти мережевої інфраструктури [2,3,4].

Для виявлення бездротових атак, розроблені відповідні алгоритми побудови класифікуємої моделі, що становить ядро бази знань бездротової системи виявлення атак, на основі: методу опорних векторів, методу k -найближчих сусідів, дерев прийняття рішень, а також нейронних мереж.

На рисунку 1 наведена узагальнена блок-схема алгоритму виявлення атак в локальній бездротовій мережі.

На першому етапі формуються масиви для запису прослуханих в ефірі кадрів F і виділених з них параметрів P , а також масив P_{em} , в який зберігаються еталонні значення параметрів, виміряні в режимі навчання системи виявлення атак. Також формуються масив T , в який набирається статистика мережевої активності на заданому інтервалі часу Δt , масив даних про віщаючих бездротових точках доступу M і заповнюється перелік інформації про довірених корпоративних точках доступу M_{em} : MAC-адрес, номер займаного радіоканалу, дозволені до використання протоколи шифрування і аутентифікації і ін.

Далі проводиться збір даних з сенсорів, їх первинний аналіз з метою виділення трафіку в окремі кадри формату 802.11 і збереження їх в масив F . Потім здійснюється формування векторів ознак подій і запис їх в масив P , нормалізація значень ознак і подача P на вхід класифікатора модуля виявлення атак. Відповідний блок виробляє класифікацію подій безпеки на базі класифікуємої моделі, що представляє собою набір вирішальних правил, неявно порівнюючи значення ознак з відповідними значеннями в масиві P_{em} . При виявленні відповідності вектора ознак якого-небудь типу шкідливої активності проводиться аналіз рівня вихідного сигналу класифікатора L . У разі досягнення або перевищення порогового рівня сигналу L_{nop} інформація про подію передається в модуль прийняття рішень, який генерує оповіщення на консоль адміністратора, а також на підставі встановлених

налаштувань розроблює заходи захисту або впливу на пристрій злоумисника. В іншому випадку, якщо $L_o \leq L < L_{пор}$, де L_o - мінімально допустимий рівень сигналу, що свідчить про підозрілу мережеву активність, то аналізований вектор ознак події зберігається в базі підозрілої активності A для подальшого аналізу.

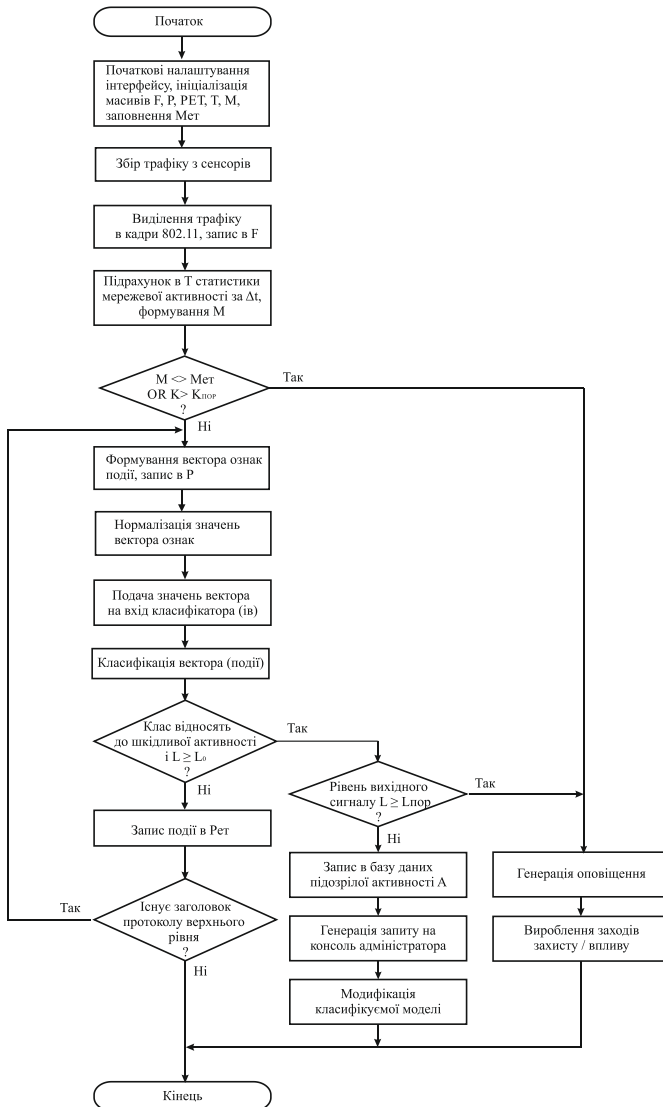


Рисунок 1 – Алгоритм виявлення бездротових мережевих атак

Після досягнення потрібної кількості однотипних подій генерується запит на консоль адміністратора, який визначає наявність або відсутність шкідливої активності в даних подіях. На підставі його рішення проводиться модифікація класифікуємої моделі (до навчання) і додавання записів про події в базу сигнатур S . Крім того, для виявлення окремих типів атак в масив T набирається статистика кількості кадрів певного типу на заданому інтервалі часу Δt з однаковими значеннями параметрів «Тип кадру», «Адреса джерела», «Адреса одержувача» і ін., а також типами протоколів верхнього рівня з числа використовуються стандартні. Додатково в процесі функціонування системи виявлення атак проводиться поповнення масиву даних про віщаючих бездротових точках доступу M . При перевищенні порогового значення $K_{пор}$ кількості кадрів K однакового типу генерується оповіщення на консоль адміністратора про можливу DoS-атаку для подальшого виявлення і фізичного усунення її джерела. При розбіжності даних масиву M з заданими значеннями Met генерується оповіщення про підозрілий пристрій в радіоефірі.

Широке розповсюдження бездротових локальних мереж та їх застосування в корпоративних інформаційних системах призводить до необхідності приділяти активну увагу вирішенню притаманних їм проблем інформаційної безпеки. Проведений аналіз загроз і їх джерел та побудова їх моделей, дозволяють більш точно оцінювати безпеку мережевої активності і рівень довіри до її джерела. Запропоновані алгоритми виявлення атак в бездротовій мережі на основі застосування класифікованої моделі з використанням технологій інтелектуального аналізу даних. Аналіз алгоритмів дозволяє зробити висновок про їх застосовності в складі системи виявлення атак

Перелік посилань

1. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем / В. Джулій та ін. Хмельницький : ХМНУ, 2021. 196 с..
2. Джулій В. М., Ленков О. С., Ряба Л. О. Моделі та алгоритми виявлення атак в бездротових мережах передачі даних. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. 2018. №59. С. 76-87.
3. Кучеренко, А. В., Шевчук, В. М. Методи шифрування даних у бездротових сенсорних мережах. Телекомунікаційні та інформаційні технології. 2020. №2(89). С. 33-38
4. Ткачов В.М., Коваленко А.А., Фесенко Т.Г. Оптимізація мережного алгоритму функціонування комп'ютерних мереж підвищеної живучості на мобільній платформі на етапі їх проектування. Системи управління, навігації та зв'язку. 2021. №.3 (65). С.143-147

УДК 004.8

Масловська В.В., Залуцька О.О.

Хмельницький національний університет

ОСОБЛИВОСТІ РОЗРОБКИ ТА ТЕСТУВАННЯ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ВИЗНАЧЕННЯ ТОНАЛЬНОСТІ В УКРАЇНОМОВНИХ ПОВІДОМЛЕННЯХ

У роботі висвітлено особливості розробки та тестування інтелектуальної системи визначення тональності в україномовних повідомленнях. Показано вибір архітектури на основі поєднання нормалізації тексту, безвчительного виокремлення ключових одиниць та лексиконної валентності з числовою шкалою. Обґрунтовано використання середовища .NET і MS SQL Server для збереження проміжних артефактів і журналів параметрів, що забезпечує відтворюваність і аудит. Описано протоколи випробувань із модульними перевірками, перехресною валідацією та аналізом хибних рішень, а також регресійні серії для оцінювання чутливості порогів. Зафіксовано стабілізацію метрик за рахунок розширеної нейтральної зони та контрольований вплив заперечення і інтенсифікаторів.

The study presents the design and testing specifics of an intelligent system for sentiment detection in Ukrainian short messages. The architecture integrates text normalization, unsupervised key unit extraction, and a lexicon based valence model with a numeric scale. The system is implemented in .NET with MS SQL Server to persist intermediate artifacts and parameter logs, which supports reproducibility and audit. The testing protocol covers module level checks, cross validation, analysis of erroneous outcomes, and regression series to assess threshold sensitivity. The results indicate steadier metrics due to an expanded neutrality zone and a controlled treatment of negation and intensifiers.

Останнім часом автоматизоване визначення тональності україномовних коротких повідомлень виходить за межі лабораторних прототипів і переходить до виробничих сценаріїв, де на перший план виходять прозорість прийняття рішень, відтворюваність обчислень і керованість параметрами [1]. Короткий формат повідомлень, висока стилістична мінливість, перемишування розмовних конструкцій із книжними, домішки емодзі, навмисні орфографічні варіації та фрагментарний синтаксис ускладнюють застосування моделей, побудованих на глибоких контекстних репрезентаціях без належної доменної адаптації [2, 3]. За таких умов практично доцільним є підхід, що тримає баланс між інженерною дисципліною та інтерпретованістю [4]: попередній контроль якості корпусу, безвчительне виділення ключових одиниць і лексиконна валентність із числовою шкалою, яка дозволяє пояснити внесок кожного слова у підсумкову полярність [5].

Методи обробки природної мови є ключовими технологіями сучасних інтелектуальних систем, що працюють із текстовими даними [6, 7]. Завдяки переходу від традиційних статистичних методів [8] до нейромережових моделей [9, 10], зокрема трансформерних архітектур [11], NLP забезпечує високий рівень точності в задачах класифікації [12], тонального аналізу [13] та семантичної інтерпретації текстів [14]. Це робить такі методи особливо цінними для розроблення систем автоматичного визначення емоційної забарвленості повідомлень, що є критично важливою складовою сучасних інформаційних сервісів, чат-ботів, систем модерації контенту, моніторингу соцмереж та інструментів аналітики громадської думки [15, 16, 17].

У контексті україномовних текстів застосування NLP стикається з низкою специфічних викликів, пов'язаних із недостатнім обсягом якісних розмічених датасетів, варіативністю української морфології та обмеженою кількістю спеціалізованих мовних моделей [18]. Попри це, останні роки характеризуються зростанням числа україномовних корпусів, появою BERT-подібних моделей української мови та активним розвитком інструментів лематизації, токенизації та частиномовного аналізу. Це створює сприятливі умови для побудови високоточних систем визначення тональності [19].

Створення системи розпочиналося з формулювання вимог до вхідних даних. Було прийнято, що об'єктом обробки є короткі україномовні повідомлення, нерідко з мінімальним контекстом і локальними тригерами, де емоційний знак часто задається одним-двома словами або стійким словосполученням. Нормалізація була спроектована як обов'язковий початковий крок, але з чіткою межею її повноважень: уніфікація лапок і тире, стабілізація апострофів, усунення невидимих службових символів, упорядкування пробілів і перетворення емодзі у нейтральні маркери, сумісні з подальшою токенизацією, без спроби повного лематизування, яке могло б привнести невинуватому неоднозначність. Такий дизайн нормалізації не намагається «зробити все одразу», але забезпечує стабільні умови для частотного аналізу й побудови ключових одиниць. Схему підсистем наведено на рисунку 1.

Наступним структуро-утворювальним етапом був контроль якості корпусу до початку тонального аналізу. Показник «нудоти» трактувався як індикатор неприродної повторюваності, що в коротких текстах здатна штучно зрушувати полярність до крайніх значень. Паралельно перевірявся профіль розподілу частот: очікувана квазілінійність у логарифмічних координатах вважалася сигналом природності, тоді як виразні «полиці» або розриви свідчили про спотворення даних. На підставі цих перевірок приймалися процедурні рішення про допуск або очищення текстів. Принциповим було документувати кожний поріг і кожну причину відсікання у спеціальних таблицях контролю якості, щоби будь-який прогін згодом можна було відтворити з ідентичними вхідними умовами.

Після допуску корпусу активувався беззвичайний модуль виділення ключових одиниць. Його роль полягала у локалізації смислових центрів короткого повідомлення без звернення до тональних індикаторів. Поєднувалися дві

взаємодоповнювальні процедури: TF-IDF як міра корпусної специфічності слів і стійких словосполучень та TextRank як графова рангово-переходова модель, що чутлива до локальних зв'язків у вікні співзустрічей. Обидва сигнали нормувалися в єдине числове поле, після чого виконувалося злиття з пріоритетом стабільності на малих вибірках. У надкоротких повідомленнях більшу довіру надавали ранговому сигналу, чутливому до структурної ролі лексем у висловлюванні, тоді як зі зростанням корпусу ваги TF-IDF і TextRank вирівнювалися. Важливо, що цей модуль не виконував класифікацію сам по собі; його завданням було сформувати вагову опору для наступного контуру, який приймає рішення про полярність.

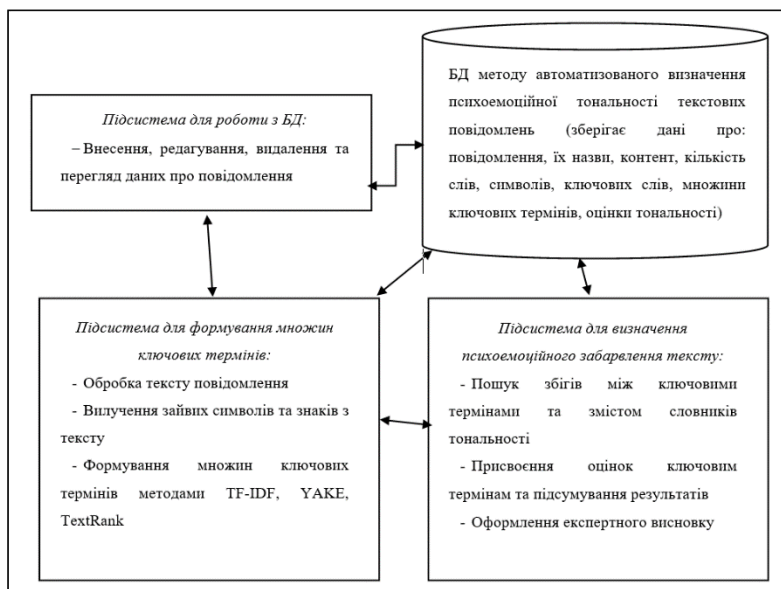


Рисунок 1 – Схема підсистем інтелектуальної системи

Ядро системи становить лексиконна валентність, де кожній лексемі надано числову оцінку у шкалі від одиниці до дев'яти. Числова природа лексикону дає можливість будувати пояснювані рішення, у яких видно, як саме окремі лексеми впливають на сумарну полярність. Агрегування реалізовувалося як зважене середнє, де ваги походили з безвчительних моделей ключових одиниць, а власне числові значення — із лексикону. Окрему увагу приділено локальній логіці заперечення: у вузькому вікні навколо дієслівної групи або прикметникового предикатива відбувалося інвертування або зменшення ефекту вихідної валентності, що дозволяло уникати помилкових позитивів, спричинених механічною сумою позитивних лексем. Інтенсиватори та димінутиви трактувалися як модифікатори відхилення від нейтральної зони з верхньою межею впливу, щоб не допустити

домінування стилістичного маркера над змістовою частиною висловлювання. Кінцеве рішення приймалося за трипороговою схемою з фіксованою «мертвою зоною» навколо нуля, призначеною для відсікань випадкових рішень у прикордонних ситуаціях. Параметри порогів і версії лексикону фіксувалися в конфігураційних таблицях бази даних разом із часовою міткою, що створювало прозору історію змін і спрощувало аудит.

Архітектурно система реалізована у середовищі .NET із використанням MS SQL Server як центральної СКБД. Розширована побудова включала сервіс прийому й нормалізації, аналітичний шар беззвичайних обчислень і лексиконного агрегування, підсистему прийняття рішень та шар збереження проміжних артефактів. Структура бази даних містила таблиці документів, токенів, словосполучень, частотних профілів, ваг TF-IDF і TextRank, лексиконних значень, проміжних агрегатів і фінальних вердиктів, а також журнали параметрів і версій. Такий устрій уможлиблював не тільки перевіряти будь-який крок постфактум, а й вибірково переобчислювати окремі шари без повного перезапуску конвеєра, що важливо для масштабування і для серійних експериментів у процесі тестування.

Методика тестування була побудована на двох рівнях. Модульний рівень перевіряв коректність і стабільність кожного етапу окремо. Для нормалізації оцінювалася інваріантність токенизації до графічних варіацій і невидимих символів; вимірювалося, наскільки різні джерела з різною пунктуаційною дисципліною дають однаковий результат. Для скринінгу якості оцінювалася чутливість показника «нудоти» до довжини і жанру, перевірялася стійкість ціпфівського профілю в тематично рознесених підвибірках. Беззвичайний модуль ключових одиниць тестувався на узгодженість із людською інтуїцією: для вибраних підмножин експерти попередньо позначали смислові ядра, після чого порівнювали ранжування системи та ручні референси. В лексиконному контурі проводилися контрольні серії на шаблонах заперечення та інтенсиваторах, щоб переконатися у відсутності систематичних перекосів до крайнього позитиву чи негативу в умовах короткого контексту.

Інтегральний рівень тестування оцінював поведінку системи як цілого. Проводилася перехресна перевірка з поділом на незалежні підвибірки; для кожної з трьох категорій: позитивної, нейтральної та негативної – обчислювалися точність, повнота і F_1 -міра, а також макро- і зважені агрегати, чутливі до дисбалансу класів, який у коротких повідомленнях виникає майже завжди. Кожна серія супроводжувалася якісним розбором помилок. У хибно позитивних рішеннях домінували іронічні патерни, інверсії сенсу за рахунок контексту поза повідомленням і поєднання позитивних емоцій з негативним вербальним змістом; у хибно негативних зауважовані оцінки з м'якими інтенсифікаторами і складними заперечними ланцюжками, що виходять за межі локального вікна. Каталог помилок зберігався як наростаюча база прикладів із фіксацією тексту, ключових одиниць, вагового внеску кожної лексеми та фінального рішення. На підставі цього каталогу виконувалися точкові корекції: звужувалася або розширювалася «мертва зона»,

уточнювалися пороги для переходу між категоріями, переглядалися правила локального врахування заперечення.

Практично уся інтелектуальна система була покрита тест-кейсами. Один з яких наведено в таблиці 1.

Таблиця 1 – Тест-кейс 1

Тест-кейс ID: АК0004	Пріоритет: 1	Створено: 12.05.2025, Залуцька О.
Назва: Перевірка коректного визначення тональності Вхідні дані: Текстове повідомлення .txt		
Кроки		Очікуваний результат
<i>Передумова:</i> на вкладці «База повідомлень» користувач має обрати рядок текстового повідомлення, подальший аналіз якого відбуватиметься. Повідомлення містить явно негативний характер, що необхідно довести. 1. Запустити додаток та обрати вкладку «База повідомлень» 2. Обрати рядок текстового повідомлення з негативним емоційним забарвленням. 3. Натиснути кнопку «Аналіз» 4. Порівняти фактичний результат з очікуваним		Система має довести, що повідомлення містить негативне забарвлення із вірогідністю, більшою за 80%. За результатами аналізу повідомлення із вірогідністю 97.4% місить негативне забарвлення.
Результат виконання тест-кейсу: пройдено успішно		

Приклад виконання тесту, наведеному в таблиці 1 для визначення психоемоційного забарвлення наведено на рисунку 2.

Під час серійних експериментів особливий акцент робився на регресійних перевірках, де змінювався лише один клас параметрів. Зокрема, варіювалася ширина вікна для заперечення, після чого оцінювалися метрики і якісні помилки. Було показано, що надто широке вікно провокує помилкові інверсії у випадках, де заперечення належить до іншого синтаксичного вузла, тоді як надто вузьке позбавляє систему здатності вчасно інвертувати полярність у розтягнутих конструкціях. Ця емпірична крива відгуку слугувала аргументом для консервативних налаштувань і була зафіксована в журнальних таблицях параметрів як еталон для наступних змін. Приклад успішного виконання юніт-тестів наведено на рисунку 3.

У питаннях продуктивності було важливо відокремити важкі та легкі шари обчислень. Матеріалізовані представлення для частотних запитів і кеші для співзвуччій дозволили зменшити латентність без модифікації логіки прийняття рішень. Збереження проміжних артефактів збільшує обсяг сховища, але дає змогу вибірково переоцінювати тільки ті компоненти, яких торкнулися зміни параметрів. Перевизначення порогів не потребує повторного підрахунку TF-IDF і TextRank; оновлення словникових норм торкається лише підмножини документів, у яких зустрічаються змінені лексеми. За такої організації даних час обробки масштабується лінійно з розміром партії, а прогнозованість затримок дозволяє планувати ресурси без завищених запасів.

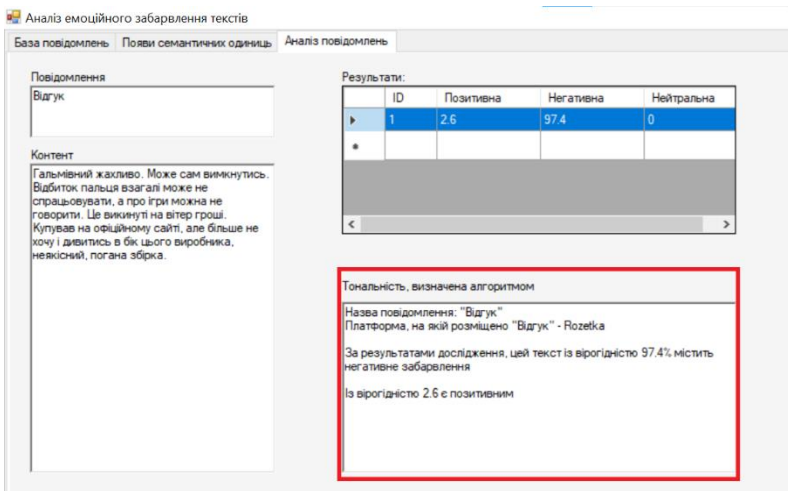


Рисунок 2 – Приклад виконання модульного тесту

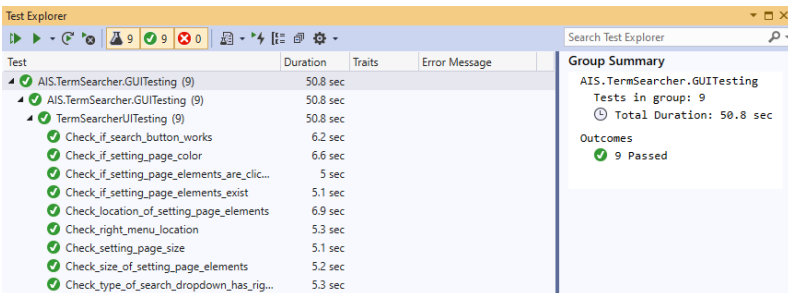


Рисунок 3 – Виконання юніт-тестів

Окремою темою стала інтерпретація нейтральної категорії. В умовах коротких повідомлень нейтральність не є тривіальною серединою між позитивом і негативом. Вона означає недостатність доказів на користь певного полюсу за наявних вагових сигналів. У зв'язку з цим нейтральна зона була розширена і підкріплена регламентом, що забороняє приймати рішучі вердикти на підставі одиничних емоційних маркерів без підтримки ключових словосполучень. Така політика зменшує кількість випадкових коливань і покращує зважені метрики на різномірних потоках.

У межах практичних сценаріїв особливої уваги вимагали повідомлення з високою насиченістю емоції. Щоби уникнути ситуацій, коли піктографічні маркери повністю визначають результат, було запроваджено вагову скидку для емоції та обмеження максимальної кількості ключових одиниць, що бере участь в агрегуванні у надкоротких повідомленнях. Це рішення продемонструвало помітне зниження частки хибно позитивних вердиктів у саркастичних конструкціях із позитивними піктограмами.

Впровадження системи в середовищах із різними тематичними доменами не вимагало змін у конвеєрі. Адаптація зводилася до перегляду порогів допуску корпусу, часткового оновлення словникових норм для специфічних лексем та регресійних перевірок на «заморожених» наборах складних випадків. Версіонування параметрів і словників, пов'язане з часовими мітками, дозволяло повернутися до попереднього стану в разі погіршення метрик. Зауважимо, що запроваджена культура тестування передбачала підтримку стабільного пулу контрольних прикладів з іронією, полісемією і складним запереченням, через які максимально швидко виявлялися деградації після найменших змін у правилах або порогах.

Обмеження підходу не приховувалися й служили орієнтирами для коректної інтерпретації результатів. Лексиконна природа моделі означає залежність від покриття словника та інерційності щодо нових мовних мод і сленгових утворень. Перевірка ціпфівського профілю на дуже малих підвибірках має скринінговий характер і може давати хибні сигнали на жанрових матеріалах із навмисною ритмікою. Іронія і сарказм лишаються найскладнішими випадками, у яких відсутність розгорнутого контексту знижує чутливість; частково це компенсується вагами ключових одиниць і консервативними порогоми, але не усувається повністю. Попри це, система забезпечує саме ті властивості, які запитують виробничі користувачі: прозорість рішень на рівні окремих лексем і фраз, відтворюваність кожного експерименту завдяки збереженню проміжних артефактів, стабільність поведінки на різномірних потоках, де тональність повинна визначатися не лише «правильно», а й однаково при повторних запусках.

Підсумовуючи, запропонований підхід консолідує інженерні та методичні засади у впорядкований конвеєр, який перетворює нестабільні короткі україномовні тексти на об'єкт керованого аналізу. Почерговість кроків: від нормалізації та допуску корпусу до виділення ключових одиниць і лексиконної агрегації забезпечує

інспектованість кожної ланки, а двоярусне тестування з каталогом помилок дозволяє не лише вимірювати якість, а й покроково її покращувати, не руйнуючи архітектурної цілісності.

Перелік посилань

1. Zavalniuk I., Bohatko V., Pavlyuk O., Kukhar N. A Comparative Study of Expressive Language Usage in Contemporary Ukrainian and English Media. *Multidisciplinary Science Journal*. 2024. Vol. 6.
2. Haladzhun Z., Kunanets N., Dvorianyn P., Makarchuk O., Veretennikova N. Compound Words as a Means of Expressing Content Tonality in the Ukrainian Text Media. *Proceedings of the 2021 IEEE 16th International Conference on Computer Sciences and Information Technologies (CSIT)*. September 2021. Vol. 2. Pp. 109–114.
3. Levchuk P., Shevchuk-Kliuzheva O. Language Choice and Changes in Speech Behavior: A Study of Bilingual Ukrainians During Wartime. *Przegląd Rusycystyczny*. 2024. No. 4(188). Pp. 154–178.
4. Olenych I., Prytula M., Sinkevych O., Khamar O. System of Automatic Determination of Ukrainian Text Tone. *Proceedings of the 2021 IEEE 12th International Conference on Electronics and Information Technologies (ELIT)*. May 2021. Pp. 80–83.
5. Navalna M., Kostusiak N. M., Stanislavchuk N., Kapeliukh D., Kushch N., Demeshko I. Call Signs of Ukrainian Military in the Language of Mass Media: Functional-Semantic Aspect. *International Journal of Basic and Applied Sciences*. 2025. Vol. 14, No. 3.
6. Shevchuk P., Molchanova M., Mazurets O. Software for Text Messages Reliability Analysis Based on the Machine Learning Models Ensemble. *Proceedings of IV International Scientific and Practical Conference «Innovative research and perspectives of the development of science and technology»*. January 29-31, 2024. Stockholm, Sweden. 2024. Pp. 347-354.
7. Залуцька О.О., Молчанова М.О., Мазурець О.В., Мельник О.І., Скрипник Т.К. Метод інтелектуального аналізу емоційної тональності текстової інформації для визначення поведінкових намірів нейромережевими засобами. *Науковий журнал «Вісник Хмельницького національного університету»* серія: Технічні науки. Хмельницький, 2023. №5 (325). Т.1. С. 67-73.
8. Молчанова М.О., Мазурець О.В., Собко О.В., Віт Р.В., Назаров В.В. Алгоритм виявлення аб'юзивного вмісту в україномовному аудіоконтенті для імплементації в об'єктно-орієнтовану інформаційну систему. *Науковий журнал «Вісник Хмельницького національного університету»* серія: Технічні науки. Хмельницький, 2024. №1 (331). С. 101-106.
9. Мазурець О.В., Козенко О.В., Собко О.В. Метод автоматизованого підбору відповідей на користувацькі запитання за семантичною подібністю. *Матеріали XII Всеукраїнської науково-практичної конференції «Глушковські читання»*. Київ – 2023. с. 106-109.
10. Молчанова М.О., Мазурець О.В., Собко О.В., Кліменко В.І., Андрощук В.І. Метод нейромережевого виявлення кібербулінгу з використанням хмарних сервісів та об'єктно-орієнтованої моделі. *Науковий журнал «Вісник Хмельницького національного університету»* серія: Технічні науки. Хмельницький, 2024. №2 (333). С. 200-206.
11. Mazurets O., Sobko O., Vit R., Pasternak V. Practical Approach for Detection by Deep Learning of Target Objects of Subject Area Based on Semantic Connectivity Indicators in Audio Database. *Proceedings of XXIV International Scientific and Practical Conference «Modern Scientific Challenges are the Driving Force of the Development of Scientific Research»*. May 22-24, 2024. Bruges, Belgium. *International Scientific Unity*. 2024. Pp. 91-96.

12. Mazurets O., Molchanova M., Klimenko V., Prosvitliuk M Practice Implementation of Neural Network Model BART-Large-CNN for Text Annotation. Prospects of Scientific Research in the Conditions of the Modern World. Proceedings of XXVII International scientific and practical conference. June 12-14, 2024. Rotterdam, Netherlands. 2024. Pp. 97-102.
13. Mazurets O.V., Sobko O.V., Molchanova M.O., Zalutska O.O., Yurchak A.V. Practical Implementation of Neural Network Method for Stress Features Detection by Social Internet Networks Posts. Global Science: Prospects and Innovations. Proceedings of the II International Scientific and Theoretical Conference «Scientific Review of the Actual Events, Achievements and Problems». May 31, 2024. Berlin, Federal Republic of Germany: International Center of Scientific Research. 2024. Pp. 160-167.
14. Мазурець О.В., Віт Р.В. Інтелектуальний метод виявлення цільових об'єктів предметної області за показниками семантичної зв'язності для класифікації текстової інформації. Розвитки інформаційно-керуючих систем та технологій.: монографія. Львів-Торунь : Lina-Pres, 2024. – С.223-244.
15. Sobko O., Mazurets O., Didur V., Chervonchuk I. Recurrent Neural Network Model Architecture for Detecting a Tendency to Atypical Behavior Of Individuals by Text Posts. Theoretical and Practical Aspects of Modern Research. Proceedings of XXVI International scientific and practical conference. June 5-7, 2024. International Scientific Unity. Ottawa, Canada. 2024. Pp. 113-117.
16. Мазурець О., Віт Р. Інтелектуальний метод виявлення цільових об'єктів предметної області для класифікації текстової інформації. Матеріали XII Міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології ІУСТ-ОДЕСА-2024». 23-25.09.2024. Одеса. 2024. С.205-208.
17. Blazhuk V., Mazurets O., Zalutska O. An Approach to Using the mBERT Deep Learning Neural Network Model for Identifying Emotional Components and Communication Intentions. The Impact of Scientific Research on the Development of the Modern World. Proceedings of the XLIV International scientific and practical conference. October 23-25, 2024. Dubrovnik, Croatia. 2024. Pp. 79-84.
18. Tymofiiiev I., Mazurets O., Hardysh D., Molchanova M. Neural Network Dual Architecture for Depression Detection Using Cloud Services. Scientific Research in the Era of Digital Technologies: Challenges and Opportunities. Proceedings of the XLVI International scientific and practical conference. November 6-8, 2024. Barcelona, Spain. 2024. Pp. 84-88.
19. Yurchenko D., Mazurets O., Didur V., Molchanova M. Approach to Using Cloud Services for Visual Analytics of Neural Network Analysis of Texts Emotional Tonality. The Future of Scientific Discoveries: New Trends and Technologies. Proceedings of the XLVII International scientific and practical conference. November 13-15, 2024. Marseille, France. 2024. Pp. 108-113.

УДК 004.4

Мацюк Д.В., Кустовський Р.С.

Хмельницький національний університет

МЕТОД ОЦІНЮВАННЯ ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ДИФЕРЕНЦІАЛЬНОГО ТЕСТУВАННЯ ФУНКЦІОНАЛЬНОЇ ПОВЕДІНКИ

Запропоновано метод для підвищення надійності програмного забезпечення шляхом інтеграції диференціального тестування в CI/CD конвейери. Метод базується на кількісній оцінці поведінкових розбіжностей між версіями ПЗ за допомогою спеціалізованих метрик, таких як індекс поведінкового дрейфу та оцінка функціональної узгодженості. Ключовою інновацією є застосування моделі зважування значущості виявлених розбіжностей, що дозволяє автоматично розрізняти критичні регресії та незначні відхилення, надаючи розробникам об'єктивний стан якості на кожному етапі розробки.

This paper proposes a method to enhance software reliability by integrating differential testing into CI/CD pipelines. The method is based on the quantitative assessment of behavioral discrepancies between software versions using specialized metrics, such as the Behavioral Drift Index and Functional Consistency Score. The key innovation is the application of a significance weighting model for identified discrepancies, which allows for the automatic distinction between critical regressions and minor deviations, providing developers with an objective quality state at every development stage.

Низька якість програмного забезпечення (ПЗ) залишається однією з найважливіших проблем сучасної інженерії, що призводить до значних економічних втрат. Згідно зі звітом Consortium for Information & Software Quality (CISQ), вартість низької якості ПЗ у США у 2022 році сягнула 2,41 трильйона доларів, а накопичений технічний борг - 1,52 трильйона доларів. Традиційні підходи до тестування, що базуються на бінарній логіці «пройшов чи не пройшов», часто не здатні надати повну картину про стабільність системи та вплив змін на її поведінку [1, 2]. Це створює потребу в розробці автоматизованих методів, які б забезпечували безперервну кількісну оцінку якості ПЗ.

Існуючі метрики, такі як підрахунок помилок або відсоток пройдених тестів, є недостатніми, оскільки справжня вартість визначається не кількістю збоїв, а їхнім впливом. Наприклад, один критичний збій у банківській системі має більший економічний вплив, ніж тисячі дрібних помилок інтерфейсу. Це створює «спіраль боргу якості», тобто тиск на швидку доставку збільшує технічний борг, що робить виправлення дорожчими і призводить до нових помилок. Таким чином, виникає гостра потреба в методах, здатних розрізняти незначні варіації та регресії з високим впливом.

Основою для розв'язання цієї проблеми є концепція тестування методом чорної скриньки, де для перевірки коректності не потрібен заздалегідь відомий еталонний результат. Диференціальне тестування є одним із провідних підходів у цій галузі та передбачає порівняння результатів роботи двох або більше версій системи на однакових вхідних даних. Якщо результати відрізняються, це свідчить про наявність помилки. Цей метод успішно застосовується для тестування компіляторів, криптографічних бібліотек та блокчейн-систем.

Найбільш поширеними є метаморфне та диференціальне тестування. Метаморфне тестування перевіряє не конкретний результат, а «метаморфні відношення» – властивості зв'язку між кількома входами чи виходами однієї програми [3]. Диференціальне тестування, навпаки, порівнює результати двох або більше еквівалентних версій системи на однакових вхідних даних [4]. Розбіжність у результатах свідчить про помилку, не вимагаючи знання «правильної» відповіді. У таблиці представлено порівняльну характеристику підходів до тестування без оракула.

Таблиця 1 – Порівняння підходів до тестування без оракула

Вимір	Традиційне тестування	Диференціальне тестування	Метаморфне тестування
Принцип	$f(x_1) \equiv E$	$f(x_1) \equiv f(x_2)$	$Relation(f(x_1), f(x_2)) \equiv T$
Тип оракула	Конкретний (значення)	Відносний (інша версія)	Реляційний (властивість)
Застосування	Загальна верифікація	Регресійне тестування	Тестування складних систем (AI, наукові)

Диференційне тестування є потужним інструментом для регресійного тестування, особливо в CI/CD, де попередня стабільна версія слугує найнадійнішим оракулом для порівняння з новою версією [4]. Хоча диференційне тестування ефективно виявляє розбіжності, існуючі підходи часто зупиняються на цьому, тобто вони не надають механізмів для автоматичної кількісної оцінки значущості цих розбіжностей. Розробник отримує список відмінностей, але не може автоматично відрізнити нешкідливий «шум» від критичної функціональної регресії [9].

Метою даної роботи є розробка методу кількісної оцінки якості ПЗ, який вирішує проблему інтерпретації результатів диференціального аналізу. Це досягається шляхом інтеграції диференціального тестування в конвеєр CI/CD для аналізу поведінкових розбіжностей між версіями стабільною версією та новою версією, впровадження набору спеціалізованих метрик («вектора якості» Q) для кількісної оцінки стабільності, включаючи оцінку функціональної узгодженості та індекс поведінкового дрейфу (BDI) та застосування формальної моделі для

автоматизованого зважування значущості виявлених розбіжностей, що базується на принципах психометричної теорії тестування [8].

Запропонований фреймворк функціонує в межах стандартного конвеєра CI/CD [10] і складається з кількох етапів.

На початкових етапах здійснюється виконання та збір «поведінкового відбитка», тобто у конвеєрі CI обидві версії ПЗ (base і test) виконуються паралельно в ідентичних, ізольованих середовищах на єдиному наборі тестів. Критичним є управління станом, наприклад, через знімки БД або ефемерні контейнери [5]. Замість бінарного результату «пройшов чи не пройшов», система збирає багатовимірний «поведінковий відбиток» для кожного тесту.

Наступний етап включає диференціальне порівняння, тобто диференціатор порівнює відбитки base та test, ігноруючи несуттєвий шум та використовуючи допуски для чисел з плаваючою комою.

Після цього здійснюється кількісна оцінка за допомогою метрик. Результати порівняння агрегуються у «вектор якості», що надає цілісну картину впливу змін. Ключові метрики включають:

Загалом, оцінка функціональної узгодженості - це відсоток тестових випадків, у яких функціональні компоненти відбитків base та test є ідентичними. Показник даної оцінки 100% означає відсутність функціональних регресій, тоді як нижчий показник вказує на ширину впливу зміни.

Індекс поведінкового дрейфу (BDI) є метрикою, що кількісно оцінює зважену величину зміни в числових або структурних вихідних даних для тих тестів, які не є узгодженими [6]. Низький BDI свідчить про незначні зміни, тоді як високий BDI вказує на суттєву зміну поведінки системи.

Метрика стабільності продуктивності (PSM) вимірює середню відсоткову зміну часу виконання та використання пам'яті. Значення PSM, близьке до нуля вказує на стабільність, тоді як позитивне значення вказує на регресію продуктивності.

Заключним етапом є зважування значущості, тобто необроблений список розбіжностей не є дієвим. Ключовою інновацією є модель для автоматичної класифікації та присвоєння числової так званої «оцінки впливу» кожній розбіжності. Ця модель натхненна психометричною теорією тестування [8], де тестове завдання (тестовий випадок) має різну «вагу» або «здатність до дискримінації».

Фактори зважування включають:

- тип розбіжності;
- критичність коду;
- історична стабільність тесту.

Цей підхід перетворює суб'єктивну оцінку серйозності помилки на формальний, керований даними процес. Агрегована оцінка використовується для автоматизації «воріт якості» в CI/CD, що реалізує парадигму «безперервної оцінки якості», де якість стає вимірюваною характеристикою кожного коміту.

Отже, запропонований метод забезпечує перехід від якісного, орієнтованого на помилки тестування до кількісної, орієнтованої на поведінку моделі оцінки якості. Набір метрик (FCS, BDI, PSM) надає багатовимірний «вектор

якості», що дає більш тонке уявлення про стабільність системи, ніж традиційні методи.

Ключовим внеском є формалізована модель зважування розбіжностей, що спирається на принципи психометричної теорії [8], яка дозволяє автоматично сортувати відхилення за значущістю, вирішуючи головну проблему інтерпретації результатів диференціального тестування [9]. Інтеграція в CI/CD конвеєри перетворює оцінку якості на безперервний, автоматизований процес [10].

Ефективність методу залежить від покриття набору тестів і він не може виявити помилки, присутні в обох версіях ПЗ.

Перспективи подальших досліджень включають застосування машинного навчання для заміни евристичного механізму класифікації розбіжностей (наприклад, з використанням LLM) [9], розширення фреймворку на нефункціональні властивості, такі як безпека та стійкість до збоїв, побудова прогностичних моделей якості.

Перелік посилань

1. Cost of Poor Software Quality in the U.S.: A 2022 Report / CISQ. 2022. URL: <https://www.it-cisq.org/the-cost-of-poor-quality-software-in-the-us-a-2022-report/> (дата звернення: 27.10.2025).
2. Software Survival in 2024: Understanding 2023 Project Failure Statistics and the Role of Quality Assurance / Beta Breakers. 2024. URL: <https://www.betabreakers.com/blog/software-survival-in-2024-understanding-2023-project-failure-statistics-and-the-role-of-quality-assurance/> (дата звернення: 27.10.2025).
3. Segura S., Hierons R. M., Chen T. Y. A Survey on Metamorphic Testing. IEEE Transactions on Software Engineering. 2016. Vol. 42(9). P. 805–824. (На основі).
4. Gulzar M. A. et al. Perception and Practices of Differential Testing. Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference (ESEC/FSE). 2019. P. 71–81. URL: <https://people.cs.vt.edu/~gulzar/assets/pdf/p71-gulzar.pdf> (дата звернення: 27.10.2025).
5. Zhu M. et al. Vive la Différence: Practical Diff Testing of Stateful Applications. Proceedings of the 13th USENIX Symposium on Operating Systems Design and Implementation (OSDI '18). 2018. URL: <https://pages.cs.wisc.edu/~rgrandl/papers/p2018-zhu.pdf> (дата звернення: 27.10.2025).
6. Romano D., Pinzger M., Villarroel L. On the uniformity of software evolution patterns. 2007 11th European Conference on Software Maintenance and Reengineering (CSMR). 2007. P. 13–22. DOI: 10.1109/CSMR.2007.13.
7. Measuring LLM Code Generation Stability via Structural Entropy / Z. Liu et al. arXiv. 2025. URL: <https://arxiv.org/pdf/2508.14288> (дата звернення: 27.10.2025).
8. Paek I., Lee G. Testing for Differential Item Functioning Under the D-Scoring Method. Psychometrika. 2022. Vol. 87(1). P. 196–219. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC8725056/> (дата звернення: 27.10.2025).
9. Vajjala A. K. et al. Using Large Language Models to Support the Workflow of Differential Testing. 2024 IEEE/ACM 1st International Workshop on Large Language Models for Software Engineering (LLM4SE). 2024. URL: <https://www.arunkv.com/HTML/assets/img/DiffViewer.pdf> (дата звернення: 27.10.2025).
10. Integrating Test Automation into the CI/CD Pipeline / QMetry. 2023. URL: <https://www.qmetry.com/blog/integrating-test-automation-into-the-ci-cd-pipeline> (дата звернення: 27.10.2025).

УДК 004.056.5

Мельник М.М., Дзіблюк К.С., Навроцька К.В., Чешун В.М.

Хмельницький національний університет

АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ДЛЯ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

В роботі розглядаються особливості розслідування кіберінцидентів у всіх сферах діяльності критичної інфраструктури України. Основний напрямок зосереджений на виявленні, розкритті, розслідуванні та документації подій. Також враховано довід Європи, США та інших країн.

The paper examines the specifics of cyber incident investigation in all areas of critical infrastructure activity in Ukraine. The main focus is on the detection, disclosure, investigation, and documentation of events. Evidence from Europe, the USA, and other countries is also taken into account.

Прогрес розвитку інформаційних технологій у суспільстві характеризується великим обсягом цифрових даних та зростанням кількості загроз та кіберінцидентів в усіх сферах життя та на об'єктах критичної інфраструктури, що спрямованні на порушення цілісності, доступності та конфіденційності важливих державних інформаційних ресурсів. Особливої уваги потребує питання вчасного виявлення, реагування та розслідування кіберінцидентів. Захист інформації – це перший етап забезпечення безпеки, проте, рівень кіберзлочинності зростає кожного дня. Важливо розуміти, що робити коли вже відбувається інцидент. В цій статті розглянуто етапи кіберінцидентів та методи, що можуть забезпечити швидку реакцію на інциденти та завершити атаки на початковому етапі.

Метою дослідження є аналіз сучасних підходів до розслідування кіберінцидентів та розроблення методичних рекомендацій для впровадження ефективного процесу реагування у державних інформаційних системах.

Відповідно до даних CERT-UA з початку 2025 року фіксується близько 15 кіберінцидентів на день та існує понад 150 кластерів кіберзагроз. Основне джерело для більшості загроз на інфраструктуру України є росія [1, 2]. Найбільш поширеними типами хакерської активності є шпигунство, саботаж та фінансово вмотивовані злочини. За період 2022-2025 стали поширені атаки на військову інфраструктуру та військовослужбовців. [8]

Активна цифровізація державного управління, впровадження електронних сервісів та систем обробки даних призводить до збільшення кількості кіберінцидентів, що становлять серйозну загрозу для стабільності функціонування державних інформаційних систем [1, 2]. Сучасні кібератаки характеризуються високим рівнем складності, цілеспрямованістю та використанням методів соціальної інженерії, що ускладнює їх своєчасне виявлення та нейтралізацію [3].

Незважаючи на наявність нормативно-правової бази України у сфері кібербезпеки – зокрема, Законів України «Про основні засади забезпечення кібербезпеки України» [4], «Про інформацію» [5], «Про захист інформації в інформаційно-телекомунікаційних системах» [6] – більшість державних установ не мають чітко визначених процедур розслідування інцидентів інформаційної безпеки. Це ускладнює процеси збору цифрових доказів, аналізу причин інцидентів та формування звітів, що відповідають міжнародним вимогам [7].

Ключовою проблемою є відсутність уніфікованого методу розслідування кіберінцидентів, який би враховував специфіку архітектури державних ІТ-систем, різнорівневість доступу до ресурсів, а також обмеження у технічному забезпеченні. Через це процес реагування часто має фрагментарний характер, а взаємодія між адміністраторами систем, фахівцями з ІБ та аналітиками CERT здійснюється без належної координації [8].

Міжнародний досвід, викладений у стандартах ISO/IEC 27035:2023 [9] та NIST SP 800-61 Rev.2 [10], демонструє ефективність системного підходу до управління кіберінцидентами, який включає етапи виявлення, аналізу, реагування, документування та вдосконалення процесів. Також цінними є рекомендації ENISA [11] і CERT-EU, що деталізують практичні аспекти організації роботи команд реагування на інциденти у державному секторі (таблиця 1).

Отже, актуальною задачею є розроблення адаптованого методу розслідування кіберінцидентів для державних інформаційних систем України, який би поєднував вимоги міжнародних стандартів з можливостями національної інфраструктури кіберзахисту.

Виклад основного матеріалу. Розслідування кіберінцидентів у державних інформаційних системах є одним із ключових напрямів забезпечення кіберстійкості державного сектору. На відміну від приватних організацій, державні структури мають справу з конфіденційними даними, які становлять державну таємницю або містять персональні відомості громадян, що робить їх потенційною цілью для складних цілеспрямованих атак [1, 2].

Згідно зі стандартом ISO/IEC 27035:2023, процес управління інцидентами інформаційної безпеки включає п'ять основних етапів: підготовку, виявлення, оцінювання, реагування та відновлення [3]. У контексті державних інформаційних

систем особливо важливим є перший етап – підготовка, який передбачає створення політики реагування, формування команди CSIRT (Computer Security Incident Response Team), налаштування моніторингу та визначення каналів комунікації між підрозділами [4].

Математична модель оцінювання ризику кіберінциденту використовується узагальнена формула [10]:

$$R = P_i \times I_i$$

де P_i – ймовірність виникнення інциденту; I_i – вплив інциденту (наслідки).

Таблиця 1 – Організація реагування на інциденти в різних країнах

Країна	Відповідальний орган / структура	Основна модель реагування	Стандарти	Ключові інструменти та технології	Особливості та результати впровадження
США	US-CERT (Department of Homeland Security)	“Incident Lifecycle” за NIST	NIST SP 800-61 Rev.2, ISO/IEC 27035	Splunk ES, QRadar, STIX/TAXII, MISP	Централізована система моніторингу інцидентів у державних установах; високий рівень автоматизації реагування.
Велика Британія	National Cyber Security Centre (NCSC)	Модель реагування “Cyber Essentials”	ISO/IEC 27035, ISO/IEC 27001	ArcSight, AlienVault, TheHive, Cortex	Високий рівень стандартизації процесів; обов’язкові політики реагування для державного сектору.
Естонія	CERT-EE (Information System Authority)	Національна інтегрована система кіберзахисту	ISO/IEC 27035, NIST SP 800-61	MISP, ELK Stack, Suricata, Wireshark	Повна інтеграція між державними IT-системами; оперативне реагування на національному рівні.
Німеччина	BSI-CERT (Federal Office for Information Security)	Модель BSI IT-Grundschutz	ISO/IEC 27001, ISO/IEC 27035	SIEM BSI Suite, OpenVAS, Nessus, Cortex	Висока регламентація процедур; глибокий аудит IT-інфраструктури держустанов.
Україна	CERT-UA, ДССЗІ України	Формування національної системи реагування	ISO/IEC 27035, NIST SP 800-61, Закон №2163-VIII	Wazuh, ELK Stack, MISP, IBM QRadar	Активна розбудова національної системи кіберзахисту; створення навчальних лабораторій у ЗВО.

Важливим інструментом для реалізації методів розслідування є впровадження систем централізованого моніторингу безпеки (SIEM), зокрема таких як Wazuh, ELK Stack (Elasticsearch, Logstash, Kibana) або IBM QRadar, що дозволяють збирати, корелювати та аналізувати події з різних джерел [5].

Методика розслідування, запропонована у дослідженні, базується на поєднанні вимог ISO/IEC 27035 та NIST SP 800-61 Rev.2 [6], які визначають структурований підхід до інцидент-менеджменту. Згідно з рекомендаціями NIST, процес складається з таких етапів: підготовка, виявлення та аналіз, усунення, нейтралізація та відновлення, післяінцидентний аналіз [7]. Додатковим елементом методу є використання форензик-інструментів – Autopsy, Volatility, FTK Imager, Wireshark, що дозволяють відновлювати хронологію подій, аналізувати трафік та ідентифікувати джерела компрометації [8].

Запропонована методика передбачає створення локального полігону розслідування кіберінцидентів, який дозволяє моделювати атаки, фіксувати події, проводити аналіз логів та тестувати алгоритми реагування без ризику для реальних систем. Вона може бути адаптована для використання у державних установах, де є потреба у створенні безпечних середовищ для відпрацювання сценаріїв реагування на інциденти без залучення зовнішніх систем [9]. Впровадження розробленого підходу дає можливість:

- скоротити час виявлення та реагування на інциденти;
- уніфікувати дії фахівців при розслідуванні;
- підвищити якість документування доказової бази;
- забезпечити відповідність вимогам міжнародних стандартів у сфері кібербезпеки [10, 11].

Таким чином, запропонований метод розслідування кіберінцидентів дозволяє підвищити рівень готовності державних інформаційних систем до реагування на загрози, мінімізувати наслідки атак і сформувавши основу для подальшої автоматизації процесів кіберзахисту.

Висновок. Проведене дослідження показало, що ефективне розслідування кіберінцидентів у державних інформаційних системах потребує комплексного підходу, який поєднує технічні, організаційні та процедурні заходи. Аналіз існуючих міжнародних стандартів (ISO/IEC 27035, NIST SP 800-61 Rev.2, ENISA Guidelines) та нормативно-правової бази України свідчить про необхідність адаптації кращих світових практик до національних умов функціонування державного сектору. Запропонований метод розслідування передбачає поетапну процедуру: виявлення інциденту, класифікацію, збір цифрових доказів, аналітичну обробку, формування звіту та коригування політик безпеки. Реалізація такого

підходу дозволяє скоротити час реагування на інциденти, знизити рівень інформаційних ризиків і підвищити достовірність результатів розслідування.

Перелік посилань

1. Symantec. Internet Security Threat Report. 2023. URL: <https://devfolio.co/projects/symantec-internet-security-threat-report-pdf-c39e> (date of access: 25.10.2025).
2. Kaspersky. Incident Response Trends 2024. Kaspersky Lab, 2024. URL: <https://securelist.com/kaspersky-incident-response-report-2024/115873/> (date of access: 25.10.2025).
3. ENISA Threat Landscape 2025/ European Union Agency for Cybersecurity, 2025. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025> (date of access: 25.10.2025).
4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : редакція від 20.04.2025. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 28.08.2025).
5. Про інформацію : Закон України від 02.10.1992 № 2657-XII : редакція від 14.06.2025. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення: 28.08.2025).
6. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР : редакція від 20.04.2025. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text> (дата звернення: 28.08.2025).
7. Державна служба спеціального зв'язку та захисту інформації України. Звіт про стан кібербезпеки України за 2024 рік. URL: <https://h7.cl/1iD43> (date of access: 25.10.2025).
8. Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 03 липня 2023 року № 570. URL: <https://h7.cl/1iD47> (date of access: 25.10.2025).
9. ISO/IEC 27035:2023. Information technology. Information security incident management. Part 1: Principles and process. URL: <https://www.iso.org/ru/standard/78973.html> (date of access: 25.10.2025).
10. NIST SP 800-61 Rev.2 — Computer Security Incident Handling Guide. URL: <https://csrc.nist.gov/pubs/sp/800/61/r2/final> (date of access: 25.10.2025).
11. ENISA. Best Practices For Cyber Crisis Management. 2024. URL: <https://h7.cl/1iD4a> (date of access: 25.10.2025).

УДК 004.8

Мізін Д.В., Мазурець О.В.

Хмельницький національний університет

НЕЙРОМЕРЕЖЕВИЙ ПІДХІД ДО РАНЬОГО ВИЯВЛЕННЯ ОЗНАК АУТИЗМУ ЗА ФОТОЗОБРАЖЕННЯМ

У роботі запропоновано нейромережевий підхід до раннього виявлення ознак розладів аутичного спектра за статичними фотозображеннями облич дітей. Архітектура базується на моделі Vision Transformer, донавчений за схемою transfer learning на спеціалізованому датасеті, з використанням розширеного препроцесингу та аугментацій для нормалізації умов зйомки й часткової компенсації класового дисбалансу. Ключовою особливістю є інтеграція піксельних ознак із морфометричними характеристиками, обчисленими за facial-landmarks MediaPipe Face Mesh, що дає змогу побудувати інтерпретовану ознакову модель ризику. Запропонований підхід розглядається як допоміжний скринінговий інструмент, що доповнює, але не замінює клінічну діагностику, та може бути покладений в основу цифрових сервісів первинного відбору пацієнтів.

This paper presents a neural network-based approach to early detection of autism spectrum disorder markers from static facial photographs of children. The proposed architecture is built upon a Vision Transformer model fine-tuned via transfer learning on a specialised facial image dataset, combined with extensive preprocessing and augmentation to normalise imaging conditions and partially address class imbalance. A key feature is the integration of pixel-level representations with morphometric characteristics derived from MediaPipe Face Mesh facial landmarks, enabling an interpretable risk-oriented feature space. The approach is positioned as an auxiliary screening tool that complements, rather than replaces, clinical diagnosis and can underpin scalable digital services for preliminary risk assessment.

Розлади аутичного спектра належать до групи нейророзвиткових порушень [1], для яких раннє виявлення є критично важливим з огляду на ефективність корекційних програм, подальшу соціалізацію та якість життя дитини [2]. Традиційні підходи до діагностики ґрунтуються на клінічних інтерв'ю, анкетуванні та тривалому поведінковому спостереженні [3], що потребує значних ресурсів, участі висококваліфікованих фахівців і часто призводить до пізнього встановлення діагнозу. На тлі розвитку методів комп'ютерного зору й глибинного навчання зростає інтерес до недорогих, масштабованих і неінвазивних скринінгових рішень, які використовують фотозображення облич як джерело фенотипічної інформації про потенційні ознаки розладів аутичного спектра.

Раннє виявлення ознак аутизму є надзвичайно актуальною проблемою сучасної медицини та психоневрології, оскільки своєчасна діагностика значно підвищує ефективність корекційних програм та соціальної інтеграції дітей із цим станом [4]. Традиційні методи оцінювання часто залежать від суб'єктивних спостережень фахівців і стандартизованих психологічних тестів, що ускладнює раннє виявлення, особливо на стадіях, коли симптоми є мінімально вираженими або мають нечітку зовнішню проявність. У цьому контексті комп'ютерне зір [5] і нейромережеві методи [6, 7] відкривають нові перспективи для об'єктивного аналізу візуальної інформації, що містить сигнали ранніх проявів аутизму, таких як міміка, погляд, жестикуляція, поведінкові патерни у побутових умовах.

Сучасні конволюційні нейронні мережі [8] здатні ефективно виділяти локальні та глобальні ознаки зі складних візуальних даних [9], стійкі до шумів і змінних умов освітлення [10], що характерні для побутових фотозображень. Адаптивні конвеєри обробки зображень [11], які враховують показники якості, такі як різкість, контраст, експозиційна збалансованість і рівень фонових завад, дозволяють оптимізувати процес тренування моделей, підвищуючи точність класифікації навіть при наявності спотворених або частково некоректних даних [12, 13]. Поєднання базових архітектур CNN із модулями донавчання на очищених і сирих датасетах забезпечує більш гнучке узагальнення патернів [14] і зменшує вплив артефактів та шумів на рішення моделі [15].

Важливим аспектом є модульна побудова системи, яка дозволяє інтегрувати попередню обробку зображень, навчальні контури, оцінку якості та прикладні інтерфейси для інтерактивного тестування [16]. Такий підхід відкриває можливості для впровадження нейромережевих рішень [17] у практику медичного скринінгу та досліджень, де потрібно автоматизовано оцінювати численні візуальні параметри, що корелюють із ризиком розвитку аутизму. Подальший розвиток включає вдосконалення механізмів пояснюваності рішень моделей, інтеграцію з мультимодальними даними, такими як відео та аудіо, а також створення адаптивних систем, що здатні навчатися на нових даних без повного перенавчання, що суттєво підвищує їхню практичну цінність.

Метою роботи є розроблення нейромережевого підходу до раннього виявлення ознак аутизму за статичними фотозображеннями облич із фокусом на пояснюваності результатів та прогнозуванні ступеня ризику, а не лише бінарній класифікації «аутизм / не аутизм». Об'єктом дослідження виступає процес автоматизованого виявлення ризику розладів аутичного спектра за зображеннями облич, а предметом – нейромережеві моделі та методи мультимодального аналізу статичних зображень, що поєднують піксельні ознаки з морфометричними характеристиками краніофасіальної області.

Поставлена мета досягається шляхом побудови гібридної архітектури, ядром якої є трансформерна модель Vision Transformer (ViT), донавчена на спеціалізованому датасеті зображень облич дітей з аутизмом і без нього. Використовується схема transfer learning: попередньо натреновані шари ViT адаптуються до домену за рахунок донавчання на маркованому наборі Autism Spectrum Detection (Kaggle + Zenodo), що забезпечує узагальнення на реалістичних даних за умов обмеженого обсягу клінічно релевантних зображень. Додатково реалізовано препроцесинг і аугментацію даних, спрямовані на нормалізацію освітлення, масштабів та варіативності пози обличчя, а також на часткову компенсацію класового дисбалансу.

Ключовою відмінністю підходу є інтеграція піксельної репрезентації з морфометричним аналізом facial-landmarks. Для цього застосовується модель MediaPipe Face Mesh, що відтворює густу сітку орієнтирів обличчя та дозволяє сформувати вектор антропометричних показників: співвідношення вертикальних і горизонтальних сегментів, оцінку симетрії, просторове положення очей, ротової щілини, носо-губного трикутника й контурів нижньої щелепи. Отримані морфометричні індекси зіставляються з картами внутрішньої уваги трансформера [18], що дає змогу пов'язати зони, на які «звертає увагу» модель, із фенотипічно осмисленими краніофасціальними структурами. Таким чином формується узагальнений вектор морфологічно-візуальних ознак, що використовується як основа для інтерпретації нейромережових рішень.

Для забезпечення пояснюваності результатів класифікації запропоновано пояснювальний модуль на основі мовної моделі типу T5, який перетворює числові характеристики морфометричних індексів та просторовий розподіл уваги ViT у короткі текстові пояснення. Ці пояснення формуються в нейтральній, недіагностичній формі й описують, які області обличчя та які структурні співвідношення були найбільш релевантними для підвищення чи зниження прогнозованого ризику. Така інтеграція карт уваги, лендмарків і генеративної мовної моделі створює багаторівневий механізм інтерпретації, який робить роботу класифікатора прозорою для фахівця й може використовуватися як допоміжний інструмент при прийнятті клінічних рішень.

Експериментальна частина підходу передбачає донавчання ViT на розділених на навчальну, валідаційну та тестову підвибірках даних з використанням класичних показників ефективності: точності, повноти, прецизійності, F1-міри та аналізу матриці неточностей. Особливу увагу приділено характеру помилок класифікації, зокрема випадкам хибнонегативних рішень, які є критичними для скринінгових сценаріїв.

Наукова новизна роботи полягає у поєднанні трансформерної класифікації зображень облич із детальним морфометричним аналізом facial-landmarks та автоматизованою генерацією пояснень рішень. На відміну від традиційних підходів, що обмежуються бінарною класифікацією та непрозорими картами уваги, запропонований нейромережевий підхід орієнтований на прогнозування ступеня ризику, забезпечує інтерпретованість на рівні антропометричних індикаторів і може бути інтегрований у скринінгові системи як допоміжний інструмент для раннього виявлення ознак аутизму. Його практичне значення полягає у створенні передумов для недорогих і масштабованих цифрових сервісів первинного скринінгу, які доповнюють, але не замінюють клінічну діагностику, з урахуванням етичних вимог до опрацювання персональних зображень дітей.

Перелік посилань

1. Autism. World Health Organization. URL: <https://www.who.int/news-room/fact-sheets/detail/autism-spectrum-disorders>
2. A Validation Study of the CARS-2 Compared With the ADOS-2 in the Diagnosis of Autism Spectrum Disorder: A Suggestion for Cutoff Scores / S.-I. Ji et al. Journal of the Korean Academy of Child and Adolescent Psychiatry. 2023. Vol. 34, no. 1. P. 45–50.
3. Kangarani-Farahani M., Malik M. A., Zwicker J. G. Motor Impairments in Children with Autism Spectrum Disorder: A Systematic Review and Meta-analysis. Journal of Autism and Developmental Disorders. 2023. URL: <https://doi.org/10.1007/s10803-023-05948-1>
4. Koehler J. C., Falter-Wagner C. M. Digitally assisted diagnostics of autism spectrum disorder. Frontiers in Psychiatry. 2023. Vol. 14. URL: <https://doi.org/10.3389/fpsyt.2023.1066284>
5. Мазурець О.В., Жарновський О.В., Гладун О.В., Собко О.В. Нейромережеве виявлення фейкових зображень людей. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2025. №5. Т.1. С. 416-422.
6. Молчанова М.О., Мазурець О.В., Шурипа М.О. Об'єктно-орієнтований підхід до нейромережевого виявлення та відстеження БПЛА з використанням хмарних технологій. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №9 (50). С. 1346-1360.
7. Мазур Є.В., Мазурець О.В., Кліменко В.І., Собко О.В., Залуцька О.О. Алгоритми та програмна архітектура інформаційної системи нейромережевого аналізу постави людини. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2025. №3. Т.1. С. 275-284.
8. Kok I.A., Kadyńska V.D., Zalutska O.O., Mazurets O.V. Object-Oriented Intelligent System for Automated Control of Smoking by Video Data. Current scientific goals, approaches and challenges. Proceedings of IV International Scientific and Theoretical Conference. June 13, 2025. Dresden, Federal Republic of Germany. Pp. 156-164.
9. Bas I.S., Kadyńska V.D., Klimenko V.I., Mazurets O.V. Convolutional Neural Network Transfer Learning Method for Aircraft Image Classification. Scientific method: reality and future

- trends of researching. Proceedings of VI International Scientific and Theoretical Conference. June 6, 2025. Montreal, Canada. Pp. 147-155.
10. Mushtyn O., Sobko O., Molchanova M., Mazurets O. Convolutional Neural Network Architecture for Image-Based Architectural Style Recognition. Evolving Science: Theories, Discoveries and Practical Outcomes. Proceedings of 4th International Scientific and Practical Conference. June 9-11, 2025. Zurich, Switzerland. Pp. 130-143.
11. Malaydakh V., Molchanova M., Shevchuk P., Mazurets O. Deep learning neural network architecture for determining sunflower growth stage from visual data. Modern Scientific Research: Theoretical and Practical Aspects. Proceedings II International Scientific and Practical Conference. May 26-28, 2025. Riga, Latvia. Pp. 143-148.
12. Ostapchenko N., Tyschenko O., Denysenko B., Mazurets O. Semantic search of relevant images using vector databases. Modern Scientific Research: Theoretical and Practical Aspects. Proceedings II International Scientific and Practical Conference. May 26-28, 2025. Riga, Latvia. Pp. 161-165.
13. Dydo R., Sobko O., Klimenko V., Mazurets O. Datalogic structure for intelligent system for areas localization in photos with the remains of buildings using neural network. Modern Scientific Research: Theoretical and Practical Aspects. Proceedings II International Scientific and Practical Conference. May 26-28, 2025. Riga, Latvia. Pp. 123-127.
14. Didur V., Molchanova M., Mazurets O. Research on the effectiveness of neural network detection of plots with the destroyed buildings remains. Modern technologies and science: problems, new and relevant developments. Proceedings XXI International Scientific and Practical Conference. May 26, 2025. Zaragoza, Spain. Pp. 245-251.
15. Hladun O.V., Molchanova M.O., Zalutska O.O., Mazurets O.V. Effectiveness research of using ViT neural network architecture for classifying the destroyed buildings remains. Achievements of Science and Applied Research. Proceedings of 2nd International Scientific and Theoretical Conference. May 19-21, 2025. Dublin, Ireland. Pp. 96-100.
16. Дидо Р.А., Мазурець О.В. Метод ідентифікації особистості на основі розпізнавання обличчя в реальному часі для систем кібербезпеки. Інформаційна, функційна і кібербезпека СКІФіК2024. Матеріали IV Всеукраїнської науково-технічної конференції. 29-30 листопада 2024. Харків. 2024. с. 36-37.
17. Похитун А.В., Мазурець О.В., Молчанова М.О., Бармак О.В. Підхід до формування датасету для нейромережевого виявлення модифікованих фотографій облич людей. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». 15-16 листопада 2024. Хмельницький, 2024. с. 428-433.
18. Zharnovskiy O., Mazurets O., Sobko O. Approach to Identification of Artificial Intelligence-Generated People Images by Means of Machine Learning. Key Aspects of the Development of Scientific Research in Modern Conditions. Proceedings of the XLV International scientific and practical conference. October 30 – November 1, 2024. Constanta, Romania. 2024. Pp. 69-73.

УДК 004.8

Молчанова М.О., Мурава В.В.

Хмельницький національний університет

ВИЯВЛЕННЯ ШАБЛОНІВ ВЕБ-ПРОПАГАНДИ НЕЙРОМЕРЕЖЕВИМИ МЕТОДАМИ

У роботі розглянуто нейромережевий підхід до виявлення шаблонів веб-пропаганди в україномовних текстах на основі трансформерних моделей BERT та RoBERTa з акцентом на оптимізації балансування навчального датасета між пропагандистськими та нейтральними фрагментами. Запропоновано інтегрований метод аналізу, який працює на рівні речень, оцінює ймовірність наявності окремих пропагандистських технік і формує узагальнені показники їх вираженості на рівні всього тексту. Експериментальні результати на корпусі з розміткою за шаблонами UNLP 2025 засвідчують, що оптимальна частка нейтральних текстів (близько 30%) забезпечує досягнення $F_1 = 0,725$ для україномовної RoBERTa, що перевищує показники відомих міжнародних підходів.

The paper presents a neural-network-based approach to detecting web propaganda patterns in Ukrainian texts using transformer models BERT and RoBERTa, with a focus on optimizing dataset balancing between propagandistic and neutral fragments. An integrated sentence-level analysis method is proposed, which estimates the likelihood of specific propaganda techniques and aggregates their intensity at the document level. Experiments on a corpus annotated with UNLP 2025 propaganda patterns show that an optimal proportion of neutral texts (around 30%) enables the Ukrainian RoBERTa model to reach an F_1 score of 0.725, outperforming a range of existing international baselines.

Стрімка медіатизація суспільних процесів і перенесення політичної комунікації у веб-простір призвели до якісно нової ролі пропагандистського контенту. Веб-платформи, соціальні мережі та новинні агрегатори стали не лише каналами поширення інформації, а й повноцінними інфраструктурами для масштабованого маніпулятивного впливу на громадську думку, електоральну поведінку та уявлення про ключові події [1]. Алгоритмічні стрічки, персоналізовані рекомендації та таргетована реклама підсилюють ефект «інформаційних бульбашок» і сприяють тому, що користувач стикається з пропагандистськими повідомленнями навіть без усвідомлення їх маніпулятивної природи [2, 3].

За таких умов завдання автоматизованого виявлення веб-пропаганди переходить із площини суто теоретичної проблеми медіазнавства в зону критично важливої інформаційної безпеки [4]. Традиційні методи аналізу тексту [5, 6], що спираються на поверхневі статистичні ознаки [7] або фіксовані словники [8], виявляються недостатніми: сучасні пропагандистські повідомлення оперують тонкими семантичними натяками [9], контекстуальними рамками [10, 11], міжтекстовими відсиланнями, стилістичними прийомами [12, 13], які важко

зафіксувати жорстко заданими правилами. У цих умовах саме трансформерні мовні моделі [14] стали базовим інструментом, здатним враховувати широкий контекст, латентні семантичні зв'язки та стилістичні патерни.

Водночас ефективність нейромережових моделей напряму залежить від структури та збалансованості навчальних вибірок [15]. Для завдання виявлення пропаганди проблема класового дисбалансу є особливою гострою: тексти з маніпулятивними патернами [16], як правило, займають меншу частку інформаційного потоку [17], тоді як нейтральні повідомлення масово переважають. Крім того, окремий текст може містити кілька різних типів пропагандистських технік одночасно [18, 19], що зумовлює багатоміткову природу завдання й робить класичну багатокласову класифікацію непридатною [20].

Запропонований у дослідженні підхід спрямований на підвищення ефективності виявлення шаблонів веб-пропаганди в україномовних текстах на основі трансформерних моделей BERT та RoBERTa через цілеспрямовану оптимізацію балансування датасета, зокрема шляхом варіювання частки нейтральних текстів у навчальній вибірці.

Автоматизоване виявлення пропаганди в текстах розвивалося від класичних методів обробки природної мови до сучасних глибоких нейромережових архітектур. На ранніх етапах дослідження фокусувалися на словникових підходах, аналізі полярності, індикаторах суб'єктивності, модальності й емоційної забарвленості висловлювань. Такі методи дозволяли фіксувати загальну настанову тексту, але були малочутливими до конкретних пропагандистських технік, як-от «апеляція до страху», «фальшива дилема», «підміна причинно-наслідкових зв'язків» тощо.

Перехід до корпусних досліджень і появи спеціалізованих датасетів, зокрема новинних корпусів із розміткою пропагандистських прийомів, відкрив можливість більш тонкої класифікації патернів. У низці робіт було показано, що використання класичних векторних представлень (TF-IDF, word2vec, doc2vec) у поєднанні з ансамблевими алгоритмами машинного навчання (SVM, Random Forest, Stacking Classifier) дозволяє досягати прийнятних значень Accuracy і F₁-міри, однак залишає обмеження щодо контекстного розуміння й переносимості моделей між доменами.

Суттєвий прогрес забезпечили трансформерні моделі BERT-подібної архітектури. Їх застосування дало змогу враховувати контекст кожного токена щодо всього тексту, моделювати семантичні та синтаксичні зв'язки й ефективно розрізняти як загальний тон повідомлення, так і специфічні маніпулятивні структури. Розроблені рішення на базі BERT, RoBERTa, XLM-RoBERTa, GPT-подібних моделей демонстрували зростання F1-міри у порівнянні з попередніми підходами, зокрема в задачах класифікації пропагандистських технік за еталонними наборами SemEval та низкою мульти- і мультимодальних корпусів.

Разом із тим у більшості робіт ключова увага приділялася або мультимодальності (поєднанню тексту з візуальними даними, зокрема мемами та зображеннями), або багатомовності (розширенню моделей на кілька мов за допомогою спільних просторових репрезентацій), або мета-навчанню й доменно-

орієнтованому донавчанню. Натомість питання організації навчальної вибірки, зокрема співвідношення між пропагандистськими та нейтральними текстами, розглядалося переважно в контексті аугментації (EDA, back-translation, синтетичні приклади) й компенсації дисбалансу через ваги класів.

Практично відсутні дослідження, де цілеспрямовано аналізується вплив частки текстів без проявів пропаганди у навчальному наборі на здатність моделей розрізняти:

- тексти з конкретним патерном;
- тексти з іншими патернами;
- нейтральні тексти без пропагандистських технік.

Ця прогалина особливо критична для україномовного інформаційного простору, де наявні корпуси маніпулятивних матеріалів лише формуються, а питання збалансованості датасетів у розрізі конкретних патернів і нейтральних повідомлень набуває не лише наукового, а й практичного значення для протидії дезінформації.

Метою дослідження є підвищення ефективності виявлення шаблонів веб-пропаганди в україномовних веб-текстах за допомогою трансформерних нейромережових моделей шляхом оптимізації балансування датасета, зокрема встановлення оптимальної частки нейтральних текстів у навчальній вибірці.

Початковий набір характеризується нерівномірним розподілом прикладів за патернами: окремі техніки («Loaded Language», «Cherry Picking») представлені значно більше, тоді як інші («Straw Man», «Thought-Terminating Cliché») мають суттєво менші обсяги анотованих фрагментів. Окрім того, існує окрема підмножина фрагментів, де не зафіксовано жодного пропагандистського шаблону.

Балансування здійснюється за двох принципів. По-перше, для кожного патерна p_i формується навчальна вибірка, де позитивні приклади репрезентують реальний розподіл цього патерна, а негативні приклади відбираються так, щоб забезпечити задану частку m нейтральних фрагментів серед усіх негативів. При цьому до негативів входять як нейтральні тексти, так і фрагменти, де присутні інші патерни, але відсутній p_i .

По-друге, формується спеціальна валідаційна вибірка, у якій усі патерни представлені рівномірно, а кількість нейтральних фрагментів співмірна з сумарною кількістю пропагандистських прикладів. Така конструкція дозволяє об'єктивно оцінити, чи не «плутає» модель окремі патерни між собою та чи зберігається її здатність розрізняти маніпуляційні й нейтральні тексти при зміні m .

Критично важливим є те, що розмітка виконується на рівні речень, а не повних текстів. Це дає змогу підвищити щільність корисних прикладів у вибірці та сконцентрувати навчання на безпосередніх носіях патернів. Водночас така глибина розмітки породжує окремі обмеження, які будуть розглянуті в обговоренні.

Побудований метод (рисунок 1) на основі бінарних моделей використовується як єдиний інтегрований інструмент аналізу веб-контенту [21]. Вхідними даними слугує довільний текст – публікація в соціальній мережі, стаття онлайн-видання або фрагмент новинної стрічки.

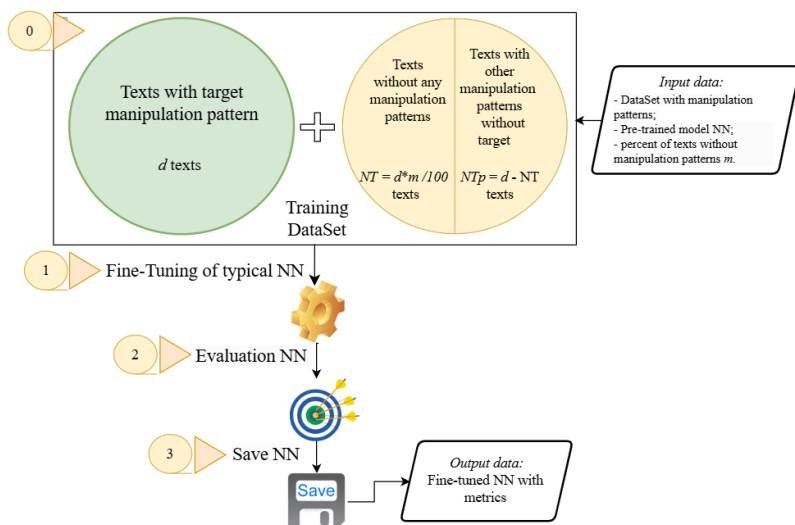


Рисунок 1 – Метод виявлення шаблонів веб-пропаганди

На першому етапі виконується попередня обробка: текст розбивається на окремі речення, здійснюється їх токенізація та перетворення у формат, придатний для подальшого опрацювання трансформерними моделями.

На другому етапі кожне речення незалежно подається на вхід усім бінарним моделям, де кожна з них відповідає окремому пропагандистському шаблону. Для кожної моделі обчислюється ймовірність того, що у відповідному реченні присутня конкретна техніка пропаганди. Якщо ця ймовірність перевищує заздалегідь обраний пороговий рівень, вважається, що речення містить відповідний шаблон. У результаті для кожного речення формується набір пропагандистських технік, які в ньому виявлено.

На третьому етапі здійснюється узагальнення результатів на рівні всього тексту. Для кожного шаблону обчислюються інтегральні показники його вираженості з урахуванням усіх речень, у яких було зафіксовано його прояв. Паралельно виділяються речення, у яких модель оцінює наявність тієї чи іншої техніки як найбільш ймовірну; саме вони можуть демонструватися користувачеві як найхарактерніші приклади. Такий підхід дає змогу не лише встановити факт наявності чи відсутності пропаганди в тексті, а й деталізувати, які саме техніки використовуються та в яких фрагментах вони проявляються найінтенсивніше.

Для об'єктивної оцінки результатів розроблений підхід було зіставлено з низкою відомих рішень, які використовують трансформерні моделі й ансамблеві підходи для виявлення пропаганди в англійських та мультимовних корпусах. У більшості таких робіт F_1 -міра коливається на рівні 0,57–0,60 для складних задач класифікації технік пропаганди за еталонними наборами даних.

На цьому тлі досягнуте значення $F_1 = 0,725$ для україномовної RoBERTa при $m = 30\%$ свідчить про суттєве покращення якості. Важливо, що йдеться не про полегшену задачу «є/немає пропаганди», а саме про виявлення різних шаблонів у межах багатоміткової постановки на складному корпусі з перетином патернів.

Цей результат особливо показовий з огляду на те, що мова йде про українську мову, для якої обсяги маркованих даних традиційно менші, ніж для англійської. Використання попередньо натренованих україномовних моделей у поєднанні з ретельно продуманим балансуванням вибірки компенсує цей недолік і демонструє, що якісні рішення для автоматизованого виявлення пропаганди можуть бути створені й для «малих» мов за умови правильного підходу до структурування даних.

Незважаючи на отримані високі показники, розроблений підхід має низку принципових обмежень.

По-перше, аналіз здійснюється на рівні речень. Це дозволяє чітко локалізувати патерни та збільшити щільність позитивних прикладів, однак водночас ігнорує ширший дискурсивний контекст. Частина маніпулятивних технік працює саме через композицію кількох речень, розміщення інформації у певній послідовності, контрастування з попереднім або наступним контекстом. Речення, яке в ізоляції виглядає нейтральним, у контексті пропагандистського наративу може виконувати ключову роль, але така роль не фіксується при суто реченнєвому аналізі.

По-друге, корпус розмічений вручну, що неминуче містить елемент суб'єктивності. Різні експерти можуть по-різному інтерпретувати межу між, наприклад, «Loaded Language» та емоційно забарвленими, але не пропагандистськими висловлюваннями. Наявність суб'єктивних похибок у розмітці впливає як на процес навчання, так і на оцінювання, формуючи верхню межу досяжної якості.

По-третє, у дослідженні розглядалася дискретна шкала значень m (10%, 30%, 50%, 70%). Теоретично, оптимальне значення може лежати між цими точками, а також залежати від конкретної архітектури, типу патерна чи домену текстів. Подальші дослідження можуть передбачати використання більш дрібного кроку варіювання m або застосування методів байєсівської оптимізації для пошуку m^* в неперервному просторі.

Перспективним напрямом є також перехід від суто реченнєвого аналізу до ієрархічних моделей, які поєднують рівень речень і рівень документа. Такі моделі можуть спочатку виявляти локальні патерни, а потім інтегрувати їх у глобальний дискурсивний контекст, оцінюючи, як локальні маніпуляції формують загальну рамку повідомлення.

Окремим вектором розвитку є інтеграція пояснювальних механізмів. Для практичних застосувань (модерація, фактчекінг, медіаграмотність) важливо не лише автоматично детектувати патерн, а й пояснити користувачеві, чому модель вважає той чи інший фрагмент маніпулятивним, які мовні маркери чи структурні особливості на це вказують. Застосування методів пояснювальної ШІ (attention-

візуалізація, градієнтні карти, локальні сурогатні моделі) може суттєво підвищити довіру до систем виявлення пропаганди.

Отримані результати мають як наукове, так і практичне значення. З наукового боку продемонстровано, що зміна частки нейтральних текстів у навчальній вибірці є окремим параметром, який суттєво впливає на узагальнювальну здатність моделей виявлення пропаганди й повинен розглядатися як об'єкт оптимізації нарівні з гіперпараметрами навчання. З практичного боку запропонований підхід може бути покладений в основу програмних систем для автоматизованого моніторингу інформаційного простору, підтримки фактчекінгових ініціатив, а також освітніх інструментів із розвитку медіаграмотності, де користувачі отримуватимуть не лише індикатор наявності пропаганди, а й марковані приклади конкретних маніпулятивних технік.

Подальші дослідження доцільно спрямувати на розширення корпусу за рахунок інших доменів (соціальні мережі, коментарі, блоги), перехід до ієрархічного аналізу на рівні документів, інтеграцію мультимодальних даних (текст плюс зображення) та розроблення пояснювальних модулів, що підвищать прозорість і довіру до нейромережевих систем виявлення веб-пропаганди.

Перелік посилань

1. Scorzato L. Reliability and Interpretability in Science and Deep Learning. *Minds and Machines*. 2024. Vol. 34, no. 3.
2. Geissler, D., Bär, D., Pröllochs, N., &Feuerriegel, S. "Russian propaganda on social media during the 2022 invasion of Ukraine". *EPJ Data Science*, vol. 12, no. 1, pp. 35, 2023.
3. Lande D. Formation and analysis of networks of events in the field of parliamentary control based on the application of artificial intelligence systems. *INFORMATION AND LAW*. 2024. No. 1(48). P. 84–89.
4. Marchenko O., Isoieva M. Automatic Generation of Coherent Natural Language Texts. *Flexible Query Answering Systems*. Cham, 2023. P. 79–92.
5. Lawrence G. The Power to Lie: Propaganda and Post-truth Politics. *Societal Deception*. London, 2024. P. 211–270.
6. Shevchuk P., Molchanova M., Mazurets O. Software for Text Messages Reliability Analysis Based on the Machine Learning Models Ensemble. *Proceedings of IV International Scientific and Practical Conference «Innovative research and perspectives of the development of science and technology»*. January 29-31, 2024. Stockholm, Sweden. 2024. Pp. 347-354.
7. Mazurets O.V., Sobko O.V., Molchanova M.O., Zalutska O.O., Yurchak A.V. Practical Implementation of Neural Network Method for Stress Features Detection by Social Internet Networks Posts. *Global Science: Prospects and Innovations. Proceedings of the II International Scientific and Theoretical Conference «Scientific Review of the Actual Events, Achievements and Problems»*. May 31, 2024. Berlin, Federal Republic of Germany: International Center of Scientific Research. 2024. Pp. 160-167.
8. Овчарук О.М., Мазурець О.В. Нейромережева архітектура з квантовим шаром для аналізу текстових повідомлень на прояви посттравматичного стресового розладу. *Науковий журнал «Наука і техніка сьогодні»*. Київ, 2024. №13 (41). С. 1192-1204.
9. Мазурець О.В., Тимофіїв І.А., Кліменко В.І., Тищенко О.О. Метод виявлення депресивного стану пов'язаного із навчанням у закладах освіти із використанням нейромережі дуальної архітектури. *Науковий журнал «Вісник Херсонського національного технічного університету»*. 2024. №4 (91). С. 311-318.

10. Віт Р.В., Мазурець О.В. Підхід до тематичної класифікації текстової інформації засобами обробки природної мови. Науковий журнал «Наукові праці Донецького національного технічного університету», серія «Проблеми моделювання та автоматизації проєктування». 2025. №1 (21). С. 94-99.
11. Овчарук О.М., Мазурець О.В. Нейромережевий метод діагностування психологічних розладів за аналізом повідомлень на основі роздільного підходу до класифікації. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». № 1, 2025. с. 210-216.
12. Murava V., Zalutska O., Didur V., Mazurets O. Software architecture of information system for exchanging LLM thematic prompts. Global Trends in the Development of Information Technology and Science. Proceedings IV International Scientific and Practical Conference. June 25-27, 2025. Stockholm, Sweden. Pp. 121-127.
13. Молчанова М.О., Мазурець О.В., Собко О.В., Кліменко В.І., Андрощук В.І. Метод нейромережевого виявлення кібербулінгу з використанням хмарних сервісів та об'єктно-орієнтованої моделі. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2024. №2 (333). С. 200-206.
14. Mazurets O., Molchanova M., Klimenko V., Prosvitliuk M Practice Implementation of Neural Network Model BART-Large-CNN for Text Annotation. Prospects of Scientific Research in the Conditions of the Modern World. Proceedings of XXVII International scientific and practical conference. June 12-14, 2024. Rotterdam, Netherlands. 2024. Pp. 97-102.
15. Tymofiiiev I., Mazurets O., Hardysh D., Molchanova M. Neural Network Dual Architecture for Depression Detection Using Cloud Services. Scientific Research in the Era of Digital Technologies: Challenges and Opportunities. Proceedings of the XLVI International scientific and practical conference. November 6-8, 2024. Barcelona, Spain. 2024. Pp. 84-88.
16. Молчанова М.О., Мазурець О.В., Собко О.В., Віт Р.В., Назаров В.В. Алгоритм виявлення аб'юзивного вмісту в україномовному аудіоконтенті для імплементації в об'єктно-орієнтовану інформаційну систему. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2024. №1 (331). С. 101-106.
17. Денисенко Б.О., Молчанова М.О., Мазурець О.В. Інтелектуальна система виявлення дезінформації з застосуванням штучних нейронних мереж. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». 15-16 листопада 2024. Хмельницький, 2024. с. 167-174.
18. Yurchenko D., Mazurets O., Didur V., Molchanova M. Approach to Using Cloud Services for Visual Analytics of Neural Network Analysis of Texts Emotional Tonality. The Future of Scientific Discoveries: New Trends and Technologies. Proceedings of the XLVII International scientific and practical conference. November 13-15, 2024. Marseille, France. 2024. Pp. 108-113.
19. Hladun O., Mazurets O., Molchanova M., Sobko O. Real Time Detection the Person Emotion State Using Neural Network. Scientific Research: Modern Innovations and Future Perspectives. Proceedings of the 2 International scientific and practical conference. November 25-27, 2024. Montreal, Canada. 2024. Pp. 119-123.
20. Крак Ю.В., Дідур В.О., Молчанова М.О., Мазурець О.В., Собко О.В., Залуцька О.О., Бармак О.В. Метод виявлення політичної пропаганди в інтернет-контенті нейромережевими засобами обробки природної мови. Науковий журнал «Проблеми програмування». Київ, 2024, №2-3. с. 288-295.
21. Molchanova M., Didur V., Sobko O., Mazurets O. Detection of Web Propaganda Patterns by Transformer Neural Networks: Improving Efficiency via Dataset Balancing, CEUR Workshop Proceedings, 2025, vol. 3988, pp. 112-126.

УДК 004.4

Морозов А.В.

Кам'янський енергетичний фаховий коледж

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СИСТЕМАХ КІБЕРБЕЗПЕКИ

У XXI столітті інформація стала одним із найважливіших стратегічних ресурсів. Розвиток цифрових технологій, інтернету речей, хмарних обчислень і мобільних сервісів створює величезні обсяги даних, що потребують надійного захисту. З іншого боку, кіберзлочинність стрімко зростає – атаки стають складнішими, а методи зловмисників – дедалі витонченішими.

Традиційні системи кіберзахисту, засновані на статичних правилах або сигнатурах, часто не встигають реагувати на нові, невідомі загрози. У зв'язку з цим особливого значення набуває штучний інтелект (ШІ) – технологія, що дозволяє системам навчатися, адаптуватися та прогнозувати атаки в режимі реального часу.

In the 21st century, information has become one of the most important strategic resources. The development of digital technologies, the Internet of Things, cloud computing and mobile services creates huge amounts of data that require reliable protection. On the other hand, cybercrime is growing rapidly - attacks are becoming more complex, and the methods of attackers are becoming more sophisticated.

Traditional cyber defense systems, based on static rules or signatures, often do not have time to react to new, unknown threats. In this regard, artificial intelligence (AI) is gaining special importance – technology that allows systems to learn, adapt and predict attacks in real time.

Метою цієї доповіді є розгляд сучасних підходів до використання штучного інтелекту у системах кібербезпеки, аналіз його переваг, викликів і перспектив розвитку.

Штучний інтелект у сфері кібербезпеки охоплює сукупність технологій – машинне навчання (ML), глибинне навчання (DL), обробку природної мови (NLP), експертні системи, які дозволяють автоматизувати процес виявлення, аналізу й запобігання загрозам.

Основна мета застосування ШІ полягає в тому, щоб виявляти аномалії та атаки швидше, ніж це може зробити людина, і мінімізувати людський фактор у процесі реагування.

Методи та технології використання ШІ у системах кіберзахисту:

1.Машинне навчання (Machine Learning)

– Моделі машинного навчання навчаються на великих масивах даних, щоб розпізнавати закономірності, характерні для шкідливої активності.

– Класифікаційні алгоритми (наприклад, Random Forest, SVM) використовуються для розпізнавання шкідливого програмного забезпечення.

– Аналіз аномалій застосовується для виявлення нетипових дій у мережевому трафіку або поведінці користувача.

– Підкріплене навчання (Reinforcement Learning) дає змогу системі самостійно вдосконалювати свої дії у відповідь на кіберзагрози.

2. Глибинне навчання (Deep Learning)

Глибинні нейронні мережі (DNN, CNN, RNN) можуть автоматично виявляти складні патерни у даних, що робить їх корисними для:

- розпізнавання фішингових листів,
- виявлення ботнетів і DDoS-атак,
- аналізу поведінки користувачів (User Behavior Analytics).

3. Обробка природної мови (NLP)

NLP допомагає аналізувати великі обсяги текстової інформації: журнали подій, звіти безпеки, електронну пошту. Наприклад, системи на основі GPT-моделей здатні автоматично класифікувати повідомлення за рівнем ризику або генерувати звіти про інциденти.

4. Інтелектуальні системи виявлення вторгнень (IDS/IPS)

Традиційні IDS працюють за принципом пошуку сигнатур, тоді як системи з елементами ШІ здатні самонавчатися, виявляючи невідомі атаки. Наприклад, платформи Darktrace або CyLance використовують алгоритми ШІ для оцінки ризиків і миттєвого реагування на аномальні події.

Переваги використання ШІ в кібербезпеці:

1. Автоматизація процесів – зменшення навантаження на аналітиків безпеки.

2. Виявлення невідомих загроз – системи ШІ здатні ідентифікувати нові типи атак без попередніх сигнатур.

3. Адаптивність – моделі навчаються на нових даних і вдосконалюються з часом.

4. Швидкість реагування – виявлення та усунення загроз у режимі реального часу.

Попри численні переваги, впровадження штучного інтелекту у сфері кіберзахисту супроводжується певними труднощами:

– Брак якісних навчальних даних. Якщо модель навчається на неповних або викривлених даних, вона може видавати хибні результати.

– Атаки на моделі ШІ (Adversarial Attacks). Зловмисники можуть маніпулювати вхідними даними, щоб обдурити систему.

- Проблема пояснюваності. Рішення, прийняті складними нейронними мережами, важко інтерпретувати.
- Високі обчислювальні витрати на навчання моделей.
- Майбутнє кібербезпеки неможливо уявити без інтеграції штучного інтелекту.
- Перспективними напрямками є:
 - Комбінування ШІ з блокчейном для підвищення прозорості та незмінності даних безпеки.
 - Використання генеративних моделей для створення сценаріїв навчання систем безпеки.
 - Розвиток автономних агентів, які зможуть реагувати на атаки без участі людини.
 - Етичне та регуляторне забезпечення – створення стандартів безпечного використання ШІ в критичних системах.

Штучний інтелект суттєво змінює підхід до кібербезпеки, перетворюючи її з реактивної на проактивну. Завдяки машинному та глибинному навчанню системи здатні не лише виявляти вже відомі атаки, а й прогнозувати нові типи загроз.

Попри технічні й етичні виклики, впровадження ШІ у сфері безпеки є необхідним етапом розвитку інформаційних технологій. У найближчі роки очікується поява гібридних систем, які поєднуюватимуть людський досвід із обчислювальними можливостями ШІ, забезпечуючи високий рівень захисту інформаційного простору.

Перелік посилань

1. Sommer P., Skinner G. Artificial Intelligence in Cybersecurity: Challenges and Opportunities. – Springer, 2023.
2. Kshetri N. 1st International Conference on AI–Driven Cyber Defense. – IEEE, 2022.
3. Баранов О.В. Штучний інтелект у системах інформаційної безпеки. – Київ: НАУ, 2021.
4. Symantec Enterprise. AI and Machine Learning in Cyber Defense. – <https://www.broadcom.com/company/news>
5. Darktrace. AI–Powered Cybersecurity Platform. – <https://www.darktrace.com>.

УДК 004.4

Москальчук С.О., Яшина О.М.

Хмельницький національний університет

УДОСКОНАЛЕННЯ МЕТРИК ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ШЛЯХОМ ВРАХУВАННЯ ІСТОРІЇ ЗМІН КОДУ ТА ДЕФЕКТІВ У СИСТЕМАХ КОНТРОЛЮ ВЕРСІЙ

Досліджено еволюцію метрик якості програмного забезпечення, продемонстровано недоліки традиційних підходів та обґрунтовано перехід до нової парадигми, заснованої на аналізі історичних даних із систем контролю версій. Запропоновано клас процесно-орієнтованих метрик, що відображають якість та динаміку розробки.

The evolution of software quality metrics has been studied, highlighting the shortcomings of traditional approaches and justifying the transition to a new paradigm based on the analysis of historical data from version control systems. A class of process-oriented metrics reflecting the quality and dynamics of software development is proposed.

Сучасна розробка програмного забезпечення стикається зі зростанням складності систем, що робить управління якістю критично важливим фактором успіху. Історичні дані свідчать, що зі збільшенням бюджету проекту його шанси на успішне завершення значно знижуються, а для проектів вартістю понад 10 мільйонів доларів ймовірність успіху наближається до нуля [1]. Основною причиною невдач є програмні дефекти, а саме помилки в коді, які призводять до некоректної роботи системи.

Традиційні підходи до забезпечення якості, що покладаються на тестування на пізніх етапах розробки є неефективними та надзвичайно дорогими. Виявлення та виправлення дефектів після випуску продукту може коштувати в рази дорожче, ніж на ранніх стадіях. У відповідь на ці виклики виникла та активно розвивається галузь прогнозування програмних дефектів (Software Defect Prediction, SDP). Її метою є ідентифікація модулів коду, які з високою ймовірністю містять дефекти, ще до того, як вони проявлять себе. Такий підхід дозволяє командам ефективно розподіляти ресурси, зосереджуючи зусилля на найбільш ризикованих ділянках кодової бази [2].

Історично перші спроби кількісної оцінки якості ПЗ були зосереджені на статичному аналізі коду. Метрики, такі як кількість рядків коду (SLOC), цикломатична складність та метрики Холстеда, здобули популярність завдяки своїй простоті та легкості автоматизації [3]. Вони повинні були надавати об'єктивну основу для оцінки складності коду і, як наслідок, його схильності до дефектів.

Однак, з часом накопичився значний обсяг доказів, які продемонстрували обмеження такого підходу. По-перше, статичні метрики надмірно спрощують реальність і не враховують контекст, тобто їхні значення сильно залежать від мови програмування, стилю кодування та інструментів. По-друге, існує виражена

кореляція більшості метрик складності з метрикою розміру коду (SLOC). Це призвело до так званого вимірювального парадоксу, а саме доцільності використання складних метрик порівняно із простим вимірюванням розміру [3].

Найбільшим недоліком статичного аналізу є те, що він ігнорує семантичні та динамічні аспекти. Два фрагменти коду можуть мати ідентичні значення статичних метрик, але один може бути надійним, а інший може містити критичний дефект. Статичні методи вимірюють продукт, а саме готовий програмний код, але повністю ігнорують процес його створення, змін тощо.

Центральним джерелом даних для сучасної методології аналізу якості є система контролю версій (VCS), така як Git. Традиційно VCS розглядаються як інструменти для розробників, що забезпечують відстеження змін у коді [4]. Вони зберігають повну історію кожної модифікації, бобто хто, коли і що саме змінив. Однак, з точки зору дослідження якості, VCS є багатим історичним архівом, що містить деталізацію процесу розробки. Це стало основою для інтелектуального аналізу репозиторіїв програмного забезпечення (Mining Software Repositories, MSR) [5], що займається аналізом даних з репозиторіїв для виявлення закономірностей.

На протипагу статичним метрикам, у даному дослідженні пропонується парадигма, заснована на аналізі процесу розробки з використанням даних VCS. Дослідження показують, що метрики, отримані з історії змін, є значно кращими та ефективнішими для передбачення майбутніх дефектів, ніж традиційні метрики продукту. Після врахування історії змін метрика SLOC втрачає свою цінність у прогнозуванні, що свідчить про те, що саме динаміка змін є ключовим індикатором якості програмного коду [6].

Основними категоріями процесно-орієнтованих метрик є:

- метрики, що базуються на історії змін, які описують як еволюція коду впливає на його якість. Кількість змін показує, скільки разів файл було модифіковано. Емпіричні дослідження свідчать, що очікувана кількість майбутніх дефектів у модулі прямо пропорційна кількості його попередніх змін [6]. Моделі, які також враховують розмір і актуальність змін, тобто кількість змінених рядків та час від останнього редагування, демонструють вищу точність прогнозування, оскільки великі й нещодавні зміни частіше призводять до появи помилок;

- метрики віку коду підкреслюють стабільність, тобто модулі з більшим середнім віком зазвичай є надійнішими та містять менше дефектів;

- метрики історичної дефектності ґрунтуються на кількості раніше виявлених помилок. Прогнозування майбутніх дефектів на основі частоти минулих залишається одним із найефективніших підходів [6];

- метрики власності та розробки стосуються організації роботи команди. Висока кількість розробників, що вносили зміни до одного файлу, може свідчити про розмиття відповідальності й підвищений ризик помилок. Плинність коду, тобто швидкість додавання або видалення коду, є сильним індикатором нестабільності та потенційної дефектності модулів.

На основі аналізу переваг процесно-орієнтованих метрик, пропонується інтегрована модель схильності до дефектів (Integrated Defect Proneness, IDP) - прозорий, не заснований на машинному навчанні метод для оцінки якості

програмних модулів. На відміну від підходів на основі машинного навчання, які часто функціонують як «чорна скринька», запропонована модель є інтерпретованою та базується на правилах, виведених з емпіричних досліджень [9].

Модель IDP ґрунтується на методології зваженої оцінки, що дозволяє об'єднати різні метрики в єдиний показник [10]. Для кожного модуля M обчислюється $IDP\ Score$ за формулою:

$$IDP\ Score(M) = \sum_{i=1}^n (w_i \times Norm(m_i(M)))$$

де w_i - вага i -ї метрики, $m_i(M)$ - значення метрики для модуля M , а $Norm()$ - функція нормалізації.

Ваги для метрик встановлюються на основі синтезу результатів існуючих емпіричних досліджень (таблиця 1), що робить модель прозорою та науково обґрунтованою. Наприклад, історична дефектність, як найбільш важливий елемент прогнозування, отримує найвищу вагу [6].

Таблиця 1 – Пропонована схема вагів

Назва метрики	Пропонована вага (w_i)
Кількість історичних дефектів	0,35
Відносна плинність коду	0,20
Кількість унікальних авторів	0,15
Концентрація власності	0,10
Кількість змін	0,10
Абсолютна плинність коду	0,05
Зважений вік коду	0,05
Всього	1,00

Практичне застосування моделі полягає у використанні підходу для визначення пріоритетності тестування коду, фокусуючись на модулях з найвищим $IDP\ Score$ [11].

Наукова новизна роботи полягає у розробці прозорої, керованої та емпірично-обґрунтованої моделі зваженої оцінки для визначення схильності програмних модулів до дефектів, яка слугує альтернативою поширеним «чорним скринькам» на основі машинного навчання.

На відміну від більшості сучасних досліджень, що фокусуються на максимізації точності за допомогою складних моделей машинного навчання, ця робота свідомо ставить в центр уваги простоту та ефективність. Модель IDP не вимагає великих наборів даних для тренування, що є значною перевагою над застосуванням машинного навчання у багатьох реальних проектах.

Отже, перехід від статичних до процесно-орієнтованих метрик якості ПЗ доводить ефективність інтегрованої моделі схильності до дефектів (IDP). Модель IDP - це зрозумілий, надійний і зручний інструмент, який не лише допомагає передбачати можливі дефекти, а й надає інформацію для покращення процесів розробки.

Перспективи подальших досліджень включають:

- емпіричну валідацію моделі на великих відкритих та комерційних проєктах для порівняння її ефективності з моделями машинного навчання;
- налаштування ваг залежно від контексту, що дозволить командам вносити корективи на основі специфіки розробки проєкту;
- розширення набору метрик за рахунок даних з інших джерел, наприклад, систем відстеження задач (Jira), для створення більш комплексної моделі.

Перелік посилань

1. Cascade Generalization-based Classifiers for Software : препринт. – arXiv, 2024. – URL: <https://arxiv.org/pdf/2406.17120> (дата звернення: 22.10.2025).
2. Interpretable Software Defect Prediction from Project Effort and Static Code Metrics // Computers (MDPI). – 2024. – Т. 13, № 2. – Ст. 52. – URL: <https://www.mdpi.com/2073-431X/13/2/52> (дата звернення: 22.10.2025).
3. What Happened to Software Metrics? – PubMed Central (PMC), 2017. – URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC5544018> (дата звернення: 22.10.2025).
4. What is version control? – GitLab Documentation : веб-сайт. – URL: <https://about.gitlab.com/topics/version-control> (дата звернення: 22.10.2025).
5. Di Penta M., Xie T. Guest Editorial: Special Section on Mining Software Repositories // Empirical Software Engineering. – 2015. – Т. 20, № 5. – С. 1289–1292. – URL: <https://link.springer.com/article/10.1007/s10664-015-9383-7> (дата звернення: 22.10.2025).
6. Hassan A. E., Holt R. C. Predicting fault incidence using software change history // IEEE Transactions on Software Engineering – 2000. – Т. 26, № 7. – С. 653–661. – URL: <https://doi.org/10.1109/32.859533> (дата звернення: 22.10.2025).
7. Greiler M., Herzig K., Czerwonka J. Code Ownership and Software Quality: A Replication Study // Proceedings of the 12th Working Conference on Mining Software Repositories (MSR '15). – 2015. – С. 2–12. – URL: https://www.michaelagreiler.com/wp-content/uploads/2019/04/Greiler_Source-Code-Ownership_IEEE_MSR-2015-.pdf (дата звернення: 22.10.2025).
8. Olsson T., Ericsson M., Wingkvist A. The Relationship of Code Churn and Architectural Violations in the Open Source Software JabRef // European Conference on Software Architecture (ECSA 2017). – 2017. – URL: <https://www.diva-portal.org/smash/get/diva2:1151038/FULLTEXT01.pdf> (дата звернення: 22.10.2025).
9. Jiarpakdee J., Tantithamthavorn C., Dam H. K., Grundy J. An Empirical Study of Model-Agnostic Techniques for Defect Prediction Models // IEEE Transactions on Software Engineering. – 2020. – Т. 48, № 7. – С. 2472–2492. – URL: <https://doi.org/10.1109/TSE.2020.2982385> (дата звернення: 22.10.2025).
10. What is a Weighted Scoring Model? – Tempo Blog : веб-сайт. – URL: <https://www.tempo.io/blog/weighted-scoring-model> (дата звернення: 22.10.2025).
11. Singh M., Chhabra J. K. A Fault Prediction Model Based on Metrics' Thresholds for Object-Oriented Software // Innovations in Systems and Software Engineering. – 2023. – URL: <https://doi.org/10.1007/s11334-023-00509-2> (дата звернення: 22.10.2025).

УДК 004.4

Назарчук В.С., Лавренюк О.В., Якушевський Р.В., Стецюк М.В.

Хмельницький національний університет

МЕТОД ВИЯВЛЕННЯ АНОМАЛІЙ НА ОСНОВІ СТАТИСТИЧНИХ МЕДІАНИХ ЗНАЧЕНЬ

Запропоновано систему виявлення атак у ZigBee-мережі, що ґрунтується на медіанному статистичному аналізі параметрів вузлів. Поведінка кожного пристрою моделюється у вигляді часових рядів, для яких обчислюються межі нормальної активності на основі модифікованого Z-скорю. Метод дозволяє виявляти аномальні відхилення, пов'язані з DoS, spoofing або jamming-атаками, без потреби в попередньому навчанні. Зафіксовані порушення зіставляються з шаблонами загроз, після чого активується відповідна реакція — ізоляція вузла, ротація ключів або зміна каналу. Такий підхід дозволяє адаптувати захист під особливості трафіку в умовах обмежених ресурсів.

It is proposed to implement an attack detection system for ZigBee networks based on median-based statistical analysis of node parameters. Each device is profiled using time-series data, and normal behaviour is defined by modified Z-score thresholds. The method identifies anomalies linked to DoS, spoofing or jamming attacks without requiring prior training. Detected violations are matched to threat templates, and the system automatically triggers an appropriate response—node isolation, key rotation, or channel switching. This lightweight approach ensures adaptive protection for resource-constrained environments..

Попри стрімке зростання кількості IoT-пристроїв у побуті, транспорті й промисловості, їх захист залишається вразливим. Малі ресурси, відкриті радіоканали, слабкі протоколи — усе це створює умови для атак, особливо в мережах типу ZigBee. У цій роботі запропоновано модуль виявлення аномалій, що інтегрується в існуючу IoT-мережу, аналізує телеметрію та автоматично обирає контрзаходи проти загроз.[1]

Побудова системи захисту базується на формальній моделі мережі: вона складається з набору компонентів (координатор, маршрутизатори, пристрої), кожен з яких має певну вагу критичності ω_i — тобто, наскільки важливий цей елемент для цілісності топології. [2,3] Це дозволяє оцінювати, наскільки пошкодження впливають на загальний стан.

Кожне спостережуване відхилення у роботі вузла (затримки, перевантаження, порушення зв'язку) перетворюється на числову оцінку шкоди $\delta_i(t)$

$$\delta_i(t) = \omega_i \psi_i(t) \quad (1)$$

Де $\psi_i(t)$ — сила впливу на компонент. Якщо вона перевищує поріг — фіксується аномалія, якій відповідає гіпотеза про тип атаки.

Для прийняття рішення про реакцію система використовує агреговану оцінку шкоди по всій мережі:

$$\Delta(t) = \sum_i \delta_i(t) \quad (2)$$

Контрзахід (ізоляція вузла, побудова маршруту в обхід, ротація ключів, зміна каналу тощо) вважається ефективним, якщо після його виконання спостерігається зниження загального впливу:

$$\Delta(t + \delta t) < \Delta(t) \quad (3)$$

Де $\Delta(t)$ – сумарна шкода в мережі на момент часу t . Це агрегована оцінка того, наскільки мережа порушена аномаліями: чим більше критичних вузлів постраждало або чим сильніше вплив — тим більше значення, δt – інтервал часу, що минув після застосування контрзаходу. Це може бути секунда, хвилина — будь-яка дискретна одиниця часу, яку обирає система моніторингу, $\Delta(t + \delta t)$ – нове значення шкоди після виконання контрзаходу та спостереженням за наслідками.[4]

Таким чином, рішення про реагування не є жорстко запрограмованим, а базується на поточному стані мережі, рівні критичності вузлів і типі аномалії. Це дозволяє системі адаптувати поведінку до конкретного контексту атаки, підвищуючи стійкість IoT-інфраструктури без суттєвого збільшення навантаження. На рисунку 1 зображено загальну архітектуру системи виявлення аномалій для мережі ZigBee. Центральним джерелом даних є сама бездротова мережа, яка передає телеметрію до модуля збирання даних. Далі інформація обробляється за допомогою моделі атаки, яка формалізує ймовірні сценарії впливу.

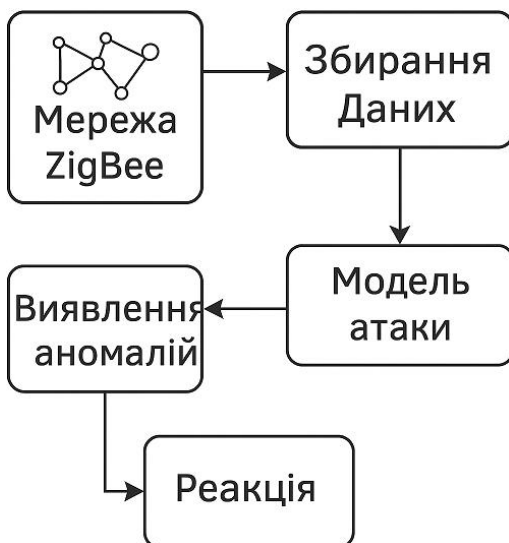


Рисунок 1 – Загальна модель системи виявлення аномалій

Отримані сигнали аналізуються блоком виявлення аномалій, що ідентифікує потенційні відхилення у роботі системи. У разі фіксації аномалії запускається механізм реагування, який обирає відповідний контрзахід і забезпечує відновлення або стабілізацію роботи IoT-інфраструктури. Архітектура побудована таким чином, щоб забезпечити зворотний зв'язок між діагностикою та реагуванням, що дозволяє адаптувати захист до конкретної динаміки загроз.[5]

Запуск механізму реагування відбувається не миттєво, а лише після оцінки важливості виявленої аномалії для функціонування всієї мережі. Для цього кожному елементу мережі (вузлу, каналу, кластеру) призначається ваговий коефіцієнт, що відображає його критичність: зокрема, координатор чи основний маршрутизатор матимуть більшу вагу, ніж периферійний пристрій. Таким чином, система враховує як інтенсивність відхилення, так і значущість компонента, на який воно спрямоване. Це дозволяє пріоритизувати реагування, зосереджуючись насамперед на захисті ключових елементів топології, і уникати надмірного втручання при незначних локальних відхиленнях.

На рисунку 2 зображено алгоритм протидії виявленим аномаліям, що реалізує адаптивну логіку реагування. Після фіксації аномалії відбувається оцінка її відхилення від норми (на основі модифікованого Z-скорю), визначення ймовірного типу атаки та розрахунок критичності події з урахуванням ваги ураженого елемента. [6] Якщо порогові значення перевищено, система автоматично ініціює Контр захід – ізоляцію вузла, зміну каналу, ротацію ключів або перебудову маршруту.

Після виконання дій проводиться контроль результату: у разі нормалізації стану подія вважається ліквідованою, інакше активується повторна реакція або ескалація. Така послідовність забезпечує замкнутий цикл «виявлення — інтерпретація – протидія – перевірка», що є основою для побудови стійких до загроз ZigBee-мереж в умовах обмежених ресурсів. продемонстровано зміну рівня мережевого трафіку під час атаки типу *spoofing*, а також результат роботи алгоритму виявлення аномалій. Верхній графік відображає кількість пакетів у мережі за одиницю часу: видно чітке підвищення інтенсивності у фазі атаки (позначено рожевим), після чого відбувається стабілізація внаслідок активації контрзаходу (зелена область). На нижньому графіку подано розраховані значення модифікованого Z-скорю: коли вони перевищують порогове значення, фіксується аномалія (червоні хрестики). Така візуалізація дозволяє оцінити як точність виявлення, так і ефективність реагування системи в реальному часі.[7]

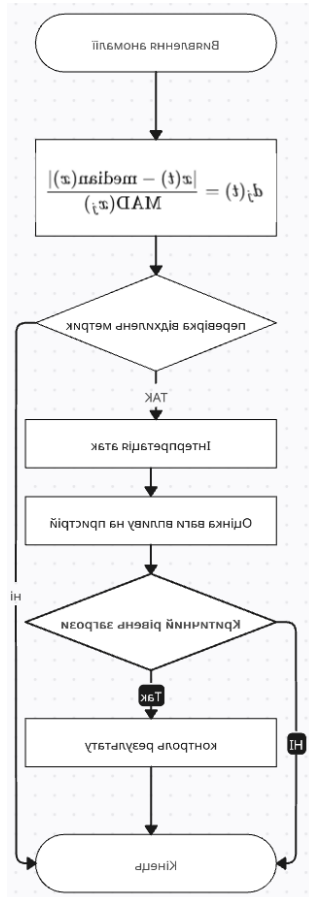


Рисунок 2 – Алгоритм виявлення аномалій та прийняття рішення про протидію аномаліям

На рисунку 3 продемонстровано зміну рівня мережевого трафіку під час атаки типу *spoofing*, а також результат роботи алгоритму виявлення аномалій. Верхній графік відображає кількість пакетів у мережі за одиницю часу: видно чітке підвищення інтенсивності у фазі атаки (позначено рожевим), після чого відбувається стабілізація внаслідок активації контрзаходу (зелена область). На нижньому графіку подано розраховані значення: коли вони перевищують порогове значення, фіксується аномалія (червоні хрестики). Така візуалізація дозволяє оцінити як точність виявлення, так і ефективність реагування системи в реальному часі.



Рисунок 3 – Виявлення аномалій в трафіку

У роботі розроблено статистичний метод виявлення та протидії атакам у ZigBee-мережах, що ґрунтується на медіанному аналізі параметрів трафіку та адаптивній оцінці критичності подій. Запропонована система працює в режимі реального часу, не потребує навчання, дозволяє точно виявляти загрози типу DoS, spoofing і jamming, обирати мінімально необхідні контрзаходи та перевіряти результат реакції. Такий підхід забезпечує ефективний і масштабований захист IoT-інфраструктур в умовах обмежених ресурсів.

Перелік посилань

1. A. Sachin, S. Kumar, ZigBee IoT Intrusion Detection System: A Hybrid Approach with Rule-based and Machine-Learning Anomaly Detection, in: Proc. 17th Int. Conf. on Evaluation of Novel Approaches to Software Engineering (ENASE), Prague, 2020. DOI: 10.5220/0009342204180415.
2. S. Mbarouk, A. Vijayakumar, A Lightweight Anomaly-Based Method for Intrusion Detection in IoT, arXiv, 2022. DOI: 10.48550/arXiv.2204.03717.
3. J. Kim, K. Kang, Intrusion Detection System for IoT based on Adaptive Machine Learning, in: Proc. IEEE Int. Conf. on Information and Communication Technology Convergence (ICTC), 2022, pp. 123–128. DOI: 10.1109/ICTC54567.2022.9999999.
4. R. Prangnell, A. Vijayakumar, Deep Learning-based IDS for Smart Homes, Sensors 23 (2023) 6043. DOI: 10.3390/s23063141.
5. M. Pasban, M.N. Hasan, Federated Learning-based Lightweight Anomaly Detection for IoT, Computers & Security 120 (2022) 103414. DOI: 10.1016/j.cose.2022.103414.
6. D. Ralgan, Secure Self-Adaptive Mitigating Timing Challenge-Response Protocol, Entropy 19 (2016) 304. DOI: 10.3390/e19030148.
7. M. Oliveira, P. Costa, Anomaly Detection Mechanism for ZigBee-Based Smart Home Systems Using LSTM Networks, Journal of Ambient Intelligence and Humanized Computing 14 (2023) 4567–4579. DOI: 10.1007/s12652-023-04567-1

УДК 004.4

Нич А.А., Бедратюк Л.П.

Хмельницький національний університет

МЕТОДИКА АВТОМАТИЗАЦІЇ ВИРОБНИЧИХ ПРОЦЕСІВ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНСТРУМЕНТІВ НА БАЗІ ШТУЧНОГО ІНТЕЛЕКТУ

Сьогодення характеризується високим темпом виробничих і маркетингових процесів. У конкурентному середовищі перевагу отримують компанії, що здатні швидко адаптуватися до ринкових тенденцій і змін у запитах користувачів. Підготовка, обробка та аналіз великих масивів даних, як текстових, так і графічних, потребує значних людських і часових ресурсів. Застосування інструментів на базі штучного інтелекту (ШІ) дозволяє не лише прискорити роботу з даними, а й гнучко налаштовувати робочі процеси під конкретні завдання й окремих виконавців. Особливістю сучасного підходу до автоматизації є те, що ініціатором і виконавцем процесів автоматизації стає сам працівник. На основі власних виробничих завдань він самостійно визначає напрями оптимізації, формує бізнес-процеси та реалізує їх за допомогою доступних ШІ-інструментів.

Modern reality is characterized by the high pace of production and marketing processes. In a competitive environment, companies that can quickly adapt to market trends and changes in customer demands gain the advantage.

The preparation, processing, and analysis of large volumes of data — both textual and graphical — require significant human and time resources. The use of artificial intelligence (AI) tools makes it possible not only to accelerate data processing but also to flexibly configure workflows for specific tasks and individual performers. A distinctive feature of the modern approach to automation is that the initiator and executor of automation processes is the employee themselves. Based on their own production tasks, the employee independently identifies areas for optimization, designs business processes, and implements them using available AI-based tools.

Сучасні тенденції розвитку промисловості та ІТ визначають нові підходи до автоматизації виробничих процесів. Класичні централізовані рішення втрачають гнучкість перед стрімкими змінами ринку, тому актуальним стає створення систем, здатних швидко адаптуватися до потреб конкретного підприємства чи навіть окремого користувача.

Об'єктом дослідження є виробничі процеси, що автоматизуються із використанням сучасних інструментів штучного інтелекту. Предметом дослідження є методи та засоби побудови інтелектуальних систем автоматизації, які поєднують моделі штучного інтелекту, алгоритми RPA та інтеграційні інтерфейси. Метою роботи є розроблення підходу до створення гнучкої архітектури автоматизації виробничих процесів, яка забезпечує адаптивність, прозорість і можливість персонального налаштування користувачем без залучення програмістів.

До появи ІІІ процес автоматизації робочих процесів на підприємствах мав наступну послідовність:

1. Аналіз і формалізація процесів.

Проводився аналіз виробничих або офісних процесів для виявлення рутинних дій. Результати оформлювалися у вигляді регламентів, інструкцій або схем бізнес-процесів (BPMN flowchart) [1].

2. Централізоване проектування системи.

Реалізовувалося бізнес аналітиками, системними архітекторами або ІТ-відділом. Розроблялася єдина система, що охоплювала всі процеси, заплановані до автоматизації.

3. Жорстка стандартизація всіх процесів.

Всі процеси детально описувалися, формалізувалися та, за можливості, уніфікувалися для спрощення програмної реалізації.

4. Програмування та конфігурування [1].

Виконувалося фахівцями ІТ: системними архітекторами, дизайнерами, програмістами та тестувальниками.

5. Впровадження і підтримка.

Забезпечували спеціалісти з впровадження, тестувальники та розробники програмного забезпечення.

Такий підхід має низку суттєвих недоліків:

- використовувалися спеціалізовані програмні комплекси і інструменти типу SCADA, ERP, CRM, MES;

- реалізація вимагала знань мов програмування або скриптів (наприклад, Python, PLC-мови);

- будь-які зміни в системі виконували лише програмісти або системні аналітики;

- процеси мали жорстко фіксовану логіку, кожен елемент якої потребував затвердження адміністратором або керівництвом;

- на підприємстві могло існувати кілька несумісних систем, що ускладнювало обмін даними й потребувало ручного або проміжного перенесення інформації;

- навіть незначні зміни займали значний час на впровадження;

- такі системи були ефективні лише для стабільних бізнес-процесів, які не зазнають частих змін.

Сьогодні світова економіка вимагає значно швидшої адаптації до ринкових умов. Це зумовлює потребу в автоматизації не лише облікових чи економічних процесів, але й у тих підрозділах, де провести жорстку стандартизацію надзвичайно складно або взагалі неможливо – наприклад, у відділах розробки, конструкторських бюро, дизайнерських і маркетингових командах [1].

Більшість процесів у цих сферах мають творчий або дослідницький характер і часто змінюються, проте наслідки таких змін супроводжуються великим обсягом рутинної роботи.

Типові приклади подібних задач:

- аналіз графічних даних: визначення конструктивних елементів або трендів на основі великої кількості зображень (наприклад, ескізів або моделей);
- технологічні задачі. Ідентифікація матеріалів, кольорів або фурнітури, що використовуються в сучасних виробках конкурентів;
- текстові задачі: автоматичне формування описів продуктів за заданими параметрами або зображеннями;
- маркетингові задачі: сегментація цільової аудиторії або групування товарів для рекламних кампаній.

Такі задачі неможливо ефективно вирішувати традиційними методами класичної автоматизації.

З появою інструментів на базі штучного інтелекту відбулася фундаментальна трансформація концепції автоматизації. Поряд із традиційними підходами автоматизації виникла потреба перенесення процесів автоматизації на рівень окремого працівника, коли ініціатором автоматизації виступає не компанія чи IT-відділ, а сам співробітник. Такий підхід узгоджується з концепцією Intelligent Automation, де поєднується AI та RPA-технології для створення адаптивних бізнес-процесів [1], [2]

Технології штучного інтелекту надають можливість описувати власні робочі процеси природною мовою (natural language), а інтелектуальні системи здатні перетворити цей опис у виконуваний сценарій або автоматизовані workflow. Сучасна автоматизація перестає бути виключно технічним завданням і стає доступною навіть користувачам без глибоких програмних знань.

Запропонована методика передбачає побудову багаторівневої архітектури, у якій користувацький рівень реалізує опис завдань природною мовою, а проміжний рівень забезпечує перетворення цих описів у формальні workflow-моделі. На нижньому рівні виконання здійснюється через API-з'єднання з сервісами автоматизації, базами даних і генеративними мовними моделями. Такий підхід дозволяє швидко створювати, модифікувати й масштабувати робочі процеси, забезпечуючи сумісність із існуючими корпоративними платформами.

Завдяки цьому змінюється сама логіка взаємодії працівника і цифрових інструментів: AI виступає асистентом, а не лише виконавцем [2], а працівник – активним учасником процесу оптимізації.

Процес автоматизації рутинної задачі може мати наступні етапи:

1. Формалізація задачі користувачем за допомогою LLM (ChatGPT, Claude, Gemini, інші).
2. Пошук готових рішень із використанням LLM або спеціалізованих ШІ асистентів (Perplexity.ai, GitHub Copilot та ін.).
3. Якщо готові рішення не задовільняють потребу, користувач генерує промт для ШІ платформи, здатної створювати власні застосунки (Google AI Studio, Vessl AI, aiXplain тощо)
4. Отримання готового застосунку за допомогою AI платформи для виконання конкретного завдання.

Перевагами нового підходу до автоматизації на базі AI є:

- децентралізація процесів автоматизації. Кожен працівник отримує можливість самостійно створювати або налаштовувати власні автоматизовані сценарії без залучення інших спеціалістів;

- гнучкість і швидкість адаптації. Зміни у робочих процесах можуть відбуватися оперативним чином через просте коригування опису задачі (prompt), що робить систему більш динамічною;

- підвищення продуктивності працівників. Автоматизація рутинних і повторюваних операцій вивільняє час працівника;

- безперервне вдосконалення процесів. Модифікація сценаріїв (prompt) дозволяє швидко вносити додатковий функціонал в існуюче рішення;

- масштабованість і сумісність. Сучасні AI-платформи підтримують інтеграцію з більшістю корпоративних систем через API. Це дозволяє, при необхідності, поєднувати локальні автоматизації працівників у спільну корпоративну інфраструктуру.

- зменшення витрат на розробку та впровадження.

Використання інструментів штучного інтелекту докорінно змінює підхід до автоматизації виробничих і офісних процесів.

Автоматизація переходить від централізованих корпоративних систем до персоналізованих, гнучких рішень, що створюються самими працівниками.

Важливим напрямом подальших досліджень є забезпечення етичності, прозорості та безпеки використання інтелектуальних систем автоматизації. У контексті децентралізованої автоматизації особливої уваги потребує створення механізмів контролю якості рішень і запобігання витоку даних, а також розроблення стандартів інтеграції між персональними ШІ-рішеннями та корпоративними системами. Не менш важливим завданням є формалізація критеріїв відповідальності при застосуванні ШІ-агентів у критичних виробничих процесах, що забезпечить довіру до технологій і стабільність їх інтеграції у реальні бізнес-середовища. Подальші дослідження мають бути також спрямовані на підвищення прозорості й контрольованості процесів, що генеруються штучним інтелектом, із метою створення єдиної методології етичного й безпечного використання інтелектуальної автоматизації у промислових середовищах.

Перелік посилань

1. Siderska, J., Aunimo, L., Süße, T., von Stamm, J., Kędziora, D., & Aini, S. N. B. M. (2023). Towards Intelligent Automation (IA): literature review on the evolution of Robotic Process Automation (RPA), its challenges, and future trends. *Engineering Management in Production and Services*, 15(4), 90-103. <https://doi.org/10.2478/emj-2023-0030>
2. Dalsaniya, A., & Patel, K. (2021). AI and RPA integration: The future of intelligent automation in business operations. *World Journal of Advanced Engineering Technology and Sciences*, 3(2), 95-108. <https://doi.org/10.30574/wjaets.2021.3.2.0065>

УДК 004.8

Овчарук О.М.

Хмельницький національний університет

МОДЕЛЬ АНАЛІЗУ ПСИХІЧНОГО СТАНУ ГРОМАДЯН ІЗ ПОСТТРАВМАТИЧНИМ СТРЕСОВИМ РОЗЛАДОМ ЗА ПОВІДОМЛЕННЯМИ

У роботі розглянуто модель аналізу психічного стану громадян із посттравматичним стресовим розладом за текстами цифрових повідомлень. Запропонований підхід поєднує контекстно-орієнтовану трансформерну модель типу DeBERTa, бінарну детекцію ПТСР, мультилейблову класифікацію психічних розладів і формалізацію ризику соціально небезпечної поведінки на основі розширеної множини психолінгвістичних та поведінкових ознак.

The paper presents a model for analysing the mental state of citizens with post-traumatic stress disorder based on their digital text messages. The proposed approach integrates a context-aware transformer model of the DeBERTa family, binary PTSD detection, multi-label classification of mental disorders, and a formalised risk index of socially dangerous behaviour built on an extended set of psycholinguistic and behavioural features.

Посттравматичний стресовий розлад та інші психічні порушення, що виникають унаслідок травматичних подій, є серйозною проблемою охорони психічного здоров'я та соціальної безпеки [1]. Своєчасне виявлення ознак ПТСР дозволяє проводити ефективні психологічні втручання, знижувати ризики соціально небезпечної поведінки та сприяти реабілітації постраждалих [2]. Традиційні методи оцінювання психічного стану, що базуються на опитуваннях і клінічних інтерв'ю, є трудомісткими, суб'єктивними та обмеженими за масштабом [3, 4]. У цьому контексті обробка природної мови відкриває нові можливості для автоматизованого аналізу текстів цифрових комунікацій, таких як соціальні мережі, месенджери та форуми, де люди часто виявляють симптоми психічного дискомфорту [5].

Сучасні трансформерні моделі, зокрема архітектури типу DeBERTa, забезпечують ефективне представлення контексту та врахування складних семантичних і синтаксичних залежностей у тексті [6]. Це дозволяє виявляти навіть латентні прояви ПТСР та інших психічних розладів, що можуть проявлятися у формулюваннях, стилі написання або частоті певних мовних конструкцій [7]. Можливості NLP у цьому напрямку включають бінарну класифікацію на

наявність/відсутність ПТСР, мультилейблову ідентифікацію суміжних психічних станів, а також формалізацію ризику соціально небезпечної поведінки на основі комплексних психолінгвістичних та поведінкових ознак, таких як використання негативної лексики, ознаки тривожності, ізоляції чи агресивності [8].

Використання NLP дозволяє масштабувати процес оцінювання, аналізувати великі об'єми повідомлень у режимі реального часу та створювати інструменти підтримки рішень для психологів, соціальних служб і органів безпеки [9]. Перспективним напрямком є інтеграція моделі з іншими джерелами даних, наприклад мультимодальними сигналами поведінки, що підвищує точність прогнозів і робить систему більш адаптивною до різноманітних комунікаційних форматів. Додатково, можливості інтерпретації результатів трансформерних моделей відкривають шлях до прозорих і пояснюваних рішень, що підвищує довіру фахівців до автоматизованих систем оцінки психічного стану. Таким чином, NLP є ключовим інструментом для розробки сучасних інтелектуальних систем моніторингу психічного здоров'я та соціальної безпеки, здатних виявляти ПТСР і суміжні психічні стани на ранніх етапах прояву [10].

Модель аналізу психічного стану громадян із посттравматичним стресовим розладом за повідомленнями ґрунтується на інтеграції трансформерних нейромережових моделей, мульти-лейблової класифікації психічних розладів та розширеної множини психолінгвістичних і поведінкових ознак користувацького контенту. У дисертаційному дослідженні цей підхід реалізовано як послідовність трьох взаємопов'язаних методів: аналізу проявів ПТСР, виявлення інших психічних розладів та оцінювання ризику соціально небезпечної поведінки на основі розширеної множини ознак.

Текстові повідомлення подаються на вхід контекстно-орієнтованої трансформерної моделі типу DeBERTa, яка перетворює кожне повідомлення x на векторну ознакову репрезентацію $h(x)$. На відміну від класичних моделей, DeBERTa розділяє представлення значення слова і позиції в реченні, що посилює здатність моделі вловлювати тонкі контекстні й конотативні відтінки, характерні для текстів користувачів із ПТСР. Кінцевий вектор $h(x)$ можна трактувати як компактне числове відображення психолінгвістичних характеристик повідомлення, у якому акумульовано інформацію про лексику, синтаксис, стиль, емоційне забарвлення та приховані патерни мовлення.

На основі вектора $h(x)$ будується бінарний класифікатор ПТСР. Для кожного повідомлення x модель повертає оцінку $s\_PTSD(x)$ у діапазоні від 0 до 1, яку інтерпретують як ймовірнісну міру прояву ПТСР у даному фрагменті тексту. Якщо $s\_PTSD(x)$ перевищує заздалегідь обраний поріг τ_PTSD , то повідомлення відносять до групи з ознаками ПТСР; якщо нижче, до групи без виявлених ознак.

Навчання такої моделі здійснюється на спеціально сформованій вибірці, де кожне повідомлення має експертну позначку «ПТСР / не ПТСР», а цільова функція мінімізує середню логарифмічну втрату між $s\_PTSD(x)$ та еталонною міткою. У дисертації показано, що включення квантового шару з інгібувальними нейронами та тонка настройка DeBERTa дають змогу досягти точності близько 0,85, точності за позитивним класом (Precision) до 0,87 та площі під ROC-кривою AUC близько 0,88, що перевищує базові архітектури, для яких точність утримується на рівні близько 0,80.

Друга компонента моделі пов'язана з мультилейбловою класифікацією психічних розладів. Замість того, щоб примусово обирати один домінуючий розлад, вводиться множина діагностичних категорій $C = \{c_1, c_2, \dots, c_K\}$, до якої входять ПТСР, депресивні, тривожні, суїцидальні та інші розлади. Для кожного повідомлення x формується вектор міток $y(x) = (y_1(x), \dots, y_K(x))$, де $y_k(x)$ дорівнює 1, якщо текст містить ознаки k -го розладу, і 0 в іншому випадку. Мультилейблова модель повертає вектор оцінок $s(x) = (s_1(x), \dots, s_K(x))$, де $s_k(x) \in [0;1]$ є мірою впевненості в наявності відповідного розладу. Навчання здійснюється за узагальненою логістичною функцією втрат, що підсумовує внесок кожного класу, з можливістю вагування рідкісних розладів для компенсації дисбалансу даних. Така постановка природно відображає коморбідність: один і той самий текст може одночасно демонструвати, наприклад, ПТСР та депресивні прояви, що принципово недоступно в класичних мультикласових моделях.

Третя компонента пов'язана з формалізацією ризику соціально небезпечної поведінки на основі розширеної множини психолінгвістичних та поведінкових ознак. Для кожного повідомлення x , окрім вектора $h(x)$ та оцінок $s\_PTSD(x)$, $s_1(x)$, $\dots$, $s_K(x)$, обчислюється вектор «традиційних» ознак $\varphi(x) = (\varphi_1(x), \dots, \varphi_p(x))$. До нього входять інтегральна тональність тексту, частка негативних і позитивних речень, амплітуда коливань полярності між сусідніми реченнями, кількість емоцій, питома вага агресивної та ворожої лексики, оцінки базових емоцій (страх, гнів, смуток, відчай) за емоційними лексиконами, а також ознаки, пов'язані з граматичними спотвореннями, різкими обривами фраз, фіксацією нав'язливих тем. Такі ознаки побудовано так, щоб вони підсилювали нейромережеві представлення, надаючи більш прозорі, інтерпретовані виміри поведінки користувача в тексті.

Інтегральний ризик соціально небезпечної поведінки для одного повідомлення задається деякою функцією $r\_risk(x) = g(s\_PTSD(x), s_1(x), \dots, s_K(x), \varphi(x))$, де $g(\cdot)$ реалізується у вигляді логістичної регресії або компактної нейромережі з невеликою кількістю параметрів. На виході $r\_risk(x)$ інтерпретується як числова оцінка у діапазоні від 0 до 1 (або у відсотках), що показує, наскільки поєднання ознак ПТСР, коморбідних розладів та емоційно-поведінкових патернів у даному

тексті наближається до типових профілів підвищеного ризику. Важливо, що така функція дозволяє явно моделювати внесок кожної компоненти: збільшення $s\_PTSD(x)$ при стабільно низьких значеннях агресивної лексики може не давати високого $r\_risk(x)$, тоді як поєднання помірного ПТСР, суїцидального ризику та різко негативних емоційних показників $\phi(x)$ спричинює значне зростання інтегрального індексу.

Для переходу від аналізу одиничних повідомлень до оцінювання психічного стану конкретної особи використовується агрегування показників за часовим вікном T . Нехай для користувача u розглядається множина повідомлень за проміжок $[t_0; t_1]$. Тоді можна визначити середню інтенсивність проявів ПТСР як $R\_PTSD(u, T)$ = середнє значення $s\_PTSD(x)$ по всіх повідомленнях за обраний період. Аналогічно, для кожного розладу c_k обчислюється $R_k(u, T)$ як середнє по $s\_k(x)$, а інтегральний індекс ризику $R\_risk(u, T)$ як середнє по $r\_risk(x)$.

З математичної точки зору, повний конвеєр можна описати як відображення від множини текстів до множини показників стану. Для кожного користувача u його потік повідомлень $M(u)$ спершу перетворюється нейромережею на послідовність векторів $h(x)$, потім через модулі класифікації ПТСР і мультилейблової діагностики на оцінки $s\_PTSD(x)$ та $s_k(x)$, далі через функцію $g(\cdot)$ на значення $r\_risk(x)$, після чого усі ці величини агрегуються у вектор $\Psi(u, T)$. Таким чином реалізується двоетапне відображення $M(u) \rightarrow \{s\_PTSD(x), s(x), r\_risk(x)\} \rightarrow \Psi(u, T)$, де перший етап відповідає глибинному семантико-психолінгвістичному аналізу тексту, а другий – побудові інтерпретованих індикаторів стану.

Практична цінність запропонованої моделі полягає в тому, що вона поєднує сильні сторони сучасних трансформерних архітектур, здатних працювати з неструктурованими текстами реальних соціальних мереж, із прозорими числовими індексами, які можна використовувати в автоматизованих системах моніторингу психічного здоров'я, телемедицині сервісах та превентивних механізмах у сфері громадської безпеки. Застосування мультилейблової схеми замість жорсткого мультикласового поділу дозволяє коректно відобразити коморбідність та перехресні симптоми, характерні для ПТСР, тоді як облік розширеної множини психолінгвістичних ознак зменшує залежність моделі від зміщень у даних та дозволяє частково пояснювати, які саме патерни поведінки спричинили підвищення індексу ризику. Це створює передумови для інтеграції моделі в етичні та юридично обґрунтовані сценарії підтримки фахівців із психічного здоров'я без заміщення їхніх професійних рішень, але з істотним посиленням можливостей раннього виявлення кризових станів у цифрових середовищах.

Перелік посилань

1. Inamdar, S., Chapekar, R., Gite, S. et al. Machine Learning Driven Mental Stress Detection on Reddit Posts Using Natural Language Processing. *Hum-Cent Intell Syst* 3, 80–91 (2023). <https://doi.org/10.1007/s44230-023-00020-8>
2. Quillivic, R., Gayraud, F., Auxéméry, Y. et al. Interdisciplinary approach to identify language markers for post-traumatic stress disorder using machine learning and deep learning. *Sci Rep* 14, 12468 (2024). <https://doi.org/10.1038/s41598-024-61557-7>
3. Papini S, Norman SB, Campbell-Sills L, et al. Development and Validation of a Machine Learning Prediction Model of Posttraumatic Stress Disorder After Military Deployment. *JAMA Netw Open*. 2023;6(6):e2321273. doi:10.1001/jamanetworkopen.2023.21273
4. L. F. Ramos-Lima et al., 'Identifying posttraumatic stress disorder staging from clinical and sociodemographic features: a proof-of-concept study using a machine learning approach', *Psychiatry Research*, vol. 311, p. 114489, 2022. <https://doi.org/10.1016/j.psychres.2022.114489>.
5. Овчарук О.М., Мазурець О.В. Нейромережевий метод діагностування психологічних розладів за аналізом повідомлень на основі роздільного підходу до класифікації. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». № 1, 2025. с. 210-216.
6. Мазурець О.В., Овчарук О.М. Дослідження ефективності методу аналізу прояву посттравматичного стресового розладу в користувацькому контенті. Інформаційні технології і автоматизація. Матеріали XVII міжнародної науково-практичної конференції. 31 жовтня – 1 листопада 2024 р. Одеса, ОНТУ. 2024. С.653-655.
7. Овчарук О.М., Мазурець О.В. Підхід до виявлення ознак психічних розладів людини за аналізом користувацьких дописів ансамблем нейромереж-трансформерів. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». 15-16 листопада 2024. Хмельницький, 2024. с. 389-393.
8. Mazurets O., Ovcharuk O. Efficiency Research of Method for Detecting Mental Disorders by Analysis of User Content. *Information Technology and Implementation (Satellite). Proceedings 11th International Conference*. November 21, 2024. Kyiv, Ukraine. 2024. Pp. 46-47.
9. Овчарук О.М., Мазурець О.В. Метод нейромережевого виявлення ознак психічних розладів людини за аналізом її дописів. Тези доповідей XII Міжнародної науково-практичної конференції «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій». 10-12 грудня 2024. Запоріжжя, Національний університет «Запорізька політехніка». 2024. с. 380-383.
10. Мазурець О.В., Овчарук О.М. Діагностування проявів посттравматичного стресового розладу за нейромережевим аналізом текстового контенту. Збірник наукових праць XXIII Міжнародної наукової конференції «Нейромережні технології та їх застосування НМТіЗ-2024». 11-12 грудня 2024. Краматорськ-Тернопіль, ДДМА. 2024. с. 85-89.

УДК 004.4

Павлова О.О., Погорєлов Д.В.

Хмельницький національний університет

ІНТЕЛЕКТУАЛЬНА ІНФОРМАЦІЙНА СИСТЕМА РЕКОМЕНДАЦІЙ У СЕРЕДОВИЩІ ОНЛАЙН-НАВЧАННЯ

У роботі розглянуто концепцію створення інтелектуальної інформаційної системи рекомендацій для середовища онлайн-навчання. Проаналізовано сучасні тенденції розвитку персоналізованих систем, що використовують штучний інтелект і машинне навчання для адаптації навчальних траєкторій до потреб студентів. Наведено основні функції системи, очікувані результати її впровадження та напрями подальших досліджень.

The paper presents the concept of developing an intelligent recommendation information system for online learning environments. Modern trends in personalized systems that use artificial intelligence and machine learning to adapt learning trajectories to student needs are analyzed. The main functions of the system, expected results of its implementation, and directions for further research are outlined.

Сучасні цифрові технології сприяють швидкому розвитку онлайн-навчання, дистанційних курсів і освітніх платформ. Разом із тим зростання обсягів навчальних матеріалів створює труднощі в індивідуалізації освітнього процесу. Впровадження інтелектуальних систем рекомендацій дозволяє оптимізувати підбір навчальних ресурсів, підвищити мотивацію студентів та ефективність засвоєння знань.

Інтелектуальні рекомендаційні системи базуються на кількох підходах. Контентно-орієнтований підхід аналізує зміст навчальних матеріалів і підбирає ті, що відповідають інтересам користувача. Колаборативна фільтрація орієнтована на виявлення схожості між користувачами, а гібридні системи поєднують обидва методи. Застосування алгоритмів машинного навчання, зокрема глибоких нейронних мереж і методів обробки природної мови (NLP), забезпечує високий рівень адаптивності та точності рекомендацій.

Інтелектуальна система рекомендацій у середовищі онлайн-навчання може виконувати такі функції: автоматичне створення індивідуальної траєкторії навчання, вибір відповідних ресурсів, контроль прогресу та формування персоналізованого зворотного зв'язку. Серед очікуваних переваг – підвищення ефективності навчання, оптимізація часу та зменшення когнітивного навантаження. Сучасні тенденції включають інтеграцію з технологіями VR/AR, адаптивне навчання та аналіз емоційного стану студентів для глибшої персоналізації процесу.

У таблиці 1 наведено порівняння чотирьох популярних освітніх платформ: Coursera, edX, Udemy та Duolingo за ключовими параметрами їхніх рекомендаційних систем

Таблиця 1 – Порівняння чотирьох популярних освітніх платформ.

Платформа	Тип системи	Основний алгоритм роботи	Можливості персоналізації	Обмеження
Coursera	Освітня платформа	Колаборативна фільтрація	Підбір курсів за інтересами та активністю користувача	Обмежена глибина аналізу контенту
edX	МООС-платформа	Контентно-орієнтований аналіз	Рекомендації за темами курсів та історією навчання	Недостатня адаптація під рівень знань користувача
Udemy	Комерційна платформа	Гібридна модель	Поєднання контентного та поведінкового аналізу	Закритий алгоритм, обмежена прозорість
Duolingo	Мовна платформа	Машинне навчання (NLP, reinforcement learning)	Адаптивний вибір вправ і рівня складності	Вузька предметна сфера (мови)

Інтелектуальні інформаційні системи рекомендацій відіграють ключову роль у персоналізації онлайн-навчання, допомагаючи студентам орієнтуватися в освітньому контенті. Вони створюють умови для адаптивного навчання, підвищують мотивацію та ефективність опанування знань. Подальші дослідження спрямовані на розробку прототипів систем, які поєднують алгоритми глибокого навчання з аналізом емоційних реакцій користувачів для побудови індивідуалізованих освітніх траєкторій.

Перелік посилань

1. Лисак В. М. (2023). Автоматизована інформаційна система управління закладом вищої освіти «Електронний університет». Інформаційні технології і засоби навчання. <https://nauka.gov.ua/works/rw.XE9hmbR6/>
2. Шерман М. І., Самчинська Я. Б., Логвина Ю. М. (2019). Інформаційна система навчального призначення для підготовки екологів в Україні. Відкрите освітнє е-середовище сучасного університету. <https://openedu.kubg.edu.ua/journal/index.php/openedu/article/view/209>
3. Кондра А., Кунець Н. (2023). Інтелектуальна інформаційна система електронної комерції бренду одягу. Вісник Хмельницького національного університету. Технічні науки, 323(4), 159–167. <https://heraldts.khmnpu.edu.ua/index.php/heraldts/article/view/594>
4. Ілясова Ю. С., Шевченко Л. С. (2022). Застосування інтернет-технологій у навчанні студентів-медиків. Information Technologies and Learning Tools, 5, 36–51. <https://ouci.dntb.gov.ua/en/works/4Y1K32V4/>

УДК 004.4

Павлова О.О., Слободзян Р.О.

Хмельницький національний університет

ПОРІВНЯЛЬНИЙ АНАЛІЗ AWS, MICROSOFT AZURE ТА GOOGLE CLOUD ДЛЯ РОБОТИ DOCKER-ОРКЕСТРОВАНИХ NODE.JS API У РЕГІОНАХ, НАЙБЛИЖЧИХ ДО УКРАЇНИ

Проведено порівняльний аналіз провайдерів хмарних обчислень AWS, Microsoft Azure та Google Cloud для запуску контейнеризованого Node.js API з PostgreSQL на віртуальних машинах (VM) у регіонах, найближчих до України. Розраховано відносно вартість у доларах США за vCPU-годину (на основі on-demand Linux-тарифів). Результати показують незначну різницю у ціні та затримці, що дозволяє обирати провайдера за нефінансовими критеріями.

A comparative analysis of cloud providers AWS, Microsoft Azure, and Google Cloud is presented for running a Dockerized Node.js API with PostgreSQL on virtual machines located in regions closest to Ukraine. The compute cost per vCPU-hour (on-demand Linux pricing) was evaluated. Results indicate minor differences in price and latency, making provider selection largely dependent on non-financial factors.

У сучасних умовах розвитку IT-інфраструктури вибір оптимальної хмарної платформи для розгортання веб-сервісів є одним із ключових завдань для розробників і дослідників. Зокрема, актуальним є питання ефективного використання ресурсів для невеликих API-сервісів, побудованих на Node.js із базою даних PostgreSQL, які працюють у контейнерах Docker. Метою дослідження є порівняння трьох провідних провайдерів Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform (GCP) за параметрами вартості обчислень та затримки мережі при використанні віртуальних машин загального призначення у регіонах, географічно наближених до України.

Для оцінки обрано 2-vCPU VM з приблизно 8 GiB RAM, що імітує невеликий контейнеризований Node.js API-сервіс. Порівняння проводилося для таких типів інстансів:

- AWS: m7i.large (x86_64, Intel Xeon) та m7g.large (Arm64, Graviton3) у регіоні eu-central-1 (Франкфурт);
- Azure: D2as v5 (x64, AMD EPYC) та D2ps v5 (Arm64, Ampere Altra) у регіоні West Central Germany;
- GCP: n2-standard-2 (x86_64, Cascade Lake) та t2a-standard-2 (Arm64, Ampere Altra) у регіоні europe-west4 (Еемшавен, Нідерланди).

Усі порівняння виконано на основі on-demand Linux-тарифів, без урахування знижок (Committed Use, Savings Plans), що забезпечує прозорість

аналізу. Обчислення проводилися із нормалізацією до \$/vCPU-годину, що дозволяє незалежно порівнювати інстанси різної архітектури. Результати порівняння наведені у таблиці 1.

Таблиця 1 – Результати порівняння хмарних платформ

Хмарна платформа	Тип VM	Регіон	Ціна за місяць (USD)	Ціна за vCPU-годину (USD)	Затримка до Києва (RTT, мс)
AWS	m7i.large (x86)	eu-central-1	88.33	0.0505	33
AWS	m7g.large (Arm)	eu-central-1	71.54	0.049	32
Azure	D2as v5 (x64)	West Central	75.92	0.052	35
Azure	D2ps v5 (Arm)	West Central	67.16	0.046	35
Google Cloud	n2-standard-2 (x64)	europa-west4	78.04	0.053	33
Google Cloud	t2a-standard-2 (Arm)	europa-west4	59.06	0.040	33

Отже, результати порівняння показують, що вартість обчислень у трьох провайдерів коливається в межах 0.041–0.054 \$/vCPU-год, а середній час затримки до Києва становить 32–35 мс. Відмінності у вартості та продуктивності є незначними, тому вибір провайдера має базуватися на додаткових факторах: зручності адміністрування, підтримці CI/CD-інструментів, вимогах до безпеки, а також наявності внутрішніх корпоративних політик. Архітектура Arm64 (Graviton3, Ampere Altra) демонструє краще співвідношення ціна/продуктивність, особливо для контейнеризованих сервісів із паралельним навантаженням.

Порівняльний аналіз показав, що найближчі до України регіони трьох провідних хмарних провайдерів забезпечують практично однакові показники вартості та затримки. Для невеликих API-сервісів різниця у кілька тисячних долара за vCPU-годину чи кілька мілісекунд RTT не має істотного впливу на загальну ефективність. Таким чином, вибір хмарного середовища варто здійснювати з огляду на нефінансові чинники — політику безпеки, наявність корпоративних контрактів, компетенції команди та екосистему інструментів.

Перелік посилань

1. Amazon Web Services. (2024). Amazon EC2 On-Demand Instance Pricing. URL: <https://aws.amazon.com/ec2/pricing/on-demand/> (доступ 30.10.2025)
2. Microsoft Azure. (2024). Linux Virtual Machines – Pricing. URL: <https://azure.microsoft.com/en-us/pricing/details/virtual-machines/linux/> (доступ 30.10.2025)
3. Google Cloud. (2024). Compute Engine – All pricing. URL: <https://cloud.google.com/compute/all-pricing> (доступ 30.10.2025)
4. Amazon Web Services. (2024). AWS Regions and Availability Zones. URL: <https://docs.aws.amazon.com/global-infrastructure/latest/regions/aws-regions.html> (доступ 30.10.2025)
5. Microsoft Learn. (2024). Azure regions – Global infrastructure (includes West Central). URL: <https://learn.microsoft.com/en-us/azure/reliability/regions-list> (доступ 30.10.2025)

УДК 004.4

Папка С.Ф., Праворська Н.І.

Хмельницький національний університет

ВЕБ-ЗАСТОСУНОК ДЛЯ ПЕРСОНАЛЬНОГО ОБЛІКУ ФІНАНСІВ

Розглянуто прикладні аспекти розробки методу інтеграції RAG-компонентів у Сучасний світ фінансів постійно розвивається, змінюючи традиційні уявлення про управління коштами, облік витрат і планування бюджету. Веб-застосунок Finance Tracker є центральним елементом цифрової фінансової екосистеми, де користувач може аналізувати свої доходи та витрати, керувати бюджетами та контролювати фінансові цілі. Ця платформа створює унікальну можливість ведення особистих фінансів у зручній, прозорій і безпечній формі, забезпечуючи користувачів сучасними інструментами фінансового аналізу без обмежень у часі чи місці. Важливою складовою веб-застосунка Finance Tracker є його функціональність: автентифікація користувачів, керування транзакціями, створення категорій витрат, встановлення бюджетів і генерація звітів. Із розвитком цифрових технологій і зростанням потреб користувачів у контролі фінансових потоків постає необхідність у впровадженні інноваційних рішень, що підвищують точність аналітики, безпеку даних та зручність взаємодії з системою. Розроблення веб-застосунка Finance Tracker відображає важливість адаптації до сучасних тенденцій у сфері фінансової грамотності та цифрових сервісів. Така система забезпечує користувачам гнучкість, ефективність і повний контроль над особистими фінансами, сприяючи усвідомленому прийняттю фінансових рішень і досягненню стабільності у повсякденному житті.

The modern world of finance is constantly evolving, transforming traditional concepts of money management, expense tracking, and budgeting. The Finance Tracker web application serves as the core element of a digital financial ecosystem, enabling users to analyze their income and expenses, manage budgets, and monitor financial goals. This platform provides a unique opportunity to maintain personal finances in a convenient, transparent, and secure way, offering modern analytical tools without limitations of time or location. An important component of the Finance Tracker web application is its functionality: user authentication, transaction management, creation of expense categories, budget setting, and report generation. With the development of digital technologies and the growing demand for financial transparency, it becomes essential to implement innovative solutions that enhance analytical accuracy, data security, and user convenience. The development of the Finance Tracker application reflects the importance of adapting to modern trends in financial literacy and digital services. Such a system provides users with flexibility, efficiency, and full control over their personal finances, helping them make informed financial decisions and achieve stability in everyday life.

Сучасний світ фінансів постійно змінюється, трансформуючи підходи до керування коштами, контролю витрат і планування бюджету. Зростання

популярності цифрових фінансових сервісів робить такі інструменти, як веб-застосунок Finance Tracker, особливо актуальними для користувачів, які прагнуть впорядкувати свої фінанси та досягти фінансової стабільності.

Метою роботи є створення веб-застосунку Finance Tracker, що забезпечить зручне середовище для ведення обліку доходів і витрат, планування бюджету та аналізу фінансових результатів. Система підтримує гнучкість у налаштуваннях, дозволяє відстежувати динаміку фінансів, контролювати виконання бюджетних цілей і формувати звіти для прийняття обґрунтованих фінансових рішень.

Аналіз сучасних тенденцій у сфері управління особистими фінансами відображає такі ключові аспекти:

- зростання популярності фінансових трекерів: світова тенденція до підвищення фінансової грамотності та контролю витрат спричинила збільшення попиту на персональні фінансові застосунки, які допомагають користувачам керувати бюджетом і накопиченнями;

- розвиток багатофункціональних аналітичних інструментів: сучасне програмне забезпечення на кшталт Finance Tracker поєднують облік, аналітику та прогнозування, надаючи користувачам повну картину фінансового стану через графіки, діаграми та звіти;

- автоматизація та інтеграція: використання алгоритмів автоматичного імпорту транзакцій із банківських рахунків та систем категоризації витрат зменшує навантаження на користувача, прискорюючи процес ведення фінансового обліку.

На основі цих тенденцій сформовано концепцію розроблюваного веб-застосунку Finance Tracker, спрямованого на підвищення ефективності фінансового планування, зручність користування та безпеку даних, що дозволяє кожному користувачу контролювати власний бюджет і досягати фінансової стабільності.

З метою глибшого аналізу функціональності веб-сайту було розроблено діаграму потоків даних (рисунок 1) та діаграму послідовності (рисунок 2) для демонстрації загальної роботи з веб-сайтом.

На діаграмі потоків даних (рисунок 1) показано основний функціонал, котрий буде виконувати веб-сайт та встановлювати зв'язок з базою даних. Також зображено на діаграмі, як зовнішні сутності взаємодіють з даними процесами.

На наступній діаграмі (рисунок 2) зображено створення транзакції. У даній діаграмі зображено алгоритм, який є основним для додавання фінансових операцій на сайті.

Основні характеристики розроблюваного веб-застосунку Finance Tracker полягають у створенні зручного, безпечного та функціонального інструменту для управління особистими фінансами:

1. Реєстрація та профіль користувача: можливість створення облікового запису, редагування особистих даних, зміни пароля та налаштування параметрів

безпеки. Кожен користувач має власний профіль із персональними фінансовими даними та статистикою.

2. Облік доходів і витрат: функціонал для додавання, редагування й видалення транзакцій із можливістю зазначення категорії, дати, суми та коментаря. Це дозволяє користувачеві чітко бачити структуру власних витрат і доходів.

3. Категоризація та планування бюджету: система дозволяє створювати категорії витрат і доходів, встановлювати бюджетні ліміти на певні періоди, контролювати їх виконання й отримувати повідомлення про перевищення бюджету.

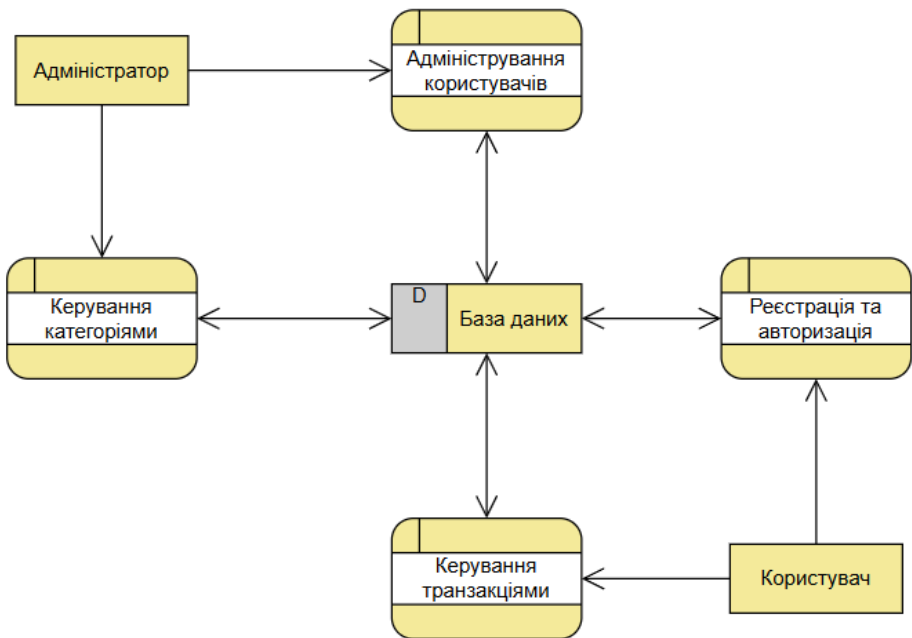


Рисунок 1 – DFD Діаграма

Звіти та аналітика: автоматичне формування графічних і табличних звітів, що відображають динаміку доходів, витрат і загальний фінансовий баланс. Це допомагає користувачу аналізувати власні фінансові звички та приймати зважені рішення.

Безпека та збереження даних: реалізація авторизації з хешуванням паролів, резервного копіювання бази даних та контролю доступу до персональної інформації.



Рисунок 2 – Flowchart діаграма

Запропонований веб-застосунок Finance Tracker має потенціал стати надійним помічником у сфері особистого фінансового планування. Його перевагами є інтуїтивний інтерфейс, точність аналітики, гнучкість у налаштуванні бюджету та високий рівень захисту даних. Завдяки цьому користувачі отримують ефективний інструмент для досягнення фінансової стабільності та усвідомленого керування власними коштами.

Перелік посилань

1. Patrick H. Personal Finance Simplified: The Step-by-Step Guide to Budgeting, Saving, and Investing / Harper Patrick – Independently Published, 2021. – 196 pages.
2. Robert T. Smart Money Habits: A Practical Approach to Managing Your Finances and Achieving Financial Freedom / Turner Robert – Pearson Education, 2023. – 248 pages.

УДК 004.4:004.9

Повстенко Р.О.

Кам'янський енергетичний фаховий коледж

ТЕХНОЛОГІЇ РОЗРОБКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Інформаційні системи (ІС) є невід'ємною частиною сучасного суспільства. Вони охоплюють широкий спектр застосувань — від управління бізнес-процесами до організації баз даних у медичних закладах чи навчальних закладах. Їх розробка вимагає інтеграції різних технологій та інструментів, що забезпечують ефективність, масштабованість та надійність систем..

Information systems (IS) are an integral part of modern society. They cover a wide range of applications — from business process management to database organization in medical institutions or educational establishments. Their development requires the integration of various technologies and tools that ensure the efficiency, scalability, and reliability of the systems.

Розглянемо основні етапи розробки інформаційних систем, популярні технології, а також перспективи їх розвитку.

Основні етапи розробки інформаційних систем

1. Аналіз вимог

На цьому етапі визначаються потреби користувачів і компаній, функції, які необхідно реалізувати, і технічні обмеження. Використовуються такі методи збору даних, як інтерв'ю, опитування та аналіз існуючих систем.

2. Проектування

Проектування ділиться на 2 рівня:

Концептуальне проектування: розробка моделі системи (наприклад, діаграми UML або ERD).

3. Фізичне проектування: визначення технічної архітектури, вибір мови програмування, баз даних та інших технологій.

Розробка

Написання коду за допомогою вибраних інструментів програмування та мов. На цьому етапі, залежно від складності та масштабу проєкту, важливо використовувати такі методології розробки, як agile та waterfall.

4. Тестування

Тестування включає перевірку функціональності, продуктивності, безпеки та сумісності системи. Популярні підходи: автоматизоване та ручне тестування.

5. Впровадження

Система інтегрується в робоче середовище користувача. Цей етап може включати в себе навчання персоналу.

6. Супровід та оновлення

Після запуску системи необхідно усунути помилки, оновити функції і підвищити безпеку.

Технології, що використовуються у розробці ІС

1. Мови програмування

– Java, Python, C#: для бекенда та складної бізнес-логіки.

– JavaScript (з використанням таких фреймворків, як React та Angular): для інтерфейсів та інтерактивних веб-додатків.

2. SQL: для управління базою даних.

– Базы даних

– Реляційні бази даних (MySQL, PostgreSQL): для структурованих даних.

– NoSQL (MongoDB, Cassandra): для обробки великих обсягів неструктурованих даних.

3. Хмарні платформи

– AWS, Google Cloud, Microsoft Azure: для розгортання, масштабування та зберігання даних. За допомогою хмари ви можете зменшити витрати на інфраструктуру та забезпечити цілодобову та 365-денну доступність послуги.

4. Інструменти управління проектами

Jira, Trello, Asana: для планування задач, моніторингу прогресу та співпраці в команді.

5. Методології розробки

– Agile: ітеративний підхід до розробки, що дозволяє швидко реагувати на зміни вимог.

– Waterfall: класична послідовна модель, придатна для проектів зі стабільними умовами.

6. Штучний інтелект (ШІ) та машинне навчання (МН). Вони використовуються для автоматизації рутинних завдань, аналізу великих даних, прогнозування та створення рекомендаційних систем.

Перспективи розвитку

1. Автоматизація процесів. Системи стають більш автономними завдяки впровадженню ШІ та МН. Наприклад, чат-боти на основі нейронних мереж замінюють класичні контакт-центри.

2. Інтернет речей (IoT). Розробка систем для інтеграції пристроїв Інтернету речей, таких як "розумний будинок", датчики на виробничих майданчиках і системи безпеки.

3. Кібербезпека. Поширення кіберзагроз вимагає впровадження нових стандартів безпеки та розробки засобів захисту інформації.

4. Гнучкі архітектури. Архітектури мікросервісів і контейнери (Docker, Kubernetes) стають стандартами для створення масштабованих систем.

5. Розширена реальність (AR) та віртуальна реальність (VR). Інтеграція цих технологій в освітні платформи, медицину та ігрову індустрію.

Висновки. Розробка інформаційних систем – це складний і захоплюючий процес, який поєднує в собі аналіз, програмування, проєктування і управління. Інструменти і технології швидко розвиваються, дозволяючи створювати більш потужні, зручні і безпечні системи. Успіх таких проєктів залежить від чіткого планування, ефективної комунікації всередині команди і використання сучасних технологічних рішень. Інформаційні системи формують основу цифрової трансформації і відкривають нові можливості для бізнесу, науки і суспільства в цілому.

Перелік посилань

1. Тягло О. В. Інформаційні системи та технології: навчальний посібник. – Харків: ХНУРЕ, 2020.
2. Pressman R. S. Software Engineering: A Practitioner's Approach. – 9th ed. – McGraw-Hill, 2019.
3. Sommerville I. Software Engineering. – 10th ed. – Pearson Education, 2016.
4. Agile Manifesto. – <https://agilemanifesto.org/>

УДК 004.4

Приймак М.О., Праворська Н.І.

Хмельницький національний університет

ІНТЕРАКТИВНА ВЕБ-СИСТЕМА ДЛЯ ПІДБОРУ КІНОТВОРІВ НА ОСНОВІ СТАНУ КОРИСТУВАЧА «MOVI.FLOW ER»

Розвиток інформаційних технологій створює сприятливі умови для широкого впровадження веб-систем, здатних адаптуватися до індивідуальних потреб користувача. Однією з найбільш перспективних галузей є персоналізовані рекомендаційні системи, що використовуються для вибору мультимедійного контенту. Традиційні алгоритми рекомендацій здебільшого базуються на жанрових уподобаннях, історії переглядів або рейтингах, однак цього вже недостатньо для забезпечення глибокої персоналізації. Врахування емоційного аспекту дозволяє створити новий рівень персоналізації, що сприяє більш глибокому залученню користувача та формуванню позитивного досвіду взаємодії із системою. Саме на вирішення цього завдання спрямоване розроблення інтерактивної веб-системи, яка поєднує сучасні технології веб-розробки, аналітику користувацьких параметрів та елементи інтерфейсу для створення рекомендацій, що відповідають не лише технічним, а й емоційним критеріям вибору кінотворів.

The development of information technologies creates favorable conditions for the widespread implementation of web systems that can adapt to the individual needs of the user. One of the most promising areas is personalized recommendation systems used to select multimedia content. Traditional recommendation algorithms are mostly based on genre preferences, viewing history or ratings, but this is no longer enough to ensure deep personalization. Taking into account the emotional aspect allows you to create a new level of personalization, which contributes to deeper user involvement and the formation of a positive experience of interaction with the system. It is precisely to solve this problem that the development of an interactive web system is aimed, which combines modern web development technologies, analytics of user parameters and interface elements to create recommendations that meet not only technical, but also emotional criteria for selecting films.

Потреба цифрових технологій та розширення можливостей мультимедійних платформ персоналізації контенту набуває особливої актуальності. Користувачі прагнуть отримувати рекомендації, які відповідають їхнім смакам, настрою та емоційному стану. Саме тому створення інтелектуальних веб-систем для автоматизованого підбору кінотворів на основі поведінкових і психологічних характеристик користувача є важливим напрямом сучасних досліджень у галузі інженерії програмного забезпечення.

Метою роботи є розроблення інтерактивної веб-системи, яка надає персоналізований підбір кінотворів на основі емоційного стану користувача.

Реалізація проєкту спрямована на створення адаптивного середовища, що формує рекомендації не лише за жанровими чи часовими параметрами, а й відповідно за певним настроєм користувача.

Аналіз сучасних тенденцій у галузі персоналізованих рекомендацій мультимедійного контенту відображає наступні ключові аспекти:

– зростання ролі емоційно-орієнтованих системи: Сучасні користувачі прагнуть не лише знайти контент за жанром та рейтингом, а отримати рекомендації, що відповідають їхньому настрою та емоційному стану;

– розвиток багатофункціональних інструментів: Сучасні веб-платформи для перегляду мультимедійного контенту активно інтегрують розширені можливості, що поєднують кілька напрямів взаємодії з користувачем в одному середовищі. Системи дозволяють не лише здійснювати пошук і перегляд інформації про кінотвори, але й створювати власні списки, оцінювати контент, формувати добірки, залишати відгуки та ділитися вподобаннями;

– інтеграція з відкритими базами даних мультимедійного контенту: Використання API сервісів, таких як TMDb, дозволяє отримувати актуальну інформацію про фільми, серіали, мультфільми та аніме, що значно спрощує наповнення системи контентом та оновлення бази даних у реальному часі.

На основі зазначених тенденцій формується концепція інтерактивної веб-системи персоналізованих рекомендацій кінотворів, яка орієнтована на вдосконалення підбору мультимедійного контенту з урахуванням емоційного стану користувача.

Основні характеристики розроблюваної системи містять:

1. Персоналізацію рекомендацій: Система формує добірку кінотворів, що відповідають емоційному стану, жанровим уподобанням та попереднім оцінкам користувача.

2. Інтерактивна взаємодія з користувачем: Динамічний інтерфейс, який змінюється відповідно до обраного стану користувача.

3. Керування списками перегляду: Можливість створювати власні добірки фільмів для зручності користувача.

4. Отримання актуальних даних із TMDb API: Автоматичне відображення описів, рейтингів та іншої інформації про кінотвори.

У процесі проєктування веб-системи було створено діаграму потоків даних (рисунок 1) та діаграму архітектури системи (рисунок 2), що демонструють загальну логіку роботи та взаємодію між компонентами.

На діаграмі потоків даних (рисунок 1) показано основний функціонал, котрий буде виконувати дана веб-система та встановлювати відповідний зв'язок з базою даних. Надана діаграма демонструє повну взаємодію характеристик та процесів проєкту, які належно функціонують між собою.

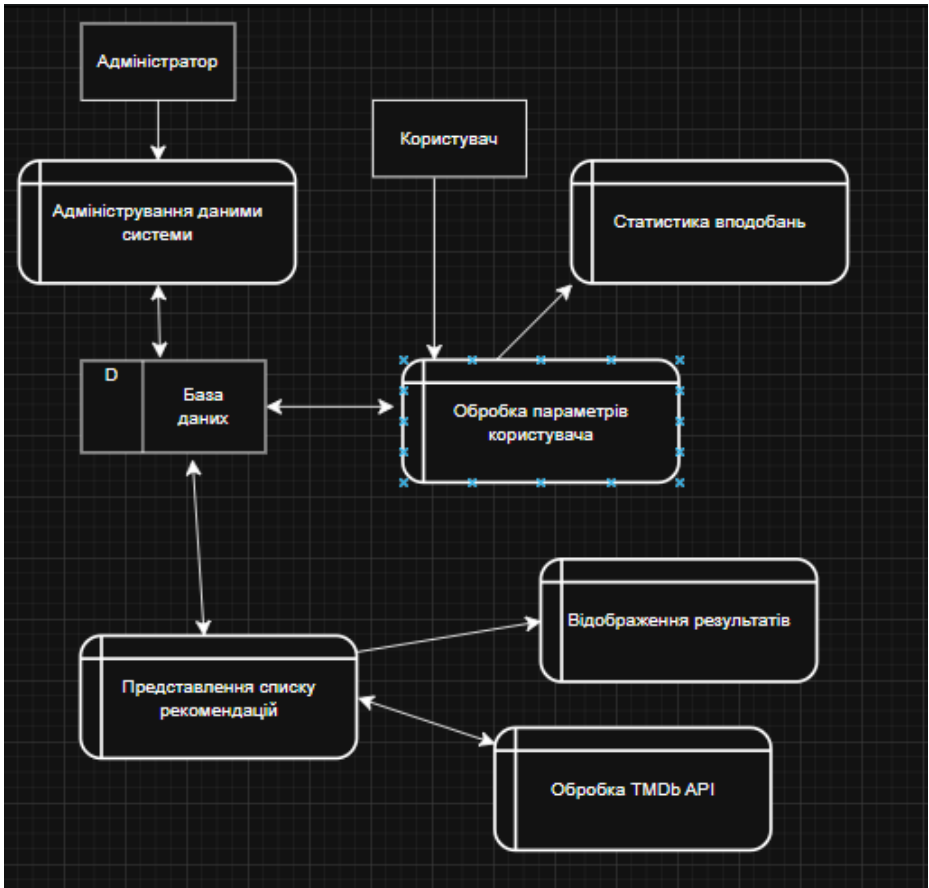


Рисунок 1 – DFD Діаграма

На наступній діаграмі (рисунок 2) зображено детальний алгоритм дій даної веб-системи. Саме така діаграма зображує головні етапи та усі зміни у взаємодії користувача та самого проєкту.

Основним призначенням веб-системи є допомога користувачам у виборі кінотворів, що відповідають їхнім персональним смакам, настрою та емоційному стану. Система забезпечує персоналізований підбір фільмів, серіалів, мультфільмів та аніме, скорочуючи час на пошук контенту та підвищуючи якість користувацького досвіду. Даний веб-застосунок реалізує інтерактивний підхід, що дозволяє створити індивідуальні рекомендації та враховувати поточний психологічний стан користувача.

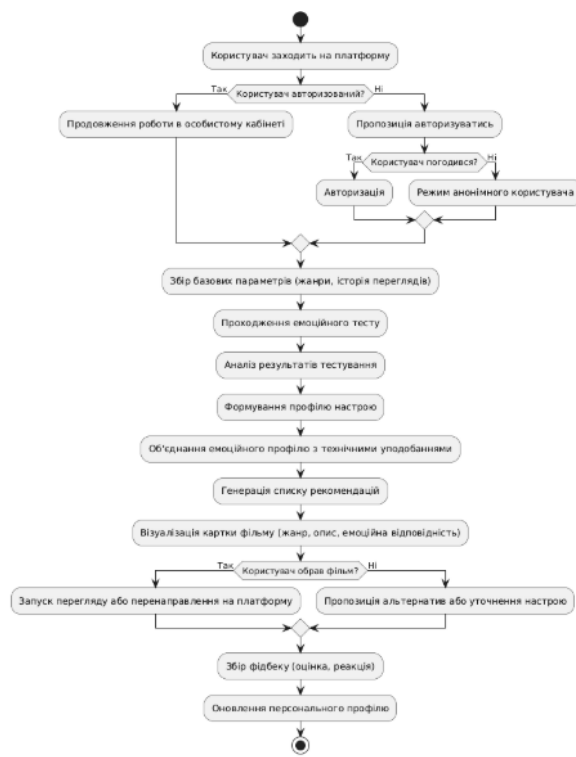


Рисунок 2 – Flowchart діаграма

Система інтегрована з базою даних TMDb API, що забезпечує отримання актуальної інформації про кінотвори, акторський склад, жанр, рейтинг і відгуки інших користувачів. Крім цього, користувач має змогу створювати власні колекції для перегляду, оцінювати фільми та формувати особистий список рекомендацій. Веб-система «MOVI.FLOW•ER» має потенціал стати сучасним інструментом персоналізованого підбору кінотворів, який поєднає емоційний аналіз, адаптивність і простоту використання, створюючи новий формат взаємодії між глядачем і цифровим контентом.

Перелік посилань

1. Білоус, М. А. Вебзастосунок для підбору фільмів на основі користувацьких колекцій. - 2022. С. 72.
2. Лишак, А. М., and Л. В. Крилик. Перспективи розробки програмного модуля підбору фільмів. Diss. BNTU. - 2024. - С. 1.

УДК 004.4

П'явкін В.О., Лисенко С.М.

Хмельницький національний університет

МЕТОД ТА ІНФОРМАЦІЙНА СИСТЕМА ВИЯВЛЕННЯ ПІДОЗРЛИХ ОБ'ЄКТІВ У ГРОМАДСЬКИХ МІСЦЯХ

У роботі запропоновано метод і архітектуру інформаційної системи для автоматичного виявлення підозрливих об'єктів у громадських місцях на основі аналізу відеопотоку. Метод поєднує детектування, трекінг і поведінкову оцінку об'єктів із контекстно-часовим регулюванням чутливості. Реалізовано пояснюваний підхід до формування рішень, що дозволяє знизити кількість хибних сповіщень і підвищити довіру до системи.

The paper proposes a method and architecture of an information system for automatic detection of suspicious objects in public places based on video stream analysis. The method combines object detection, tracking, and behavioral evaluation with context- and time-dependent sensitivity regulation. An explainable decision-making approach is implemented to reduce false alarms and increase system reliability.

Вступ. Сучасні тенденції розвитку міської інфраструктури та підвищення рівня громадської безпеки вимагають використання інтелектуальних систем відеоаналітики, здатних самостійно ідентифікувати небезпечні ситуації. Одним із таких завдань є виявлення підозрливих об'єктів, залишених без нагляду у громадських місцях. Це завдання має критичне значення для попередження терористичних загроз і забезпечення безпеки населення.

Більшість існуючих систем відеоспостереження функціонують у напівавтоматичному режимі, коли основна аналітика покладається на оператора. Проте людський фактор обмежує швидкість і точність реагування, особливо у випадках, коли необхідно аналізувати десятки відеопотоків одночасно. Таким чином, виникає потреба у створенні методу та інформаційної системи, здатних автономно визначати підозрілі об'єкти, аналізуючи поведінкові ознаки та контекст сцени.

Дослідження відомих методів. В роботі запропоновано багаторівневу структуру методу та інформаційної системи виявлення підозрливих об'єктів у громадських місцях, що поєднує детектування, трекінг і поведінкову оцінку з контекстно-часовою адаптацією чутливості. Запропонована політика прийняття рішень враховує типи подій і профілі людських потоків, використовує просторову

«карту ризику» сцени та добові профілі порогів і інерційності, а також застосовує «тонкі» зворотні зв'язки від високорівневих індикаторів до нижчих рівнів обробки для стабілізації роботи у складних умовах. Розроблена аналітична модель описує затримки формування рішень та накопичення доказів у сценаріях «камера–edge вузол–центральный сервер» для відеоаналітики громадських просторів.

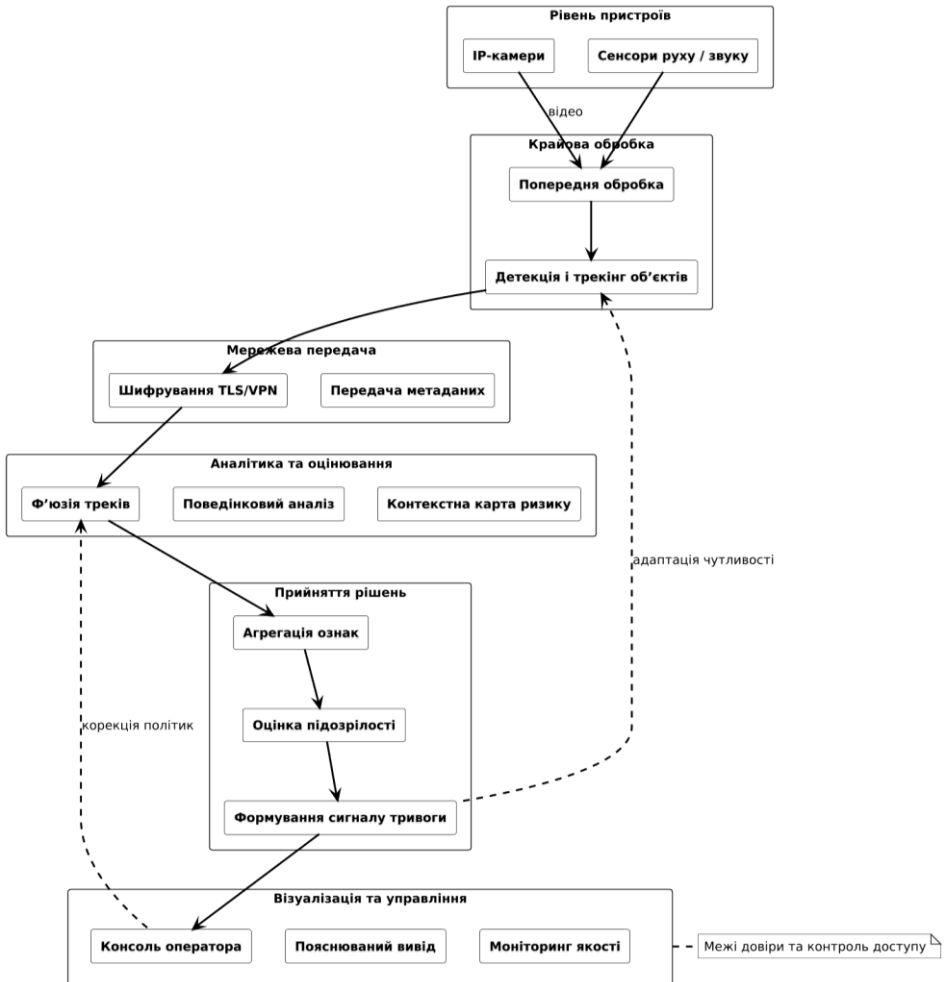


Рисунок 1. Узагальнена архітектура методу та інформаційної системи виявлення підозрілих об'єктів у громадських місцях

Також було досліджено виклики впровадження пояснюваної відеоаналітики у міській інфраструктурі та запропоновано адаптивну операційну платформу керування потоками й обчисленнями на крайових пристроях, що зменшує обсяг переданих даних і фільтрує трафік за пріоритетами безпеки. Показано, що поєднання локального попереднього аналізу на камерах/edge з централізованою агрегацією ознак дозволяє знизити навантаження мережі та пришвидшити реакцію системи без втрати якості рішень.

У рамках обговорення фреймворків та моделей для практичної реалізації, було представлено платформні рішення підтримки малопотужних камер та вбудованих пристроїв з прикладами на транспортних вузлах і в публічних просторах, розроблено модуль кооперативного спостереження між камерами для підвищення стійкості до перекриттів і пропусків, що критично важливо для коректної оцінки «залишення предмета» у багатолюдних сценах.

Безпековий аспект розглянуто окремо. Проаналізовано механізми пояснюваності та аудиту: формування «кадру-доказу» з вкладом кожного індикатора, криптографічні журнали подій, контроль цілісності та відстежуваність рішень. Запропоновано політики приватності, які зменшують регуляторні ризики. Досліджено питання безпеки інтеграції міського відеонагляду з суміжними IoT-сервісами, наголосивши на необхідності формалізації «меж довіри», захищених каналів між підсистемами та відповідної конфігурації середовища виконання.

Висновок. Запропонований «Метод та інформаційна система виявлення підозрілих об'єктів у громадських місцях» забезпечує узгоджену інтеграцію детектування, багатооб'єктного трекінгу та поведінкового аналізу з контекстною адаптацією у просторі та часі.

Використання нормованих індикаторів у поєднанні з каліброваними коефіцієнтами довіри джерел і механізмом часової акумуляції з гістерезисом дає змогу знизити хибні сповіщення та підвищити стабільність рішень за реальних умов експлуатації.

Окремою перевагою є пояснюваність, система формує прозорий кадр-анотацію з внесками індикаторів і поточною впевненістю, що спрощує верифікацію результатів оператором.

Практична цінність полягає в можливості масштабованого розгортання у вузлах міської інфраструктури та в інтеграції з існуючими платформами відеонагляду.

Архітектура підтримує тонкі зворотні зв'язки, завдяки яким високорівневі висновки можуть коригувати чутливість нижчих рівнів без порушення їх автономії, що особливо важливо під час пікових навантажень і в зонах підвищеного ризику.

Результати експериментальних випробувань засвідчили покращення інтегральних метрик якості порівняно з базовими підходами без контекстної

адаптації, а також зменшення часу до підтвердження події у спокійні періоди при збереженні стійкості в пікові години.

Подальші роботи доцільно спрямувати на поглиблення моделей невизначеності та на використання прогнозної аналітики для побудови динамічних карт ризику за історією подій. Перспективним також є розширення набору поведінкових патернів і інтеграція легковагових моделей на крайових пристроях для зменшення трафіку до центрального вузла.

Перелік посилань

1. Redmon J., Farhadi A. YOLOv3: An Incremental Improvement. arXiv:1804.02767, 2018.
2. Wojke N., Bewley A., Paulus D. Simple Online and Realtime Tracking with a Deep Association Metric. IEEE ICIP, 2017.
3. Bochkovskiy A., Wang C.-Y., Liao H.-Y.M. YOLOv4: Optimal Speed and Accuracy of Object Detection. arXiv, 2020.
4. Chen K. et al. MMDetection: Open MMLab Detection Toolbox and Benchmark. arXiv:1906.07155, 2019.
5. Khan S. et al. A Survey of the Recent Architectures of Deep Convolutional Neural Networks. Artificial Intelligence Review, 2020.
6. Баранов О. В., Мельник В. А. Методи виявлення об'єктів на відео за допомогою нейронних мереж. Вісник ХНУРЕ, 2022.
7. Коваленко І. І. Застосування машинного навчання для систем спостереження. Вісник КНУ, 2021.
8. Liu W. et al. SSD: Single Shot MultiBox Detector. ECCV, 2016.
9. Hu J. et al. Squeeze-and-Excitation Networks. CVPR, 2018.
10. Ioffe S., Szegedy C. Batch Normalization: Accelerating Deep Network Training. arXiv:1502.03167, 2015.

УДК 621.391.1, 621.391.8

Разовий О.О., Пивовар О.С., Голевич О.Б.

Хмельницький національний університет

МОДЕЛЬ СИСТЕМНОЇ ЗАВАДИ ДЛЯ БАГАТОКАНАЛЬНИХ ХАОТИЧНИХ СИСТЕМ ПЕРЕДАЧІ ДАНИХ

Запропоновано Simulink модель системної завади для дослідження завадостійкості систем зв'язку із використанням сигналів детермінованого хаосу в структурі цифрової передачі даних із детектуванням хаотичних режимів на основі допоміжного генератора.

A Simulink-based interference source model is proposed for evaluating the robustness of multi-channel data transmission systems that use deterministic chaotic signals. The work targets communication schemes in which each channel transmits a chaotic waveform generated by a nonlinear dynamic system (the Rucklidge system) with distinct bifurcation parameters, and the receiver performs nonlinear detection of the active chaotic regime. The model reproduces realistic "system interference," i.e. structured in-band interference generated by other active channels rather than by natural additive noise.

Щільне заповнення радіочастотного спектра випромінювачами створює перехресні завади та ускладнює забезпечення електромагнітної сумісності (ЕМС). У багатоканальних і багатокористувацьких системах рівень взаємних завад між каналами часто перевищує рівень природних шумів. Такі завади мають структуру сигналу і не придушуються стандартними часовими, частотними, просторовими або поляризаційними методами фільтрації. Це вимагає нетрадиційних методів підвищення стійкості каналу зв'язку. Одним із перспективних напрямів є використання сигналів детермінованого хаосу та нелінійної обробки на приймальній стороні.

Традиційне застосування систем часової, частотної, просторової та поляризаційної фільтрації не призводить до пригнічення таких системних завад (СЗ) через те, що їх форма подібна до форми сигналу. Для роботи в таких умовах слід застосовувати нетрадиційні підходи до забезпечення стійкості передачі даних. Перспективними в цьому аспекті є застосування сигналів детермінованого хаосу (СДХ) та нелінійного способу їх обробки в приймальних трактах багатоканальної системи зв'язку [1].

Метою роботи є розробка відтворюваної моделі джерела системної завади для багатоканальної системи передачі даних на основі хаотичних сигналів нелінійної динамічної системи типу Rucklidge.

Основними вимогами, виходячи із визначення системної завади та умов її взаємодії із сигналом, є: наближеність форми та спектру сигналу завади до СДХ, що діє в системі; статистичний характер гаусівського процесу, що враховує сукупну дію багатьох СДХ сусідніх каналів; стабілізація рівня суміші корисного сигналу та СЗ та відсутність точок розриву для можливості неперервної нелінійної обробки.

Відповідно цим вимогам розроблена Simulink модель (рис.1) що дозволила провести синтез параметрів Simulink-блоків для створення системної завади хаотичним каналам зв'язку на базі нелінійної динамічної системи (НДС) Rucklidge [2-4].

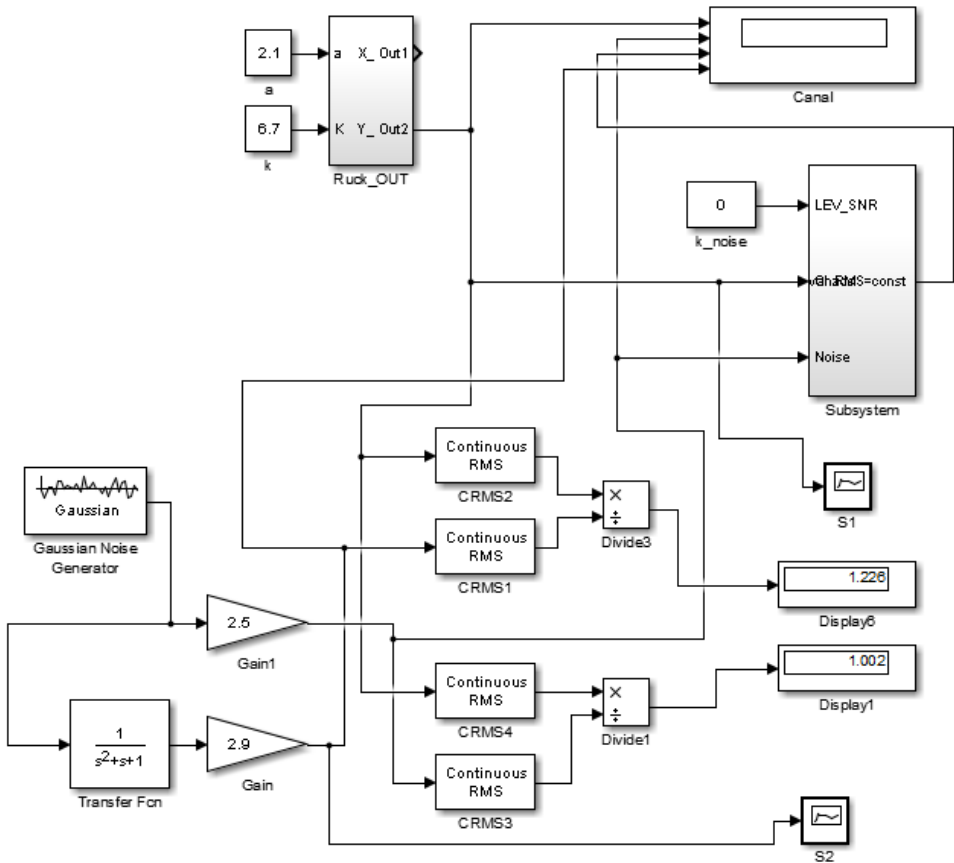


Рисунок 1 – Імітаційна модель системних завад

Модель складається із НДС Rucklidge [3] із певними параметрами біфуркації, гаусівського генератора випадкових чисел із системним фільтром другого порядку та блоків візуалізації. Проблема синтезу саме системної завади полягає в узгодженні дискретного потоку даних гаусівського генератора із аналоговими результатами генерації СДХ моделлю НДС Rucklidge через оптимальних вибір їх параметрів налаштувань.

Через дискретний характер сигналу генератора завад запропоновано для забезпечення плавної зміни сигналу в зоні зміни застосувати інтегруючий елемент у вигляді фільтра низької частоти (ФНЧ) із характеристикою ланки подвійного інтегрування:

$$K(s) = \frac{1}{as^2 + bs + c}, \quad (1)$$

де $s = j\omega$ - комплексна частота.

Регулюванням параметрів (1) можливо обробити дискретизований та квантований сигнал генератора випадкових чисел (рис.1) таким чином, щоб отримати коливання максимально наближене по формі та структурі із хаотичним коливанням (рис.2). Шляхом моделювання встановлено, що найбільш оптимальним є фільтр із параметрами $a, b=1$. Таке узгодження виключає розриви сигналу і забезпечує коректну подальшу нелінійну обробку в приймачі.

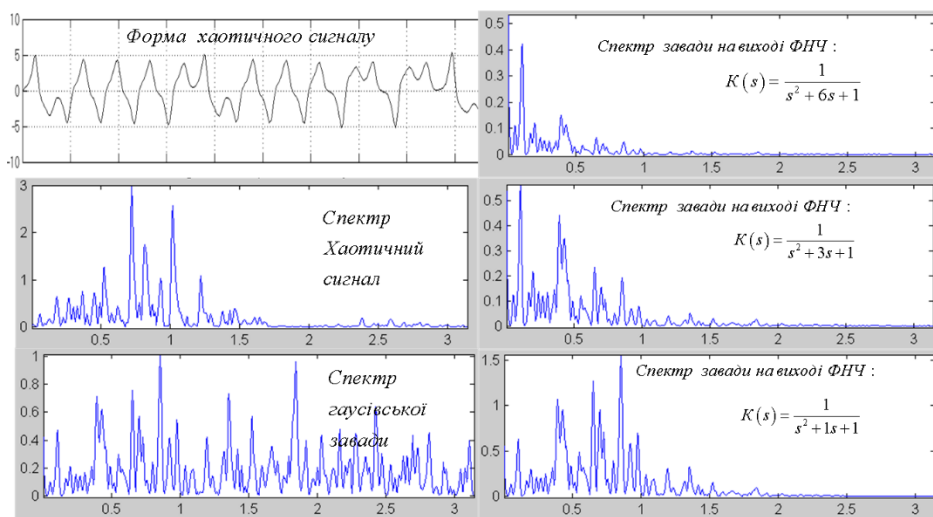


Рисунок 2 – Форма та спектри завади після обробки ФНЧ для досягнення заданих властивостей системної завади для систем передачі на базі НДС Rucklidge

Таким чином, під час досліджень оптимізовано параметр Simulink-блоку гаусівський завад як «Sample time» = 1 та параметри формуючого фільтру таким чином, щоб форма, структура та спектр відповідали СДХ в НДС Rucklidge.

Модель дозволяє згенерувати заваду, яка відтворює як часову форму, так і спектральні властивості корисного каналу. При цьому система зберігає коректне детектування активного хаотичного режиму за відношення сигнал/завада приблизно 10 дБ. Це підтверджує можливість роботи багатоканальної хаотичної лінії зв'язку в умовах сильної внутрішньосистемної взаємодії каналів.

Сформована Simulink-модель може бути використана як еталон при побудові апаратного генератора системних завад для лабораторних випробувань стійкості та ЕМС хаотичних каналів зв'язку на базі НДС Rucklidge.

Перелік посилань

1. Прикладне застосування теорії хаотичних систем у телекомунікаціях : монографія / Ю. Я. Бобало, С. Д. Галюк, М. М. Климаш, Р. Л. Політанський; Міністерство освіти і науки України, Національний університет "Львівська політехніка". – Львів; Дрогобич : Коло, 2015. – 184 с.
2. Golevych.O, Pyvovar. O. Dumenko.P "Synchronization of non-linear dynamic systems under the conditions of noise action in the channel", Latvian Journal of Physics and Technical Sciences Открытый доступ Volume 55, Issue 3, 1 June 2018, Pages 70-76 DOI: <https://doi.org/10.2478/lpts-2018-0023>
3. Pyvovar, O.S., Polikarovskiykh, O.I. A System of Secure Communication with Chaos Masking Based on Rucklidge Generators, 2018 IEEE 38th International Conference on Electronics and Nanotechnology, ELNANO 2018 - Proceedings DOI: 10.1109/ELNANO.2018.8477566.
4. Boccaletti S. The synchronization of chaotic systems / S. Boccaletti, J. Kurths, G. Osipov, D. L. Valladares, and C. S. Zhou // Physics Report. – 2002. – Vol. 366. – № 1–2. – P. 1–101.

УДК 004.6

Ратушняк М.В., Рябчук І.С., Муляр І.В.

Хмельницький національний університет

АНАЛІЗ УПРАВЛІННЯ РЕСУРСАМИ КІБЕРЗАХИСТУ В УМОВАХ НЕВИЗНАЧЕНОСТІ ТА АСИМЕТРІЇ ІНФОРМАЦІЇ ШЛЯХОМ АДАПТИВНОЇ ПРІОРИТЕЗАЦІЇ ЗАХОДІВ ЗАХИСТУ

Розглянуто розробку, теоретичне обґрунтування та експериментальну перевірку методу, що дозволяє системі захисту приймати оптимальні рішення щодо розподілу ресурсів в умовах стратегічної протидії та інформаційної невизначеності.

Considered the development, theoretical justification, and experimental verification of a method that allows the defense system to make optimal decisions regarding resource allocation under conditions of strategic opposition and informational uncertainty.

Сучасний ландшафт кіберзагроз характеризується не просто зростанням їхньої кількості, а якісною еволюцією від масових, автоматизованих атак до цілеспрямованих, багатоступінчастих кампаній, відомих як Advanced Persistent Threats (APTs). Ці кампанії проводяться раціональними супротивниками з високою мотивацією, які адаптують свою тактику в реальному часі, щоб обійти існуючі засоби захисту. Професіоналізація кіберзлочинності, що виражається в моделях Ransomware-as-a-Service (RaaS) та атаках на ланцюги постачання, створює фундаментальну асиметрію: зловмиснику достатньо знайти одну вразливість, тоді як захисник повинен захищати весь периметр та всі вектори атак.

Ця ситуація оголює ключову слабкість традиційних систем безпеки, які функціонують на основі статичних правил, сигнатурного аналізу та реактивних механізмів. Вони виявляються неефективними проти атак "нульового дня" та не здатні протистояти супротивнику, який стратегічно мислить, маскує свої дії та вводить в оману системи моніторингу. Як наслідок, організації зазнають колосальних фінансових та репутаційних втрат.

Таким чином, виникає гостра науково-практична проблема в розробці та обґрунтування методів управління кібербезпекою, які здатні функціонувати в умовах стратегічної невизначеності та асиметрії інформації. Необхідно здійснити парадигмальний зсув від реактивного реагування на інциденти до проактивного, керованого ризиками та адаптивного захисту, здатного передбачати дії раціонального супротивника.

Аналіз існуючих підходів до вирішення цієї проблеми виявив їхні суттєві обмеження. Статистичні моделі корисні для аналізу масових атак, вони не враховують ключового фактору – інтенціональності (намірів) та креативності зловмисника. Вони моделюють загрози як стохастичні процеси, ігноруючи стратегічне планування та адаптацію з боку супротивника.

Якісні фреймворки (MITRE ATT&CK, Cyber Kill Chain) надають неоціненну таксономію технік та тактик атак, створюючи загальну мову для опису інцидентів. Однак вони є дескриптивними, а не прескриптивними. Вони допомагають зрозуміти, що сталося, але не пропонують формального математичного апарату для вибору оптимальної контрстратегії в умовах обмежених ресурсів.

Системи на основі машинного навчання ефективні для виявлення аномалій та відомих патернів у великих обсягах даних. Проте, вони вразливі до змагальних атак (adversarial attacks), таких як "ухилення" (evasion) та "отруєння даних" (data poisoning), де зловмисник цілеспрямовано маніпулює вхідними даними, щоб обійти модель.

Платформи SOAR автоматизують стандартні процедури реагування, але їхня ефективність обмежується жорсткістю заздалегідь визначених сценаріїв (плейбуків). Вони не здатні приймати оптимальні рішення в умовах нових, непередбачуваних векторів атак.

Теорія ігор у кібербезпеці – хоча існують дослідження, що застосовують теорію ігор, багато з них обмежуються статичними (однокроковими) іграми або припускають наявність повної інформації та загальновідому раціональність гравців, що є нереалістичним для справжніх кіберконфліктів [1, 3].

Цей аналіз виявляє ключову прогалину в дослідженнях: відсутність інтегрованого, обчислювально ефективного методу, який би поєднував динаміку багатоетапного протистояння, невизначеність щодо типу та намірів зловмисника, та здатність знаходити оптимальну стратегію захисту в реальному часі.

Метою дослідження є підвищення кіберстійкості інформаційної системи шляхом розробки та наукового обґрунтування методу динамічного адаптивного управління безпековими ресурсами. Метод має базуватися на синергії апарату стохастичних байесівських ігор для моделювання невизначеності та навчання з підкріпленням для обчислення оптимальної політики захисту.

Для досягнення поставленої мети розроблено комплексний метод, наукова новизна якого полягає в інтеграції двох потужних парадигм. Математична модель – динамічна байесівська гра. Кіберпротистояння формалізується як послідовна гра з неповною інформацією. На відміну від класичних моделей, тут захисник не знає точного "типу" атакуючого (вектора його характеристик: рівень кваліфікації, наявність 0-day експлойтів, фінансування, схильність до ризику). Замість цього, захисник підтримує ймовірнісний розподіл ("belief state") щодо можливих типів супротивника. Після кожної дії атакуючого (наприклад, спроби сканування певного порту) захисник, використовуючи правило Байєса, оновлює свої уявлення, уточнюючи оцінку того, з ким він має справу.

Обчислювальний алгоритм – навчання з підкріпленням (Q-learning). Оскільки простір станів та дій у реалістичних сценаріях є надзвичайно великим, аналітичне рішення такої гри є неможливим. Тому запропоновано використовувати навчання з підкріпленням (Reinforcement Learning, RL). Агент (захисник) навчається оптимальній політиці π^* , яка кожному стану системи (включаючи поточні уявлення про тип атакуючого) ставить у відповідність оптимальну дію (наприклад, перерозподіл обчислювальних потужностей на аналіз трафіку, ізоляцію сегмента

мережі, розгортання приманок). RL дозволяє знаходити немиопічну (далекоглядну) стратегію, максимізуючи сукупну довгострокову винагороду (мінімізуючи збитки) без необхідності мати явну модель поведінки супротивника [2].

Синергія підходу полягає в тому, що байєсівська модель надає формальну структуру для роботи з невизначеністю, а RL – масштабований обчислювальний інструмент для пошуку оптимальної поведінки в цій структурі.

Ефективність методу було перевірено на програмному симуляторі, що імітував корпоративну мережу з різномірними активами різної цінності. Моделювалися атаки від супротивників з різними стратегічними профілями. Порівняльний аналіз показав, що запропонований адаптивний метод, у порівнянні зі статичними політиками та реактивними стратегіями, дозволив знизити сукупні очікувані збитки та підвищити коефіцієнт повернення інвестицій у безпеку (ROSI) за рахунок раціонального, обґрунтованого розподілу ресурсів захисту в кожен момент часу.

У дослідженні вирішено актуальну науково-прикладну задачу розробки методу адаптивного управління кіберзахистом в умовах стратегічної протидії. Запропонований метод, що поєднує строгість теорії байєсівських ігор та обчислювальну потужність навчання з підкріпленням, є кроком до створення нового покоління автономних систем кіберзахисту. Він дозволяє перейти від пасивного, заснованого на сигнатурах захисту до динамічного, інтелектуального та стратегічно обґрунтованого процесу забезпечення безпеки.

Подальший розвиток даного дослідження можливий у наступних напрямках:

- дослідження застосування алгоритмів глибокого навчання з підкріпленням (Deep Q-Networks, Actor-Critic) для подолання "прокляття розмірності" у великомасштабних гетерогенних мережах.

- інтеграція моделей з поведінкової економіки для врахування обмеженої раціональності та когнітивних упереджень зловмисників.

- використання даних з платформ аналізу загроз (TIPs) для формування початкових апріорних ймовірностей щодо типів атакуючих.

- розробка механізмів інтерпретації рішень, що приймаються системою, для підвищення довіри та ефективної взаємодії з аналітиками Security Operation Center (SOC).

Перелік посилань

1. Wang, J., & Cui, L. (2023). Patrolling games with coordination between monitoring devices and patrols. *Reliability Engineering & System Safety*, 233, 109109. DOI: 10.1016/j.res.2023.109109.
2. McDonald, G., Li, L., & Al Mallah, R. (2024). Finding the Optimal Security Policies for Autonomous Cyber Operations With Competitive Reinforcement Learning. *IEEE Access*, PP(99), 1–1. DOI: 10.1109/ACCESS.2024.3446310.
3. Zhu, M., Anwar, A., & Wan, Z. (2021). Game-Theoretic and Machine Learning-based Approaches for Defensive Deception: A Survey. *arXiv preprint arXiv:2101.10121*. DOI: 10.48550/arXiv.2101.10121

УДК 004.4

Рибак А.М., Лисенко С.М, Лисенко Н.С.

Хмельницький національний університет

АБСТРАКТНА МОДЕЛЬ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ

У роботі розглянуто підхід до побудови віртуального навчального середовища для формування soft skills, у якому взаємодія користувача моделюється як динамічний процес із частковим спостереженням.

The paper considers an approach to building a virtual learning environment for developing soft skills, in which user interaction is modelled as a dynamic process with partial observation.

Вступ. Віртуальне середовище у навчанні soft skills ґрунтується на створенні імітованого простору, який відтворює умови реальної взаємодії, але надає можливість безпечного експериментування з поведінкою [1-3]. Його функціонування базується на трьох ключових складових: сенсорному сприйнятті користувача, відтворенні контенту у вигляді 3D-сцен та динамічній адаптації середовища під дії й реакції особистості. Функціонування VR-середовища будується на принципі зворотного зв'язку: будь-яка дія користувача відображається у віртуальному просторі через зміну поведінки віртуальних співрозмовників або трансформацію сценарію. Такий підхід забезпечує відчуття реалізму і створює умови для формування стійких навичок через ітеративне навчання [4-6].

Абстрактна модель віртуальної реальності. Модель взаємодії в VR-середовищі з урахуванням часткового спостереження може бути формалізована як динамічна система, де кожен агент (включно з тьютором) діє на основі неповної інформації про стан системи. Кожен користувач u_j керує своїм аватаром a_j , який виконує дії в середовищі E . Аватари взаємодіють один з одним і з тьютором-агентом, який може виступати як наставник або фасилітатор. Дії аватарів a_j впливають на прихований стан системи $s \in S$ (наприклад, емоційний стан користувача або контекст сценарію).

Сценарії E визначають правила взаємодії та обмеження. Наприклад, у сценарії "переговори" дії аватарів можуть змінювати емоційний стан учасників або динаміку діалогу. Сценарій також впливає на те, які спостереження $o \in O$ будуть доступні агентам (наприклад, міміка, жести, інтонація).

Стан s включає емоційний стан користувачів, їхні наміри, рівень стресу або залученості. Цей стан не спостерігається безпосередньо, але може бути частково відтворений через спостереження o . Наприклад, за допомогою аналізу голосу, рухів або фізіологічних даних (пульс, тонус м'язів).

Сенсорні дані o надходять від користувачів і середовища. Це можуть бути відеопотік, аудіосигнали, дані трекерів руху або лог дій.

Тьютор-агент аналізує ці спостереження, щоб оцінити прихований стан s і адаптувати свою поведінку. Наприклад, якщо користувач почав говорити тихіше, це може вказувати на нервозність.

Ймовірнісний оператор T описує, як стан системи s змінюється під впливом дій аватарів a_j і зовнішніх факторів. Наприклад, агресивна дія одного аватара може призвести до зростання рівня конфлікту в сценарії. Функція R оцінює, наскільки успішно аватари виконують завдання з розвитку soft-skills. Винагорода може залежати від досягнення цілей сценарію (наприклад, успішне завершення переговорів) або від зміни емоційного стану користувачів (наприклад, зниження рівня стресу). Тьютор-агент може використовувати R для оптимізації своїх дій, щоб максимізувати позитивний результат.

Розглянемо динаміку взаємодії. Аватари виконують дії на основі своїх політик і спостережень o . Тьютор-агент аналізує o і оновлює свою віру в прихований стан s (наприклад, за допомогою фільтра Калмана або байєсівських методів).

На основі оновленої віри тьютор вибирає дії, які спрямовані на покращення стану s (наприклад, заспокоїливі коментарі або підказки).

Оператор T оновлює стан системи, враховуючи дії всіх аватарів і випадкові фактори. Функція R оцінює результат дій і коригує поведінку аватарів для досягнення цілей сценарію.

Розглянемо приклад. У сценарії "конфлікт" тьютор-агент може помітити підвищений тон голосу (спостереження o) і припустити, що емоційний стан користувача s погіршився. Він може втрутитися з медіативною дією, щоб знизити напругу. Якщо це призведе до зниження рівня конфлікту, функція R нагородить тьютора за успішне втручання. Таким чином, задамо VR-середовище кортежем:

$$M = \langle U, A, E, S, O, T, R \rangle, \quad (1)$$

де U – множина користувачів u_i ; A – множина аватарів/агентів (включно з тьютором-агентом), a_j ; E – простір середовищ/сценаріїв (наприклад, переговори, презентація, конфлікт тощо); S – простір прихованих (реальних) станів системи $s \in S$ (емоційний стан користувача, контекст); O – простір спостережень (сенсорні дані, телеметрія, дії), $o \in O$; T – оператор переходу станів (можна задати як ймовірнісний оператор); R – функції винагороди/оціночні функції для завдань soft-skills.

Через обмеженість сенсорних сигналів моделлю середовища зручніше керувати як засобами математична модель для прийняття рішень у середовищах, де агент не має повної інформації про стан системи (POMDP)ю

Формалізацію часткового спостереження задамо так:

$$\langle S, A_{sys}, O, T, Z, R, \gamma \rangle, \quad (2)$$

де A_{sys} – множина системних дій (виклик подій у VR, зміна сценарію, підказки), $T(s' | s, a)$ – ймовірність переходу прихованого стану в s' , коли застосовано дію a , $Z(o | s)$ – ймовірність отримати спостереження (o) при стані (s), $R(s, a)$ – функція

винагороди (напр., поліпшення навички, емоційний комфорт), γ – коефіцієнт дисконтів (для довготривалого планування).

Розглянемо об'єкти спостереження. Нехай спостереження o – вектор, що об'єднує:

$$O = \{O_{gesture}, O_{voice}, O_{eye}, O_{task}\}, \quad (3)$$

де кожен компонент – числовий або категорійний сигнал (наприклад, інтенсивність голосу, час відповіді, вираз обличчя).

Об'єкти спостереження у віртуальній реальності відіграють ключову роль у визначенні того, як саме користувач взаємодіє із середовищем. Кожне спостереження o можна подати як вектор, що складається з чотирьох компонентів: $O_{gesture}$, O_{voice} , O_{eye} та O_{task} . Кожен із них є джерелом даних про поведінку, емоційний стан і особистісні риси користувача у VR-сценарії, орієнтованому на розвиток soft skills. Компонент $O_{gesture}$ відображає тілесні рухи користувача. Система фіксує жести, положення рук, нахили голови та інші мікроруки тіла за допомогою сенсорів, вбудованих у VR-обладнання. Це дозволяє виявити ступінь комфорту людини у ситуації: чи відчуває вона себе впевнено, чи навпаки – демонструє закритість, скутість або стрес. Ці рухи тіла є непрямим, але важливим джерелом інформації про те, як людина себе почуває і наскільки активно залучена до діалогу чи симуляції.

Компонент O_{voice} охоплює всі характеристики голосу користувача під час взаємодії з віртуальними агентами. До нього належать такі параметри, як гучність, висота, тембр, інтонаційний малюнок, а також темп мовлення. Наприклад, підвищена гучність у поєднанні з чіткою артикуляцією може свідчити про впевненість і контроль над ситуацією, тоді як приглушений або тремтячий голос – про знервованість або невпевненість. Голос є важливим носієм емоцій, тому він дозволяє системі оцінювати як емоційний стан, так і комунікативну ефективність користувача.

Компонент O_{eye} відповідає за поведінку очей. За допомогою технології відстеження погляду фіксується напрямок, фіксації, тривалість зорового контакту з віртуальним співрозмовником або об'єктами в середовищі. Якщо користувач уникає зорового контакту, це може вказувати на невпевненість або сором'язливість. Якщо він слідує за співрозмовником, підтримує погляд, це розглядається як ознака соціальної активності та включеності в діалог. Очі також можуть бути джерелом непрямих сигналів тривожності чи стомлення, наприклад, у вигляді частого кліпання.

Компонент O_{task} охоплює ті аспекти поведінки користувача, які пов'язані безпосередньо з виконанням завдання у VR-сценарії. Це може бути вибір дій у симульованій ситуації, час реакції, точність відповідей, послідовність кроків або логічна побудова висловлювань. Така інформація дає змогу оцінити, наскільки ефективно користувач застосовує свої soft skills на практиці: як він приймає рішення, чи вміє слухати, чи здатний до діалогу, чи може проявити ініціативу.

Усі чотири компоненти спостереження не ізольовані – навпаки, вони взаємопов'язані. Аналізуючи їх у сукупності, інформаційна система формує

повноцінну картину поведінки користувача, від якої залежить адаптація сценарію, складність завдання, тип фідбеку і, зрештою, ефективність навчання. Спостереження, таким чином, є головним джерелом даних для оцінки рівня навичок і динаміки їх розвитку, а також для побудови моделі особистості.

Розглянемо типовий сценарій, який розбито на кроки $t = 0, 1, \dots, T$. На кожному кроці виконуємо дії: агент/система обирає дію a_t ; середовище переходить $s_{t+1} \sim T(\cdot | s_t, a_t)$; спостерігається $o_{t+1} \sim Z(\cdot | s_{t+1})$; нараховується нагорода $r_{t+1} = R(s_{t+1}, a_t)$.

Висновок. Запропонована абстрактна модель VR-середовища для розвитку soft skills демонструє, що такі середовища доцільно описувати як системи з частковим спостереженням, у яких навчання відбувається через замкнений зворотний зв'язок між діями користувача та зміною сценарію. Формалізація у вигляді POMDP дозволяє врахувати неповноту сенсорних даних і будувати політики тьютора-агента, орієнтовані на зниження конфліктності, підтримку користувача чи ускладнення завдання. Декомпозиція спостережень на чотири канали (жести, голос, погляд, поведінка в завданні) забезпечує більш точне відтворення прихованого стану та підвищує якість адаптації. Модель дає можливість оцінювати не лише кінцевий результат сценарію (наприклад, успішність переговорів), а й динаміку емоційного стану, що особливо важливо для тренування комунікативних і стресостійких навичок. На цій основі можуть проєктуватися VR-тренажери з автоматизованим тьюторингом і персоналізацією навчальних траєкторій.

Перелік посилань

1. GBD 2021 Stroke Risk Factor Collaborators. (2024). Global, regional, and national burden of stroke and its risk factors, 1990–2021: A systematic analysis for the Global Burden of Disease Study 2021. *The Lancet Neurology*, 23(10), 973–1003.
2. Feigin, V. L., & Owolabi, M. O. (2023). Pragmatic solutions to reduce the global burden of stroke: A World Stroke Organization–Lancet Neurology Commission. *The Lancet Neurology* Commissions, 22(12), 1160–1206.
3. GBD 2019 Stroke Collaborators. (2021). Global, regional, and national burden of stroke and its risk factors, 1990–2019: A systematic analysis for the Global Burden of Disease Study 2019. *The Lancet Neurology*, 20(10), 795–820.
4. Jiménez-Picón, N., Romero-Martín, M., Ponce-Blandón, J. A., Ramirez-Baena, L., Palomo-Lara, J. C., & Gómez-Salgado, J. (2021). The relationship between mindfulness and emotional intelligence as a protective factor for healthcare professionals: Systematic review. *International Journal of Environmental Research and Public Health*, 18, 5491.
5. Mata, Á. N. D. S., de Azevedo, K. P. M., Braga, L. P., de Medeiros, G. C. B. S., de Oliveira Segundo, V. H., Bezerra, I. N. M., Pimenta, I. D. S. F., Nicolás, I. M., & Piuevam, G. (2021). Training in communication skills for self-efficacy of health professionals: A systematic review. *Human Resources for Health*, 19, 1–9.
6. Skills You Need. (2024). Rapport: Interpersonal skills. <https://www.skillsyouneed.com/ips/rapport.html>

УДК 004.056

Рисований О.М.

Національний Технічний Університет "Харківський політехнічний інститут"

РОЗРОБКА АЛГОРИТМУ ОТРИМАННЯ ПСЕВДОВИПАДКОВОЇ ПОСЛІДОВНОСТІ НА ОСНОВІ РЕГИСТРУ ЗСУВУ

У роботі приводиться алгоритм отримання псевдовипадкової послідовності на основі реєстру звернення зі зворотними зв'язками та кроки по перетворенню цього алгоритму для отримання псевдовипадкової послідовності для кінцевого поля Галуа $GF(3)$.

The paper presents an algorithm for obtaining a pseudo-random sequence based on a feedback shift register and steps for transforming this algorithm to obtain a pseudo-random sequence for a finite Galois field $GF(3)$.

У сучасному світі псевдовипадкові послідовності відіграють ключову роль у безлічі інформаційних та технічних систем. Їх використання є актуальним завдяки тому, що вони дозволяють моделювати випадковість в умовах, коли справжні джерела випадкових даних недоступні або надто дорогі для реалізації.

Сучасні обчислювальні системи, телекомунікації та кібербезпека вимагають надійних механізмів генерації даних, що мають властивості випадковості.

Псевдовипадкові послідовності дозволяють формувати унікальні ключі та сесії при шифруванні даних; моделювати невизначені процеси у симуляціях та обчислювальній математиці; створювати тестові дані у системах контролю та діагностики.

Псевдовипадкові послідовності використовуються в генераторах тестових послідовностей, в псевдовипадкових модуляторах (CDMA, GSM), потокових шифрах (A5/1, LFSR-коди в Bluetooth, Wi-Fi), в CRC-кодах при контролі помилок, а апаратних генераторах випадкових чисел.

Метою роботи є розробка алгоритму отримання псевдовипадкової послідовності, який без значних додаткових перетворень міг би застосовуватися і для отримання такої послідовності з нелінійними елементами перетворення в кінцевому полі.

Основним способом отримання псевдовипадкової послідовності є спосіб, заснований на застосуванні поліном $P(x)$ [1-3]. І тут застосуємо весь математичний апарат алгебри, дискретної математики та інших галузей математики. Це дозволяє математично описувати такі послідовності, виконувати розрахунки характеристик поліномів та за необхідними критеріями вибирати оптимальні, проводити математичне моделювання поведінки таких послідовностей.

Поліном $P(x)$ (він же багаточлен), який застосовується при отриманні псевдовипадкової послідовності має вигляд:

$$P(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x + a_0x^0$$

де знак $+$ - це операція mod, n - ступінь полінома, a_i - коефіцієнти при відповідних ступенях, $a_0 = 1$.

Для отримання псевдовипадкової послідовності з використанням $P(x)$ інших ступенів необхідно отримати їх стани матриці і кожен стовпець перевести в десяткове число.

Операція mod2 застосовується у тому випадку, якщо обробляються 2 стани: 0 та 1.

На підставі полінома $P(x)$ будується цифрова схема, основою якої є зсувний регістр, а зворотні зв'язки на вхід першого тригера через суматор модуля подаються на основі ступенів обраного полінома.

Таким чином формується матриця вихідних станів:

$$H = /h_1, h_2, h_3, h_4 \dots h_n /$$

Алгоритм отримання псевдовипадкової послідовності може бути таким:

1. Вибирається поліном. Він повинен мати максимальний період генерації, $T_{max} = 2^n - 1$. Мінус 1 означає, що в послідовності немає стовпця з нульовими станами, інакше регістр почне зрушувати нулі і перестане генерувати псевдовипадкову послідовність.

2. За показниками ступенів обраного полінома будується схема генератора на основі регістру зсуву зі зворотними зв'язками.

3. У перший тригер регістру зсуву записується 1 (якщо застосовується mod2). Практично – цей стан дорівнює a^0 полінома. Перший стан регістру $h_1 = 1000$.

Кількість розрядів h_i дорівнює максимальному ступеню полінома.

4. Розраховуємо наступний стовпець.

Для отримання значень 2-го стовпця в комірки другого стовпця робиться косий зсув з першого, а у вільний перший тригер другого стовпця записується сума по mod2 станів з першого (попереднього) стовпця, номери яких рівні ступеням обраного полінома.

Таким чином формуються всі стовпці матриці псевдовипадкової послідовності.

5. Після отримання кожного нового стовпця робиться порівняння з першим стовпцем. Якщо стовпці збігаються, то всі попередні стовпці сформували псевдовипадковий цикл і процес генерації зупиняється. Розрахунок наступних циклів потрібно припинити, так як значення всіх циклів одного полінома однакові. А якщо псевдовипадкова послідовність використовується, наприклад, при тестуванні і не перший цикл генерації, то повністю порушується математичне обґрунтування пошуку розрядів, якими з'явився збій.

Кожен стовпець матриць станів є числом, послідовність яких називається псевдовипадковою. Для деяких поліномів $P(x)$ з них така псевдовипадкова послідовність наведена нижче:

- для $P(x) = 100101$:
1,2,5,10,21,11,23,14,29,27,22,12,24,17,3,7,15,31,30,28,25,19,6,13,26,20,9,18,4,8,16;
- для $P(x) = 101001$:
1,2,4,9,18,5,11,22,12,25,18,7,15,31,30,28,24,17,3,6,13,27,23,14,29,26,21,10,20,8,16;
- для $P(x) = P(x) = 101111$:
1,3,6,12,25,18,4,9,19,7,15,31,30,29,27,23,14,28,24,17,2,5,10,21,11,22,13,26,20,8,16;
- для $P(x) = P(x) = 111011$:
1,3,7,14,28,25,19,6,13,27,23,15,31,30,29,26,20,8,17,2,4,9,18,5,10,21,11,22,12,24,16.

Для отримання псевдовипадкової послідовності з використанням $P(x)$ інших ступенів необхідно отримати їх стани матриці і кожен стовпець перевести в десяткове число.

Запропонований алгоритм ґрунтується на суматорах за модулем 2. А для отримання псевдовипадкової послідовності в полі Галуа $GF(3)$ треба використовувати суматор $\text{mod}3$ і замість однієї лінії передачі чисел використовують пару ліній.

Операція підсумовування по модулю кінцевого поля 3 ($\text{mod}3$) відноситься до шифрування, при використанні операцій за правилами цього поля. При використанні трьох логічних станів (0, 1, 2) використовується $\text{mod}3$. Різниця при шифруванні між $\text{mod}2$ і $\text{mod}3$ в тому, що при $\text{mod}2$ необхідно один раз скласти дані, а при $\text{mod}3$ - виконати дві однакові додавання.

Таким чином, у роботі наводиться алгоритм отримання псевдовипадкової послідовності на основі регістру зсуву зі зворотними зв'язками та кроки щодо перетворення цього алгоритму для отримання псевдовипадкової послідовності для кінцевого поля Галуа $GF(3)$.

Перелік посилань

1. Рисований О.М., Ігнат'єв К.І., Рибалка Р.В., Рудаковський Д.Р. Механізм шифрування повідомлень з максимальною довжиною // Інформатика, управління та штучний інтелект. Тези одинадцятої міжнародної науково-технічної конференції. – Харків: НТУ "ХПІ", 2024. – 176 с. - С.127. Доступно: https://web.kpi.kharkov.ua/ai/wp-content/uploads/sites/249/2024/10/TEZY_IUSHI_2024.pdf (дата звернення: 5 вересня. 2025 р.).
2. Рисований О.М., Ігнат'єв К.І., Рибалка Р.В., Рудаковський Д.Р. Вибір багаточленів з максимальним періодом генерації станів // Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: тези доповідей XXXII міжнародної науково-практичної конференції MicroCAD-2024, 22-25 травня 2024 р. / за ред. проф. Сокола Є.І. – Харків: НТУ «ХПІ». – С. 1421 <https://science.kpi.kharkov.ua/wp-content/uploads/2024/05/Zbirnik-tez-MicroCAD-2024.pdf>.
3. Рисований О.М. Криптостійний генератор псевдовипадкової наслідності з використанням майстер-ключа // Проблеми інформатики та моделювання (ПІМ-2024). Тези двадцять четвертої міжнародної науково-технічної конференції. – Харків: НТУ "ХПІ", 2024. – С.120. https://web.kpi.kharkov.ua/pim/wp-content/uploads/sites/248/2024/10/Programma_PYM_2024_09_20.pdf

УДК 004.8

Романов Б.А., Бармак О.В., Багрій Р.О., Скрипник Т.К.

Хмельницький національний університет

МЕТОД КЛАСИФІКАЦІЇ ПРОГРАМНИХ ВИМОГ З ВИКОРИСТАННЯМ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ (LLM)

Запропоновано підхід до класифікації програмних вимог, який поєднує великі мовні моделі (LLM) з некерованими методами кластеризації. Розглянутий метод використовує попередньо навчену модель RoBERTa для генерації глибоких контекстно-залежних векторних представлень текстів вимог. Розглянуто можливість доменної-адаптації LLM як спосіб покращення результатів некерованих методів кластеризації.

Proposed an approach of classification of software requirements combines Large Language Models (LLMs) with unsupervised clustering methods. Proposed method is using pre-trained RoBERTa model to generate deep context-dependent vectorized features of software requirements. The possibility of domain-adaptation of LLM is considered as a way to improve the results of unsupervised clustering methods.

Одною з основних проблем для класифікації програмних вимог є неоднозначність та суб'єктивність, оскільки вимоги часто можуть формуватися повсякденною мовою, це може призвести до їх неоднозначного сприйняття при спілкуванні з клієнтом.

Як приклад неоднозначності, слово «productivity» у загальному контексті може стосуватись ефективності праці, тоді як у вимогах до ПЗ воно часто набуває технічного відтінку (наприклад, швидкість обробки даних). Такі терміни, як «масштабованість», «зручність супроводу» чи «безпека», мають складні, багатогранні значення, повне розуміння яких вимагає спеціальних знань. Модель, яка не «розрізняє» тонкощі предметної області, змушена орієнтуватися лише на поверхневі синтаксичні шаблони, що знижує її надійність [1].

Для класифікації програмних вимог використовуються різні методи обробки текстів – від моделей з фіксованими ознаками до нейромережевих підходів. Сучасні дослідження спрямовані на створення спеціалізованих моделей, адаптованих до мови розробки програмного забезпечення (наукові публікації, технічна документація, вимоги з реальних проєктів) [2].

На початковому етапі для класифікації вимог активно використовувалися архітектури CNN та RNN. Моделі на основі CNN ефективно виділяли локальні ознаки (ключові слова та фрази), тоді як RNN/LSTM добре вловлювали послідовні залежності в тексті вимоги [3]. Їх основним недоліком є обмежене розуміння контексту – ці моделі мали труднощі з аналізом довгих та складних речень через

проблеми із «затухаючим градієнтом» та обмеженою здатністю враховувати контекст усієї вимоги.

Трансформерні архітектури, зокрема BERT, RoBERTa, в порівнянні є дещо кращими, оскільки мають перевагу наявності глибокого контекстуального розуміння. Завдяки механізму уваги (attention) та двонаправленому навчанню, BERT враховує контекст кожного слова з обох боків, що дозволяє краще розуміти семантику вимоги [4]. Але при цьому їх основними недоліками є великі обчислювальні потреби та чутливість до якості даних. Ефективність моделей сильно залежить від якості та розміру даних, на яких проводиться тонке налаштування.

Також, варто зазначити, що більшість існуючих робіт зосереджені на використанні керованого підходу навчання класифікатора [5]. Великі мовні моделі формують вектори ознак, де подібні вимоги можуть утворювати природні кластери, але при цьому некеровані методи класифікації, наприклад кластеризація, є малодослідженими.

Метою дослідження є розробка та експериментальна перевірка методу класифікації програмних вимог на основі кластеризації векторних представлень текстів, сформованих великою мовною моделлю. Запропонований підхід орієнтований на виявлення природних груп функціональних і нефункціональних вимог з можливістю проведення доменної адаптації для покращення результатів некерованої кластеризації.

Запропонований метод базується на використанні попередньо навченої великої мовної моделі RoBERTa-base, яка забезпечує отримання контекстно-залежних векторних представлень програмних вимог. Використання готової архітектури дає змогу уникнути тривалого етапу навчання з нуля та зосередитись на обробці ембедінгів і аналізі їхньої структури.



Рисунок 1 – Загальна схема методу класифікації програмних вимог, з використанням методів кластеризації

Першими кроками методу є завантаження та підготовка даних. Для тестування якості класифікації використано вибірку *FR_NFR_dataset* [6],

збалансовану до 1000 точок на клас (всього 2000 записів). На цьому етапі відбувається перетворення текстів в початкові числові представлення за допомогою функції токенизації. Оскільки в даному випадку використовується модель RoBERTa, для сумісності було використано токенизатор RoBERTa-base.

Наступним кроком є отримання векторних представлень ознак текстів. Для цього попередньо токенозовані тексти подаються на вхід мовної моделі, після чого вихідні вектори різних шарів об'єднуються використовуючи функції *pooling*. В якості *pooling* було використано останній шар [CLS].

Отримані вектори ознак розподіляються на групи використовуючи функцію кластеризації. Для цього використано метод HDBSCAN з мінімальним розміром кластеру 5 та значенням *cluster_selection_epsilon* = 0.

Останнім кроком є аналіз отриманих кластерів та оцінка точності конкретного підходу. Для цього було застосовано метрики *precision*, *recall* та F1. Метрика F1 об'єднує в собі значення *precision* та *recall*, доцільним є саме її використання для поверхневої оцінки якості розпізнавання функціональних та не функціональних вимог. Для оцінки якості кластеризації мітки, отримані алгоритмом HDBSCAN, зіставлялися з істинними мітками датасету FR_NFR_dataset з використанням оптимального зіставлення для розрахунку F1-міри.

Оскільки HDBSCAN може розпізнавати деякі значення як «шум», не відносячи їх до конкретних кластерів, було застосовано три основних стратегії оцінювання, а саме, використання «шуму» як окремого кластеру, припущення, що всі записи, помічені як «шум» є неправильними та оцінка лише розпізнаних кластерів без урахування «шуму».

Для початкового аналізу кластеризації використано базову модель RoBERTa. Початкові результати показали, що між функціональними та нефункціональними вимогами є видима межа, яку обраний метод кластеризації не зміг розпізнати. Також, спостерігалось значне змішування класів на графіку, що свідчить про неоднозначність деяких вимог тестової вибірки FR_NFR_dataset [6]. Кластеризація на виходах базової моделі RoBERTa показала низьку якість, що підтверджує необхідність доменної адаптації для завдань класифікації програмних вимог.

Тому, для покращення розподілу між цільовими класами, застосовано доменну адаптацію моделі з використанням стандартного та контрастивного навчання. Під час додаткового навчання використано окремий набір даних PROMISE [7] на протязі 20 епох навчання та голову-класифікатор, що приймає [CLS] токен останнього шару на вході [8]. Для оптимізації ваг застосовувався алгоритм AdamW з низькою швидкістю навчання ($lr = 2e - 5$) та регуляризацією ($weight\_decay = 0.01$). З метою забезпечення стабільності на початковому етапі навчання використовувався планувальник швидкості навчання з функцією «розігріву». Фінальна модель для подальшого аналізу була відібрана на основі найвищого значення F1-метрики на валідаційній вибірці.

Після завершення доменної адаптації відібрана модель, використовуючи безпосередньо навчену голову-класифікатор, досягла значень $F1 \sim 0.80$, за результатом тестування навченої голови-класифікатора.

При проведенні некерованої кластеризації з тими ж самими параметрами було досягнуто практично ідентичного результату $F1 \sim 0.80$ (при використанні різних підходів до обробки записів, розпізнаних як «шум»). Така наближеність до результату керованого класифікатора свідчить про те, що кластеризація може бути повноцінною альтернативою керованим методам після якісної доменної адаптації моделі (Рис. 2).

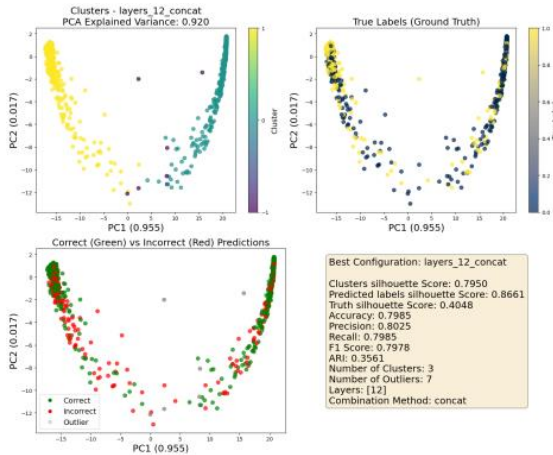


Рисунок 2 – Результати кластеризації після донавчання

Оскільки спостерігається помітний перетин між класами функціональних та нефункціональних вимог (Рис. 2), було застосовано метод контрастивного навчання для доменної адаптації, з ціллю створення більш чіткого розподілу вимог між класами. Контрастивне навчання проводилось з тими ж параметрами, що і початкове навчання, з використанням ваги 0.9 для функції втрат контрастивного навчання та 0.1 для функції втрат звичайного навчання.

Після завершення цього навчання було проведено порівняльний аналіз. Перевірка навченої голови-класифікатора показала F1 метрику ~ 0.80 , що наближається до результату стандартного донавчання.

Після цього було повторено аналіз з використанням некерованої кластеризації HDBSCAN ембедингів з самої мовної моделі з тими ж початковими параметрами (Рис. 3).

В результаті повторного аналізу F1-метрика некерованої кластеризації, залежно від стратегії обробки «шуму», досягла $F1 \sim 0.81\text{--}0.83$. Цей показник є вищим, ніж у еталонного керованого класифікатора ($F1 \sim 0.80$).

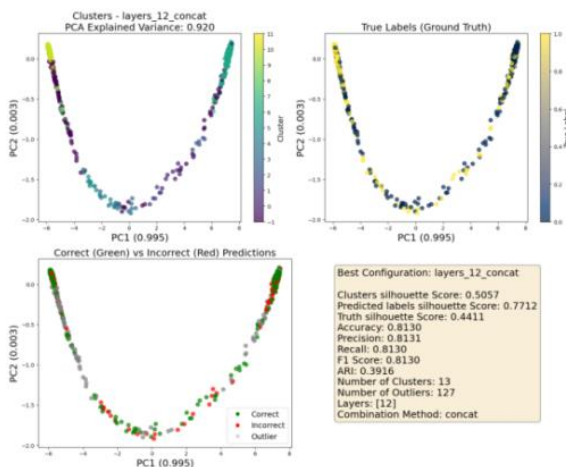


Рисунок 3 – Результат кластеризації HDBSCAN, навченої моделі, після контрастивного навчання

Ключова причина такого покращення полягає в тому, що контрастивне навчання змусило алгоритм HDBSCAN розпізнати значно більшу кількість семантично неоднозначних точок як «шум» (127) та змістити їх у простір між основними класами. Таким чином, експериментально доведено, що некерований підхід не лише перевершує за якістю керований, але й надає цінний інструмент для автоматичної ідентифікації та ізоляції проблемних вимог

Перелік посилань

1. Tiger Data. General-Purpose vs. Domain-Specific Embedding Models [Електронний ресурс]. URL: <https://www.tigerdata.com/blog/general-purpose-vs-domain-specific-embedding-models>.
2. Braun D., Klymenko O., Schopf T., Kaan Akan Y., Matthes F. The language of engineering: Training a domain-specific word embedding model for engineering // Proceedings of the 2021 3rd International Conference on Management Science and Industrial Engineering. Osaka, Japan, 2021.
3. Khayashi F., Jamasb B., Akbari R., Shamsinejadbabaki P. Deep learning methods for software requirement classification: A performance study on the PURE dataset. Shiraz, Iran, 2022.
4. Xu H. Applying the BERT algorithm for software requirements classification. 2024.
5. Rahman K., Ghani A., Misra S., Rahman A. U. A deep learning framework for non-functional requirement classification. 2024. T. 14, № 1.
6. Sonali S., Thamada S. FR_NFR_dataset [Електронний ресурс]. Mendeley Data, 2024. URL: <https://data.mendeley.com/datasets>.
7. Mitrevski A., Bezemer C.-P. PROMISE_exp: A collection of datasets for software requirements classification // Proceedings of the 13th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM). 2019.
8. Fine-tuning BERT and RoBERTa for high accuracy text classification in PyTorch [Електронний ресурс]. URL: <https://towardsdatascience.com/fine-tuning-bert-and-roberta-for-high-accuracy-text-classification-in-pytorch-c9e63cf64646>

УДК 004.4

Савчук В.В., Гартрамф М.С., Шкребета В.С., Мулярь І.В.

Хмельницький національний університет

МЕТОД ЗАХИСТУ ВЕБЗАСТОСУНКІВ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ТРАФІКУ

Розглянуто методи захисту інформаційних систем від загрозових програм на основі механізмів контролю доступу та розмежувальних політик. Запропоновано підхід до побудови багаторівневої системи захисту, що поєднує дискреційний, мандатний та рольовий контроль доступу з динамічними політиками безпеки. Результати дослідження демонструють, що правильно налаштовані механізми контролю доступу можуть суттєво знизити ймовірність успішного зараження системи та обмежити масштаби можливих наслідків.

Methods of protecting information systems from malicious programs based on access control mechanisms and separation policies are considered. An approach to building a multi-level protection system is proposed, combining discretionary, mandatory, and role-based access control with dynamic security policies. The results of the study demonstrate that properly configured access control mechanisms can significantly reduce the likelihood of successful system infection and limit the scale of possible consequences.

Шкідливе програмне забезпечення залишається однією з найважливіших проблем сучасної інформаційної безпеки. За даними дослідницьких компаній, щодня виявляється понад 450 000 нових зразків шкідливого програмного забезпечення, що ставить безпрецедентні виклики перед традиційними засобами безпеки [1]. Класичні антивірусні рішення, засновані на аналізі сигнатур, все частіше виявляються неефективними проти нових і модифікованих загроз, особливо коли зловмисники використовують техніки обфускації та поліморфізму [2].

У цьому контексті особливого значення набувають методи превентивного захисту, серед яких провідну роль відіграють механізми контролю доступу до інформаційних ресурсів. На відміну від реактивних методів виявлення загроз, контроль доступу запобігає виконанню шкідливих дій до їх здійснення, обмежуючи можливості потенційно небезпечного програмного забезпечення незалежно від його конкретної реалізації [3].

Метою даного дослідження є аналіз ефективності різних моделей контролю доступу в боротьбі зі шкідливими програмами та розробка рекомендацій щодо побудови комплексної системи захисту на основі політики розділення доступу. Актуальність дослідження обумовлена необхідністю пошуку альтернативних і

доповнюючих методів захисту в умовах постійної еволюції загроз і зростаючої складності інформаційних систем.

Для виявлення шкідливих програм використовуються різні методи аналізу коду. Одним з них є статичний аналіз. Статичний аналіз означає аналіз шкідливого програмного забезпечення без його виконання. Шаблони виявлення, що використовуються при статичному аналізі, включають підписи рядків, послідовності байтів, n-грами, виклики синтаксису бібліотеки, графіки потоків управління, аналіз частотного коду операційних кодів тощо. Аналіз виконується шляхом попереднього розпакування та декодування виконуваного файлу. Інструменти для розбирання та налагодження, аналізу дампа пам'яті використовуються для перегляду принципу роботи. Процес реінжинірингу показаний на рис. 1



Рисунок 1 – Аналіз загрозливих програм за використання підходу реінжинірингу

Технічні методи ухилення від статичного аналізу зловмисниками призвели до розвитку динамічного аналізу. Використання обфускації коду доводить неадекватність статичного аналізу для виявлення або класифікації шкідливих програм. Згідно з дослідженнями, динамічний аналіз є необхідним доповненням до статичного аналізу, оскільки він менш вразливий до затування.

Традиційний статичний контроль доступу, що базується на заздалегідь визначених політиках, може бути недостатнім проти складних цільових атак та загроз нульового дня. Динамічний контроль доступу, що адаптується на основі аналізу поточної ситуації безпеки, дозволяє автоматично підвищувати рівень захисту при виявленні підозрілої активності.

Системи виявлення аномалій аналізують поведінку процесів та користувачів, ідентифікуючи відхилення від встановлених базових показників. Машинне навчання дозволяє автоматично виявляти патерни, що характерні для шкідливої активності, навіть якщо конкретна загроза є новою та невідомою. При виявленні аномалій система може автоматично коригувати політики контролю доступу, обмежуючи можливості підозрілих процесів або користувачів до мінімуму. Наприклад, якщо процес починає звертатися до незвично великої кількості файлів, що може свідчити про активність програми-вимагача, його права доступу можуть бути автоматично обмежені до моменту з'ясування ситуації [4].

Контроль доступу на основі атрибутів (ABAC) є найбільш гнучкою та виразною моделлю серед сучасних підходів до управління доступом. На відміну від традиційних моделей, заснованих на ідентичності або ролях користувачів, ABAC приймає рішення на основі атрибутів суб'єктів, об'єктів, операцій та контексту середовища. Атрибутами можуть бути будь-які властивості, такі як відділ користувача, час доступу, рівень конфіденційності документа, тип операції, географічне розташування або поточний рівень загрози безпеці системи.

Політики ABAC формуються як правила, що визначають умови надання доступу на основі комбінацій атрибутів. Наприклад, правило може дозволяти тільки бухгалтерам читати фінансові документи в робочий час з корпоративної мережі, блокуючи доступ у всіх інших випадках. Така гнучкість дозволяє реалізовувати складні політики безпеки, що відображають реальні бізнес-вимоги та автоматично адаптуються до змін контексту.

Пропоноване рішення передбачає використання методу, заснованого на задачі матриці доступу. Цей метод контролю доступу кардинально відрізняється тим, що правила доступу формуються вже не для об'єкта, а для суб'єкта доступу. Для суб'єктів доступу встановлено, до яких об'єктів і за якими правилами (з якими правами) їм дозволений доступ, тобто правила доступу тут вже належать не об'єкту, а суб'єкту доступу. Запитуючи доступ, менеджер доступу отримує доступ до матриці доступу (таблиці правил) і зчитує з неї дозволені правила доступу суб'єкта до об'єкта, що з'являються в запиті, на основі чого аналізується правильність запиту. Крім того, необхідна інформація вноситься до журналу аудиту. Загальна схема реалізації ПД зображена на рис. 2.

Розроблено методи захисту від шкідливого програмного забезпечення з урахуванням вимог до побудови безпечної системи, спрямованої на запобігання витоку прав доступу під час її функціонування. Показано, що реалізація цих вимог на практиці істотно змінює традиційні підходи до організації контролю доступу до ресурсів, забезпечуючи більш гнучке та надійне управління дозволами користувачів і процесів.

Створено політику безпеки, яка підтверджує можливість практичної реалізації запропонованих методів і демонструє їх ефективність, а також зручність

адміністрування та експлуатації системи захисту. Політика визначає механізми моніторингу дій користувачів, виявлення ненормальної активності, динамічного оновлення прав доступу та ізоляції потенційно небезпечних процесів.

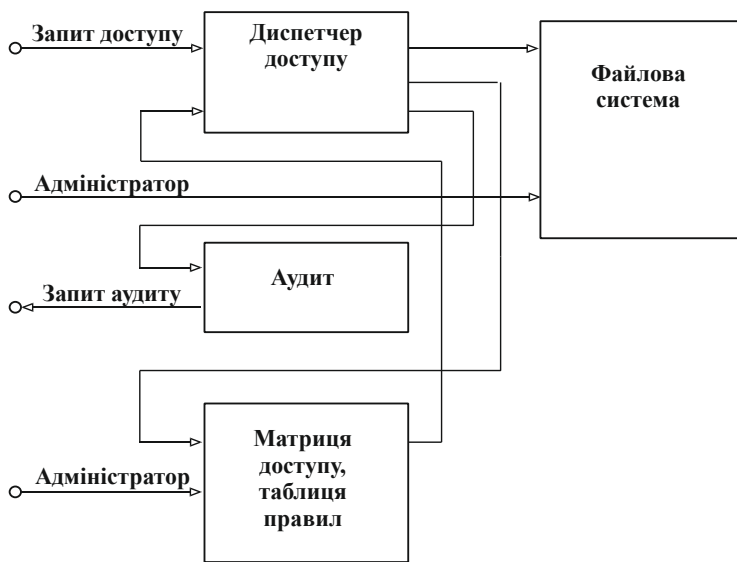


Рисунок 2 – Реалізація запропонованого рішення

Це підвищує стійкість системи до внутрішніх і зовнішніх загроз, знижує ризик несанкціонованого доступу та забезпечує відповідність сучасним вимогам кібербезпеки в інформаційних і обчислювальних середовищах.

Перелік посилань

1. AV-TEST Institute. Malware statistics & trends report 2024. AV-TEST GmbH, 2024. 45 p.
2. Information Security Handbook/ Noor Zaman Jhanjhi, Khalid Hussain, Mamoona Humayun, Azween Bin Abdullah, João Manuel R.S. Tavares. CRC Press, 2022. 250 p.
3. Інформаційна безпека в комп'ютерних мережах: навч. посіб./ О.А. Смірнов, Конопліцька-О.К. Слободенюк, С.А. Смірнов, К.О. Буравченко, Т.В. Смірнова, Л.І. Поліщук. Кропивницький: Видавець Лисенко В. Ф., 2020. 295 с.
4. Research of the Neural Network Module for Detecting Anomalies in Network Traffic/ Klots Y., Titova V., Petliak N., Cheshun V., Salem A.-B.M. CEUR Workshop Proceedings, 2022. 3156. P. 378–389

УДК 004.4

Сиротенко Д.А., Троц В.В., Анікін В.А.

Хмельницький національний університет

РИЗИКИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ З ПЕРСПЕКТИВИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Розглядається класифікація та аналіз ризиків, що виникають внаслідок швидкого впровадження систем штучного інтелекту (ШІ) у критичні сфери суспільного життя. Аналізується непрозорість моделей («чорна скринька»), упередженість у даних та потенціал до зловмисного використання, що створюють нові виклики для соціальної, економічної та кібернетичної безпеки. Окрім переваг автоматизації, розглянуто фундаментальні технічні та етичні проблеми, пов'язані з вирівнюванням цілей ШІ та людськими цінностями.

The classification and analysis of risks arising from the rapid implementation of artificial intelligence (AI) systems into critical areas of public life are examined. It is analyzed how model opacity ("black box"), data bias, and the potential for malicious use create new challenges for social, economic, and cybersecurity. In addition to the benefits of automation, the fundamental technical and ethical problems associated with aligning AI goals with human values are considered.

Штучний інтелект (ШІ) є однією з найдинамічніших технологій сучасності, яка впливає практично на всі сфери людської діяльності — від медицини до освіти, від кібербезпеки до державного управління. Проте разом із можливостями ШІ створює і нові ризики, пов'язані з безпекою, етикою, довірою та соціальними наслідками його застосування. Аналіз таких ризиків є необхідною умовою для формування ефективної стратегії впровадження та регулювання інтелектуальних систем.

Одним із головних викликів є поширення дезінформації та шахрайських схем на основі генеративних моделей. Від 2023 року спостерігається стрімке зростання кількості контенту, створеного за допомогою ШІ, зокрема зображень, відео та аудіо, що імітують реальність. Такі матеріали використовуються для маніпулювання громадською думкою, створення фейкових новин і навіть проведення фінансових шахрайських маніпуляцій через підробки голосу, створених за допомогою «deepfake». ШІ-боти здатні автоматично генерувати коментарі в соціальних мережах, імітуючи людську поведінку, що ускладнює виявлення неправдивої інформації. Це веде до втрати суспільної довіри та зростання інформаційної вразливості громадян [1].

Засоби штучного інтелекту також активно використовуються як для атак, так і для захисту на відеотрафік, системи цифрової автентифікації, та інші об'єкти інформаційної безпеки, з мінімізацією людського фактору зловмисника, та суттєво знижуючи поріг вимог до його професійної підготовки та навичок. Фактор наявності подібних систем захисту важливо враховувати при проектуванні сучасних систем захисту. З іншого боку, подібні засоби можуть застосовуватись також і в безпосередньо системах захисту підприємств, делегуючи частину рутинних обов'язків ШІ, проте вони обов'язково повинні обладнуватись додатковими засобами моніторингу, або експертними системами для додаткової перевірки.

Наступним аспектом є етичні виклики та можливі упередження в алгоритмах. Навіть найрозвинутіші системи машинного навчання не є нейтральними. Вони відображають структуру та упередження даних, на яких їх навчено, що може призвести до дискримінації певних соціальних або етнічних груп. На конференції NeurIPS (Ванкувер, 2020) було наголошено на необхідності прозорості та контролю над системами, які використовуються у сферах, де існує ризик шкоди для вразливих категорій населення, зокрема у прогновному поліцейському аналізі або системах розпізнавання обличч. Застосування таких технологій без належного етичного нагляду може створювати алгоритмічну упередженість і навіть посилювати соціальну нерівність [2].

Крім того, важливим класом ризиків є проблеми конфіденційності та прозорості прийняття рішень. ШІ системи часто функціонують як «чорні скриньки», що ускладнює можливість пояснення логіки їхніх рішень. Це створює труднощі для користувачів і регуляторів, адже людина може не мати можливості оскаржити рішення, ухвалене автоматизованою системою. Також зберігання та аналіз великих обсягів персональних даних створює ризики витоку, несанкціонованого доступу або неетичного використання інформації [2].

Окрему увагу варто приділити технічним та операційним ризикам. ШІ системи можуть функціонувати непередбачувано внаслідок помилок у навчальних даних або некоректного налаштування параметрів. Коли система стикається з невідомими умовами, вона може ухвалювати некоректні рішення, що призводить до небезпечних наслідків. Цю проблему описують як необхідність «людини в циклі» – постійного нагляду людини над процесом прийняття рішень ШІ. Це особливо важливо у критичних галузях, таких як медицина або транспорт, де помилка системи може мати фатальні наслідки [3].

Існує також соціальний вимір ризиків, пов'язаний із впливом ШІ на ринок праці, освіту та демократичні інститути. Масова автоматизація процесів може призвести до втрати робочих місць у низці професій, тоді як інші сфери потребуватимуть нових компетенцій. Це створює загрозу технологічної нерівності, коли доступ до передових інструментів мають лише великі корпорації або висококваліфіковані працівники. Європейська стратегія щодо ШІ (EU AI Act)

робить акцент на етичності та людському контролі, тоді як США зосереджуються на стимулюванні інновацій, а Китай — на державному регулюванні та централізованому використанні ШІ у публічному секторі [3].

Узагальнюючи, можна виділити такі основні класи ризиків, пов'язаних із впровадженням систем штучного інтелекту:

Інформаційні ризики – поширення дезінформації, маніпуляції та втрати довіри суспільства.

Етичні ризики – алгоритмічна упередженість, дискримінація та порушення прав людини.

Конфіденційність і прозорість — обмежений контроль користувачів над прийняттям рішень системами ШІ.

Технічні ризики – непередбачувані збої, помилки та необхідність людського нагляду.

Соціально-економічні ризики — нерівність, втрати робочих місць, відсутність адаптації до нових технологій.

Для мінімізації цих загроз необхідне створення етичних стандартів, законодавчої бази та механізмів аудиту ШІ, а також навчання населення медійної грамотності та критичному мисленню. Важливо забезпечити міждисциплінарний підхід, де розробники, юристи, етики та освітяни спільно формуватимуть правила безпечного та справедливого використання штучного інтелекту.

Таким чином, штучний інтелект є не лише технологічним проривом, а й серйозним викликом для сучасного суспільства. Його впровадження має супроводжуватися всебічним аналізом ризиків, спрямованим на збереження безпеки, прозорості, рівності та довіри між людиною і технологіями.

Перелік посилань

1. The impact of AI. URL: <https://www.ibm.com/think/insights/impact-of-ai>.
2. The impact of artificial intelligence on human society and bioethics. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC7605294/>.
3. The Impact of Artificial Intelligence on Modern Society. URL: <https://www.mdpi.com/2673-2688/6/8/190>.

УДК 004.8

Скрипнюк О.Ю., Манзюк Е.А., Багрій Р.О., Петровський С.С.

Хмельницький національний університет

МЕТОД ВИЯВЛЕННЯ ТРАСУВАЛЬНИХ ЗВ'ЯЗКІВ МІЖ ВИМОГАМИ ТА ПРОГРАМНИМ КОДОМ ІЗ ВИКОРИСТАННЯМ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ

Запропоновано метод автоматичного встановлення трасувальних зв'язків між вимогами програмного забезпечення та програмним кодом на основі великих мовних моделей (LLM). Метод реалізує багаторівневу архітектуру, що складається з модулів підготовки даних, генерації ембедингів, пошуку, оцінювання та візуалізації результатів. Проведено експериментальне дослідження на наборі MSR-2021, у якому порівняно модель CodeBERT із TF-IDF та SBERT, а також оцінено вплив структурного контексту, параметра Top-K. Отримані результати підтверджують ефективність методу та можливість його масштабування для реальних проєктів.

A method for automatic detection of traceability links between software requirements and source code using Large Language Models (LLMs) is proposed. The method implements a multi-layer architecture with modules for data preparation, CodeBERT-based embedding generation, retrieval, evaluation, and visualization. Experiments on the MSR-2021 dataset compare CodeBERT with TF-IDF and SBERT, analyzing the effects of structural context, Top-K parameter. Results confirm the method's efficiency and scalability for real software projects.

Трасування вимог у програмному забезпеченні забезпечує контроль узгодженості між вимогами й реалізацією, даючи змогу виявляти невідповідності, оцінювати вплив змін і підтримувати прозорість процесу розробки [1]. Ручне виконання трасування є трудомістким і схильним до помилок, особливо у великих проєктах. Класичні методи, засновані на статистичних або лексичних підходах, таких як TF-IDF чи LSI, враховують лише частотні співвідношення слів, не розуміючи їхнього контексту [2]. Розвиток трансформерних архітектур і поява великих мовних моделей дозволяють застосовувати семантичне зіставлення між текстовими та програмними артефактами [3]. Що стало підґрунтям для подальших досліджень у цій сфері.

Проблема трасування вимог розглядається у численних працях як один із ключових аспектів управління вимогами. У подальших дослідженнях [4] було запропоновано референтні моделі та інструменти автоматизації. Впровадження глибинного навчання та моделей типу трансформерів дозволило формувати спільний embedding-простір для тексту й коду, де семантично близькі об'єкти розміщуються поруч [5]. Для оцінювання ефективності таких моделей створено

еталонний набір Traceability Dataset for Open Source Systems (MSR-2021), що містить чотири відкриті проєкти (GanttProject, eTour, SMOS, iTrust) [6].

А також застосування нейронних підходів до трасування показало можливість суттєвого підвищення якості ідентифікації зв'язків між вимогами та кодом [7], а дослідження у сфері Explainable AI підтвердили, що LLM можуть пояснювати знайдені відповідності природною мовою [8]. На основі цього було сформульовано мету роботи.

Метою дослідження є розроблення методу виявлення трасувальних зв'язків між вимогами та програмним кодом із використанням великих мовних моделей, що забезпечує підвищення точності трасування та скорочення часу аналізу.

Запропонований метод складається з п'яти послідовних етапів (рис. 1):

1. Підготовка даних. Вхідними даними є JSON-файли вимог, методів і трасувальних пар. Дані очищуються від шуму, токенізуються й нормалізуються.

2. Генерація ембеддингів. Для кожного тексту вимоги та методу коду обчислюється векторне представлення за допомогою моделі microsoft/CodeBERT-base. Отримані вектори зберігаються у матрицях для подальшого пошуку.

3. Пошук схожих елементів. Для кожної вимоги обчислюється косинусна схожість із усіма методами, формуються топ-k кандидатів за значенням схожості.

4. Ранжування результатів. Отримані кандидати упорядковуються за релевантністю, після чого застосовується поріг для формування трасувальних зв'язків.

5. Оцінювання ефективності. Порівняння виявлених зв'язків із еталонними проводиться за метриками Precision, Recall, F1-score, MAP та MRR.

На рисунку 1 показана схема методу трасування.

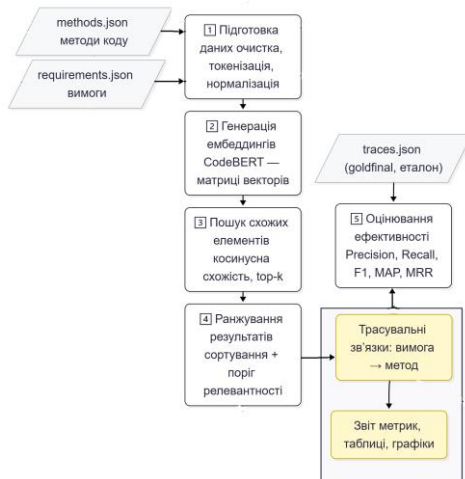


Рисунок 1 – Схему методу трасування вимог

Експериментальне дослідження проводилося на наборі MSR-2021 (з основним проектом GanttProject) з використанням метрик Precision, Recall, F1-score, MAP та MRR.

Першочерговим завданням було визначити оптимальну конфігурацію методу на основі CodeBERT. Оскільки модель CodeBERT дозволяє враховувати структурні елементи коду, було досліджено вплив структурного контексту (додавання назви класу та тіла методу до аналізу) на якість трасування.

У таблиці 1 наведено порівняльні результати для конфігурації CodeBERT з урахуванням повного контексту (className + sourceCode) та без нього (fullmethod)

Таблиця 1 – Вплив урахування структурного контексту на якість трасування

Конфігурація CodeBERT	Precision	Recall	F1-score	MAP	MRR	Top-K Recall
Без контексту (fullmethod)	0.74	0.0185	0.0363	0.0159	1.00	1.00
З урахуванням className + sourceCode	0.85	0.0237	0.0460	0.0212	1.00	1.00

Як видно з таблиці 1, додавання структурної інформації забезпечує суттєвий приріст ефективності. Найбільш показовим є стрибок точності з 0.74 до 0.85. Показник F1-score, що балансує точність і повноту, також демонструє зростання (з 0.0363 до 0.0460). Це пояснюється тим, що модель отримує доступ до повного семантичного змісту коду, а не лише до його назв, що дозволяє їй генерувати надійніші трасувальні зв'язки.

Оскільки конфігурація з урахуванням контексту показала себе як значно ефективніша, саме вона була використана для подальшого порівняння з іншими базовими методами трасування: TF-IDF та SBERT. Для цього порівняння було зафіксовано параметр K=100. Порівняльні результати роботи моделей наведено в таблиці 2.

Таблиця 2 – Порівняльні результати моделей TF-IDF, SBERT і CodeBERT

Модель	Precision	Recall	F1-score	MAP	MRR	Top-K Recall
TF-IDF	0.78	0.0217	0.0422	0.0168	1.00	1.00
SBERT	0.79	0.0220	0.0428	0.0188	1.00	1.00
CodeBERT	0.85	0.0237	0.0460	0.0212	1.00	1.00

Як видно із таблиці 1, усі три моделі демонструють порівняно низький F1-score (в діапазоні 0.042–0.046). Це пояснюється вкрай низькими показниками

повноти (Recall $\sim 0.022-0.024$), що є характерним для налаштувань з високим пріоритетом точності.

Ключовим та найбільш показовим результатом з цього порівняння є суттєве зростання точності. Модель CodeBERT досягає Precision = 0.85, що значно перевершує TF-IDF (0.78) та SBERT (0.79).

Важливо, що це значне підвищення надійності знайдених зв'язків досягається без погіршення повноти, яка залишається на стабільному, хоча й низькому рівні для всіх моделей. Це свідчить про те, що CodeBERT здатний краще враховувати семантичний контекст і структурні зв'язки, генеруючи більш релевантні (точні) трасувальні зв'язки, ніж лексичні чи стандартні семантичні моделі.

Оскільки було доведено ефективність використання розширеного представлення коду, наступним важливим елементом аналізу став параметр Top-K. Він визначає кількість кандидатів у списку знайдених зв'язків і безпосередньо впливає на повноту трасування – тобто на те, наскільки велика частка правильних зв'язків буде знайдена серед перших K варіантів.

Залежність якості трасування від значення K наведено в таблиці 3.

Таблиця 3 – Залежність метрик від параметра Top-K

K	Precision	Recall	F1-score	MAP	MRR	Top-K Recall
10	1.0000	0.0028	0.0055	0.0028	1.0000	1.0000
20	0.9000	0.0050	0.0100	0.0050	1.0000	1.0000
50	0.8600	0.0120	0.0236	0.0110	1.0000	1.0000
100	0.8500	0.0237	0.0460	0.0212	1.0000	1.0000
200	0.7950	0.0442	0.0838	0.0381	1.0000	1.0000
500	0.7700	0.1071	0.1881	0.0871	1.0000	1.0000
1000	0.7180	0.1998	0.3126	0.1564	1.0000	1.0000
2000	0.7110	0.3957	0.5084	0.2957	1.0000	1.0000

Як видно з таблиці 3, параметр K має вирішальний вплив на компроміс між точністю та повнотою. Зі зростанням K від 10 до 2000 спостерігається чітка тенденція: показник Повноти зростає зі слідового значення 0.0028 до суттєвого 0.3957. Водночас Точність поступово знижується з 1.0 до 0.711, оскільки у ширшій вибірці неминуче з'являється більше хибних зв'язків.

Завдяки такому домінуючому зростанню повноти, збалансований F1-score також демонструє значне покращення, піднімаючись з 0.0055 до 0.5084. Це підтверджує, що зі збільшенням кількості кандидатів (тобто "глибини пошуку") модель знаходить значно більше релевантних зв'язків.

Узагальнюючи наведені результати, можна стверджувати, що запропонований метод трасування вимог до програмного коду на основі великих

мовних моделей суттєво перевершує традиційні підходи. Модель CodeBERT забезпечує найвищі показники точності (0.85) та збалансованості метрик ($F1 = 0.046$ при $K = 100$, $F1 = 0.5084$ при $K = 2000$). Врахування структурного контексту підвищує семантичну точність, а оптимальне значення $\text{Top-K} = 500\text{--}1000$ забезпечує раціональний баланс між точністю й повнотою.

Отримані результати підтверджують ефективність запропонованого підходу для автоматизованого трасування вимог у масштабних програмних системах.

Перелік посилань

1. Mucha J., Kaufmann A., Riehle D. A systematic literature review of pre-requirements specification traceability. *Requirements Engineering*. 2024. Vol. 29, № 1. P. 1–25. - DOI: 10.1007/s00766-023-00412-z.
2. Horber D., Schleich B., Wartzack S. Procedure Model for Structured Relational Modeling of Requirements to Support Requirements-Oriented Decision Making. *Proceedings of the International Conference on Engineering Design (ICED21)*. 2021. P. 1–10. - DOI: 10.1017/pds.2021.505.
3. Rodriguez A. D., Dearstyne K. R., Cleland-Huang J. Prompts Matter: Insights and Strategies for Prompt Engineering in Automated Software Traceability. *arXiv*. 2023. arXiv:2308.00229. - URL: <https://arxiv.org/abs/2308.00229>.
4. Rodriguez A. D., Dearstyne K. R., Cleland-Huang J. Prompts Matter: Insights and Strategies for Prompt Engineering in Automated Software Traceability. *arXiv*. 2023. arXiv:2308.00229. - URL: <https://arxiv.org/abs/2308.00229>.
5. Gao H., Kuang H., Assunção W. K. G., Mayr-Dorn C., Rong G., Zhang H., Ma X., Egyed A. TRIAD: Automated Traceability Recovery based on Biterm-enhanced Deduction of Transitive Links among Artifacts. *Proceedings of the 46th International Conference on Software Engineering (ICSE 2024)*. 2024. P. 1–13. - DOI: 10.1145/3597503.3639164.
6. Hammoudi M., Mayr-Dorn C., Mashkoor A., Egyed A. A Traceability Dataset for Open Source Systems. 2021 IEEE/ACM 18th International Conference on Mining Software Repositories (MSR). 2021. P. 555–559. - DOI: 10.1109/MSR52588.2021.00073.
7. Ali S. J., Naganathan V., Bork D. Establishing Traceability between Natural Language Requirements and Software Artifacts by Combining RAG and LLMs. *Proceedings of the 26th International Conference on Model-Driven Engineering Languages and Systems (MODELS '24)*. 2024. P. 1–16.
8. Borg M. Code Gradients: Towards Automated Traceability of LLM-Generated Code to Requirements Using Explainable AI. 2024 IEEE/ACM 46th International Conference on Software Engineering Companion (ICSE-Companion). 2024. P. 261–263. - DOI: 10.1109/ICSE-Companion58145.2024.00070.

УДК 004.8

Соколовський В.С., Манзюк Е.А.

Хмельницький національний університет

МЕТОД КЛАСИФІКАЦІЇ ПАТОЛОГІЙ ЛИСТЯ РОСЛИН НА ОСНОВІ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ

Розглянуто метод автоматичної класифікації патологій листя рослин з використанням згорткових нейронних мереж глибокого навчання. Запропонована архітектура включає п'ять згорткових блоків для ієрархічного витягнення візуальних ознак та два повноз'єднані шари для класифікації. Метод забезпечує точність розпізнавання 93.2%.

A method for automatic classification of plant leaf diseases using deep learning convolutional neural networks is considered. The proposed architecture includes five convolutional blocks for hierarchical visual feature extraction and two fully connected layers for classification. The method achieves recognition accuracy of 93.2%.

Автоматична діагностика захворювань рослин є критично важливою для сучасного сільського господарства, оскільки дозволяє виявляти патології на ранніх стадіях та швидко реагувати на їх поширення [1-3]. Традиційні методи діагностики потребують експертизи агрономів та займають значний час, що ускладнює масштабування контролю. Використання згорткових нейронних мереж дозволяє автоматизувати процес розпізнавання патологій з точністю, порівнянню з експертною оцінкою. Дослідження в області застосування глибокого навчання охоплюють різноманітні напрямки: від адаптивної дистиляції знань у моделях глибокого навчання [5] до пояснюваного штучного інтелекту в медичній діагностиці [11]. Адаптивні підходи до навчання моделей, включаючи методи дистиляції знань [8] та генерації синтетичних даних [9], можуть бути використані для подальшого покращення точності класифікації. Методи машинного навчання також успішно застосовуються для аналізу складних патернів у різних предметних областях [4, 7, 10].

Метою роботи є розробка методу автоматичної класифікації патологій листя рослин на основі згорткових нейронних мереж, який забезпечує високу точність розпізнавання при прийнятній швидкості обробки для практичного застосування.

Запропонований метод базується на використанні глибокого навчання для автоматичного витягнення ознак з вхідних RGB-зображень листя рослин розміром 224×224 пікселі. На відміну від традиційних підходів, які потребують ручного проектування ознак, згорткові мережі автоматично навчаються виявляти значущі візуальні патерни через ієрархію шарів. Метод складається з трьох послідовних

етапів (рисунок 1), а саме попередня обробка зображення, витягнення ознак згортковими шарами та класифікація повнозв'язними шарами.



Рисунок 1 – Загальна схема методу класифікації патологій

Етап попередньої обробки включає зміну розміру зображень до фіксованих розмірів 224×224 пікселі з використанням білінійної інтерполяції та нормалізацію

значень пікселів до діапазону $[0, 1]$ шляхом ділення на 255. Для збільшення різноманітності навчальних даних застосовується аугментація: випадкове обертання ($\pm 20^\circ$), горизонтальне та вертикальне відзеркалення, зміна яскравості ($\pm 20\%$) та контрастності ($\pm 20\%$), випадковий зсув (до 10% розміру). Аугментація виконується в режимі реального часу під час навчання.

Базова архітектура мережі побудована на основі послідовного з'єднання п'яти згорткових блоків та двох повнозв'язних шарів (рисунок 2). Кожен згортковий блок має однакову структуру: згортковий шар з фільтрами розміром 3×3 , функція активації ReLU, батч-нормалізація та максимальний пулінг з вікном 2×2 . Така послідовність операцій є базовим будівельним блоком архітектури.

Перший блок використовує 32 фільтри для виявлення простих візуальних патернів, таких як краї, текстури та кольорові переходи. Другий блок має 64 фільтри для виявлення більш складних комбінацій простих ознак. Третій блок містить 128 фільтрів для формування середньорівневих представлень візуальних структур. Четвертий та п'ятий блоки використовують по 256 фільтрів кожен для витягнення високорівневих абстрактних ознак, специфічних для різних типів патологій. Така архітектура забезпечує поступове зменшення просторової розмірності при збільшенні кількості каналів ознак (таблиця 1).

Таблиця 1 – Параметри згорткових блоків архітектури

Блок	Фільтри	Розмір фільтра	Вихідний розмір
Блок 1	32	3×3	$112 \times 112 \times 32$
Блок 2	64	3×3	$56 \times 56 \times 64$
Блок 3	128	3×3	$28 \times 28 \times 128$
Блок 4	256	3×3	$14 \times 14 \times 256$
Блок 5	256	3×3	$7 \times 7 \times 256$

Після згорткової частини застосовується глобальний усереднений пулінг, який перетворює карти ознак розміром $7 \times 7 \times 256$ у вектор розмірністю 256, обчислюючи середнє значення по кожній карті. Це значно зменшує кількість параметрів порівняно з простим розгортанням карт у вектор. Перший повнозв'язний шар містить 512 нейронів з активацією ReLU для запобігання перетренуванню. Другий повнозв'язний шар має 256 нейронів також з ReLU та dropout 0.5. Вихідний шар використовує функцію софтмакс для перетворення виходів у розподіл ймовірностей по класах патологій.

Процес навчання моделі. Навчання виконується з використанням функції втрат крос ентропії та оптимізатора Адама з початковою швидкістю навчання 0.001. Використовується батч розміром 32 зображення та навчання протягом 50 епох з ранньою зупинкою при відсутності покращення на валідаційній вибірці протягом 10 епох. Батч-нормалізація прискорює збіжність та стабілізує процес навчання, а dropout запобігає перетренуванню.

Обґрунтування архітектурних рішень. Додавання п'ятого згорткового блоку після четвертого базового блоку дозволяє моделі формувати ще більш абстрактні представлення візуальних ознак патологій. Використання 256 фільтрів у останніх двох блоках забезпечує достатню виразну потужність для кодування складних патернів захворювань. Глобальний усереднений пулінг обраний замість простого розгортання через значне зменшення кількості параметрів (з 12544 до 256), що знижує ризик перетренування. Батч-нормалізація застосовується після кожного згорткового шару для нормалізації розподілу активацій, що прискорює навчання на 30-40%.

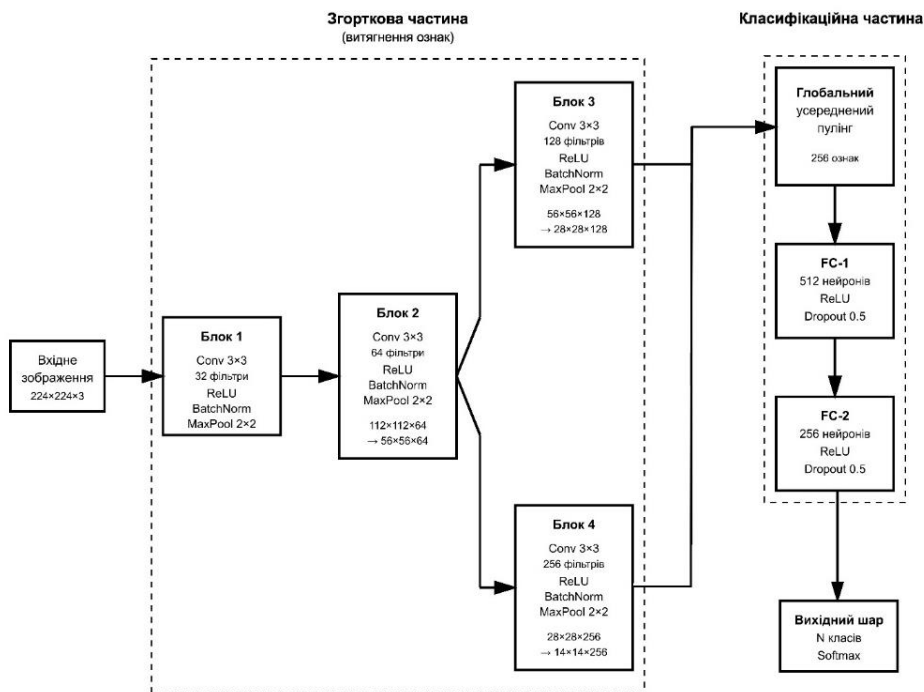


Рисунок 2 – Архітектура згорткової нейронної мережі

Метод було протестовано на датасеті, що містить близько 50000 зображень листя 14 культур з класами захворювань. Модифікована архітектура з п'ятьма згортковими блоками демонструє покращення точності на 1.8% порівняно з базовою версією. Аналіз матриці помилок показав, що найскладнішими для розпізнавання є ранні стадії захворювань, коли візуальні прояви є мінімальними. Модель найкраще розпізнає патології з яскраво вираженими візуальними

симптомами, такі як пізня стадія фітофторозу (F1-score 97.3%) або бактеріальна плямистість (F1-score 96.1%).

Отже, розроблений метод класифікації патологій листя на основі згорткових нейронних мереж забезпечує точність 93.2%. П'ятишарова згорткова архітектура з батч-нормалізацією ефективно витягує ієрархічні візуальні ознаки для розпізнавання класів захворювань. Метод є придатним для практичного застосування в мобільних системах діагностики та моніторингу здоров'я рослин.

Перелік посилань

1. Ningappa S. Detection and Classification of Diseases in Multi-Crop Leaves using LSTM and CNN Models // arXiv. – 2025. – URL: <https://arxiv.org/abs/2505.00741>
2. Yao J., Son T. Deep Learning for Plant Identification and Disease Classification from Leaf Images: Multi-prediction Approaches // arXiv. – 2023. – arXiv:2310.16273. – URL: <https://arxiv.org/abs/2310.16273>.
3. Ibrahim M. Plant Disease Detection using Region-Based Convolutional Neural Network // arXiv. – 2023. – arXiv:2303.09063. – URL: <https://arxiv.org/abs/2303.09063>.
4. Pavlyshyn V., Ryzhanskyi O., Manziuk E., Radiuk P., Barmak O., Krak I. Establishing Patterns of the Urban Transport Flows on Clustering Analysis. In Proceedings of the Second International Conference of Young Scientists on Artificial Intelligence for Sustainable Development (YAISD 2025). 2025. Vol. 3974. Pp. 1–9. URL: <https://ceur-ws.org/Vol-3974/paper01.pdf>.
5. Pavlyshyn V., Manziuk E., Barmak O., Radiuk P., Krak I. An Adaptive Machine Learning Approach to Sustainable Traffic Planning: High-Fidelity Pattern Recognition in Smart Transportation Systems. Future Transportation. 2025. Vol. 5, No. 4. URL: <https://doi.org/10.3390/futuretransp5040152>.
6. Pavlyshyn V., Manziuk E., Barmak O., Radiuk P., Krak I. Adaptive Cascade Clustering for High-Fidelity Urban Traffic Pattern Recognition. Computer Science and Mathematics, 2025. URL: <https://doi.org/10.20944/preprints202508.0637.v1>.
7. Manziuk E. A., Sobko O. V., Podhorniuk I. O., Molchanova M. O., Mazurets O. V. Multifactorial analysis of mobbing behavioral signs in educational environments posts by NLP means. Journal of Physics: Conference Series. 2025. Vol. 3105, No. 1. Pp. 012025. URL: <https://doi.org/10.1088/1742-6596/3105/1/012025>.
8. Chaban O., Manziuk E., Radiuk P. Method of adaptive knowledge distillation from multi-teacher to student deep learning models. Journal of Edge Computing. 2025. URL: <https://doi.org/10.55056/jec.978>.
9. Прийма А., Манзюк Е., Пасічник О., Скрипник Т. Метод генерації багатотрекових символічних композицій за допомогою генеративного штучного інтелекту. Herald of Khmelnytskyi National University. Technical sciences. 2025. Vol. 357, No. 5.1. Pp. 114–119. URL: <https://doi.org/10.31891/2307-5732-2025-357-59>.
10. Манчур О., Манзюк Е., Скрипник Т., Пасічник О., Петровський С. Метод визначення навантаження тренування атлетів з використанням машинного навчання. Herald of Khmelnytskyi National University. Technical sciences. 2025. Vol. 353, No. 3.2. Pp. 342–348. URL: <https://doi.org/10.31891/2307-5732-2025-353-48>.
11. Radiuk P., Barmak O., Manziuk E., Krak I. Explainable Artificial Intelligence: Transitioning DL Model Decisions to User-Understandable Features in Healthcare. 2024.

УДК 022

Старостенко К.В.

Кам'янський енергетичний фаховий коледж

АНАЛІЗ ЕФЕКТИВНОСТІ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК ТИПУ DDOS

У статті здійснено ґрунтовне дослідження проблеми ефективного виявлення розподілених атак типу "відмова в обслуговуванні" (DDoS). Проведено критичний аналіз існуючих сигнатурних методів захисту, які демонструють недостатню ефективність у протидії новим та гібридним атакам. Запропоновано підхід, що передбачає порівняльне оцінювання алгоритмів машинного навчання для класифікації мережевого трафіку з метою покращення результативності виявлення атак. Основним завданням роботи є ідентифікація найбільш ефективного алгоритму на основі таких критеріїв, як точність і швидкодія. В експериментальній частині дослідження використано публічно доступний датасет CIC-DDoS2019, результати аналізу якого свідчать про переваги ансамблевого методу "Випадковий ліс" ($F1\text{-score} = 0.988$) у порівнянні з лінійними підходами. Отримані дані підтверджують перспективність запропонованого підходу для створення високоефективних систем виявлення вторгнень у режимі реального часу.

The article provides a thorough study of the problem of effective detection of distributed denial of service (DDoS) attacks. A critical analysis of existing signature-based protection methods is carried out, which demonstrate insufficient effectiveness in countering new and hybrid attacks. An approach is proposed that involves comparative evaluation of machine learning algorithms for classifying network traffic in order to improve the effectiveness of attack detection. The main objective of the work is to identify the most effective algorithm based on criteria such as accuracy and speed. The experimental part of the study used the publicly available CIC-DDoS2019 dataset, the analysis results of which indicate the advantages of the ensemble method "Random Forest" ($F1\text{-score} = 0.988$) compared to linear approaches. The obtained data confirm the prospects of the proposed approach for creating high-performance intrusion detection systems in real time.

Метою даної доповіді є дослідження методів і технологій забезпечення Інтенсивна цифровізація сучасного суспільства та зростаюча залежність від інтернет-сервісів підсилюють загрозу, яку становлять атаки типу DDoS, перетворюючи їх на одну з найсерйозніших викликів у сфері кібербезпеки. Можливість таких атак призводити до дестабілізації функціонування критично важливої інфраструктури, фінансових організацій і державних ресурсів через перенасичення їх мережевим трафіком зумовлює необхідність розроблення високоефективних протидійних заходів. Зважаючи на те, що традиційні сигнатурні

системи виявлення часто демонструють низьку ефективність у боротьбі з новими, динамічно модифікованими і гібридними DDoS-атаками, виникає гостра потреба в розробці та впровадженні проактивних інтелектуальних підходів, заснованих на методах машинного навчання.

Питання виявлення DDoS-атак із застосуванням методів машинного навчання є предметом широко розглянутих наукових досліджень. У працях [1, 2] для класифікації мережевого трафіку ефективно використовуються алгоритми дерев рішень і випадкових лісів, які демонструють високу точність результатів. Водночас інші дослідження [3] пропонують застосування методів глибокого навчання, зокрема рекурентних нейронних мереж (RNN), для аналізу часових рядів, що описують мережеву активність. Попри досягнутий прогрес у цій галузі, питання порівняльної ефективності різноманітних алгоритмів залишається актуальним. Зокрема, ключовими аспектами аналізу залишаються показники точності, обчислювальної ефективності та здатності алгоритмів виявляти нуль-денні атаки. Саме ці аспекти становлять предмет дослідження в даній роботі.

Мета роботи полягає в здійсненні порівняльного аналізу ефективності алгоритмів класифікації машинного навчання для вирішення завдання виявлення DDoS-атак, а також у визначенні найбільш оптимального методу, який забезпечує баланс між точністю та швидкістю класифікації.

Для досягнення поставленої мети були виконані ключові етапи роботи. Як вихідні дані використано відкритий набір даних CIC-DDoS2019, що включає широкий спектр сучасних DDoS-атак. Із цього набору даних виділено основні характеристики мережевого трафіку, зокрема середню тривалість потоку, кількість пакетів за секунду, середній розмір пакета та протокольні параметри. Попередня обробка даних охоплювала видалення дублікатів, заповнення відсутніх значень і нормалізацію.

Для порівняння було обрано три алгоритми класифікації: логістичну регресію (як базовий класифікатор), випадковий ліс (потужний ансамблевий метод) та метод опорних векторів (SVM) із лінійним ядром. Ефективність моделей оцінювалася на основі метрик класифікації, таких як Accuracy, Precision, Recall, F1-score, а також за часом навчання та класифікації.

Результати експерименту продемонстрували, що алгоритм Випадковий ліс досяг найкращого співвідношення між точністю і продуктивністю, отримавши F1-score 0.988. Логістична регресія продемонструвала дещо нижчі результати (F1-score = 0.923), проте мала найкоротший час навчання. SVM показав високу точність (F1-score = 0.975), але потребував значних обчислювальних ресурсів для виконання класифікації. Це підкреслює ефективність ансамблевих методів для аналізу складних мережевих даних.

У дослідженні проведено порівняльний аналіз трьох алгоритмів машинного навчання для виявлення DDoS-атак. Серед них найкращі результати за сукупністю характеристик продемонстрував алгоритм Випадковий ліс, який відзначається високою точністю виявлення атак і прийнятною швидкістю. Отримані дані підтверджують доцільність його впровадження у системи виявлення вторгнень (IDS) реального часу. У подальших дослідженнях передбачається тестування глибоких нейронних мереж на більших наборах даних, а також створення гібридних моделей, здатних гнучко адаптуватися до нових видів DDoS-атак.

Перелік посилань

1. Aamir M., Zaidi S. M. A. DDoS Attack Detection with Feature Engineering and Machine Learning: The Framework and Performance Evaluation // International Journal of Information Security. – 2021. – Vol. 20. – P. 335–356.
2. Praseed A., Thilagam P. S. DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications // IEEE Communications Surveys & Tutorials. – 2019. – Vol. 21. – P. 661–685.
3. Yuan X., Li C., Li X. DeepDefense: Identifying DDoS Attack via Deep Learning // Proceedings of the IEEE International Conference on Smart Computing (SMARTCOMP). – 2017. – P. 1-8.
4. CIC-DDoS2019 Dataset [Електронний ресурс]. – Режим доступу: <https://www.unb.ca/cic/datasets/ddos-2019.html>.

УДК 004.41

Стецюк П.П., Форкун Ю.В.

Хмельницький національний університет

МЕТОД УДОСКОНАЛЕНОГО МОДУЛЬНОГО ПРОЄКТУВАННЯ АГЕНТНО-ОРІЄНТОВАНИХ ПРОГРАМНИХ СИСТЕМ З ПІДТРИМКОЮ РОЗШИРЮВАНOSTІ ТА ПОВТОРНОГО ВИКОРИСТАННЯ

У роботі представлено онтологічний підхід до модельного проектування мультиагентних систем. Розроблено метамодель та інструмент для автоматичної генерації коду. Запропонований підхід підвищує узгодженість моделей, скорочує час розробки й забезпечує формальну верифікацію систем.

The paper presents an ontological approach to model-based design of multi-agent systems. A metamodel and a tool for automatic code generation are developed. The proposed approach increases model consistency, reduces development time, and provides formal verification of systems.

Розглянуто підхід до вдосконалення процесів розробки мультиагентних систем (MAS) шляхом поєднання методів модельно-орієнтованої інженерії (MDE) та онтологій. Запропонована методика забезпечує уніфіковану модель, що охоплює три ключові виміри MAS — агентний, середовищний та організаційний — з метою інтеграції проектування, кодування та верифікації систем у єдиному семантичному просторі.

Мета роботи полягає у проведенні комплексного дослідження різних методів, для розробки онтологічних підходів у галузі моделювання MAS, зокрема для підтримки розробників MAS та дослідження його використання, а також збору та підготовці матеріалу для виконання наукової роботи.

Проведено аналіз існуючих методологій AOSE (агентно-орієнтованої інженерії програмного забезпечення), таких як наприклад Prometheus, які демонструють високий потенціал у створенні гнучких інтелектуальних систем, проте не забезпечують повної інтеграції різних рівнів моделювання. Запропонований підхід ґрунтується на онтологічній метамоделі, яка дозволяє здійснювати семантичне міркування, автоматичну генерацію коду та перевірку узгодженості між моделями та реалізацією.

У межах дослідження розроблено вдосконалений інструмент, що забезпечує перетворення моделей у вихідний код для платформи MAS. Цей підхід дозволяє скоротити час розробки, підвищити точність відтворення моделей у коді та уникнути розбіжностей між проектною специфікацією та реалізацією. Використання онтології як метамоделі забезпечує формальну специфікацію знань і

створює передумови для багаторазового використання компонентів MAS у різних проектах.

Ключові результати дослідження полягають у:

- формалізації методології онтологічного моделювання мультиагентних систем;
- створенні інтегрованої моделі, що поєднує агентів, середовище та організацію;
- розробці механізмів автоматичної генерації коду з онтологічних моделей;
- розробці інструментального середовища;
- оцінюванні ефективності підходу на різних прикладах проектів MAS.

Результати експериментів засвідчують, що використання онтологій на етапах проектування та програмування підвищує узгодженість компонентів, зменшує ризики помилок та сприяє підвищенню продуктивності розробки. Семантичне моделювання також забезпечує можливість автоматизованої перевірки властивостей системи на логічну несуперечність, що є важливим кроком до створення надійних та масштабованих інтелектуальних систем.

Запропонована методологія може бути застосована для розробки широкого спектра багатокомпонентних систем — від систем підтримки прийняття рішень до розподілених сервісних платформ. Отримані результати відкривають перспективи подальших досліджень у напрямі автоматизації агентного програмування, розвитку стандартів представлення знань та інтеграції онтологій у процеси інженерії програмного забезпечення.

Перелік посилань

1. Muhammad Yaseen, Esraa Ali , Nadeem Sarwar, Leila Jamel, Irfanud Din, Farrukh Yuldashev, Foongli Law. Design of Minimal Spanning Tree and Analytic Hierarchical Process (SAHP) Based Hybrid Technique for Software Requirements Prioritization. WileyIET SoftwareVolume 2025. Article ID 8819735, 23. URL: <https://doi.org/10.1049/sfw2/>
2. Harder D.W. A practical introduction to real-time systems for undergraduate engineering. University of Waterloo, 2023. 744p.
3. Ikram A., Jalil M. A., Ngah A. B. Project Assessment inOffshore Software Maintenance Outsourcing Using DeepEltreme Learning Machines, Computers, Materials and Continua 74.2023. 1871–1886
4. Alzayed A. Evaluating the Role of Requirements EngineeringPractices in the Sustainability of Electronic GovernmentSolutions, Sustainability 16, no. 1.2024
5. Hassan M. A., Zhang D. A Review on Industrial Robot Control and Applications. IEEE Access. 2021. Vol. 9. pp. 112–130.
6. Левченко Л. О. Архітектура системного програмного забезпечення: підручник. Київ.КІП ім. І. Сікорського. 2022. 497 с.
7. Копиленко О. Внутрішній пристрій MySQL для фахівців з оптимізації. Літура. 2023. 420с.

УДК 004.8

Тимофієв І.А., Мазурець О.В.

Хмельницький національний університет

НЕЙРОМЕРЕЖЕВИЙ ПІДХІД ДО ВИЯВЛЕННЯ ДЕПРЕСИВНИХ ПАТЕРНІВ ЗА АНАЛІЗОМ ТЕКСТОВОГО КОНТЕНТУ ЦИФРОВИХ СЕРВІСІВ У ЗАКЛАДАХ ОСВІТИ

Запропоновано метод виявлення депресивних патернів за аналізом текстового контенту цифрових сервісів у закладах освіти, що призначений для перетворення вхідних даних у вигляді тексту та навченої нейромережевої моделі дуальної архітектури у вихідні дані у вигляді числової оцінки наявності депресивного стану. Запропонований метод виявлення депресивних патернів за аналізом текстового контенту цифрових сервісів у закладах освіти відрізняється від аналогів тим, що поєднує двопоточну архітектуру, яка базується на використанні двох паралельних нейронних мереж, кожна з яких спеціалізується на аналізі різних аспектів тексту – синтаксичного та семантичного. Потік синтаксичного аналізу спрямований на виявлення синтаксичної структури тексту, а потік семантичного аналізу – на розуміння змісту та контексту тексту. Після обробки тексту кожним потоком результати комбінуються на рівні вищого шару, що дозволяє врахувати як деталі мовної структури, так і зміст тексту для точнішого визначення депресивного стану.

The method for detecting depressive patterns by analyzing the text content of digital services in educational institutions is proposed, which is designed to transform input data in the form of text and a trained neural network model of a dual architecture into output data in the form of a numerical assessment of the presence of a depressive state. The proposed method for detecting depressive patterns by analyzing the text content of digital services in educational institutions differs from its analogues in that it combines a two-stream architecture based on the use of two parallel neural networks, each of which specializes in analyzing different aspects of the text – syntactic and semantic. The syntactic analysis stream is aimed at detecting the syntactic structure of the text, and the semantic analysis stream is aimed at understanding the content and context of the text. After processing the text by each stream, the results are combined at the level of a higher layer, which allows taking into account both the details of the linguistic structure and the content of the text for a more accurate determination of the depressive state.

В умовах сучасного соціального і академічного середовища тиск, стрес і тривожність стали поширеними явищами, що можуть призвести до розвитку депресії [1, 2]. Особливо це актуально в умовах інтенсивного навчального процесу, високих вимог та обмеженого часу для відпочинку і саморегуляції [3]. Виявлення депресивних станів на ранніх етапах може суттєво вплинути на своєчасну підтримку та профілактику серйозніших психічних розладів [4].

В умовах цифровізації та широкого використання комунікаційних платформ [5], NLP стає потужним інструментом для моніторингу психологічного

стану студентів під час навчального процесу [6, 7]. Розробка і впровадження сучасних методів для автоматизованого виявлення депресивних ознак допоможе вчасно ідентифікувати осіб, які потребують допомоги, і забезпечити їм необхідну підтримку для покращення їхнього психічного здоров'я.

Сучасні підходи NLP, зокрема трансформерні моделі (BERT, RoBERTa, GPT-похідні моделі) [8, 9], контекстні ембеддинги та багаторівневі рекурентні архітектури [10], забезпечують високу чутливість до лінгвістичних маркерів [11], що можуть вказувати на емоційне виснаження [12], зниження мотивації [13], безнадійності або самоізоляцію [14] – ключові індикатори депресивних станів за текстовими даними. Нейромережеві моделі здатні виявляти як поверхневі [15], так і латентні [16] патерни: зменшення різноманітності лексики, часте використання негативно забарвлених слів, зниження рівня персональної агентності (“не можу”, “не знаю”, “мені байдуже”), емоційні контрасти, зміни тональності та синтаксичної структури [17, 18].

Важливою перевагою сучасного NLP є можливість моделювання контексту в широкій часовій перспективі: аналіз динаміки повідомлень користувача, виявлення стійких тенденцій, а не лише одиничних висловлювань [19]. Крім того, методи багатомодального аналізу дозволяють поєднувати текстові дані з поведінковими сигналами (активність у сервісі, частота звернень, часові патерни), що підвищує точність виявлення [20].

Подальший розвиток даного напрямку передбачає створення нейромережевих систем підтримки, здатних працювати в режимі анонімного, етичного та безпечного моніторингу текстового контенту. Особливо важливими є інтерпретованість моделей, використання методів Explainable AI (XAI) для пояснення рішень системи, а також адаптація лінгвістичних маркерів саме до українськомовного освітнього середовища, яке характеризується власними мовними, стилістичними та культурними особливостями.

Додаткові перспективи пов'язані з інтеграцією таких систем у цифрові освітні платформи для формування інтелектуальних модулів раннього сповіщення, персоналізованої підтримки та психологічної допомоги. Це сприятиме створенню безпечного освітнього простору, де цифрові технології використовуються не лише для навчання, а й для підтримки добробуту учасників освітнього процесу.

Метою роботи є розробка нейромережевого підходу до виявлення депресивних патернів за аналізом текстового контенту цифрових сервісів у закладах освіти.

Метод виявлення депресивних патернів за аналізом текстового контенту цифрових сервісів у закладах освіти полягає в трансформації вхідних текстових даних за допомогою навченої нейромережної моделі для отримання числової оцінки, що відображає ймовірність наявності депресивних проявів. Схема та кроки методу виявлення депресивних патернів за аналізом текстового контенту цифрових сервісів у закладах освіти наведені на рисунку 1.

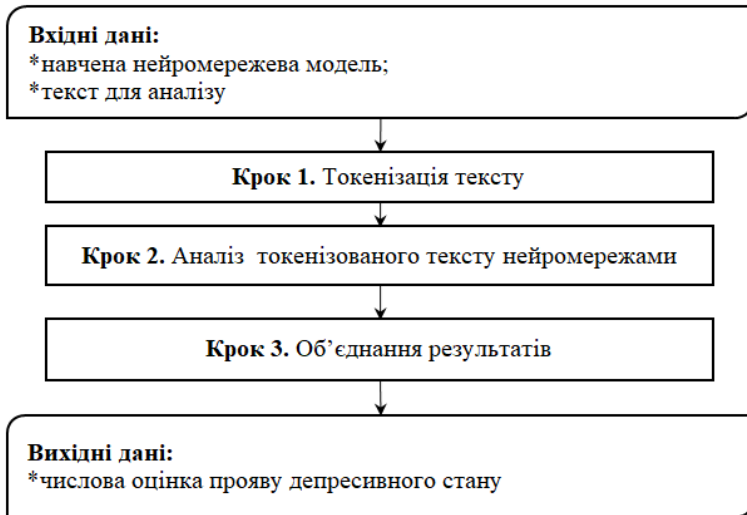


Рисунок 1 – Схема та кроки методу виявлення депресивних патернів за аналізом текстового контенту цифрових сервісів у закладах освіти

Вхідними даними методу виявлення депресивних патернів за аналізом текстового контенту цифрових сервісів у закладах освіти є нейромережева модель з дуальною архітектурою на основі трансформерів, що поєднує моделі BERT та GPT2, які відповідають за аналіз синтаксичного та семантичного контексту тексту користувача. Модель BERT використовується для синтаксичного аналізу, а GPT2 – для семантичного відповідно.

Першим етапом є токенизація тексту користувача з використанням токенизаторів моделей BERT та GPT2. Токенизатори використовуються такі, на яких було навчено нейромережу.

Наступним етапом є паралельний аналіз токенованого тексту обома нейромережами: BERT обробляє текст з точки зору синтаксичних залежностей, а GPT2 – з семантичної.

Третій етап передбачає об'єднання результатів обробки за допомогою спеціального злитого шару, що дозволяє отримати числову оцінку рівня депресивних проявів у тексті користувача. Вихідними даними є числова оцінка наявності депресивного стану в аналізованому тексті.

Вихідні дані методу виявлення депресивних патернів за аналізом текстового контенту цифрових сервісів у закладах освіти представляють собою числову оцінку прояву репресивності.

У якості даних дослідження буде використано набір «Student-Depression-Text», що містить інформацію у форматі «Excel», яка включає близько 7489 даних із

соціальних мереж, коментарів у «Facebook» тощо. Приклад даних з датасету наведено на рисунку 2.

Student-Depression-Text

14

New Notebook



Data Card Code (2) Discussion (3) Suggestions (0)

Detail	Compact	Column	5 of 5 columns			
Δ text	# label	# Age	Δ Gender	Δ Age Category		
7371 unique values			Male 54% Female 46% Other (3) 0%	Young Age 53% Teen Age 47% Other (3) 0%		
dis...						
keep it up hahaha	0	16	Male	Teen Age		
The match cycle I had.Buy-brought-out-lost.	0	16	Male	Teen Age		
nctb! jewel case dream, which doesn't have a poster, you can choose members using dhl, pls rep fp wi...	0	16	Male	Teen Age		
college but it's like not going to college, but not on vacation too confused	0	16	Male	Teen Age		
I often dream during the day np da :{	0	16	Male	Teen Age		
The romantic guy when he wants to eat at the warteg, the warteg is hugged from behind and then	0	16	Male	Teen Age		

Рисунок 2 – Приклад даних для навчання

Набір даних є анотованим англomовним набором, зібраним з людей які дуже добре володіють англійською мовою та є студентами, віковий діапазон від 15 до 17 [21]. Датасет містить текст, мітку, вік, вікову категорію та стать. У текстових стовпцях наявний текст «Нормальний стан» і «тривога/депресія», а стовпець мітки вказує, чи позначає відповідний текст тривогу чи депресію. Таке анотоване маркування дозволяє точно визначити та проаналізувати психологічний стан підлітків на основі їхніх висловлювань у соціальних мережах.

Записи в датасеті охоплюють віковий діапазон, що відповідає підлітковому періоду, коли ризик розвитку депресії є особливо високим. Датасет також містить демографічну інформацію, таку як стать і вікова категорія. Ці додаткові параметри дозволяють враховувати вплив гендерних та вікових факторів на прояви депресивних станів.

Продуктивність нейромережових моделей визначається метриками, до яких належать: точність, влучність, повнота, F_1 -міра та матриця невідповідностей.

Матриця невідповідностей представляє собою таблицю та відображає результати класифікації за такими полями: істинно позитивні, хибно позитивні, істинно негативні, хибно негативні. Матриця невідповідностей – на рисунку 3.

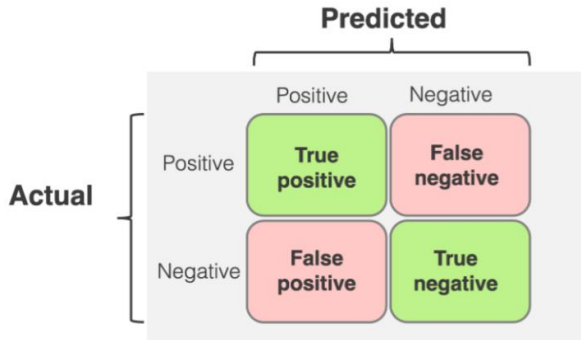


Рисунок 3 – Вигляд матриці невідповідностей для бінарної класифікації

Точність є часткою правильно класифікованих об'єктів у загальній кількості об'єктів. Ця метрика показує, як часто модель правильна в цілому. Ілюстрація змісту метрики точності на прикладі фільтрації спам-повідомлень наведена на рисунку 4.

Accuracy

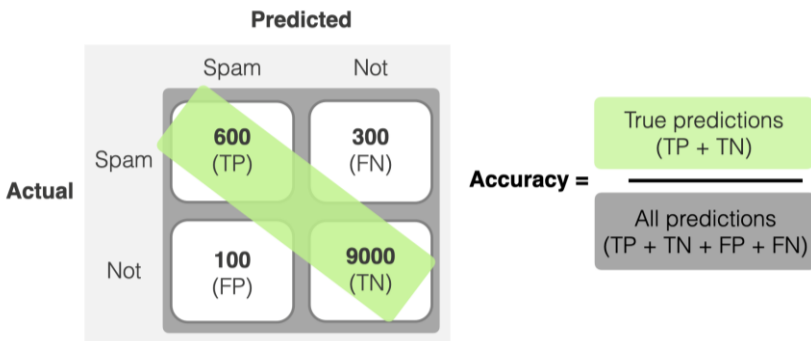


Рисунок 4 – Зміст метрики точності (Accuracy)

Влучність (Precision) є часткою правдивих позитивних прогнозів у всіх позитивних прогнозах. Іншими словами, влучність показує, як часто модель права,

коли прогнозує цільовий клас. Ілюстрація змісту метрики влучності на прикладі фільтрації спам-повідомлень наведено на рисунку 5.

Precision

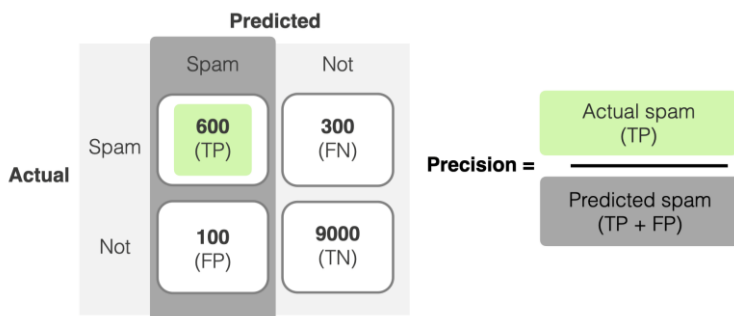


Рисунок 5 – Зміст метрики влучності (Precision)

Повнота (Recall) показує частку істинно позитивних прогнозів, зроблених моделлю, серед усіх позитивних зразків у наборі даних. Іншими словами, повнота показує, яку кількість зразків цільового класу може знайти модель. Ілюстрація змісту метрики повноти на прикладі фільтрації спам-повідомлень наведено на рисунку 6.

Recall

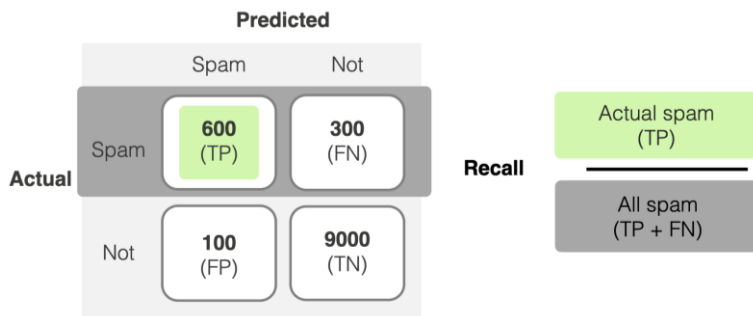


Рисунок 6 – Зміст метрики точності (Accuracy)

F₁-міра є середнім гармонійним показником влучності та повноти моделі. Обчислюється шляхом підсумовування зворотного значення кожного значення в наборі даних, а потім ділення кількості значень у наборі даних на цю суму. На відміну від інших типів середніх, середнє гармонічне надає більшої ваги меншим

значенням у наборі даних, що є корисним у ситуаціях, коли викиди або екстремальні значення можуть спотворити результати.

Для дослідження ефективності методу виявлення депресивного стану засобами NLP було проведено експериментальне порівняння архітектур-трансформерів GPT-2, BERT та розробленої нейромережевої моделі дуальної архітектури. Експеримент було проведено на 20 текстах, сформованих з використанням мовної моделі GPT 3.5, де 10 текстів з проявами депресії та 10 без проявів депресії. Результат класифікації та оцінок прояву депресивного стану наведено в таблиці 4.6 та 4.7.

Загалом, дуальна архітектура не допустила жодної помилки під час класифікації, а її результати за винятком 3-х текстів з 20 корелюють із моделями трансформерами GPT-2 та BERT. Це пов'язано з тим, що дані моделі самі по собі є потужними з малою похибкою, однак при підході з поєднанням, відбувається комбінація їх сильних сторін. BERT краще аналізує синтаксичні структури, тоді як GPT-2 забезпечує глибше розуміння контексту. Результати наведені на рисунку 7.

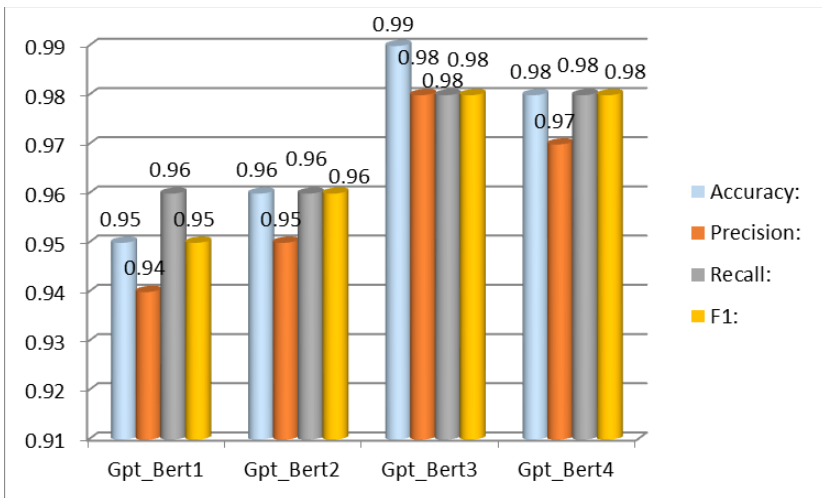


Рисунок 7 – Результати навчання нейромережевих моделей за метриками

Як видно з рисунку 7, найкращі результати отримала модель Gpt_Bert3, яка навчалась з параметрами кількість епох 2, швидкість навчання $2e-5$, розмір батча 16 та довжиною вхідної послідовності 128.

Однак, решта результатів також є доволі високими, що говорить про можливість всіх навчених моделей до коректної ідентифікації депресивного стану, що пов'язаний із навчанням у закладах освіти.

Для найкращої моделі також було проведено тестування на розміченій вибірці з понад 7000 текстових зразків, результат наведено на рисунку 8 у вигляді матриці сплутувань.



Рисунок 8 – Матриця сплутувань моделі Gpt_Bert3

Як показує матриця сплутувань, неймережа дійсно має мінімальний показник хибних відповідей.

Отже, було розроблено метод виявлення депресивних патернів за аналізом текстового контенту цифрових сервісів у закладах освіти, що призначений для перетворення вхідних даних у вигляді тексту та навченої неймережевої моделі дуальної архітектури у вихідні дані у вигляді числової оцінки наявності депресивного стану. Запропонований метод виявлення депресивних патернів за аналізом текстового контенту цифрових сервісів у закладах освіти відрізняється від аналогів тим, що поєднує двопоточну архітектуру, яка базується на використанні двох паралельних нейронних мереж, кожна з яких спеціалізується на аналізі різних аспектів тексту – синтаксичного та семантичного. Потік синтаксичного аналізу спрямований на виявлення синтаксичної структури тексту, а потік семантичного аналізу – на розуміння змісту та контексту тексту. Після обробки тексту кожним потоком результати комбінуються на рівні вищого шару, що дозволяє врахувати як

деталі мовної структури, так і загальний зміст тексту для більш точного визначення депресивного стану.

Подальші дослідження будуть спрямовані на продовження навчання нейромережі дуальної архітектури з різними параметрами, такими як кількість епох, розмір батча, швидкість навчання з метою зменшення похибки.

Перелік посилань

1. Havigerová, J. M., Haviger, J., Kučera, D., & Hoffmannová, P. (2019). Text-based detection of the risk of depression. *Frontiers in psychology*, 10, 513.
2. William, D., & Suhartono, D. (2021). Text-based depression detection on social media posts: A systematic literature review. *Procedia Computer Science*, 179, 582-589.
3. Tejaswini, V., Sathya Babu, K., & Sahoo, B. (2024). Depression detection from social media text analysis using natural language processing techniques and hybrid deep learning model. *ACM Transactions on Asian and Low-Resource Language Information Processing*, 23(1), 1-20.
4. Rahman, A. B. S., Ta, H. T., Najjar, L., Azadmanesh, A., & Gönül, A. S. (2024). DepressionEmo: A novel dataset for multilabel classification of depression emotions. *Journal of Affective Disorders*, 366, 445-458.
5. Thekkekara, J. P., Yongchareon, S., & Liesaputra, V. (2024). An attention-based CNN-BiLSTM model for depression detection on social media text. *Expert systems with applications*, 249, 123834.
6. Shevchuk P., Molchanova M., Mazurets O. Software for Text Messages Reliability Analysis Based on the Machine Learning Models Ensemble. *Proceedings of IV International Scientific and Practical Conference «Innovative research and perspectives of the development of science and technology»*. January 29-31, 2024. Stockholm, Sweden. 2024. Pp. 347-354.
7. Молчанова М.О., Мазурець О.В., Собко О.В., Віт Р.В., Назаров В.В. Алгоритм виявлення аб'юзивного вмісту в україномовному аудіоконтенті для імплементації в об'єктно-орієнтовану інформаційну систему. *Науковий журнал «Вісник Хмельницького національного університету»* серія: Технічні науки. Хмельницький, 2024. №1 (331). С. 101-106.
8. Овчарук О.М., Мазурець О.В. Нейромережеве діагностування проявів ПТСР у текстовому контенті з використанням помилко-орієнтованого навчального набору даних. *Науковий журнал «Вісник Хмельницького національного університету»* серія: Технічні науки. Хмельницький, 2024. №6, Т.1 (343). С. 195-200.
9. Молчанова М.О., Мазурець О.В., Собко О.В., Кліменко В.І., Андрощук В.І. Метод нейромережевого виявлення кібербулінгу з використанням хмарних сервісів та об'єктно-орієнтованої моделі. *Науковий журнал «Вісник Хмельницького національного університету»* серія: Технічні науки. Хмельницький, 2024. №2 (333). С. 200-206.
10. Mazurets O., Sobko O., Vit R., Pasternak V. Practical Approach for Detection by Deep Learning of Target Objects of Subject Area Based on Semantic Connectivity Indicators in Audio Database. *Proceedings of XXIV International Scientific and Practical Conference «Modern Scientific Challenges are the Driving Force of the Development of Scientific Research»*. May 22-24, 2024. Bruges, Belgium. International Scientific Unity. 2024. Pp. 91-96.
11. Залуцька О.О., Молчанова М.О., Мазурець О.В., Мельник О.І., Скрипник Т.К. Метод інтелектуального аналізу емоційної тональності текстової інформації для визначення поведінкових намірів нейромережевими засобами. *Науковий журнал «Вісник*

- Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2023. №5 (325). Т.1. С. 67-73.
12. Мазурець О.В., Козенко О.В., Собко О.В. Метод автоматизованого підбору відповідей на користувачські запитання за семантичною подібністю. Матеріали XII Всеукраїнської науково-практичної конференції «Глушковські читання». Київ – 2023. с. 106-109.
 13. Мазурець О.В., Віт Р.В. Інтелектуальний метод виявлення цільових об'єктів предметної області за показниками семантичної зв'язності для класифікації текстової інформації. Розвитки інформаційно-керуючих систем та технологій.: монографія. Львів-Торунь : Lina-Pres, 2024. – С.223-244.
 14. Mazurets O., Vit R. Practical Application of Method of Thematic Classification of Text Information Using LDA. Information Technology and Implementation (Satellite). Proceedings 11th International Conference. November 21, 2024. Kyiv, Ukraine. 2024. Pp. 151-152.
 15. Sobko O., Mazurets O., Didur V., Chervonchuk I. Recurrent Neural Network Model Architecture for Detecting a Tendency to Atypical Behavior Of Individuals by Text Posts. Theoretical and Practical Aspects of Modern Research. Proceedings of XXVI International scientific and practical conference. June 5-7, 2024. International Scientific Unity. Ottawa, Canada. 2024. Pp. 113-117.
 16. Mazurets O., Molchanova M., Klimenko V., Prosvitliuk M Practice Implementation of Neural Network Model BART-Large-CNN for Text Annotation. Prospects of Scientific Research in the Conditions of the Modern World. Proceedings of XXVII International scientific and practical conference. June 12-14, 2024. Rotterdam, Netherlands. 2024. Pp. 97-102.
 17. Tymofiiiev I., Mazurets O., Hardysh D., Molchanova M. Neural Network Dual Architecture for Depression Detection Using Cloud Services. Scientific Research in the Era of Digital Technologies: Challenges and Opportunities. Proceedings of the XLVI International scientific and practical conference. November 6-8, 2024. Barcelona, Spain. 2024. Pp. 84-88.
 18. Mazurets O., Tymofiiiev I., Dydo R. Approach for Using Neural Network BERT-GPT2 Dual Transformer Architecture for Detecting Persons Depressive State. Ricerche scientifiche e metodi della loro realizzazione: esperienza mondiale e realtà domestiche. Raccolta di articoli scientifici con gli atti della VI Conferenza scientifica e pratica internazionale. 15 novembre, 2024. Bologna, Repubblica Italiana. 2024. Pp. 147-151.
 19. Тимофієв І.А., Масловська В.В., Молчанова М.О., Мазурець О.В. Виявлення пов'язаного із навчанням у закладах освіти депресивного стану за дописами з використанням нейромережевої моделі дуальної архітектури. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». 15-16 листопада 2024. Хмельницький, 2024. с. 494-498.
 20. Мазурець О.В., Тимофієв І.А., Кліменко В.І., Тищенко О.О. Метод виявлення депресивного стану пов'язаного із навчанням у закладах освіти із використанням нейромережі дуальної архітектури. Науковий журнал «Вісник Херсонського національного технічного університету». 2024. №4 (91). С. 311-318.
 21. Kaggle. URL: <https://www.kaggle.com/datasets/nidhiy07/student-depression-text>

УДК 004.4

Тростянецький Н.О., Кльоц Ю.П., Калій К.В. Откидач В.В.

Хмельницький національний університет

ВИЯВЛЕННЯ АТАК ТИПУ «БЛОКУВАННЯ IP ЧЕРЕЗ NAT» В ПУБЛІЧНИХ МЕРЕЖАХ

Розглянуто виявлення атак типу «блокування IP через NAT» у публічних мережах із багатьма користувачами за спільною IP-адресою. Запропоновано методику аналізу трафіку на основі порівняння параметрів у нормальному стані та під час атаки з використанням NAT-шлюзу, Suricata і Snort. Отримані результати підтверджують ефективність підходу для точного виявлення аномалій і його придатність до інтеграції у системи мережевого моніторингу.

The study addresses the detection of “IP blocking through NAT” attacks in public networks with multiple users sharing a single IP address. A traffic analysis methodology is proposed based on comparing network parameters under normal operation and during an attack, using a NAT gateway together with Suricata and Snort systems. The obtained results confirm the effectiveness of the proposed approach for accurate anomaly detection and its suitability for integration into network monitoring systems.

Поширення публічних мереж доступу, зокрема міських Wi-Fi-хабів, мереж освітніх закладів і операторських CGNAT-сегментів, різко підвищує навантаження на механізми трансляції адрес і ускладнює атрибуцію трафіку. Масове застосування CGNAT фрагментує простір адрес, приховує множину абонентів за спільними публічними IP та змінює спостережні властивості трафіку, що створює додаткові вектори зловживань і перешкод для традиційних засобів моніторингу. Сучасні вимірювальні дослідження підтверджують широку присутність і різноманітні поведінкові профілі NAT-пристроїв на мережевому периметрі провайдерів, включно з Carrier-Grade NAT, які впливають на сумісність застосунків і ускладнюють безпекову діагностику у публічних доменах. Вразливості реалізацій NAT можуть бути використані для спричинення відмови в обслуговуванні на транспортному рівні шляхом маніпуляції таблицями відображень [1].

Метою дослідження є обґрунтування та розроблення підходу до виявлення атак типу «блокування IP через NAT» у публічних мережах через аналіз структурної та часової узгодженості подій на межі трансляції. Реалізація таких кроків має забезпечити своєчасне виявлення цілеспрямованого порушення досяжності ресурсів, підвищити надійність експлуатації публічних мереж і створити основу для

інтеграції з існуючими NIDS/IPS-компонентами у сценаріях, де класичні сигнатурні підходи виявляються недостатніми.

Дослідження проводилося в умовах публічної мережі з механізмом трансляції адрес типу NAT, що моделює середовище міського Wi-Fi-хабу або корпоративної мережі з багатьма клієнтами за спільною зовнішньою IP-адресою. Архітектура передбачала шлюз із реалізованою трансляцією адрес та ізольований сегмент клієнтів, що генерують звичайний трафік і контрольовані аномальні події, пов'язані з блокуванням IP. Структурна схема системи виявлення атак представлена на рис. 1.

Для збору ідентифікаційних та діагностичних даних використовувались інструменти пасивного моніторингу й аналізу пакетів, зокрема Wireshark та tcpdump, які забезпечували фіксацію повних сеансів TCP і UDP у різних часових інтервалах. З метою статистичної обробки потоків і агрегації даних застосовувався NetFlow, що дозволив визначати частоту повторних спроб встановлення з'єднань і зміни внутрішніх портів. Для кореляції подій і виявлення потенційно зловмисних шаблонів поведінки були використані IDS/IPS-системи Suricata та Snort, які слугували базовою платформою для інтеграції експериментального модуля детектування [2].

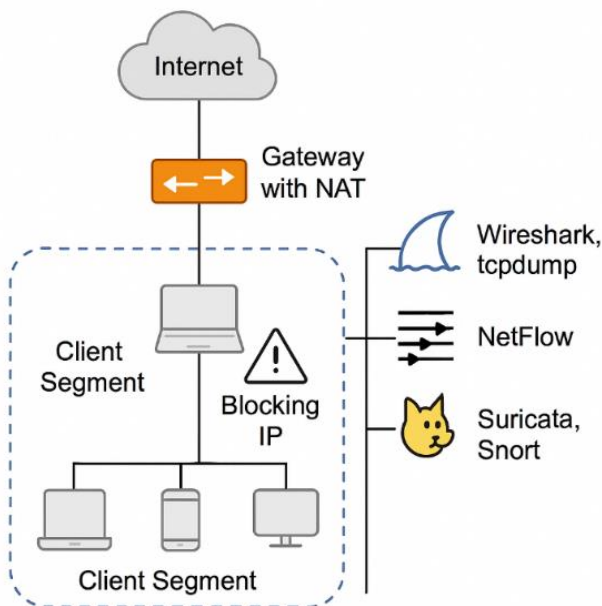


Рисунок 1 – Система виявлення атак на мережу

Методика виявлення ґрунтувалася на поетапному порівнянні характерних параметрів мережевого трафіку під час нормальної роботи механізму трансляції адрес і в умовах спровокованої атаки, спрямованої на блокування IP. У процесі дослідження було створено контрольну базову модель NAT-функціонування, що описувала типовий розподіл TTL, частоту ініціації TCP-з'єднань і середню тривалість активних відповідей у таблиці трансляцій. Ці параметри формували еталон стабільного стану мережі. У фазі атаки спостерігалися відхилення від норми, зокрема зменшення середнього часу життя сесій, поява коротких повторних SYN-послідовностей та підвищення кількості ICMP-повідомлень типу «Destination unreachable», що сигналізувало про примусове видалення або блокування певних записів у NAT-таблиці [3].

Додатково аналізувалися часові інтервали між повторними пакетами SYN та ACK, що дозволяло відстежити повторні спроби встановлення з'єднань після втрати відповідності у трансляції. На основі цих інтервалів формувалися часові ряди, які відображали поведінку потоків у динаміці. Аномалії виявлялися через обчислення середньоквадратичного відхилення параметрів, побудову ковзних вікон і застосування евристичних правил для фіксації нетипових стрибків у кількості зірваних сесій. Особливу увагу приділяли змінам у динаміці портів — фіксували випадки багаторазового перепризначення зовнішніх портів для одного внутрішнього клієнта, що свідчило про спробу обходу або підміни трансляції.

Важливою складовою методики стала багаторівнева кореляція журналів NAT, системного фаєрвола та моніторингу потоків NetFlow. Для кожного пакета формувався запис із часовою міткою, внутрішньою й зовнішньою IP-адресою, портом і станом з'єднання. Ці дані об'єднувалися у єдиний часовий простір, де алгоритм кореляції визначав послідовності подій, що призводили до втрати доступності ресурсу. Порівняння журналів дозволило відокремити легітимне завершення TCP-сеансів, викликане таймаутами або помилками маршрутизації, від штучного видалення відповідей, ініційованого атакуючим.

Узгодження отриманих метрик дало змогу сформувати набір поведінкових сигнатур, що описують фазу блокування IP через NAT. До таких сигнатур належали поєднання зменшення TTL на один або два кроки, поява серій SYN-пакетів без успішного завершення тристороннього рукостискання та одночасна реєстрація ICMP-відповідей з різних зовнішніх адрес для одного внутрішнього хоста. Виявлення таких патернів у комплексі дало змогу підвищити точність діагностики аномалій й мінімізувати кількість хибнопозитивних спрацювань. У результаті узгоджена система аналізу показала здатність точно ідентифікувати атаки типу «блокування IP через NAT» навіть у публічних середовищах з високим рівнем

мультиарендності, забезпечуючи достовірне розмежування природних коливань трафіку від навмисних втручань у процес трансляції адрес.

Проведене дослідження довело ефективність поєднання аналізу поведінкових характеристик трафіку, часових рядів параметрів NAT і багаторівневої кореляції журналів у задачі виявлення атак типу «блокування IP через NAT». Розроблена методика забезпечує можливість розмежування природних і зловмисних відхилень у роботі механізму трансляції адрес, що підвищує надійність функціонування публічних мереж із великою кількістю клієнтів за спільною IP-адресою. Отримані результати підтверджують доцільність інтеграції запропонованого підходу в сучасні IDS/IPS-системи для оперативного виявлення прихованих атак у середовищах із багаторівневим NAT, де класичні сигнатурні методи є малоефективними.

Перелік посилань

1. Feng X., Yang Y., Li Q., Zhan X., Sun K., Wang Z., Wang A., Du G., Xu K. ReDAN: An Empirical Study on Remote DoS Attacks against NAT Networks. Network and Distributed System Security Symposium (NDSS 2025). Reston, VA: Internet Society, 2025. DOI: 10.14722/ndss.2025.230972.
2. Boukebous A. A. E., Fettache M. I., Bendiab G., Shiaeles S. A Comparative Analysis of Snort 3 and Suricata. 2023 IEEE Global Conference on Emerging Technologies (GlobConET). IEEE, 2023.
3. Dhumal C. T., Pingale D. S. V. Analysis of Intrusion Detection Systems: Techniques, Datasets and Research Opportunity. SSRN Electronic Journal. 2024. URL: <https://doi.org/10.2139/ssrn.4749820>.

УДК 004.8

Трохимчук О.В., Пасічник О.А., Поплавська О.А., Міхалевський В.Ц.

Хмельницький національний університет

ПІДХІД ДО ОЦІНЮВАННЯ ВІДПОВІДНОСТІ ХЕШТЕГІВ КОРОТКИМ ТЕКСТАМ ЗАСОБАМИ NLP

Розглянуто задачу автоматизованого оцінювання відповідності хештегів коротким текстам соціальних мереж в умовах змішаних мов, неформальних конструкцій та маніпулятивного маркування контенту. Запропоновано підхід, що базується на контекстних мовних моделях типу трансформерів і побудові спільного семантичного простору для текстів і хештегів, попередньо сегментованих і перетворених на фрази природної мови. Показано можливість інтеграції підходу в модулі модерації, рекомендаційні сервіси й аналітичні системи для виявлення нерелевантних і маніпулятивних тегів та підвищення якості тегування.

The paper addresses the task of automated assessment of hashtag relevance to short social media texts under conditions of mixed languages, informal style and manipulative tagging. The proposed approach relies on transformer-based contextual language models and a joint semantic space for texts and hashtags, which are first segmented and converted into natural-language phrases. The approach can be integrated into moderation modules, recommender systems and analytical platforms to detect irrelevant or manipulative hashtags and improve the overall quality of tagging.

Поширення соціальних мереж та мікроблогів сформувало окрему «мову» коротких повідомлень, у якій хештеги виконують роль компактних маркерів тематики, настрою, події та цільової аудиторії [1]. Від коректності їх використання залежать якість пошуку, релевантність рекомендацій, прозорість аналітики та можливості автоматизованого моніторингу інформаційних потоків. Натомість практика свідчить про масове зловживання хештегами: від випадкового добору «модних» тегів до цілеспрямованого маніпулятивного маркування контенту. Це актуалізує задачу автоматизованого оцінювання відповідності хештегів коротким текстам, яка природно розв'язується засобами обробки природної мови.

Проблема є нетривіальною вже на рівні формалізації. Короткі тексти соціальних мереж містять розмовні конструкції, емодзі, скорочення, змішані мови, орфографічні відхилення, а хештеги поєднують словосполучення, сленг та елементи брендованої лексики [2]. Семантика хештегу не завжди збігається із буквальним змістом його компонентів: теги можуть позначати кампанію, мем, локальний

інформаційний контекст. Тому прості евристики на кшталт підрахунку перетину лем чи збігу окремих ключових слів дають обмежені результати. Потрібна модель, яка працює в спільному семантичному просторі для тексту й хештегу, враховує контекст уживання та здатна відрізнити тематичну релевантність від поверхневої схожості.

Мета роботи полягає у розробленні підходу до оцінювання відповідності хештегів коротким текстам на основі сучасних моделей NLP із використанням контекстних подань, що дає змогу формувати кількісні показники релевантності, придатні для інтеграції в системи модерації, рекомендаційні сервіси та аналітичні панелі. Для досягнення мети пропонується узгоджена послідовність етапів: формування корпусу, лінгвістичний препроцесинг, побудова семантичних подань текстів і хештегів, навчання моделей оцінювання відповідності та валідація результатів на експертно розмічених даних.

На рівні даних базовою сутністю є пара «короткий текст - множина хештегів». Для дослідження формується корпус постів із соціальних платформ, де хештеги використовуються як основний механізм індексування. Для частини записів здійснюється експертне маркування, коли кожен хештег віднесено до одного з рівнів: релевантний змісту, частково релевантний (дуже широкий або вторинний щодо основної теми) та нерелевантний або маніпулятивний. Така градація важлива для навчання моделей, які мають відрізнити цілком доречні теги від тегів, що лише формально не суперечать тексту, але не відображають його змістового ядра. Додатково фіксуються метадані, зокрема час публікації, домінантна мова, тип акаунта, що дозволяє у подальшому враховувати платформні та часові зсуви.

Лінгвістичний препроцесинг коротких текстів передбачає очищення від надлишкової технічної інформації, нормалізацію скорочень та приведення токенів до лематизованої форми із збереженням емотивних маркерів і ключових емодзі, які впливають на інтерпретацію. Особливу увагу приділено обробці змішаних текстів із поєднанням української, англійської та транслітераційних форм. Хештеги проходять окрему фазу сегментації: розбиття композитних тегів на складники, усунення декоративних символів, перетворення на фразу природної мови.

Ключовим компонентом підходу є побудова спільного семантичного простору для текстів і хештегів. Для цього застосовуються контекстні мовні моделі типу трансформерів, які навчені на багатомовних або спеціалізованих соціально-медійних корпусах. Короткий текст пропускається через модель для отримання векторного подання, що агрегує інформацію на рівні висловлювання, а хештег, попередньо перетворений на фразу, обробляється тим самим механізмом. У

результаті і текст, і хештег репрезентовано у спільному латентному просторі, в якому семантично узгоджені об'єкти розташовані близько один до одного.

Оцінювання відповідності реалізується двома взаємодоповнювальними способами. Перший базується на безпосередньому вимірюванні подібності між векторами тексту та хештегу за допомогою косинусної метрики та подальший калібровці порогових значень на валідаційній вибірці. Цей підхід є обчислювально економним і підходить для масової первинної фільтрації. Другий спосіб розглядає пару «текст-хештег» як єдину послідовність і подає її на вхід моделі типу cross-encoder, яка навчається класифікувати ступінь відповідності на основі повного контексту, включно з лексичними, синтаксичними та прагматичними ознаками. Така модель краще захоплює складні випадки, зокрема іронію, метафоричне вживання та тематичні зсуви.

Навчання моделей здійснюється у напівконтрольованій постановці. Експертно розмічена частина корпусу використовується для супервізованого навчання класифікатора ступеня релевантності, тоді як невеликі вбудовані у корпус блоки даних без явних анотацій залучаються через контрастивні схеми: правильні пари «текст-хештег» протиставляються штучно згенерованим негативним прикладам, утвореним шляхом перестановки тегів між текстами схожої тематики. Це підсилює здатність моделі розрізняти не лише довільні нерелевантні поєднання, а й тонкі відмінності між близькими за тематикою, але семантично відмінними тегами.

Для оцінювання якості запропонованого підходу використовуються стандартні метрики класифікації, а також ранжувальні показники. На рівні окремих пар аналізуються точність, повнота та F_1 -міра для кожного рівня релевантності, а також зважені усереднення за класами. На рівні множини хештегів для одного тексту розглядаються метрики, що характеризують порядок, у якому система пропонує або підтверджує теги, зокрема середня позиція релевантних хештегів та нормалізована кумулятивна оцінка приросту. Порівняння з базовими підходами, що використовують лише статистичні співзв'язі слів або поверхневі подібності, демонструє переваги контекстних моделей у розв'язанні задачі, особливо для коротких, емоційно насичених і семантично неоднозначних текстів.

Практичне значення розробленого підходу полягає у його здатності працювати як модуль у складі ширших інформаційних систем. У середовищі модерації контенту він дає змогу автоматично виявляти маніпулятивні чи «шумові» хештеги, які не відбивають зміст поста, але використовуються для привернення уваги або паразитування на трендових темах. У рекомендаційних сервісах оцінка відповідності може застосовуватись для очищення вхідних сигналів, що формують профіль користувача, зменшуючи вплив некоректних тегів на моделі персоналізації.

У системах аналітики підхід забезпечує побудову більш надійних карт тематичних кластерів, де хештеги виступають не довільними маркерами, а семантично верифікованими індикаторами дискусійних полів.

Окремим напрямом розвитку є поєднання оцінки відповідності з виявленням специфічних типів ризикового контенту. Нерелевантні або надто загальні хештеги часто супроводжують маніпулятивні повідомлення, приховану рекламу чи спроби обійти прості фільтри модерації. Інтеграція семантичних оцінок релевантності з іншими модулями аналізу, наприклад класифікаторами токсичності, дезінформації чи цифрової втоми, відкриває можливості для побудови багатовимірних профілів постів, де невідповідність хештегів є одним із сигналів ризику.

Підсумовуючи, запропонований підхід до оцінювання відповідності хештегів коротким текстам базується на використанні контекстних мовних моделей, спільного семантичного простору для текстів і тегів, а також поєднання подібнісних та класифікаційних процедур. Він враховує лінгвістичні особливості коротких, неформальних повідомлень, підтримує багатомовність, а також допускає гнучке налаштування порогів прийняття рішень залежно від завдань системи-споживача. Отримані результати свідчать про перспективність такого підходу для побудови інструментів контролю якості тегування, підвищення прозорості інформаційних потоків та зменшення впливу маніпулятивних практик у цифрових середовищах.

Перелік посилань

1. DialogueGCN: A Graph Convolutional Neural Network for Emotion Recognition in Conversation / D. Ghosal et al. Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP), Hong Kong, China. Stroudsburg, PA, USA, 2019. URL: <https://doi.org/10.18653/v1/d19-1015>
2. Wang L., Zhang L. Hawkes processes for understanding heterogeneity in information propagation on Twitter. *Frontiers in Physics*. 2022. Vol. 10. URL: <https://doi.org/10.3389/fphy.2022.1019380>

УДК 004.891

Філюк Є.В., Джулій В.М.

Хмельницький національний університет

МЕТОД БЕЗПЕКИ КРИПТОАКТИВІВ НА ОСНОВІ ТЕХНОЛОГІЇ БАГАТОСТОРОННІХ ОБЧИСЛЕНЬ

Метод конфіденційності та безпеки криптоактивів на основі технології багатосторонніх обчислень для Ethereum мережі полягає в: забезпеченні високого рівня безпеки для збереження приватних ключів та процесу підписання транзакції, використовуючи передові методи криптографічного захисту; гарантуванні конфіденційності та приватності користувачів, захищаючи їх особисту інформацію від несанкціонованого доступу та витоку даних.

The method of confidentiality and security of crypto assets based on multi-party computing technology for the Ethereum network consists of: ensuring a high level of security for the storage of private keys and the transaction signing process, using advanced cryptographic protection methods; guaranteeing the confidentiality and privacy of users, protecting their personal information from unauthorized access and data leakage.

Основною перевагою криптовалют є їх децентралізація: вони не контролюються центральними органами управління, такими як уряди чи банки, і можуть бути використані у будь-якій частині світу без обмежень. Додатковими перевагами є анонімність, що дозволяє користувачам зберігати конфіденційність своїх фінансових операцій, та зручність, що забезпечує швидкі та прості перекази без посередників.

Найвідомішою криптовалютою є біткоїн, також існує безліч інших криптовалют, як Ethereum, Ripple, Tether та інші. Криптовалютні гаманці є ключовими інструментами для зберігання, відправлення та отримання криптовалют. Вони можуть бути онлайн-сервісами, програмами для смартфонів або настільними програмами, дозволяючи користувачам відстежувати свої баланси та історію транзакцій. У зв'язку з цим створення ефективного та безпечного криптовалютного гаманця є актуальним завданням для багатьох галузей, які працюють з криптовалютами, таких як фінансові послуги, торгівля, інтернет-магазини, туризм та благодійність [1, 2, 3].

Протокол багатосторонніх обчислень для системи конфіденційності та безпеки криптоактивів є основою на якій будується принцип контролю приватних ключів користувачів та здійснення усіх необхідних операцій, таких як підписання транзакції та її валідація. При проектуванні таких протоколів необхідно запобігти усім наявним мінусів попередніх протоколів.

Проблемою алгоритму секретного поділу Шаміра є одна точка відмови, а саме центральний сервер який виконує розподіл і збирання секретного ключа, і цей фактор потрібно врахувати при проектуванні протоколу для системи. Проте перевагою є можливість розділити приватний ключ на частинки з порогом відновлення.

Для знаходження компромісу між ефективністю та безпекою в системі, для покращення безпеки, використано принцип з інтервальним оновленням спільних поділених частин та не використанню механізму доказів нульової довіри для покращення продуктивності.

Протокол повинен відповідати властивостям багатосторонніх обчислень, а саме конфіденційності, де кожна сторона гарантує, що жодна зі сторін не знає загального секрету, але може гарантувати правильне розподілене обчислення над даними. Це можна досягти за допомогою розподіленої генерації ключа для ECDSA в контексті Ethereum. Такий підхід забезпечує, що приватний ключ ніколи не розкривається жодній стороні, а підписання транзакцій виконується спільно, що підвищує безпеку та конфіденційність. Даний алгоритм необхідно розширити інтервальним оновленням частин секрету, без втрати оригінального секрету, що є важливим аспектом забезпечення довготривалої безпеки в розподілених системах.

Процес розподіленої генерації ключа складається з наступних етапів: ініціалізація; генерація поліному; обрахунок частин ключа; надсилання частин ключа сторонам; обчислення власної частини стороною секрету. Ініціалізація розпочинається з ініціалізації однієї зі сторін протоколу генерації, і тоді кожен учасник генерує свою частину секретного ключа s_i випадковим чином, але так щоб згенероване значення відповідало вимозі, що число додатне та менше за встановлений порядок поля q , де q - кінцева точка обраної еліптичної кривої для системи. У нашому випадку використовується крива secp256k1, що задається рівнянням (1)

$$y^2 = x^3 + ax + b \quad (1)$$

де a, b – параметри, задаються для кривої secp256k1 дорівнюють 0 та 7 відповідно.

Далі відбувається генерація поліному кожною стороною з $f(x)$ ступеня t з випадковими коефіцієнтами a_i , поліном задається наступним виразом (2):

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_tx^t \quad (2)$$

де t – поріг відновлення; a_0 – коефіцієнт який дорівнює s_i (згенерований секрет).

Після того як поліном згенеровано, сторона обчислює частки ключа для кожної іншої сторони передаючи до поліному $f(x)$ порядковий номер вузла у якості параметру x . Згенерований перелік частин власного секретного ключа, сторона розсилає до відповідного учасника через безпечний канал зв'язку. Алгоритм розподіленої генерації спільного секретного ключа наведений на рис. 1.

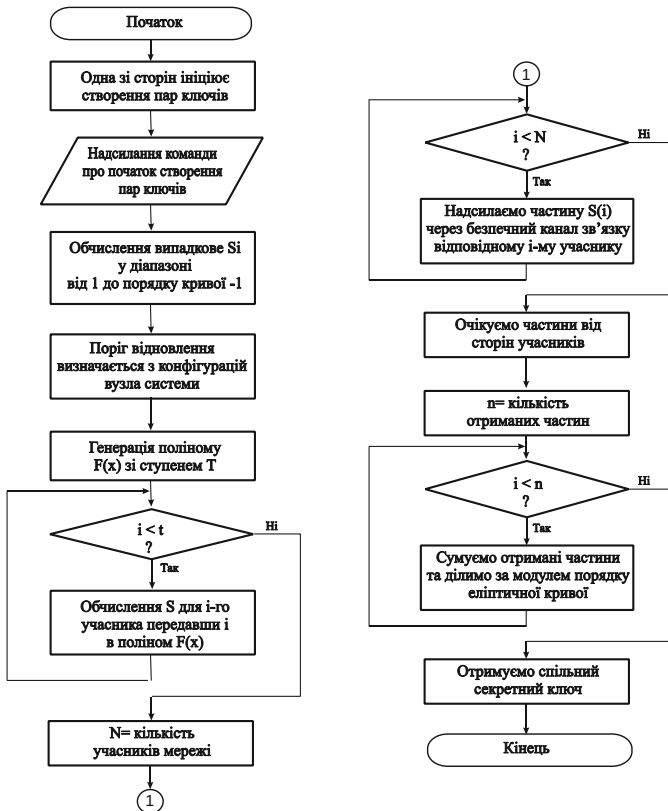


Рисунок 1 – Алгоритм генерації спільного секретного ключа

Тепер необхідно розробити механізм інтервального оновлення часток секретного ключа, опираючись на математичні операції які застосовувались для їх генерації. Опираючись на поділ секрету Шаміра [3,4] можна виділити наступні кроки оновлення часток спільного секретного ключа: ініціалізація; генерація та розподіл; обчислення нових часток.

Оновлення ключа розпочинається з того, що один із учасників повідомляє інших про початок раунду оновлення часток. Тоді кожен учасник повинен згенерувати випадкове число n_i , відповідно до того яке він генерував для власного секретного ключа. Це випадкове число буде використано для зміни його частки секретного ключа. Згенеровані частки обмінюються між учасниками через безпечний канал зв'язку. Після обміну новими частками ключа, учасники повинні об'єднати свій новий спільний ключ (3):

$$s'_i = s_i + \sum_{j=i} n_j - n_i \quad (3)$$

де s_i — це поточна частка учасника j ; s_i' — оновлена частка ключа.

Сума n , що надходить від інших учасників, додається, а своє власне n віднімається, щоб зберегти загальну суму секретного ключа незмінною.

Таким чином можемо досягти регулярного оновлення часток секретного ключа, зменшуючи ризики компрометації і підтримуючи високий рівень безпеки в розподілених системах. Шляхом розробки та впровадження протоколу багатосторонніх обчислень з ключами, розподіленими та періодично оновлюваними - ефективно покращуємо рівень безпеки, у порівнянні з традиційними методами зберігання ключів у єдиному місці, наш підхід забезпечує значно вищий ступінь захисту від потенційних атак. Замість того, щоб мати один централізований пункт доступу, який може стати мішенню для зловмисників, ми розподіляємо ключі між декількома довіреними елементами системи. Кожен ключ періодично оновлюється або змінюється, ускладнюючи можливість несанкціонованого доступу. Цей підхід не лише робить процес взлому системи значно складнішим завданням, але й активно захищає систему від потенційних атак, надаючи більшу впевненість у безпеці та надійності обчислень.

Системи керування криптоактивами на основі багатосторонніх обчислень включає кілька важливих етапів: вибір хмарних провайдерів, створення та налаштування інстансів, контейнеризація додатків, налаштування захищеного зв'язку та маршрутизації. Система надає можливість надійного зберігання криптоактивів, зокрема приватних ключів до гаманців Ethereum мережі, з використанням технології MPC, яка може бути використана у різних криптопроектах для безпечного переказу криптоактивів.

На основі проведеного дослідження та аналізу характеристик стандартів протоколів багатосторонніх обчислень запропонований протокол, який враховує наявні покращення та недоліки попередніх протоколів. Для покращення безпеки, у протоколі було впроваджено принцип інтервального оновлення спільного секрету.

Архітектура системи передбачає взаємодію основних компонентів для забезпечення надійної та безпечної роботи. Запропоновано схему встановлення безпечного з'єднання вузлів та описано модель локального сховища, яке забезпечує безпечне зберігання часток ключів, підписів та системних логів.

Перелік посилань

1. Доктрина інформаційної безпеки України, затвердженої Указом Президента України від 25 лютого 2017 року № №47/2017, 15с.
2. What Makes a Blockchain Secure? Академія Binance: веб-сайт. URL: <https://academy.binance.com/en/articles/what-makes-a-blockchain-secure> (дата звернення: 20.02.2025).
3. Бем, М. В. Стандарти захисту персональних даних в соціальній сфері. / М. В.Бем, І. М. Городиський -Львів:, 2018р. - 110 с.
4. Що таке транзакції у блокчейні? Incrypted : веб-сайт. URL: <https://incrypted.com/tranzakcii-v-blokcheyn/> (дата звернення: 20.02.2025).

УДК 004.896

Футорний Р.В., Медведчук Н.К.

Хмельницький національний університет

ДОСЛІДЖЕННЯ ВИЯВЛЕННЯ КІБЕРАТАК В АГРО-ІОТ З ВИКОРИСТАННЯМ АНАЛІЗУ ЕНЕРГОСПОЖИВАННЯ

Досліджено проблему кібербезпеки в системах «розумного фермерства» (Агро-ІоТ). Проаналізовано специфічні вразливості ІоТ-пристроїв в агроінженерії, такі як обмежені обчислювальні ресурси та відсутність вбудованих механізмів захисту. Запропоновано комбінований двоетапний метод виявлення та локалізації кібератак. Перший етап базується на аналізі енергоспоживання пристроїв з використанням нечіткої кластеризації c-means та динамічного вирівнювання часових рядів (DTW) для виявлення аномалій. Другий етап забезпечує локалізацію шкідливого ПЗ шляхом аналізу послідовностей опкодів та класифікації за відстанню Махаланобіса.

The problem of cybersecurity in smart farming systems (Agro-IoT) is investigated. Specific vulnerabilities of IoT devices in agroengineering, such as limited computing resources and the lack of built-in security mechanisms, are analyzed. A combined two-stage method for detecting and localizing cyberattacks is proposed. The first stage is based on device power consumption analysis using fuzzy c-means clustering and Dynamic Time Warping (DTW) to detect anomalies. The second stage ensures malware localization by analyzing opcode sequences and classifying them using Mahalanobis distance.

Впровадження Інтернету речей (ІоТ) у агроінженерії формує нову високотехнологічну галузь «розумного фермерства». Використання дронів, систем моніторингу ґрунту, автономної сільськогосподарської техніки та роботизованих комплексів дає змогу оптимізувати виробничі процеси, зменшити витрати ресурсів (палива, добрив, води) і підвищити врожайність. Проте така глибока цифровізація та мережева інтеграція створює нові безпрецедентні кіберзагрози. Кожен підключений пристрій, від простого датчика вологості до складного бортового комп'ютера трактора, стає потенційною точкою входу для атак. Це перетворює агросектор на об'єкт критичної інфраструктури, здатний впливати на продовольчу безпеку держави [1].

Аналіз останніх досліджень і публікацій. Безпека ІоТ-пристроїв є предметом численних досліджень. Основна вразливість полягає в їхній гетерогенності та суттєвих обмеженнях: слабкі мікроконтролери, малий обсяг пам'яті та орієнтація на низьке енергоспоживання. Це унеможливорює використання

традиційних антивірусних систем чи складних брендмауерів. Такі пристрої часто мають слабкі або незмінні паролі, що полегшує їх компрометацію, створення бот-мереж (наприклад, Mirai) і проведення масштабних DDoS-атак.

Одним із нових неінвазивних напрямів є аналіз побічних каналів, зокрема енергоспоживання, для виявлення шкідливої активності. Доведено, що виконання стороннього коду (вірусу, майнера, шпигунського ПЗ) неминуче змінює енергетичний профіль пристрою, створюючи аномально високе або нехарактерне навантаження. Цей підхід розвинули Бобровнікова К. Ю. та співавт., які запропонували метод і алгоритми виявлення кібератак у мережах інтернету речей на основі енергетичних профілів [2]. Подібні результати щодо ефективності аналізу енергетичних "відбитків" (energy fingerprints) для ідентифікації шкідливих програм наведено й у роботах Hoffmann J. et al. [3], Shi Y. et al. [4] та Azmoodeh A. et al., які успішно застосували цей метод для виявлення програм-вимагачів [5].

Попри перспективність, методи, що базуються лише на енергоспоживанні, мають суттєві недоліки. Вони демонструють велику кількість хибних спрацьовувань (false positives), оскільки легітимне оновлення ПЗ або нештатний режим роботи також можуть спричинити сплеск енергоспоживання. Крім того, такий підхід дозволяє лише констатувати факт атаки ("щось не так"), але не дає змоги визначити конкретне шкідливе ПЗ чи локалізувати загрозу. Необхідний комплексний підхід, який забезпечує як високоточне виявлення атаки, так і подальшу ідентифікацію джерела.

Метою роботи є комбінований метод виявлення кібератак у агро-IoT-системах, який поєднує аналіз побічних каналів (енергоспоживання) з аналізом програмного коду. Такий метод має враховувати різні режими роботи обладнання для зниження хибних спрацьовувань та давати змогу ідентифікувати конкретний тип шкідливого ПЗ, що є джерелом атаки.

Вразливість агросектору обумовлена не лише економічними збитками, але й ризиками для продовольчої безпеки. Специфічні загрози для Агро-IoT включають:

- Несанкціонований доступ до контролерів [2]. Злам системи керування іригацією може призвести до посухи або, навпаки, затоплення полів. Отримання контролю над системами клімат-контролю в тваринницьких комплексах може спричинити масову загибель поголів'я.

- DDoS-атаки, які виводять з ладу критичні системи. Атака на центральний сервер агрохолдингу може зупинити збір даних із полів, що унеможливить прийняття рішень, або паралізувати логістику (збір та вивіз урожаю).

- Атаки програм-вимагачів (Ransomware). Шифрування даних бортових комп'ютерів комбайнів чи тракторів під час посівної або збору врожаю може призвести до повної зупинки робіт та колосальних збитків [5].

- Маніпуляція даними датчиків. Найбільш підступний вид атаки. Зловмисник може "підмінити" дані, що надходять від датчиків ґрунту (наприклад, показувати, що ґрунт вологий, хоча насправді він сухий) або GPS-дані (GPS-spoofing), що призведе до неправильного внесення добрив, пропусків в обробці поля або навіть фізичного пошкодження техніки.

- Атаки на ланцюг постачання. Впровадження шкідливого коду у прошивку пристроїв (датчиків, дронів) ще на етапі їх виробництва або налаштування [1].

Для протидії цим загрозам запропоновано двоетапний комбінований метод, що поєднує переваги аналізу побічних каналів та статичного аналізу коду.

На етапі виявлення атаки (аналіз енергоспоживання) використовується моніторинг енергоспоживання в реальному часі. Ключовою особливістю є врахування режимів користувацьких налаштувань (UPM – User Profile Modes). Для кожного пристрою (наприклад, IoT-контролера насоса) формуються еталонні енергетичні профілі для різних станів: «сон», «очікування», «активна робота (полив)», «оновлення ПЗ». Класифікація поточного стану здійснюється нечітким алгоритмом c-means. На відміну від жорстких алгоритмів (як k-means), c-means дозволяє одному виміру належати до кількох кластерів з різним ступенем приналежності. Це важливо, оскільки перехідні процеси в роботі пристрою можуть бути схожі на аномалію. Для порівняння поточного профілю з еталонним використовується динамічне вирівнювання часових рядів (DTW – Dynamic Time Warping). DTW дозволяє знаходити схожість між двома часовими рядами, які мають різну швидкість або фазові зсуви. Наприклад, якщо легітимний процес і атака мають схожу форму енергоспоживання, але різняться в тривалості, DTW виявить цю різницю ефективніше, ніж просте порівняння "точка до точки". Такий підхід дає точність виявлення аномалій близько 99,88 % [2, 3].

Якщо перший етап фіксує стійку аномалію, яка не відповідає жодному з профілів UPM, запускається другий етап - локалізація загрози (аналіз опкодів). Його мета – не просто виявити, а ідентифікувати шкідливе ПЗ. Для цього аналізується програмний код (прошивка) пристрою, який підозрюється в зараженні, через послідовності його опкодів (машинних інструкцій, наприклад MOV, ADD, JMP). Будується вектор ознак, що відображає частоту появи певних n-грам опкодів – так званий Malware Sequence Profile (MSP). Далі виконується класифікація за допомогою відстані Махаланобіса. На відміну від евклідової відстані, цей метод враховує кореляцію між різними ознаками (опкодами). Це дозволяє виявити, наскільки "далеко" профіль підозрілого ПЗ знаходиться від хмари "чистих" програм, навіть якщо шкідливий код використовує ті самі опкоди, але в інших комбінаціях. Це дає змогу не лише підтвердити зараження, але й класифікувати тип загрози

(наприклад, "майнер", "шпигун", "шифрувальник"), зв'язуючи його з базою відомих шкідливих MSP. Точність визначення типу шкідливого ПЗ сягає 99,66 % [2].

Отже, впровадження IoT в агроінженерії є невідворотним технологічним трендом, яке супроводжується специфічними кіберзагрозами — від саботажу та шпигунства до маніпуляції даними датчиків, що ставить під загрозу продовольчу безпеку. Традиційні методи захисту (антивіруси, брандмауери) малоефективні для обмежених ресурсів IoT-пристроїв, що вимагає розробки нових, неінвазивних методів детекції. Запропонований комбінований метод, що поєднує енергетичний аналіз (з урахуванням UPM та DTW) для виявлення та аналіз опкодів (з відстанню Махаланобіса) для локалізації, забезпечує високу інтегральну точність (вище 99%) і дозволяє ідентифікувати тип загрози. Подальші дослідження доцільно спрямувати на апаратну реалізацію таких систем моніторингу, їх тестування в реальних агро-господарствах та створення єдиних галузевих стандартів безпеки для Агро-IoT [5].

Перелік посилань

1. Trend Micro. Inside the Smart Home: IoT Device Threats and Attack Scenarios. [Електронний ресурс]. URL:<https://www.trendmicro.com/vinfo/it/security/news/internet-of-things/inside-the-smart-home-iot-device-threats-and-attack-scenarios> (дата звернення: 25.10.2025).
2. Бобровнікова К. Ю., Гурман І. В., Чорненький В. І., Муляр І. В. Метод та алгоритми виявлення кібератак у мережах інтернету речей на основі аналізу енергоспоживання. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка, № 88, Київ, 2025, с. 82–95.
3. Hoffmann J., Neumann S., Holz T. Mobile malware detection based on energy fingerprints – a dead end? International Workshop on Recent Advances in Intrusion Detection. Berlin, Springer, 2013, pp. 348–368.
4. Shi Y., Li F., Song W., Li X. Y., Ye J. Energy audition based cyber-physical attack detection system in IoT. Proceedings of the ACM Turing Celebration Conference – China, 2019, pp. 1–5.
5. Azmoodeh A., Dehghantanha A., Conti M., Choo K. K. R. Detecting crypto-ransomware in IoT networks based on energy consumption footprint. Journal of Ambient Intelligence and Humanized Computing, 2018, Vol. 9 (4), pp. 1141–1152.
6. Ленков С., Джулій В., Муляр І., Димбовський М. Модель визначення актуальних загроз безпеки конфіденційних даних в розподіленій інформаційній системі. Underwater Technologies: Industrial and Civil Engineering. 2023. Issue 13. С. 45–59.

УДК 004.8:336.76

Ціцьвіра І.О., Радюк П.М., Скрипник Т. К.

Хмельницький національний університет

МЕТОД АГЕНТНО-ОРІЄНТОВАНОГО АНАЛІЗУ РИНКУ КРИПТОВАЛЮТ З ВИКОРИСТАННЯМ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ

Запропоновано новий експериментальний метод агентно-орієнтованого аналізу ринку криптовалют, що використовує спільноту великих мовних моделей (LLM) для імітації реальних торгових процесів. Система включає спеціалізованих LLM-агентів, які виконують ролі аналітиків новин, ринкових даних та соціальних мереж. Ключовим елементом є механізм дебатів між агентами-«биками» та «ведмедями», що забезпечує збалансовану оцінку ринкової ситуації. Такий підхід дає можливість проводити комплексний аналіз ринкової інформації, враховуючи як кількісні, так і якісні чинники, створюючи більш адаптивні та інтелектуальні системи автоматизованої торгівлі, що підвищує точність та обґрунтованість прийняття торгових рішень.

This work proposes a novel experimental method for agent-oriented analysis of the cryptocurrency market, leveraging a community of Large Language Models (LLMs) to simulate real-world trading processes. The system comprises specialized LLM agents assigned to roles such as news, market data, and social media analysis. A key feature is a dialectical debate process between "bull" and "bear" researcher agents to ensure a balanced market assessment. This approach enables an analysis by integrating both quantitative data and qualitative factors, aiming to create more adaptive and intelligent automated trading systems, thereby improving the accuracy and rationale behind trading decisions.

Спостерігається значний прогрес у автоматизації завдань завдяки застосуванню мультиагентних систем на основі великих мовних моделей (LLM). Однак дослідження у фінансовій галузі були спрямовані переважно на одноагентні архітектури чи фреймворки з незалежним збором даних. Відтак, потенціал мультиагентних систем для моделювання колаборативної динаміки, що є властивою реальним торговим процесам, залишається нерозкритим [1].

Автономні агенти на базі LLM втілюють трансформаційний підхід до прийняття рішень, відтворюючи повсякденні та робочі процеси у різноманітних застосунках. Одним із ключових напрямів є фінансові та криптовалютні ринки – системи виняткової складності [2], що зазнають впливу численних чинників: від фундаментальних показників компаній і ринкових настроїв до технічних індикаторів та макроекономічних подій [3].

Традиційні алгоритмічні торгові системи не можуть повною мірою охопити складну взаємодію цих факторів. Натомість LLM демонструють високу ефективність в обробці даних природної мови, що робить їх незамінними для

аналізу новин чи настроїв у соціальних мережах. Водночас системи глибокого навчання мають суттєвий недолік – низьку пояснюваність, оскільки їхні рішення ґрунтуються на прихованих ознаках, які складно інтерпретувати [4]. Новітні LLM-підходи відкривають можливості для подолання цих обмежень, створюючи системи пояснюваного ШІ, де рішення підкріплені прозорим обґрунтуванням [5].

Метою цього дослідження є підвищення точності прийняття торгових рішень через впровадження нового методу агентно-орієнтованого аналізу ринку криптовалют на основі великих мовних моделей. Розроблення та впровадження методу агентно-орієнтованого аналізу ринку криптовалют даємо змогу отримати кращі результати під час прийняття торгових рішень через комплексний аналіз ринкової інформації та створення більш адаптивних та інтелектуальних систем автоматизованої торгівлі криптовалютами.

Розроблений метод визначає шість різних ролей агентів, натхнених структурою реальних торгових процесів (рис. 1).

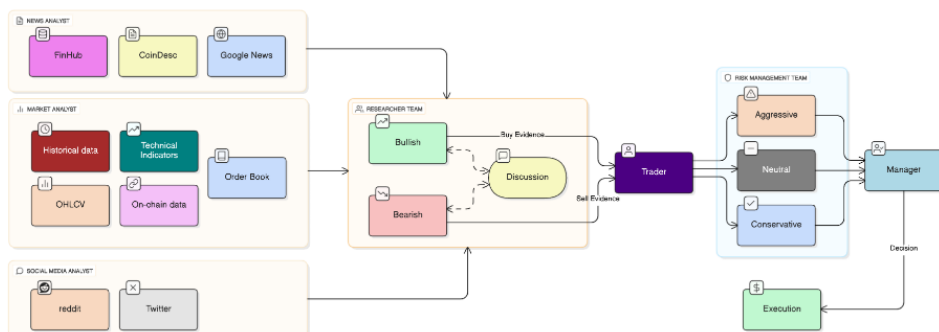


Рисунок 1 – Блок схема роботи інформаційної системи на основі запропонованого методу агентно-орієнтованого аналізу крипторинку

Команда аналітиків складається зі спеціалізованих агентів, відповідальних за збір та аналіз різних типів ринкових даних:

- аналітики постів обробляють великі обсяги постів у соціальних мережах та оцінюють ринкові настрої для прогнозування впливу колективної поведінки інвесторів на ціни у короткостроковій перспективі;

- аналітики новин аналізують новинні статті, урядові оголошення та макроекономічні індикатори для оцінювання макроекономічного стану ринку;

- технічні аналітики аналізують on-chain дані, дані про актуальну та історичні ціни, OHLCV, релевантні технічні індикатори, такі як MACD та RSI, для прогнозування майбутніх рухів цін.

Команда дослідників відповідає за критичну оцінку інформації через кількох раундів дебатів:

– “дослідники-бики” агітують за інвестиційні можливості, підкреслюючи позитивні індикатори та потенціал зростання;

– “дослідники-ведмеді” зосереджуються на потенційних негативних аспектах, ризиках та несприятливих ринкових сигналах.

Через діалектичний процес дебатів команда дослідників прагне досягти збалансованого розуміння ринкової ситуації. Дослідження показують, що різноманітність думок та структуровані дебати між агентами значно покращують якість рішень у мультиагентних системах [6].

Агенти-трейдери відповідають за формування торгових рекомендацій на основі комплексного аналізу команди аналітиків та нюансованих перспектив команди дослідників. Вони оцінюють синтезовану інформацію для визначення оптимальних торгових дій, включаючи час та розмір угод.

Переважно наявні агенти (фреймворки) на основі LLM використовують природну мову як основний комунікаційний інтерфейс. Однак покладання виключно на природну мову часто виявляється недостатнім для вирішення складних, довгострокових завдань. Щоб вирішити це обмеження, метод використовує структурований підхід до комунікації, натхненний фреймворком MetaGPT [7].

Всі агенти в рамках методу слідуєть фреймворку підказок ReAct (Reasoning and Acting), який синергізує обґрунтування та дії. Фреймворк ReAct, запроваджений у 2022 році, дає змогу LLM генерувати як вербальні сліди обґрунтування, так і специфічні дії для завдань [8]. ReAct працює ітеративно через послідовність кроків Думка-Дія-Спостереження. Стан середовища є спільним та моніториться агентами, що дає змогу їм виконувати контекстно-відповідні дії. Цей дизайн забезпечує колаборативний, динамічний процес прийняття рішень, що відображає реальні торгові процеси.

Центральною інновацією в архітектурі LLM-агентів є впровадження систем багаторівневої пам'яті, розроблених для відображення людської когнітивної пам'яті [9].

Наприклад, TradingGPT використовує трирівневу ієрархію пам'яті де кожен рівень керується користувацькою функцією згасання, яка математично визначається для забезпечення, що агенти фокусуються на найбільш релевантних даних для поточних ринкових умов. Багаторівнева структура пам'яті дає змогу агенту пріоритизувати інформацію, зосереджуючись на даних, найбільш релевантних для поточних ринкових умов [10].

У підсумку, запропонований метод вирішує ключові обмеження наявних підходів, симулюючи процеси мультиагентного прийняття рішень, що властиві професійним торговим командам. Створена на основі запропонованого методу інформаційна система включає спеціалізованих агентів та використовує гібридний підхід до комунікації: поєднання структурованих виходів для контролю з діалогом природною мовою для ефективних дебатів, що забезпечує точність і гнучкість. Важливою перевагою є висока пояснюваність завдяки природномовним

обґрунтуванням дій. Отже, впровадження методу дає можливість створювати адаптивні інтелектуальні системи автоматизованої торгівлі, які досягають кращих результатів через симуляцію динамічного колаборативного середовища та комплексний аналіз ринку.

Перелік посилань

1. A comprehensive review on financial explainable AI / W. J. Yeo et al. Artificial Intelligence Review. 2025. Vol. 58, no. 6. P. 189. URL: <https://doi.org/10.1007/s10462-024-11077-7> (date of access: 15.10.2025).
2. Shupta A., Radiuk P., Krak I. Feature computation procedure for fake news detection: An LLM-based extraction approach. Proceedings of the 6th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS 2025) : CEUR-Workshop Proceedings, Khmelnytskyi, 4 April 2025. Aachen, 2025. P. 112–124. URL: <https://ceur-ws.org/Vol-3963/paper10.pdf> (date of access: 10.10.2025).
3. Toward explainable deep learning in healthcare through transition matrix and user-friendly features / O. Barmak et al. Frontiers in Artificial Intelligence. 2024. Vol. 7. P. 1482141. URL: <https://doi.org/10.3389/frai.2024.1482141> (date of access: 28.09.2025).
4. CryptoTrade: a reflective LLM-based agent to guide zero-shot cryptocurrency trading / Y. Li et al. Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing, Miami, FL, USA, 12–16 November 2024. Stroudsburg, PA, USA, 2024. P. 1094–1106. URL: <https://doi.org/10.18653/v1/2024.emnlp-main.63> (date of access: 13.10.2025).
5. FinMem: A performance-enhanced LLM trading agent with layered memory and character design / Y. Yu et al. IEEE Transactions on Big Data. 2025. P. 1–18. URL: <https://doi.org/10.1109/TBDATA.2025.3593370> (date of access: 15.10.2025).
6. Radiuk P. Application of a genetic algorithm to search for the optimal convolutional neural network architecture with weight distribution. Herald of Khmelnytskyi National University. Technical sciences. 2020. Vol. 281, no. 1. P. 7–11. URL: <https://doi.org/10.31891/2307-5732-2020-281-1-7-11> (date of access: 30.09.2025).
7. MetaGPT: meta programming for A multi-agent collaborative framework / S. Hong et al. Ithaca, NY, USA : Cornell University, 2024. 29 p. (Preprint. Cornell University ; 2308.00352). URL: <https://doi.org/10.48550/arXiv.2308.00352> (date of access: 14.10.2025).
8. ReAct: synergizing reasoning and acting in language models / S. Yao et al. Ithaca, NY, USA : Cornell University, 2024. 33 p. (Preprint. Cornell University ; 2210.03629). URL: <https://arxiv.org/abs/2210.03629> (date of access: 15.10.2025).
9. TradingAgents: multi-agents LLM financial trading framework / Y. Xiao et al. Ithaca, NY, USA : Cornell University, 2025. 38 p. (Preprint. Cornell University ; 2412.20138). URL: <https://doi.org/10.48550/arXiv.2412.20138> (date of access: 15.10.2025).
10. TradingGPT: multi-agent system with layered memory and distinct characters for enhanced financial trading performance / Y. Li et al. Ithaca, NY, USA : Cornell University, 2023. 7 p. (Preprint. Cornell University ; 2309.03736). URL: <https://doi.org/10.48550/arXiv.2309.03736> (date of access: 15.10.2025).

УДК 004.8

Червончук І.С.

Хмельницький національний університет

АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ЛОГІВ У ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ

Розглянуто поняття журналів логів програмного забезпечення, їх важливість та актуальність. Проаналізовано існуючі задачі та проблеми, що стосуються логування, а також подано методи та засоби виявлення логів у програмному забезпеченні.

The concept of software log files and their importance and relevance are considered. Existing tasks and problems related to logging are analyzed, and methods and means of detecting logs in software are presented.

Величезні обсяги даних журналів логів щодня генеруються програмним забезпеченням. Разом з тим, ці дані містять цінну інформацію про поведінку та стан системи, яка рідко використовується через свій обсяг та неструктурованість. Ручне переглядання файлів журналів є трудомісткою та тривалою процедурою для розробників [3, 5].

Проте, інформація журналів може допомогти у виявленні проблемного виконання програмного забезпечення, навіть якщо кінцевий результат здається цілком нормальним. В сучасних умовах автоматичний аналіз файлів журналів має вирішальне значення для виявлення проблем, але головним чином для розуміння того, як поводить себе програмне забезпечення, що було б корисним для запобігання збоєм та вдосконалення самого програмного забезпечення. Тому досить актуальним є задача виявлення неочікуваних виконань програмного забезпечення та визначення корінної причини їх виникнення. Більш детально, очікувану поведінку програмного забезпечення можна апроксимувати за допомогою методів модельного висновку, а нові спостережувані дані можна проаналізувати, щоб перевірити, чи відповідають вони очікуваній поведінці.

Разом з тим існують такі проблемні питання, що доцільно розглядати в якості дослідницьких напрямків. До таких питань відносяться:

- об'єм даних;
- контекст;
- налаштування політики.

Нові способи логування включають перехід від текстів до структури, а саме централізоване логування (Centralized Logging) та структуроване логування (Structured Logging).

Концепція централізованого логування полягає у тому, що замість того, щоб зберігати лог-файли локально на кожному сервері чи в контейнері, усі логи збираються та агрегуються в єдиному місці. Перевагами є спрощення пошуку, а також кореляція подій, що відбуваються в різних мікросервісах, і значно покращує моніторинг розподілених систем [2].

Концепція структурованого логування полягає у тому, що логи записуються у форматі, який легко читається машиною, найчастіше JSON або XML. Замість неструктурованого рядка, кожен запис є об'єктом із чітко визначеними полями. Перевагами є забезпечення високої швидкості обробки та аналізу, а також можливість створювати складні фільтри та запити, а також легко інтегрується із системами моніторингу та аналітики. Це є стандартом для сучасних хмарних і мікросервісних архітектур.

Трасування відноситься до розширеного методу логування, що сфокусований на відстеженні повного шляху виконання запиту через усі мікросервіси у розподіленій системі. Перевагами є можливість виявити «вузькі місця» та затримки у складному ланцюжку викликів, що є неможливим при звичайному логуванні. Стандарти, такі як OpenTelemetry, стають ключовими для реалізації трасування.

Найпопулярнішим набором інструментів для централізованого, структурованого логування є стек ELK або Elastic Stack.

Аналоги та хмарні рішення:

- Splunk - це комерційний лідер у сфері SIEM та логування, відомий потужними можливостями аналізу та кореляції даних.

- Loki (Grafana Labs) - альтернатива, орієнтована на ефективне зберігання та індексацію логів, де індексація відбувається лише за метаданими, а не за повним текстом, що робить її економічною.

- хмарні сервіси, наприклад, AWS CloudWatch, Azure Monitor, Google Cloud Logging, що надають повністю керовані сервіси для збору, аналізу та зберігання логів.

Сучасні технології виходять за рамки простого пошуку та візуалізації. В сучасних реаліях широко використовуються інтелектуальний аналіз логів, що включає:

- аномальне виявлення, що полягає у використанні машинного навчання для аналізу шаблонів логування та автоматичного виявлення нетипової поведінки, яка може свідчити про збої, атаки або несподівані зміни;

– автоматичне усунення неполадок, що полягає в інтеграції систем логування з інструментами автоматизації, наприклад, системами оповіщення та автоматичним перезапуском сервісів, для мінімізації часу простою;

– Log-as-Code полягає в управлінні конфігурацією логування, фільтрами та дашбордами за допомогою коду, наприклад, Terraform, що забезпечує узгодженість та можливість відстеження змін.

Впровадження цих засобів і способів дозволяє ІТ-фірмам не лише діагностувати проблеми, а й активно їх запобігати, перетворюючи логи з архіву даних на оперативний інтелект.

Перелік посилань

1. Peter Evers. A large-scale evaluation of tracing back log data to its origin with static analysis. Master's thesis, Delft University of Technology, 2018.
2. Hen Amar, Lingfeng Bao, Nimrod Busany, David Lo, and Shahar Maoz. Using finite-state models for log differencing. In Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, pages 49-59. ACM, 2018.
3. Log analytics, log mining, anomaly detection. URL: <https://www.xenonstack.com/blog/data-science/log-analytics-log-mining-anomalydetection> (last accessed: 11.10.2025).
4. Лог-файли як невід'ємна частина процесу розробки. URL: <https://foxminded.ua/shcho-take-loh-faily/> (дата звернення: 21.10.2025).

.

УДК 004.056.5

Чешун В.М.

Хмельницький національний університет

СВІТОВІ ПРАКТИКИ РЕГУЛЮВАННЯ ТА СТАНДАРТИЗАЦІЇ КІБЕРБЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

В роботі здійснюється аналіз світових практик регулювання та стандартизації кібербезпеки Інтернету речей у відповідь на зростаючі загрози. Виділено ключові фреймворки та нормативні документи, що охоплюють життєвий цикл IoT-пристроїв. Розглянуто британські Рекомендації (Code of Practice) та федеральний закон США «IoT Cybersecurity Improvement Act of 2020». Описано CSA Framework для корпоративного IoT та європейський стандарт ETSI EN 303 645. Підкреслено роль ISO/IEC 27001 та 27701 для формування комплексних СУІБ та управління конфіденційністю.

The paper analyzes global practices of regulating and standardizing IoT cybersecurity in response to growing threats. Key frameworks and regulatory documents covering the lifecycle of IoT devices are highlighted. The British Code of Practice and the US federal law “IoT Cybersecurity Improvement Act of 2020” are reviewed. The CSA Framework for corporate IoT and the European standard ETSI EN 303 645 are described. The role of ISO/IEC 27001 and 27701 for the formation of comprehensive ISMS and privacy management is emphasized.

Безпека Інтернету речей (IoT) є однією з найгостріших задач сьогодення, хоча системна увага до її вирішення на рівні законів та стандартів почала з'являтися порівняно нещодавно. Наразі існує низка фреймворків та нормативних документів, які забезпечують безпеку IoT-пристроїв та систем.

Однією з перших у світі спроб стимулювати ринок споживчого IoT до самоорганізації у сфері кібербезпеки стали Рекомендації щодо безпеки споживчих IoT-пристроїв (Code of Practice for Consumer IoT Security) [1], опубліковані Міністерством цифрових технологій, культури, медіа та спорту Великої Британії (UK DCMS) у 2018 році.

Цей політичний документ сформулював 13 мінімальних вимог безпеки, що охоплюють повний життєвий цикл IoT-пристрою: від розробки до утилізації. Ключові принципи включали:

- унікальні або змінні паролі при першому налаштуванні;
- впровадження політики управління вразливостями та визначення контактної точки;

- зрозумілі механізми оновлення прошивки протягом чітко оголошеного строку підтримки;
- обробка особистих даних згідно з принципами GDPR (мінімізація, шифрування);
- забезпечення функціоналу та доступу на основі принципу мінімальних привілеїв;
- реалізація захисту цілісності через контроль несанкціонованих змін конфігурації;
- захист каналу зв'язку сучасними протоколами шифрування;
- функціонал для безпечного стирання (знеособлення) персональних даних при утилізації;
- журналювання безпечної діяльності для виявлення інцидентів;
- стійкість до збоїв (здатність відновлюватися після аварійного оновлення);
- чітке інформування користувачів про налаштування безпеки та терміни підтримки.

Цей документ став основою для формування практики «безпечного дизайну» (security by design) для IoT у Європі.

Базисом для стандартизації безпеки IoT у США став федеральний закон «IoT Cybersecurity Improvement Act of 2020» [2]. Це перший системний нормативний документ на федеральному рівні, що встановлює мінімальні стандарти кіберзахисту для IoT-пристроїв, які закуповуються та експлуатуються урядовими структурами. Мета закону – усунути ризики, пов'язані з вразливостями IoT-пристроїв, які часто не мають належних механізмів автентифікації чи оновлення.

Закон зобов'язує Національний інститут стандартів і технологій США (NIST) розробляти технічні стандарти та рекомендації для безпечного проектування, ідентифікації, конфігурації, оновлення й управління IoT-пристроями. Федеральні агентства зобов'язані закуповувати лише ті пристрої, які відповідають стандартам NIST, що гарантує постачальникам дотримання базових вимог щодо конфіденційності, цілісності, доступності та управління уразливостями.

На виконання закону NIST розробив серії спеціальних публікацій SP 800-213 та NISTIR 8259.

Серія спеціальних публікацій SP 800-213 [3] надає керівництво для федеральних установ щодо використання пристроїв IoT у їхніх системах, визначаючи вимоги до кібербезпеки та унікальні ризики.

Фреймворк IoT Device Cybersecurity Guidance for the Federal Government [4] (у рамках SP 800-213) є ключовим орієнтиром, що надає чіткі рекомендації, як безпечно впроваджувати, експлуатувати й управляти IoT протягом усього

життєвого циклу. Фреймворк допомагає замовникам інтегрувати вимоги кібербезпеки пристроїв вже на етапі закупівель.

Серія публікацій NISTIR 8259 [5] спрямована на формування уніфікованого підходу до кібербезпеки IoT-пристроїв у контексті їхнього життєвого циклу (проектування, виробництво, експлуатація, утилізація). Головна мета – забезпечити прозорість між постачальниками та користувачами у федеральному секторі.

До серії публікацій NISTIR 8259 входить 3 документи:

- NISTIR 8259 [6] описує базові заходи з кібербезпеки, що мають бути виконані виробниками;

- NISTIR 8259A [7] містить перелік мінімальних технічних можливостей безпеки;

- NISTIR 8259B (Draft) [8] описує нефункціональні вимоги (політики, підтримка), що забезпечують безпечну експлуатацію.

Також заслуговує на увагу фреймворк CSA IoT Security Controls Framework, орієнтований на безпеку корпоративного IoT.

CSA IoT Security Controls Framework [9], створений Cloud Security Alliance (CSA), є рамковим документом для організацій, які проєктують, розробляють або впроваджують корпоративні IoT-системи (пристрої, хмара, мережі). Його мета – надати структуровану систему заходів контролю безпеки, що дозволяє зменшувати ризики вразливостей протягом життєвого циклу.

Фреймворк структурований за доменами IoT-архітектури:

- пристрої (Device/Thing Security);

- мережевий рівень (Network Security);

- шлюзи (Gateway Security);

- IoT-платформи / хмара (Cloud/Platform Security);

- додатки (Application Security);

- операційні процеси та управління (Operations and Lifecycle Security).

Ключові принципи контролів включають:

- ідентифікація та автентифікація (унікнення загальних облікових даних, багатофакторна автентифікація);

- управління конфігурацією та цілісністю (захист конфігурацій, перевірка цілісності пз/прошивки);

- захищені оновлення (цифровий підпис оновлень, своєчасне усунення уразливостей);

- захист даних (шифрування «у спокої» та «у русі», мінімізація збору даних);

- безпека комунікацій (захищені протоколи, сегментація мереж);

– моніторинг та реагування (постійний моніторинг, інтеграція з SIEM/IDS/IPS);

– управління доступом (принцип мінімальних привілеїв, RBAC/ABAC);

– безпечний життєвий цикл (*security by design*, політика утилізації/перепродажу).

CSA Framework є практичним посібником, який часто використовується для аудиту IoT-середовищ та розробки політик безпеки, особливо актуальний для організацій, що поєднують IoT із хмарними сервісами.

Рамка відповідності (IoTSEF Compliance Framework) [10] Фонду безпеки IoT (IoTSEF) є добровільним методичним документом, що допомагає виробникам уніфікувати мінімальні вимоги до безпеки, забезпечити їх перевірку й стимулювати ринок гарантувати належний рівень кіберстійкості. Рамка організована за розділами: процес, програмне забезпечення, фізичний захист та зв'язок.

Стандарт кібербезпеки ЄС для споживчих пристроїв IoT ETSI EN 303 645 [11] охоплює широкий спектр побутових пристроїв (розумні камери, телебачення, побутова техніка тощо). Він встановлює базовий рівень безпеки для запобігання великомасштабним атакам, вимагаючи відсутності паролів за замовчуванням, впровадження політики розкриття уразливостей та забезпечення актуальності ПЗ. Хоча він не є обов'язковим, його дотримання важливе для європейського ринку і є основою для потенційних схем сертифікації.

Комплексну методологічну основу для побудови надійної Системи управління інформаційною безпекою (СУІБ) та конфіденційністю в IoT-середовищах забезпечують міжнародні стандарти ISO/IEC 27001 [12] і ISO/IEC 27701 [13]:

ISO/IEC 27001 визначає вимоги до побудови, впровадження та постійного вдосконалення СУІБ. У контексті IoT це вимагає комплексної оцінки ризиків, ідентифікації активів, впровадження політик контролю доступу, шифрування, моніторингу та забезпечення цілісності даних;

ISO/IEC 27701 фокусується на управлінні конфіденційністю та персональними даними. Він розширює вимоги 27001 до системи управління конфіденційністю, пропонуючи механізми для дотримання вимог, подібних до GDPR (інформована згода, мінімізація збору даних, управління доступом до персональних даних).

Застосування цих стандартів у сфері IoT сприяє формуванню структурованих та прозорих процесів управління безпекою й конфіденційністю. Їх імплементація особливо актуальна для критичних галузей (охорона здоров'я, транспорт, енергетика), де компрометація IoT-пристроїв може мати серйозні наслідки для безпеки людей.

Перелік посилань

1. Code of Practice for Consumer IoT Security. Government of the United Kingdom: Department for Digital, Culture, Media & Sport. 2018. 20 p. URL: <https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security> (date of access: 25.10.2025).
2. IoT Cybersecurity Improvement Act of 2020. CONGRESS.GOV. URL: <https://www.congress.gov/bill/116th-congress/house-bill/1668/text> (date of access: 21.10.2025).
3. SP 800-213 Series. NIST. URL: <https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/sp-800-213-series> (date of access: 23.10.2025).
4. NIST SP 800-213: IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements. NIST. URL: <https://csrc.nist.rip/Pubs/sp/800/213/Final> (date of access: 24.10.2025).
5. NISTIR 8259 Series. NIST. URL: <https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series> (date of access: 25.10.2025).
6. NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers. National Institute of Standards and Technology Interagency or Internal Report 8259. U.S. Department of Commerce: National Institute of Standards and Technology (NIST). 2020. 36 p.
7. NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline. National Institute of Standards and Technology Interagency or Internal Report 8259A. U.S. Department of Commerce: National Institute of Standards and Technology (NIST). 2020. 23 p.
8. Draft NISTIR 8259B: IoT Non-Technical Supporting Capability Core Baseline. National Institute of Standards and Technology Interagency or Internal Report 8259B. U.S. Department of Commerce: National Institute of Standards and Technology (NIST). 2020. 20 p.
9. CSA IoT Security Controls Framework v2. Cloud Security Alliance. URL: <https://cloudsecurityalliance.org/artifacts/csa-iot-security-controls-framework-v2> (date of access: 20.10.2025).
10. Understanding IoT Security: Threats, Standards & Best Practices [Electronic resource] – URL: <https://sternumiot.com/iot-blog/understanding-iot-security-challenges-standards-and-best-practices/> (Accessed: 13.06.2025). – Screen Title.
11. ETSI EN 303 645. Cyber Security for Consumer Internet of Things: Baseline Requirements. ETSI. 2024. 41 p.
12. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. ISO. – URL: <https://www.iso.org/standard/27001> (date of access: 23.10.2025).
13. ISO/IEC 27701:2019. Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guidelines. ISO. URL: <https://www.iso.org/standard/71670.html> (date of access: 23.10.2025).

УДК 004.891

Чорненко С.В., Джулій В.М.

Хмельницький національний університет

МЕТОД ВЗАЄМОДІЇ КВАНТОВОЇ АПАРАТУРИ З КОРИСТУВАЛЬНИЦЬКИМИ СИСТЕМАМИ ЗАХИСТУ

В результаті проведеного аналізу виявлено проблеми, що виникають у процесі формування загальних секретів, при узгодженні послідовностей квантової мережі для системи захисту інформації та при передачі цих секретів. Запропоновано метод взаємодії квантової апаратури з користувальницькими системами захисту, уточнює процеси синхронізації ключів квантової мережі та їх передачі в систему захисту інформації.

As a result of the analysis, problems that arise in the process of forming shared secrets, when coordinating quantum network sequences for the information protection system and when transferring these secrets are identified. A method of interaction of quantum equipment with user protection systems is proposed, which clarifies the processes of synchronization of quantum network keys and their transfer to the information protection system.

Технологія квантового розподілу ключів – отримання ідентичних випадкових послідовностей абонентами, отриманих із використанням передачі між абонентами деякої інформації, з використанням квантових частинок. Абоненти використовують квантові пристрої, що реалізують протокол квантового розподілу ключів. Протокол квантового розподілу ключів включає: підготовку та перетворення інформаційних квантових станів в пристрої, який повинен мати джерело квантових станів; спосіб передачі квантовим каналом інформаційних квантових станів; спосіб інтерпретації, реєстрації та перетворення результатів вимірювань на з'єднаному пристрої; спосіб обробки отриманої за результатами вимірювань, послідовності, із застосуванням відкритого автентифікованого каналу зв'язку [1,2,3].

Результатом роботи протоколу квантового розподілу ключів є отримання секретного квантового ключа, ідентичного на обох вузлах мережі квантового каналу. Квантовий комплекс, що реалізує протокол квантового розподілу ключів, є апаратура з двох пристроїв, з'єднаних квантовим каналом. Архітектура комплексу наведена на рисунку 1.

Клієнт квантового розподілу ключів містить джерело (генератор) одиночних фотонів. Під'єднаний пристрій, що містить приймач (детектор) одиночних фотонів, називають Сервер квантового розподілу ключів. Кожен із вузлів квантового каналу містить датчик випадкових чисел. Таким чином можна отримати випадкову істинну послідовність, з якої в подальшому буде формуватиметься квантовий секретний ключ.

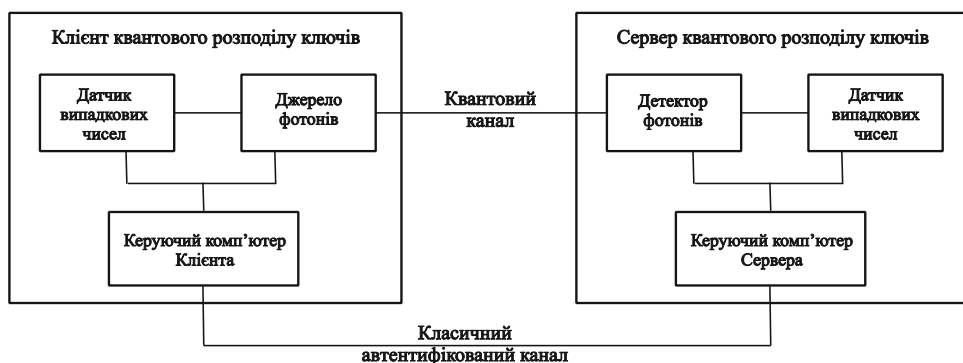


Рисунок 1 – Спрощена архітектура комплексу квантової апаратури

Сервер та Клієнт квантового розподілу ключів з'єднані двома логічними каналами: класичним та квантовим. Квантовий канал, зазвичай реалізується оптоволоконном, призначений для передачі фотонів, квантових інформаційних станів. Існують системи квантового розподілу ключів, в яких використовується повітряне середовище передачі, як квантовий канал, проте вони знаходяться ще в стадії лабораторних розробок [2, 3, 4].

Системи квантового розподілу ключів мають граничну довжину квантового каналу, визначається протоколом квантового розподілу ключів. Пристрої користувача, для яких генеруються квантові ключі, можуть довільно розташовуватися, на відстанях, що перевищують допустиму довжину квантового каналу. Необхідно розглянути задачу розподілу квантових ключів для довільних пар пристроїв квантової мережі, що розташовані поза граничної довжини квантового каналу.

В результаті проведеного дослідження та аналізу виявлених недоліків пропонується структура комплексу квантової апаратури захисту інформації, наведена на рисунку 2. У запропонованому комплексі квантової апаратури використовується одна транспортна лінія зв'язку, яка з'єднує дві системи захисту інформації, два вузли квантової мережі системи квантового розподілу ключів.

Логічний канал системи квантового розподілу ключів передачі службових повідомлень складається з каналів передачі інформації: автентифікований канал передачі службової інформації з використанням квантових ключів мережі та квантових ключів із приймального вузла квантової мережі системи квантового розподілу ключів з пов'язаною системою захисту інформації; автентифікований канал передачі користувальницької інформації з використанням квантових ключів мережі між системами захисту інформації; автентифікований канал передачі квантових ключів та службової інформації з використанням квантових ключів із передавального вузла квантової мережі системи квантового розподілення ключів з пов'язаною системою захисту інформації.

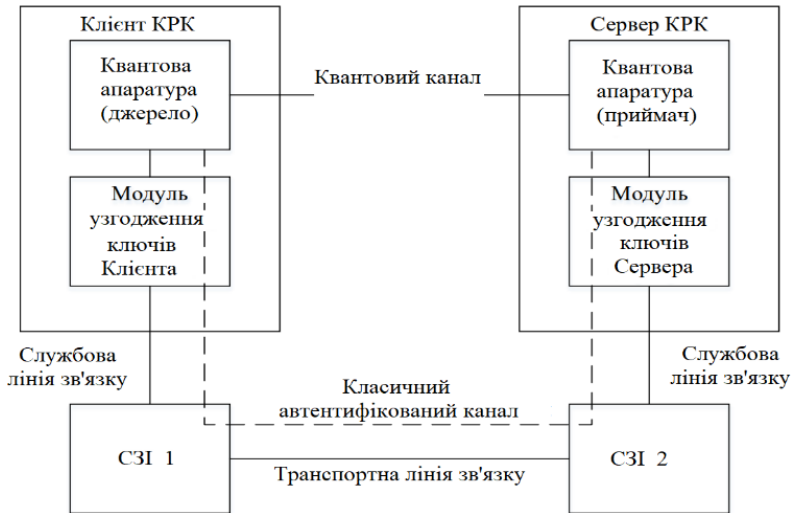


Рисунок 2 – Комплекс квантової апаратури захисту інформації

Таким чином, порівняно з розглянутими підходами, в запропонованому рішенні немає необхідності в окремому каналі мережі для обміну службовою інформацією вузлів системи квантового розподілення при генерації квантових ключів, використовується один канал для передачі зашифрованих даних користувача та службових повідомлень системи квантового розподілення ключів, в результаті знижуються витрати на розгортання, експлуатацію, створення комплексу.

У запропонованому комплексі квантової апаратури реалізовані додаткові модулі узгодження квантових ключів, що виконують функції формування квантових ключів мережі та накопичення випадкової послідовності. Після накопичення необхідної кількості ключів, формуються загальні секрети для системи захисту інформації та ключі для аутентифікації службової інформації системи квантового розподілення ключів, для передачі між Сервером та Клієнтом у процесі виконання протоколу квантового розподілення ключів (достатня кількість накопичених ключів квантової мережі - кількість квантових ключів, довжина яких більше сумарної довжини ключа аутентифікації та загального секрету, довжини ключів аутентифікації та загального секрету визначаються способом аутентифікації та застосовуванням алгоритмом шифрування системою захисту інформації).

Перед подальшим формуванням ключів аутентифікації та шифрування, за рахунок використання накопичення квантових ключів, досягається підвищення надійності комплексу квантової апаратури у випадку непередбачених збоїв системи квантового розподілення ключів (тимчасове припиненні генерації квантових ключів, атаки на квантовий канал зв'язку). У даній ситуації, згенеровані квантові

ключі зберігаються, після відновлення системи квантового розподілення ключів продовжується накопичення квантових ключів до згенерованих.

Пропонується на двох кінцях квантового каналу, два варіанти контролю ідентичності квантових ключів в залежності від збоїв при роботі квантової апаратури.

У першому випадку, що випадкове повідомлення, отримане в результаті роботи протоколу квантового розподілення ключів ідентичне, формування квантових ключів з повідомлення відбувається без збоїв. Контроль цілісності передачі в систему захисту інформації від квантової апаратури проводиться безпосередньо засобами квантового каналу, через службову лінію зв'язку, і передача інформації, в даному випадку, захищена від випадкових спотворень. У такому підході можливе узгодження квантових ключів та їх ідентифікаторів шляхом порівняння. Якщо ідентифікатори не співпадають, то ключі видаляються (відкидаються). За рахунок порівняння ідентифікаторів переданих секретів у систему захисту інформації досягається підвищення надійності комплексу квантової апаратури у разі спотворень, які вносяться службовою лінією зв'язку.

Результатом запропонованого методу взаємодії квантової апаратури з користувальницькими системами захисту є:

1. Підвищення надійності комплексу квантової апаратури, у разі спотворень (навмисних, випадкових), які вносяться службовою лінією зв'язку; у разі виникнення короточасних збоїв системи квантового розподілення ключів (припиненні генерації квантових ключів); у разі спотворень ідентифікаторів ключів.

2. Зниження витрат на експлуатацію, створення, розгортання комплексу за рахунок зменшення класичних ліній зв'язку.

3. Підвищення стійкості квантових ключів, згенерованих системою квантового розподілення ключів, за рахунок аутентифікації службової інформації системи розподілу на ключах аутентифікації, згенерованих з квантових ключів, та аутентифікації службової інформації системи квантового розподілення ключів, розбиття на блоки, при передачі по лінії зв'язку, та наступного шифрування службової інформації у транспортній лінії зв'язку між системами захисту інформації.

Перелік посилань

1. Доктрина інформаційної безпеки України, затвердженої Указом Президента України від 25 лютого 2017 року № №47/2017, 15с.
2. Квантова криптографія. Пояснення [Електронний ресурс] // Quantum Xchange. – 2019. – Режим доступу: <https://quantumxc.com/blog/quantum-cryptography-explained/> (дата звернення 02.03.2025).
3. Satish Kumar. Quantum Cryptography [Електронний ресурс] // Tutorialspoint. – 2023. – Режим доступу: <http://surl.li/fjebs> (дата звернення 05.03.2025).
4. Грамблінг Е., Горовіч М. Квантові обчислення. Прогрес і перспективи. Вашингтон: Національні академії наук, техніки та медицини, 2019. 272 с.

УДК 004.8

Чумак М.В.¹, Мазурець О.В.²

¹ Ліцей №4 ім. Павла Жука Хмельницької міської ради

² Хмельницький національний університет

ПОЯСНЕННЯ ВИЯВЛЕННЯ ФІШИНГОВИХ ПОВІДОМЛЕНЬ НЕЙРОМЕРЕЖЕВИМИ ЗАСОБАМИ В СИСТЕМАХ КІБЕРЗАХИСТУ

Робота присвячена поясненню виявленню фішингових повідомлень, у якому нейромережева модель не лише класифікує текст як «фішинг / нефішинг», а й ідентифікує домінуючий тип маніпуляції (терміновість дії, апеляція до авторитету, емоційний або раціональний тиск). Запропонована інформаційна технологія базується на трансформерній архітектурі глибокого навчання, що аналізує текстові представлення повідомлень і виконує бінарну та багатокласову класифікацію. Поясненість результатів досягається завдяки використанню механізмів уваги та градієнтно орієнтованих атрибуцій, які виділяють фрагменти тексту, що найбільше вплинули на прийняте рішення. Інтеграція такого модуля в системи кіберзахисту підвищує якість виявлення соціоінженерних атак і рівень довіри до нейромережевих засобів захисту.

The paper addresses explainable detection of phishing messages, where a neural model not only classifies text as «phishing / non-phishing» but also identifies the dominant type of manipulation (urgency, authority appeal, emotional or rational pressure). The proposed information technology relies on a transformer-based deep learning architecture that operates on textual representations and performs both binary and multiclass classification. Explainability is achieved through attention mechanisms and gradient-based attribution methods that highlight text fragments with the strongest impact on the decision. Integration of the module into cybersecurity systems improves the detection of social engineering attacks and increases trust in neural network-based defence tools.

Проблематика виявлення фішингових повідомлень традиційно розглядалася крізь призму технічних характеристик атаки: підозрілих URL, доменів, вкладень, сигнатур і структурних аномалій електронних листів [1, 2]. Проте сучасні фішингові кампанії дедалі частіше ґрунтуються не на шкідливому коді, а на стратегіях соціальної інженерії, де ключову роль відіграють маніпулятивні мовні патерни [3]. Повідомлення будуються таким чином, щоб викликати у користувача відчуття терміновості, штучно сконструйованої довіри або неминучої втрати, а також спонукати до негайної дії без критичного аналізу змісту [4]. За таких умов рішення, що орієнтуються лише на формальні параметри, виявляються недостатніми, оскільки не охоплюють приховану комунікативну природу загрози.

Зростання кількості кібератак та поширення фішингових повідомлень становлять серйозну загрозу безпеці інформаційних систем і користувачів. Традиційні методи виявлення фішингу, що базуються на жорстко визначених правилах або сигнатурах, часто не встигають за швидко змінюваними техніками шахраїв і не здатні ефективно працювати з великими потоками електронної кореспонденції та повідомлень. У цьому контексті застосування нейромережових методів обробки природної мови [4] та машинного навчання [5] відкриває нові можливості для автоматизованого і масштабованого виявлення фішингових атак.

Нейромережові моделі дозволяють аналізувати лінгвістичні [6], синтаксичні [7] та семантичні [8] патерни повідомлень, виявляючи ознаки маніпулятивного або шахрайського контенту [9], що не завжди очевидні при поверхневому аналізі. Використання трансформерних архітектур [10] і моделей глибокого навчання [11] забезпечує контекстне розуміння тексту [12], дозволяючи системам не лише класифікувати повідомлення як фішингові або безпечні, а й ідентифікувати ключові елементи ризику, такі як підроблені домени, соціальна інженерія або загрози фінансового характеру [13].

Особливо важливим є інтегрування пояснюваності у нейромережові моделі, що дозволяє фахівцям з кібербезпеки розуміти, на яких ознаках базується класифікація, підвищуючи довіру до автоматизованих систем і полегшуючи процес реагування на інциденти [14, 15].

Метою роботи є розроблення поясненої нейромережової технології виявлення фішингових повідомлень за маніпулятивними патернами для інтеграції в системи кіберзахисту. У межах такої технології автоматизоване рішення повинно не лише визначати, чи є повідомлення фішинговим, а й ідентифікувати домінуючий вид маніпуляції, за допомогою якого здійснюється психологічний вплив. Йдеться насамперед про стратегії, що апелюють до терміновості дії, авторитету відправника або переконання через емоційні та раціональні аргументи; у реальних сценаріях вони можуть поєднуватися у межах одного тексту, формуючи складну структуру мовного тиску.

Для досягнення поставленої мети пропонується інформаційна технологія, у межах якої текстові повідомлення проходять поетапну обробку: нормалізацію і токенизацію, перетворення в векторні представлення, подальший аналіз трансформерною архітектурою глибокого навчання, що виконує одночасно бінарну класифікацію «фішинг / нефішинг» і багатокласову або багатоміткову класифікацію типів маніпулятивного впливу.

Ключовою відмінністю запропонованого підходу є акцент на поясненості результатів. Нейромережева модель доповнюється модулем інтерпретації, який на основі механізмів уваги, градієнтно-орієнтованих атрибутів або інтегрованих градієнтів будує візуалізацію важливості окремих фрагментів повідомлення для

прийнятого рішення. У результаті користувач або аналітик системи кіберзахисту отримує не лише мітку «фішингове повідомлення з домінуванням стратегії терміновості» чи «апеляції до авторитету», а й текст із виділенням тих словосполучень і конструкцій, які зумовили таку класифікацію. Це забезпечує можливість верифікації та критичного аналізу роботи моделі, а також полегшує інтеграцію технології у регламентовані процеси реагування на інциденти.

Запропонована технологія спирається на попереднє маркування корпусу фішингових і нефішингових повідомлень з урахуванням типів маніпулятивного впливу, що створює підґрунтя для навчання і об'єктивної оцінки якості моделі. Порівняння з підходами, орієнтованими лише на технічні індикатори або плоскі текстові ознаки, дає змогу продемонструвати приріст ефективності для сценаріїв, де зловмисники свідомо мінімізують формальні маркери загрози, натомість ускладнюючи мовні стратегії соціальної інженерії.

Практична значущість роботи полягає у можливості інтеграції поясненої нейромережевої технології в існуючі системи кіберзахисту як окремого інтелектуального модуля для аналізу вхідних повідомлень. Такий модуль дозволяє знизити ймовірність успішного фішингу за рахунок раннього виявлення текстових загроз, підвищити обґрунтованість рішень щодо блокування або маркування повідомлень, а також сформувати базу для навчальних і просвітницьких заходів, які демонструють користувачам типові маніпулятивні патерни. Поясненість результатів у поєднанні з високими показниками якості класифікації є ключовою передумовою для зростання довіри до нейромережових засобів кіберзахисту та їхнього системного впровадження в організаціях різного масштабу.

Перелік посилань

1. Elberri, M. A., Tokeşer, Ü., Rahebi, J., & Lopez-Guede, J. M. (2024). A cyber defense system against phishing attacks with deep learning game theory and LSTM-CNN with African vulture optimization algorithm (AVOA). *International Journal of Information Security*, 23(4), 2583-2606.
2. Abed, A. K. (2025). Utilizing artificial intelligence in cybersecurity: A study of neural networks and support vector machines. *Babylonian Journal of Networking*, 2025, 14-24.
3. Feng, F., Zhou, Q., Shen, Z., Yang, X., Han, L., & Wang, J. (2024). The application of a novel neural network in the detection of phishing websites. *Journal of Ambient Intelligence and Humanized Computing*, 15(3), 1865-1879.
4. Murava V., Zalutska O., Didur V., Mazurets O. Software architecture of information system for exchanging LLM thematic prompts. *Global Trends in the Development of Information Technology and Science. Proceedings IV International Scientific and Practical Conference*. June 25-27, 2025. Stockholm, Sweden. Pp. 121-127.
5. Юрченко Д.Ю., Овчарук О.М., Мазурець О.В., Шевчук П.О. Метод використання нейромережі гібридної архітектури для визначення емоційної тональності текстових повідомлень. *Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах»*. № 2, 2025. с. 136-141.

6. Віт Р.В., Мазурець О.В. Метод виявлення психологічного цифрового перевантаження за аналізом текстових даних нейромережевими моделями глибокого навчання. Науковий журнал «Вісник Херсонського національного технічного університету». 2025. №2 (93). Т. 2. С. 107-114.
7. Sobko O., Mazurets O., Didur V., Chervonchuk I. Recurrent Neural Network Model Architecture for Detecting a Tendency to Atypical Behavior Of Individuals by Text Posts. Theoretical and Practical Aspects of Modern Research. Proceedings of XXVI International scientific and practical conference. June 5-7, 2024. International Scientific Unity. Ottawa, Canada. 2024. Pp. 113-117.
8. Овчарук О.М., Мазурець О.В. Нейромережевий метод діагностування психологічних розладів за аналізом повідомлень на основі роздільного підходу до класифікації. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». № 1, 2025. с. 210-216.
9. Mazurets O.V., Sobko O.V., Molchanova M.O., Zalutska O.O., Yurchak A.V. Practical Implementation of Neural Network Method for Stress Features Detection by Social Internet Networks Posts. Global Science: Prospects and Innovations. Proceedings of the II International Scientific and Theoretical Conference «Scientific Review of the Actual Events, Achievements and Problems». May 31, 2024. Berlin, Federal Republic of Germany: International Center of Scientific Research. 2024. Pp. 160-167.
10. O. Mazurets, R. Vit, M. Molchanova, I. Tymofiiiev, O. Sobko, Context-enriched approach to students depression monitoring in education using BERT-GPT hybrid model, CEUR Workshop Proceedings 4096 (2025) 167-176.
11. Molchanova M., Didur V., Sobko O., Mazurets O. Detection of Web Propaganda Patterns by Transformer Neural Networks: Improving Efficiency via Dataset Balancing, CEUR Workshop Proceedings, 2025, vol. 3988, pp. 112-126.
12. E. A. Manziuk, O. V. Sobko, I. O. Podhorniuk, M. O. Molchanova, O. V. Mazurets, Multifactorial analysis of mobbing behavioral signs in educational environments posts by NLP means, Journal of Physics Conference Series 3105(1) (2025) 012025.
13. Мазурець О.В., Козенко О.В., Собко О.В. Метод автоматизованого підбору відповідей на користувацькі запитання за семантичною подібністю. Матеріали XII Всеукраїнської науково-практичної конференції «Глушковські читання». Київ – 2023. с. 106-109.
14. Кок І.А., Мазурець О.В., Молчанова М.О. Пояснений підхід на основі трансферного навчання Vision Transformers до виявлення куріння у публічних просторах. Матеріали XIII Міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології ІУСТ-ОДЕСА-2025». 24-26.09.2025. Одеса. 2025. С.147-149.
15. Юрченко Д.Ю., Мазурець О.В., Залуцька О.О., Безпрозвана Ю.Г. Підхід до візуального пояснення результатів нейромережевого аналізу емоційної тональності повідомлень у соціальних мережах. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». 15-16 листопада 2024. Хмельницький, 2024. с. 565-571.

УДК 004.4

Шаповалов О.О., Петренко Ю.О.

Кам'янський енергетичний фаховий коледж

АРХІТЕКТУРА БЕЗПЕЧНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

У сучасному світі комп'ютерні мережі є основою функціонування інформаційного суспільства. Вони забезпечують передачу даних між користувачами, серверами, мобільними пристроями, промисловими системами та державними структурами. Проте зі зростанням обсягів даних та глобалізацією інтернет-простору виникає дедалі більше загроз інформаційній безпеці.

In the modern world, computer networks are the basis for the functioning of the information society. They ensure the transfer of data between users, servers, mobile devices, industrial systems and government agencies. However, with the growth of data volumes and the globalization of the Internet space, more and more threats to information security arise.

Кіберзлочинність, атаки типу DDoS, несанкціонований доступ, викрадення персональних даних та шкідливе програмне забезпечення – усе це вимагає побудови безпечної архітектури комп'ютерних мереж, яка забезпечує стійкість систем до зовнішніх і внутрішніх загроз.

Метою цієї доповіді є розгляд основних принципів побудови безпечних мережевих архітектур, аналіз сучасних технологій захисту та підходів до забезпечення надійності інформаційних систем.

Безпечна архітектура комп'ютерної мережі – це сукупність структурних, програмних і організаційних рішень, спрямованих на забезпечення захищеного обміну інформацією між усіма вузлами системи.

Мережа вважається безпечною, якщо вона забезпечує:

- Конфіденційність дані доступні лише авторизованим користувачам.
- Цілісність – виключається можливість зміни або знищення інформації.
- Доступність – гарантується постійна робота системи навіть у разі спроб злоумисників порушити її функціонування.
- Автентичність і невідомність – підтверджується особа користувача або джерело інформації.

Мережа поділяється на логічні зони з різним рівнем довіри:

- зона зовнішнього доступу (Інтернет),
- демілітаризована зона (DMZ) для публічних сервісів,

– внутрішня корпоративна зона.

Такий підхід обмежує поширення атаки у разі компрометації одного сегмента.

На межах мережі встановлюються між мережеві екрани (firewalls), шлюзи безпеки та системи виявлення вторгнень (IDS/IPS). Вони контролюють вхідний і вихідний трафік, фільтруючи шкідливі пакети.

Кожен користувач або служба повинні мати лише ті права доступу, які необхідні для виконання їхніх завдань. Це знижує ризик зловживань і випадкових помилок.

Безпека не обмежується одним механізмом. Використовуються одночасно антивірусні програми, IDS/IPS, VPN, шифрування, моніторинг та резервне копіювання.

Системи SIEM (Security Information and Event Management) збирають журнали подій з різних джерел, аналізують аномалії та генерують сповіщення про можливі інциденти.

Основні компоненти безпечної архітектури:

1. Міжмережеві екрани (Firewall)

Firewall – це перший рубіж оборони, який контролює потоки даних між внутрішньою мережею та зовнішнім середовищем.

Існують:

- мережеві фаєрволи (контролюють IP-трафік),
- прикладні шлюзи (аналізують дані на рівні програм),
- нового покоління (NGFW) – з інтегрованими функціями *IDS/IPS* та фільтрацією шкідливих програм.

Вони аналізують трафік, виявляють підозрілу активність і блокують атаки. Використовують методи сигнатурного та поведінкового аналізу, а також алгоритми машинного навчання для виявлення невідомих загроз.

2. Віртуальні приватні мережі (VPN)

VPN забезпечує захищене з'єднання між користувачем і сервером через публічну мережу. Для цього використовуються протоколи IPSec, SSL/TLS, OpenVPN.

3. Системи управління ідентифікацією (IAM)

Дають змогу централізовано керувати користувачами, контролювати доступ і здійснювати автентифікацію через LDAP, Kerberos, OAuth 2.0, SAML тощо.

Криптографічний захист даних

Шифрування інформації як під час передачі, так і під час зберігання гарантує конфіденційність навіть у разі перехоплення. Застосовуються алгоритми AES, RSA, ECC, SHA-3.

Моделі безпечних мереж:

Zero Trust Architecture (ZTA) – концепція, що базується на принципі «нікому не довіряй». Кожен запит на доступ перевіряється незалежно від місця походження користувача.

SASE (Secure Access Service Edge) – поєднання мережевих і захисних технологій у єдину хмарну платформу, що забезпечує безпеку віддалених користувачів.

Software-Defined Networking (SDN) Security – централізоване управління мережевою інфраструктурою, яке спрощує реалізацію політик безпеки.

Захист бездротових і промислових мереж

– У Wi-Fi-мережах безпеку забезпечують протоколи WPA3, автентифікація EAP і фільтрація MAC-адрес.

– У промислових системах (ICS/SCADA) важливо відокремлювати виробничу мережу від корпоративної та використовувати шлюзи моніторингу.

– Безпечна архітектура комп'ютерних мереж є критично важливою складовою сучасної IT-інфраструктури. Вона забезпечує надійний захист інформаційних потоків, мінімізує ризики порушення конфіденційності, цілісності та доступності даних.

Створення ефективної системи захисту потребує поєднання технічних, програмних і організаційних рішень: від використання фаєрволів і VPN до впровадження концепції Zero Trust та автоматизованого моніторингу подій безпеки.

Подальший розвиток безпечних архітектур буде спрямований на використання штучного інтелекту для проактивного виявлення атак, інтеграцію хмарних технологій і розробку постквантових алгоритмів захисту.

Перелік посилань

1. Stallings W. Network Security Essentials: Applications and Standards. – 7th ed. – Pearson, 2023.
2. NIST Special Publication 800-207. Zero Trust Architecture. – National Institute of Standards and Technology, 2020.
3. Tanenbaum A.S., Wetherall D.J. Computer Networks. – 6th ed. – Pearson, 2022.
4. Сидоренко І.В. Архітектура безпечних комп'ютерних мереж: навчальний посібник. – Київ: КПІ ім. І. Сікорського, 2021.
5. Cisco Systems. Enterprise Network Security Architecture Guide. – <https://www.cisco.com>.

УДК 004.8

Шашок Д.А., Микитюк М.О., Кліменко В.І.

Хмельницький національний університет

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ДЛЯ НЕЙРОМЕРЕЖЕВОГО ВИЯВЛЕННЯ ГЕНДЕРНОЇ ДИСКРИМІНАЦІЇ У СОЦІАЛЬНО-ОРІЄНТОВАНИХ СЕРВІСАХ

У роботі обґрунтовується необхідність розроблення інтелектуальної системи для автоматизованого виявлення гендерної дискримінації в соціально-орієнтованих сервісах, що функціонують у середовищах інтенсивної цифрової комунікації. Підкреслюється, що значний обсяг діалогового контенту, висока варіативність мовних форм і наявність прихованих дискримінаційних патернів роблять традиційні підходи моніторингу малоефективними. Використання сучасних методів обробки природної мови на основі трансформерних моделей створює можливість контекстуального аналізу повідомлень, урахування семантичних і прагматичних особливостей, а також виявлення латентних форм упередженості.

The paper justifies the need to develop an intelligent system for automated detection of gender discrimination in socially oriented services operating in environments of intensive digital communication. It is emphasized that a significant amount of dialogic content, high variability of language forms and the presence of hidden discriminatory patterns make traditional monitoring approaches ineffective. The use of modern methods of natural language processing based on transformer models creates the possibility of contextual analysis of messages, taking into account semantic and pragmatic features, as well as the detection of latent forms of bias.

У сучасному цифровому середовищі соціально-орієнтовані сервіси, такі як гарячі лінії, чати підтримки, сервіси електронної демократії, платформи звернень громадян, тематичні спільноти у месенджерах і соціальних мережах стають ключовим посередником між людиною та інституціями, що забезпечують соціальний захист, психологічну підтримку, доступ до послуг та участь у суспільному житті. Саме в цих комунікаційних просторах особливо гостро проявляються як явні, так і латентні форми гендерної дискримінації: від відкрито агресивних образ і сексистського тролінгу до «м'яких» патерналістських висловлювань, знецінення компетентності, прихованих стереотипів у відповідях операторів сервісів чи модераторів спільнот [1]. Така дискримінація не лише травмує окремих користувачів, а й підриває довіру до інституцій, які позиціонують себе як інклюзивні та орієнтовані на права людини.

Традиційні підходи до виявлення гендерної дискримінації в подібних середовищах спираються або на ручний моніторинг, або на прості ключові слова та

поверхневі фільтри [2]. Це створює дві критичні проблеми. По-перше, людиноорієнтований моніторинг погано масштабується, поглинає значні ресурси й не може забезпечити постійний контроль у режимі реального часу. По-друге, поверхневі лексичні фільтри майже не виявляють контекстуальних, іронічних, завуальованих чи структурно складних висловлювань, які несуть дискримінаційний зміст без використання очевидних «заборонених» слів. У результаті виникає наукове й практичне протиріччя: з одного боку, соціально-орієнтовані сервіси декларують цінності інклюзивності, з іншого, не мають інструментів об'єктивного, систематичного й відтворюваного контролю за гендерно-дискримінаційним контентом, що циркулює в їхньому інформаційному просторі.

Наразі соціально-орієнтовані сервіси, зокрема онлайн-спільноти, форуми й платформи підтримки, акумулюють значні масиви текстових повідомлень, у яких прояви упереджень, стереотипів чи образ можуть бути як явними, так і прихованими [3]. Через великий обсяг даних і варіативність мовних конструкцій ручний моніторинг стає практично неможливим, що підсилює актуальність застосування методів автоматизованого аналізу природної мови [4].

Розвиток нейромережових моделей обробки природної мови [5], зокрема трансформерів [6], відкрив можливість працювати з текстом не лише на рівні окремих слів [7], а й на рівні контексту [8], семантичних ролей [9], тональних і прагматичних характеристик [10]. Це дозволяє формувати задачу виявлення гендерної дискримінації у соціально-орієнтованих сервісах як задачу контекстуальної класифікації висловлювань, послідовностей реплік чи цілих діалогів, де рішення базується на інтегральному аналізі мовних патернів [11, 12], а не на механічній перевірці окремих лексем [13]. Попередні розробки нейромережових методів виявлення сексизму в медіаданих демонструють, що трансформерні моделі, адаптовані до спеціалізованих корпусів, здатні досить надійно відрізнити нейтральні повідомлення від дискримінаційних, включно з латентними формами, за умови коректного проектування конвеєра підготовки даних, навчання моделей та організації програмної системи [14].

Сучасні підходи NLP забезпечують ефективну обробку великих текстових потоків і здатні виявляти не лише буквальні образливі висловлювання [15], а й приховані форми дискримінації [16], такі як мікроагресії, стереотипні припущення чи непряму об'єктивацію. Моделі глибокого навчання, включно з трансформерними архітектурами [17, 18], дозволяють аналізувати контекст на рівні цілого повідомлення, урахувати семантичні й прагматичні зв'язки та виявляти залежності, недоступні для класичних лексичних методів. Розширені техніки, такі як контекстуальне ембедування, класифікація з багатьма мітками та моделі з пояснюваністю, підвищують точність визначення упереджених висловлювань і полегшують подальшу валідацію рішень фахівцями [19].

У випадку соціально-орієнтованих сервісів специфіка предметної області є суттєво складнішою, ніж у класичному аналізі відкритих медіа. По-перше, контент тут часто діалоговий: дискримінаційність репліки може виявлятися лише у взаємодії з попередніми повідомленнями, роллю мовця (користувач, консультант, модератор), статусом сервісу (державний, громадський, волонтерський) та очікуваннями користувача щодо підтримки. По-друге, у таких сервісах особливо важливий баланс між чутливістю й специфічністю: система не повинна надмірно «штрафувати» складні, але професійно виважені повідомлення консультантів, водночас має бути здатною виявляти навіть м'які форми знецінення чи стереотипного приписування ролей. По-третє, мова комунікації у соціальних сервісах часто змішана, неформальна, з жаргоном, емодзі, код-міксингом між українською, російською та англійською, що ускладнює застосування стандартних лінгвістичних моделей. Це вимагає спеціальної уваги до формування корпусів, анотування даних, мульти- чи крослінгвального навчання моделей та адаптації токенизаторів до реальної мовної практики.

Проектування інтелектуальної системи для нейромережевого виявлення гендерної дискримінації у соціально-орієнтованих сервісах доцільно розглядати як багаторівневий процес, що починається з концептуалізації предметної області й закінчується побудовою програмної архітектури, готової до інтеграції у реальні сервіси. Схема запропонована на рисунку 1. На концептуальному рівні ядром системи є модуль аналізу тексту на основі трансформерної моделі, донавченої на корпусі повідомлень соціальних сервісів з позначками «гендерно-дискримінаційне» та «недискримінаційне», а також, за потреби, додатковими підкласами, які відображають різні типи дискримінаційних проявів, наприклад відкрите приниження, сексуалізовані образи, патерналістські формулювання чи скритий стереотипний розподіл ролей. Навколо цього ядра вибудовується інфраструктура, яка забезпечує захоплення й нормалізацію даних із сервісів, знеособлення персональної інформації, зберігання історій взаємодій, формування сигналів для модерації, аналітики та звітності, а також механізми аудиту і контролю якості самого алгоритму.

Систему доцільно організувати за клієнт-серверною моделлю з виділенням кількох логічних шарів: шару інтеграції з каналами комунікації, де реалізується приймання повідомлень із чат-ботів, веб-форм, API соціальних мереж чи контакт-центрів; шару обробки й зберігання даних, який відповідає за нормалізацію тексту, знеособлення, побудову діалогових контекстів та ведення бази даних; інтелектуального шару, де реалізовано пайплайн нейромережевого аналізу, обчислення індикаторів ризику й формування пояснень; а також прикладного шару, що надає інтерфейси для модераторів, адміністраторів сервісу, аналітиків і, у спрощеному вигляді, для користувачів, які можуть отримувати зворотний зв'язок

щодо неприйнятних формулювань. Така багарівнева організація дозволяє розвести проблеми масштабованості, захисту даних, навчання моделей і користувацької взаємодії, роблячи систему гнучкою щодо подальшого розширення.

На рівні моделі даних ключовим є представлення комунікації не як набору окремих повідомлень, а як мережі взаємопов'язаних сутностей. Кожна сесія взаємодії у соціально-орієнтованому сервісі може бути змодельована як діалог, що має час початку, тип каналу, анонімізовані профілі учасників та послідовність реплік. Кожна репліка має текст, метадані (час, канал, роль мовця, мовні налаштування, технічні параметри) і результати аналізу: оцінку ймовірності гендерної дискримінації, тип виявленого патерну, індикатори впевненості моделі та, за потреби, фрагменти тексту, які зробили найбільший внесок у рішення. На цьому ж рівні фіксуються випадки ручної корекції результатів модераторами, що дозволяє використовувати їх надалі в циклі донавчання моделі та контролю її упередженості.

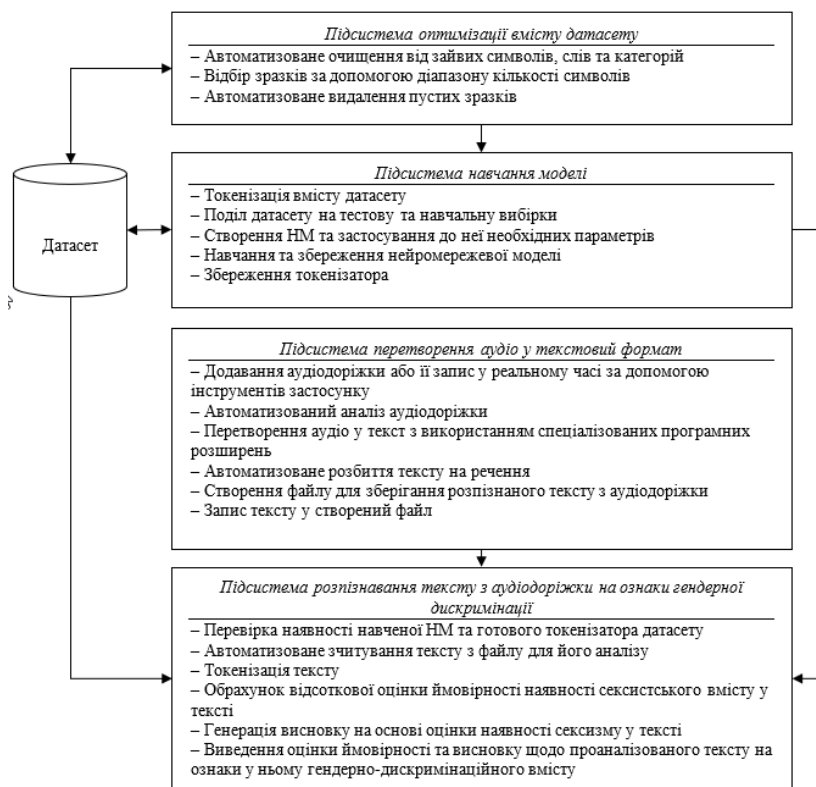


Рисунок 1 – Взаємодія складових інтелектуальної системи

Опис проєктування інтелектуальної системи неможливий без деталізації процесу побудови нейромережевого ядра. Базовим вибором є використання багатомовної трансформерної архітектури типу mBERT або XLM-R, здатної обробляти україномовні, російськомовні й англійськомовні фрагменти у межах однієї моделі. Початкове налаштування передбачає адаптацію токенизатора до специфіки текстів соціальних сервісів, з урахуванням характерних скорочень, емодзі, хештегів, посилань, слів із транслітерацією та кодуванням латиницею. Далі формується навчальний корпус, що включає анонімізовані дані з реальних сервісів (за умови дотримання етичних норм і правового регулювання), а також доповнюється відкритими корпусами сексистських висловлювань і нейтральних текстів із соціальних мереж, форумів, петицій чи коментарів до публікацій. Анотація здійснюється за чітко визначеною схемою, що передбачає розмежування гендерної дискримінації від інших видів токсичності, зокрема загального хейту, політичної агресії чи мови ворожнечі за іншими ознаками.

Сам процес навчання організовується як задача бінарної або багатокласової класифікації з можливістю подальшого переходу до багатоміткової постановки, якщо виникає потреба виділяти різні типи гендерної дискримінації паралельно. На вхід моделі подаються токенизовані репліки або короткі фрагменти діалогу, зафіксовані у певному часовому вікні. Модель видає вектор ймовірностей по класах, який далі використовується для прийняття рішення на рівні окремого повідомлення, а також агрегується на рівні діалогу, користувача чи сервісу. Для контролю якості використовуються стандартні метрики класифікації, але в інтерпретації, що враховує асиметрію вартості помилок: хибно-негативні рішення, коли дискримінаційний контент не виявлено, мають вищу критичність, ніж хибно-позитивні, що маркують нейтральні висловлювання як підозрілі.

Проектування класів програмної системи відображається у вигляді діаграми класів (рисунок 2), яку доцільно організувати навколо кількох концептуальних центрів. Першим центром є доменні класи, що описують структуру соціально-орієнтованих сервісів і комунікацій у них. До них належать класи, які моделюють користувача сервісу з його анонімізованим профілем, роль у системі, історію взаємодій, а також клас оператора або консультанта, що репрезентує сторону сервісу. Діалог як процес відображається окремим класом, який утримує колекцію реплік, пов'язаних із певною сесією, та метадані каналу взаємодії. Репліка представлена окремим класом із полями для тексту, часових міток, посилань на автора, структуру контексту та результатів аналізу.

Другим концептуальним центром є класи, що реалізують інтелектуальний модуль. Центральне місце посідає клас, що інкапсулює нейромережеву модель, вміє завантажувати ваги, виконувати прямий прохід і повертати ймовірнісні оцінки за

класами. Допоміжні класи реалізують попередню обробку тексту, включно з нормалізацією, очищенням від технічних елементів, сегментацією діалогу та побудовою входів моделі, а також постобробку результатів, зокрема формування текстового або структурованого висновку про наявність і тип гендерної дискримінації. Окремий клас може відповідати за генерацію пояснень, використовуючи методи пояснюваного машинного навчання, наприклад виділення фрагментів тексту, які зробили максимальний внесок у рішення, у вигляді вагових коефіцієнтів чи теплових карт.

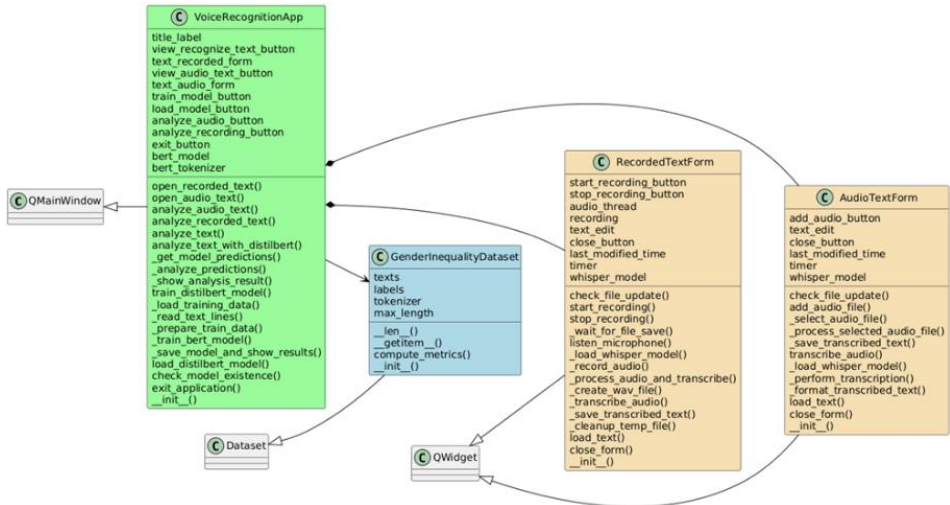


Рисунок 2 – Діаграма класів інтелектуальної системи

Третій центр діаграми класів стосується інфраструктури зберігання та інтеграції. Тут доцільно виокремити класи, які реалізують репозиторії для діалогів, користувачів, результатів аналізу та журналів модерацийних дій. Ці класи виступають абстракцією над конкретною СКБД, забезпечуючи транзакційність, логування змін, підтримку історії перегляду та можливість відновлення процесу у разі помилок. Їм протистоять класи, відповідальні за інтеграцію з зовнішніми сервісами – адаптери до API месенджерів, модулі обробки вебхуків, компоненти для імпорту історичних даних. Такий поділ дозволяє мінімізувати зв'язність між бізнес-логікою й технічними засобами доставки даних.

Нарешті, четвертий центр об'єднує класи користувацького інтерфейсу та сервісних компонентів. Окремі класи відповідають за вікна модератора чи адміністратора, у яких відображаються черги повідомлень із високим ризиком

дискримінації, детальні пояснення рішень моделі, агреговані статистики за каналами й тематичними категоріями. Інші класи представляють налаштування системи, конфігурацію порогів спрацювання, сценарії обробки інцидентів, ролі й права доступу. Логічним центром цього шару є клас, що координує взаємодію між інтерфейсом, репозиторіями даних та інтелектуальним модулем, реалізуючи шаблон фасаду для спрощення внутрішніх залежностей.

Діаграма класів, побудована з урахуванням описаних центрів, демонструє низку важливих відносин. Клас діалогу агрегаційно пов'язаний із класом репліки, оскільки утримує множину реплік, але вони можуть зберігатися автономно у базі даних. Репліка асоційована з класом користувача і класом оператора, що відображає напрямок та суб'єкта висловлювання. Клас інтелектуального модуля композиційно містить класи попередньої обробки та генератора пояснень, оскільки без них не може коректно функціонувати. Класи репозиторіїв перебувають у відношенні залежності з класами доменної моделі, оскільки реалізують збереження їхніх екземплярів, тоді як інтерфейсні класи використовують доменну модель для відображення й редагування відповідних сутностей.

У процесі проєктування особливу увагу приділяється питанням етичності й мінімізації вторинної дискримінації, яку потенційно можуть відтворювати алгоритми. Це виявляється у необхідності контролю якості моделі не лише на глобальних метриках, а й окремо для різних підгруп користувачів, з урахуванням гендерної ідентичності, мови, типу сервісу. Система має зберігати результати валідаційних експериментів, журнали ручних корекцій модераторів, а також надавати інструменти для аудиту рішень у проблемних випадках, коли користувачі оскаржують дії модерації. Такі механізми не лише підвищують прозорість, а й створюють зворотний зв'язок, необхідний для поступового донавання моделі на більш репрезентативних і збалансованих корпусах.

У підсумку проєктована інтелектуальна система поєднує концептуально виважений підхід до аналізу гендерної дискримінації у соціально-орієнтованих сервісах із чітко структурованою програмною архітектурою. Нейромережевий модуль на основі трансформерної моделі забезпечує здатність виявляти як явні, так і приховані форми дискримінації в умовах «шумної» реальної мовної практики, тоді як багаторівнева система класів, від доменної моделі до інтерфейсів адміністратора, робить можливим безперервний моніторинг, модерацію, аналітику та аудит. Така система здатна стати ключовим елементом цифрової інфраструктури соціально-орієнтованих сервісів, підтримуючи досягнення цілей гендерної рівності та побудови інклюзивних комунікаційних просторів у відповідності до глобальних орієнтирів сталого розвитку.

Перелік посилань

1. Jakob, M., Klauer, K. C., & Shechter, A. (2024). Detecting Gender Discrimination in a Context Disfavoring and Favoring Both Men and Women—a Signal Detection Approach.
2. Foley, S., Ngo, H. Y., Loi, R., & Zheng, X. (2015). Gender, gender identification and perceived gender discrimination: An examination of mediating processes in China. *Equality, Diversity and Inclusion: An International Journal*, 34(8), 650-665..
3. Молчанова М.О., Мазурець О.В., Собко О.В., Віт Р.В., Назаров В.В. Алгоритм виявлення аб'юзивного вмісту в україномовному аудіоконтенті для імплементації в об'єктно-орієнтовану інформаційну систему. *Науковий журнал «Вісник Хмельницького національного університету»* серія: Технічні науки. Хмельницький, 2024. №1 (331). С. 101-106.
4. Молчанова М.О., Мазурець О.В., Собко О.В., Кліменко В.І., Андрощук В.І. Метод неймережевого виявлення кібербулінгу з використанням хмарних сервісів та об'єктно-орієнтованої моделі. *Науковий журнал «Вісник Хмельницького національного університету»* серія: Технічні науки. Хмельницький, 2024. №2 (333). С. 200-206.
5. Денисенко Б.О., Молчанова М.О., Мазурець О.В. Інтелектуальна система виявлення дезінформації з застосуванням штучних нейронних мереж. *Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024»*. 15-16 листопада 2024. Хмельницький, 2024. с. 167-174.
6. Blazhuk V., Mazurets O., Zalutska O. An Approach to Using the mBERT Deep Learning Neural Network Model for Identifying Emotional Components and Communication Intentions. The Impact of Scientific Research on the Development of the Modern World. *Proceedings of the XLIV International scientific and practical conference*. October 23-25, 2024. Dubrovnik, Croatia. 2024. Pp. 79-84.
7. Sobko O., Mazurets O., Didur V., Chervonchuk I. Recurrent Neural Network Model Architecture for Detecting a Tendency to Atypical Behavior Of Individuals by Text Posts. Theoretical and Practical Aspects of Modern Research. *Proceedings of XXVI International scientific and practical conference*. June 5-7, 2024. International Scientific Unity. Ottawa, Canada. 2024. Pp. 113-117.
8. Tymofiiiev I., Mazurets O., Hardysh D., Molchanova M. Neural Network Dual Architecture for Depression Detection Using Cloud Services. *Scientific Research in the Era of Digital Technologies: Challenges and Opportunities*. *Proceedings of the XLVI International scientific and practical conference*. November 6-8, 2024. Barcelona, Spain. 2024. Pp. 84-88.
9. Mazurets O., Molchanova M., Klimenko V., Prosvitliuk M Practice Implementation of Neural Network Model BART-Large-CNN for Text Annotation. *Prospects of Scientific Research in the Conditions of the Modern World*. *Proceedings of XXVII International scientific and practical conference*. June 12-14, 2024. Rotterdam, Netherlands. 2024. Pp. 97-102.
10. Shevchuk P., Molchanova M., Mazurets O. Software for Text Messages Reliability Analysis Based on the Machine Learning Models Ensemble. *Proceedings of IV International Scientific and Practical Conference «Innovative research and perspectives of the development of science and technology»*. January 29-31, 2024. Stockholm, Sweden. 2024. Pp. 347-354.
11. Yurchenko D., Mazurets O., Didur V., Molchanova M. Approach to Using Cloud Services for Visual Analytics of Neural Network Analysis of Texts Emotional Tonality. *The Future of Scientific*

Discoveries: New Trends and Technologies. Proceedings of the XLVII International scientific and practical conference. November 13-15, 2024. Marseille, France. 2024. Pp. 108-113.

12. Hladun O., Mazurets O., Molchanova M., Sobko O. Real Time Detection the Person Emotion State Using Neural Network. Scientific Research: Modern Innovations and Future Perspectives. Proceedings of the 2 International scientific and practical conference. November 25-27, 2024. Montreal, Canada. 2024. Pp. 119-123.

13. Mazurets O., Sobko O., Vit R., Pasternak V. Practical Approach for Detection by Deep Learning of Target Objects of Subject Area Based on Semantic Connectivity Indicators in Audio Database. Proceedings of XXIV International Scientific and Practical Conference «Modern Scientific Challenges are the Driving Force of the Development of Scientific Research». May 22-24, 2024. Bruges, Belgium. International Scientific Unity. 2024. Pp. 91-96.

14. Овчарук О.М., Мазурець О.В. Нейромережний метод діагностування психологічних розладів за аналізом повідомлень на основі роздільного підходу до класифікації. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». № 1, 2025. с. 210-216.

15. Mazurets O.V., Sobko O.V., Molchanova M.O., Zalutska O.O., Yurchak A.V. Practical Implementation of Neural Network Method for Stress Features Detection by Social Internet Networks Posts. Global Science: Prospects and Innovations. Proceedings of the II International Scientific and Theoretical Conference «Scientific Review of the Actual Events, Achievements and Problems». May 31, 2024. Berlin, Federal Republic of Germany: International Center of Scientific Research. 2024. Pp. 160-167.

16. Овчарук О.М., Мазурець О.В. Нейромережева архітектура з квантовим шаром для аналізу текстових повідомлень на прояви посттравматичного стресового розладу. Науковий журнал «Наука і техніка сьогодні». Київ, 2024. №13 (41). С. 1192-1204.

17. Віт Р.В., Мазурець О.В. Підхід до тематичної класифікації текстової інформації засобами обробки природної мови. Науковий журнал «Наукові праці Донецького національного технічного університету», серія «Проблеми моделювання та автоматизації проектування». 2025. №1 (21). С. 94-99.

18. Murava V., Zalutska O., Didur V., Mazurets O. Software architecture of information system for exchanging LLM thematic prompts. Global Trends in the Development of Information Technology and Science. Proceedings IV International Scientific and Practical Conference. June 25-27, 2025. Stockholm, Sweden. Pp. 121-127.

19. Мазурець О.В., Тимофієв І.А., Кліменко В.І., Тищенко О.О. Метод виявлення депресивного стану пов'язаного із навчанням у закладах освіти із використанням нейромережі дуальної архітектури. Науковий журнал «Вісник Херсонського національного технічного університету». 2024. №4 (91). С. 311-318.

УДК 004.4

Швець Б.А., Праворська Н.І.

Хмельницький національний університет

ОНЛАЙН СЕРВІС ДЛЯ РЕДАГУВАННЯ ДОКУМЕНТІВ З МОЖЛИВІСТЮ КОМАНДНОЇ РОБОТИ У РЕАЛЬНОМУ ЧАСІ

Основним суттєвим фактором продуктивності команд розробників програмного забезпечення в сьогоденних умовах постійно зростаючої глобалізації та швидкого переходу до роботи у віддаленому форматі виявляється ефективне спільне опрацювання документів. В представленій роботі досліджено проблематику цього процесу, проаналізовано існуючі рішення для редагування документів та виявлено потребу у гнучких, високопродуктивних системах, побудованих на сучасному стеку технологій. Метою роботи є розробка веб-застосунку для редагування документів з використанням фреймворку Next.js 15, що забезпечує спільне редагування документів у реальному часі. Система включає розширений текстовий редактор, механізми коментарів та згадувань, робочі простори для організацій та автентифікацію. Розробка демонструє ефективність сучасних веб-технологій для створення комплексних інтерактивних платформ.

With the rapid rise of remote and hybrid work formats, organizing effective collaboration has become critically important. This paper investigates the problems of this process, analyzes existing solutions for document editing, and identifies the need for flexible, high-performance systems built on a modern technology stack. The aim of the work is to develop the web application using the Next.js 15 framework, which provides real-time collaborative document editing. The system includes a rich text editor, comment and mention mechanisms, organization workspaces, and authentication. The development demonstrates the effectiveness of modern web technologies for creating complex interactive platforms.

В умовах глобалізації та стрімкого переходу до віддаленого формату роботи, ефективна спільна робота над документами стає критично важливим фактором продуктивності команд [1]. Традиційні текстові процесори, що не підтримують одночасне редагування, створюють перешкоди для комунікації та призводять до виникнення конфліктів версій. Це зумовлює високий попит на платформи, що забезпечують безшовну взаємодію користувачів у реальному часі.

Існуючі ринкові лідери, такі як Google Docs та Notion, встановили високі стандарти для колаборативних платформ. Водночас, аналіз сучасних тенденцій у веб-розробці вказує на значний прогрес у технологіях реального часу (WebSockets, CRDTs) та розвиток серверних фреймворків, як-от Next.js 15 [2]. Ці інновації дозволяють створювати більш легкі, швидкі та гнучкі рішення, порівняно з монолітними пропрієтарними системами. Однак, залишається відкритою задача інтеграції повного спектра функцій – від розширеного форматування тексту до

управління організаційними просторами – у єдину систему, побудовану на найновішому стеку.

Метою дослідження є розробка інноваційного програмного застосунку, що надає користувачам інструменти для спільного редагування документів у реальному часі, використовуючи сучасні технології, включаючи Next.js 15, React, Tailwind CSS та Shadcn UI.

На основі сформульованої мети було розроблено концепцію та архітектуру системи. Основними характеристиками розробленого застосунку є:

- багатофункціональний текстовий редактор: Підтримка розширеного форматування тексту, створення таблиць, списків, контрольних списків (checklists), вбудовування посилань та завантаження зображень;

- спільна робота в реальному часі: Одночасне редагування документа кількома користувачами, відстеження курсорів, система коментарів та згадувань (@mentions) для миттєвої комунікації;

- управління версіями та контентом: Реалізовано історію змін з функціями скасування/повтору (Undo/Redo), копіювання та вставлення форматowanego тексту, а також підтримка шаблонів документів;

- організаційна структура: Система підтримує автентифікацію користувачів, створення профілів, організаційних робочих просторів та механізм запрошення нових членів до команди.

- додаткові можливості: Наявна система сповіщень, контроль полів документа (margins) та функції експорту у формати PDF, HTML, TXT та JSON;

- технологічна реалізація: Застосунок побудовано на фреймворку Next.js 15, що забезпечує високу продуктивність. Інтерфейс реалізовано з використанням Tailwind CSS та бібліотеки компонентів Shadcn UI, що гарантує повну адаптивність (Responsive Design). Розгортання системи здійснюється на платформі Vercel.

Для демонстрації взаємодії компонентів системи було розроблено діаграму потоків даних (DFD), що зображена на рисунку 1.

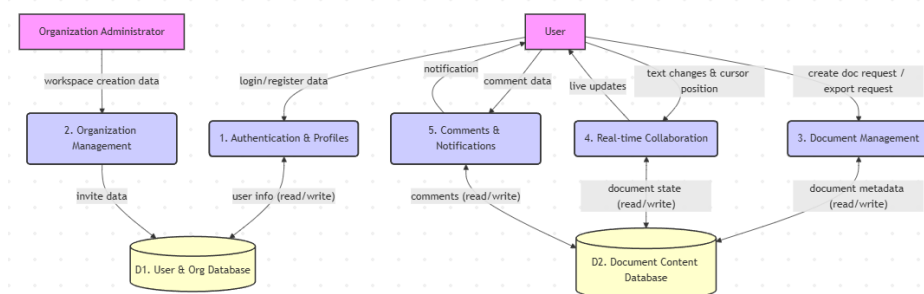


Рисунок 1 – DFD Діаграма

На діаграмі (рисунк 1) показано основні процеси: управління користувачами та організаціями, редагування документів та обмін даними в реальному часі, а також взаємодію цих процесів з базою даних. Для деталізації процесу спільного редагування було розроблено flowchart-діаграму (рисунк 2).

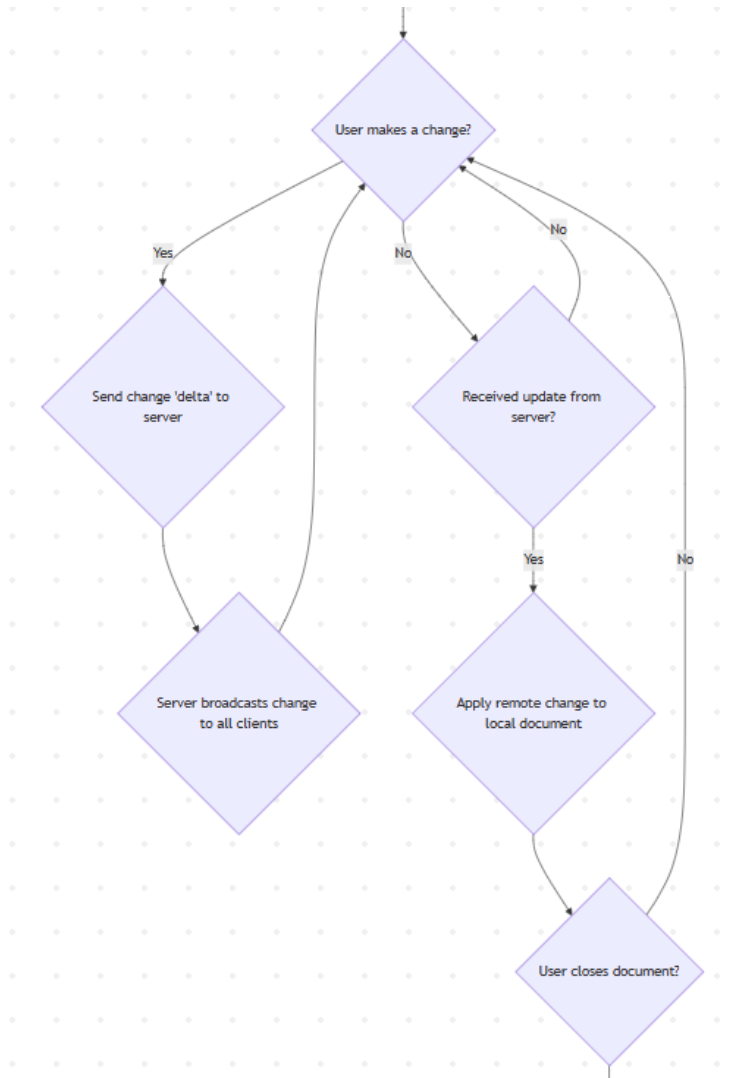


Рисунок 2 – Flowchart діаграма

Ця діаграма (рисунок 2) ілюструє алгоритм підключення користувача до сесії редагування, відправлення змін на сервер та синхронізацію стану документа з іншими учасниками.

В ході роботи було досліджено та розроблено програмний застосунок для спільної роботи з документами в реальному часі. Система демонструє високу ефективність використання фреймворку Next.js 15 для побудови складних, високоінтерактивних веб-платформ. Розроблене рішення має потенціал для впровадження в освітніх установах, малих та середніх бізнес-командах, що потребують гнучкого інструменту для документообігу.

Перспективи подальших досліджень включають інтеграцію інструментів на базі штучного інтелекту для генерації та рефакторингу тексту, розширення системи прав доступу на рівні окремих блоків документа та розробку мобільних клієнтів.

Перелік посилань

1. A Guide to the Project Management Body of Knowledge (PMBOK® Guide). Seventh Edition. USA: Project Management Institute, 2021. 250 p.
2. Next.js 15 Documentation / Vercel. – 2024. [URL]: <https://nextjs.org/docs>

УДК 004.4:378.1

Шиманська С.А., Мельников О.Ю.

Донбаська державна машинобудівна академія

ПОРІВНЯЛЬНИЙ АНАЛІЗ МАТЕМАТИЧНИХ МЕТОДІВ ДЛЯ РОЗРАХУНКУ ПЕРЕДБАЧЕННЯ ОБИРАННЯ ОСВІТНІХ ДИСЦИПЛІН ЗДОБУВАЧАМИ ОСВІТИ

Статтю присвячено порівняльному аналізу ефективності різних алгоритмів машинного навчання для прогнозування вибору дисциплін здобувачами вищої освіти. Дослідження ґрунтується на реальних даних студентів і порівнює результати восьми моделей. Встановлено, що розроблена нейромережа демонструє найвищу точність та стабільність. Результати доводять перевагу глибоких нейромереж для виявлення складних нелінійних залежностей у даних та їх придатність для впровадження в системах підтримки прийняття рішень в освіті.

The article is devoted to a comparative analysis of the effectiveness of various machine learning algorithms for predicting the choice of disciplines by higher education applicants. The study is based on real student data and compares the results of eight models. It has been established that the developed neural network demonstrates the highest accuracy and stability. The results prove the superiority of deep neural networks for identifying complex nonlinear dependencies in data and their suitability for implementation in decision support systems in education.

Сучасна вища освіта характеризується тенденцією до індивідуалізації навчальних траєкторій. Відповідно до Закону України «Про вищу освіту», обсяг дисциплін вільного вибору становить не менше 25% від загальної кількості кредитів ЄКТС [1]. Це створює виклик як для студентів, які стикаються зі складним вибором, що впливає на їхню майбутню кар'єру, так і для адміністрації закладів освіти, яка має оптимально формувати навчальне навантаження. Ефективний вибір дисциплін безпосередньо пов'язаний із задоволеністю студентів, їхньою успішністю та мотивацією, зниженням рівня відсіву та створенням продуктивного навчального середовища. Тому розробка інтелектуальних систем підтримки прийняття рішень, здатних прогнозувати оптимальний вибір дисциплін на основі індивідуальних характеристик здобувачів освіти, є актуальним науковим та практичним завданням [2].

Методи штучного інтелекту та машинного навчання дедалі частіше використовуються для прогнозування поведінкових рішень студентів. Ahmad & Kardan [3] та Sun et al. [4] доводять тісний зв'язок між вибором курсу та задоволеністю студентів, що є ключовим фактором ефективності навчального процесу.

У сфері застосування штучного інтелекту в освіті відзначається значний потенціал нейронних мереж. Дослідження показують, що нейромережі здатні розпізнавати та діагностувати навчальні здібності, а також враховувати інтереси та вподобання студентів.[5] Крім того, науковці підкреслюють, що рівень засвоєння нових знань безпосередньо залежить від базового рівня підготовки, що робить академічну успішність важливим прогностичним фактором [6].

Ефективність нейронних мереж в аналізі навчальних даних знаходить підтвердження в останніх дослідженнях. Ця технологія розвивається в рамках концепції систем підтримки прийняття рішень (DSS), які, як зазначається в науковій літературі [4][7], покликані розширювати можливості спеціалістів.

Попри наявні дослідження, залишається недостатньо вивченим питання порівняльної ефективності різних математичних методів та алгоритмів машинного навчання саме для задачі прогнозування вибору дисциплін в умовах обмеженого обсягу даних, характерного для окремих факультетів чи спеціальностей.

Метою даного дослідження є порівняльний аналіз ефективності різних математичних методів та алгоритмів машинного навчання, зокрема глибокої нейромережі, для прогнозування вибору дисциплін здобувачами вищої освіти, та визначення найбільш адекватної моделі для впровадження як ядро системи підтримки прийняття рішень.

Для аналізу використано дані про академічну успішність студентів факультету автоматизації машинобудування та інформаційних технологій Донбаської Державної Машинобудівної Академії. Вхідними ознаками моделей були: стать студента, середній бал з технічних дисциплін, середній бал з гуманітарних дисциплін та середній бал зі спортивних дисциплін. Цільовою змінною був вибір однієї з п'яти дисциплін вільного вибору. Була створена багатошарова нейронна мережа (4–64–32–5) – модель глибокого навчання з функціями активації ReLU і Softmax. Навчання моделей здійснювалось у середовищі Python із використанням бібліотек TensorFlow, Keras, Scikit-learn, Pandas і NumPy.

Було реалізовано і порівняння із сімома моделями (рис. 1):

1. Логістична регресія [8] – базовий статистичний метод, що визначає зв'язок між ознаками та ймовірністю вибору певної дисципліни. Вона працює швидко, але погано враховує складні, нелінійні взаємозв'язки між параметрами. У нашому дослідженні цей метод показав середню точність близько 57%, що свідчить про обмеженість моделі для подібних завдань.

2. Метод опорних векторів [9] – один із найточніших алгоритмів для задач класифікації, здатний працювати з невеликими наборами даних. Його перевагою є вміння будувати оптимальну межу розділення між класами. У нашому випадку точність прогнозування склала близько 71%, що є хорошим результатом, але нижчим, ніж у нейромережі.

3. Випадковий ліс [10] – ансамблевий метод, що поєднує багато «дерев рішень» для покращення точності. Він добре справляється з великими наборами

даних, але схильний до втрати узагальнюючої здатності при невеликій кількості прикладів. У дослідженні точність цього алгоритму склала приблизно 43%.

4. Градієнтний бустинг [11] – більш складна ансамблева техніка, яка послідовно вдосконалює попередні моделі. Проте через невеликий обсяг навчальних даних у нашій вибірці він не показав високої ефективності — близько 29% точності.

5. Метод k-найближчих сусідів [12] – простий і зрозумілий підхід, який класифікує новий приклад, орієнтуючись на найбільш подібних студентів у базі даних. Попри інтуїтивність, метод показав лише 57% точності, бо він чутливий до вибору параметрів і розподілу даних.

6. Наївний баєсівський класифікатор [13] – дуже швидкий, але спрощений алгоритм, що припускає незалежність усіх ознак. Через це він не зміг адекватно врахувати складні зв'язки між оцінками та інтересами студентів, показавши найнижчу точність — 14%.

7. Дерево рішень [14] – метод, що будує логічні правила для передбачення результату. Хоча модель зрозуміла для користувача, вона легко перенавчається. У нашому випадку точність становила близько 28%.

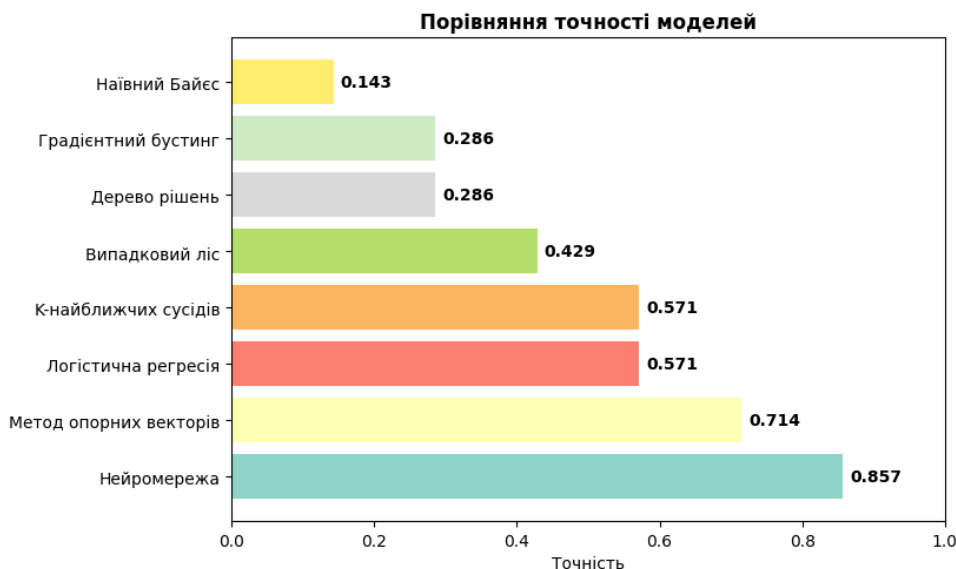


Рисунок 1 – Порівняння передбачень моделей

Створена нейромережа продемонструвала точність 85,7%, що значно перевищує результати інших алгоритмів.

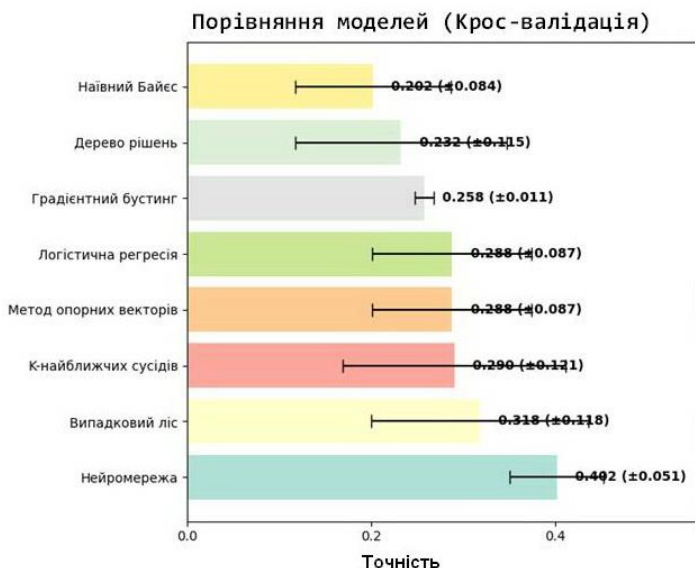


Рисунок 2 – Порівняння стійкості моделей за допомогою крос-валідації (середня точність $\pm$ стандартне відхилення)

Для перевірки стійкості та узагальнюючої здатності моделей було застосовано 3-фолдову крос-валідацію [15]. Результати підтвердили стабільність нейромережі та здатність до узагальнення (рис. 2). Нейромережа показала найвищий середній показник точності (0.492) та найменший розкид результатів (± 0.051) серед усіх протестованих моделей. Це свідчить про здатність моделі виявляти складні нелінійні залежності між характеристиками студентів і їх освітніми уподобаннями.

Важливо зауважити, що абсолютні значення точності при крос-валідації нижче через обмежений обсяг даних та строгішу процедуру оцінки, проте відносне положення моделей збереглося. Перевага нейромережі пояснюється її здатністю виявляти складні нелінійні залежності між вхідними ознаками та цільовим вибором, які є менш доступними для лінійних методів (Логістична регресія, Метод опорних векторів) та менш потужних нелінійних методів (дерева рішень). Низька результативність ансамблевих методів (Випадковий ліс, Градієнтний бустинг) може бути пов'язана з недостатнім для їх ефективного навчання обсягом даних.

Проведений порівняльний аналіз показав, що для задачі прогнозування вибору навчальних дисциплін найбільш ефективним є використання глибокої нейронної мережі, яка забезпечує високу точність та стійкість до зміни даних. Класичні статистичні методи можуть бути застосовані для початкової оцінки тенденцій, але не здатні повною мірою враховувати нелінійні взаємозв'язки між параметрами.

Розроблена модель може бути інтегрована в систему підтримки прийняття рішень у закладах освіти, що сприятиме підвищенню персоналізації навчання. Перспективи подальших досліджень полягають у розширенні набору характеристик студентів (мотивація, кар'єрні орієнтири, активність у навчальному середовищі) та тестуванні інших архітектур нейронних мереж.

Перелік посилань

1. Закон України «Про вищу освіту» № 1556-VII від 01.07.2014 року URL: <https://zakon.rada.gov.ua/laws/show/1556-18> (Дата звернення 22.10.2025)
2. Наливайко О. О. Перспективи використання нейромереж у вищій освіті України. Інформаційні технології і засоби навчання. 2023. Том 97. №5, 2–3 с. URL: www.researchgate.net/publication/375670837 (Дата звернення 22.10.2025)
3. Sun P.C., Tsai R.J., Finger G., Chen Y.Y. and Yeh D., What drives a successful e-Learning? An empirical investigation of the critical factors influencing learner satisfaction. Computers & Education. 50 (4) (2008), 1183–1202 с. URL: <https://doi.org/10.1016/j.compedu.2006.11.007> (Дата звернення 22.10.2025)
4. Ahmad A. Kardan, Hamid Sadeghi, A Decision Support System for Course Offering in Online Higher Education Institutes. International Journal of Computational Intelligence Systems. Volume 6, 2013 - Issue 5, 929с. URL: <https://doi.org/10.1080/18756891.2013.808428> (Дата звернення 22.10.2025)
5. С. В. Буртовий, В. А. Чубенко, С. В. Василюк-Зайцева Використання нейромереж у розпізнаванні та діагностиці навчальних здібностей здобувачів освіти. Академічні візії. №29, 2024, 2–3 с. URL: <https://academy-vision.org/index.php/av/article/view/971/884> (Дата звернення 22.10.2025)
6. О. Ю. Мельников, В. Б. Гітіс, Дослідження впливу якості засвоєння попереднього матеріалу на успішність здобувачів освіти з окремої дисципліни. Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології. Харків: НТУ «ХПІ», 2022, № 2 (7), 70 с. URL: <https://doi.org/10.20998/2079-0023.2022.01.12> (Дата звернення 22.10.2025)
7. Turban E., Sharda R. and Delen D., Decision support and business intelligence systems. 9th Edition, New Jersey: Prentice Hall, (2010).
8. Fangfang Lee, What is logistic regression? URL: <https://www.ibm.com/think/topics/logistic-regression> (Дата звернення 22.10.2025)
9. Eda Kavlakoglu, What are support vector machines (SVMs)? URL: <https://www.ibm.com/think/topics/support-vector-machine> (Дата звернення 22.10.2025)
10. Niklas Donges, Random Forest: A Complete Guide for Machine Learning. URL: <https://builtin.com/data-science/random-forest-algorithm> (Дата звернення 22.10.2025)
11. Bryan Clark, Fangfang Lee, What is Gradient Boosting? URL: <https://www.ibm.com/think/topics/gradient-boosting> (Дата звернення 22.10.2025)
12. Eda Kavlakoglu, What is the k-nearest neighbors (KNN) algorithm? URL: <https://www.ibm.com/think/topics/knn> (Дата звернення 22.10.2025)
13. Eda Kavlakoglu, What are Naïve Bayes classifiers? URL: <https://www.ibm.com/think/topics/naive-bayes> (Дата звернення 22.10.2025)
14. Eda Kavlakoglu, What is a decision tree? URL: <https://www.ibm.com/think/topics/decision-trees> (Дата звернення 22.10.2025)
15. Jason Brownlee, A Gentle Introduction to k-fold Cross-Validation URL: <https://machinelearningmastery.com/k-fold-cross-validation> (Дата звернення 22.10.2025)

УДК 004.8

Шимко А.С., Зваричук М.Д., Собко О.В.

Хмельницький національний університет

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ МЕТОДУ ВИЯВЛЕННЯ СТРЕСУ НА ОСНОВІ АНАЛІЗУ ВІЗУАЛЬНИХ ХАРАКТЕРИСТИК ОБЛИЧЧЯ ЗА ФОТО НЕЙРОМЕРЕЖЕВИМИ ЗАСОБАМИ

У даному дослідженні розглянуто проблему автоматизованого виявлення стресу за фотозображенням обличчя як актуальну задачу комп'ютерного зору та штучного інтелекту. Запропоновано підхід на основі глибоких нейронних мереж із використанням архітектури MobileNetV2, адаптованої до бінарної класифікації станів «стрес» та «без стресу». Проведено попередню обробку та аугментацію зображень із Stress Faces Dataset, що забезпечило покращене узагальнення моделі. Розроблено інтелектуальну систему з модульною архітектурою для інтеграції у веб- та мобільні платформи, яка здійснює повний цикл аналізу: завантаження фото, обробку, прогнозування та візуалізацію результатів. Експериментальні дослідження підтвердили високу точність класифікації на рівні 86 %, що перевищує показники існуючих методів. Результати демонструють ефективність підходу для неінвазивної оцінки психоемоційного стану, відкриваючи перспективи застосування у психологічній підтримці, дистанційній медицині, освітній аналітиці та системах безпеки.

This study considers the problem of automated stress detection from facial images as a relevant task of computer vision and artificial intelligence. An approach based on deep neural networks using the MobileNetV2 architecture, adapted to the binary classification of “stress” and “non-stress” states, is proposed. Pre-processing and augmentation of images from the Stress Faces Dataset were performed, which provided improved generalization of the model. An intelligent system with a modular architecture for integration into web and mobile platforms was developed, which performs a full cycle of analysis: photo loading, processing, prediction and visualization of results. Experimental studies confirmed high classification accuracy at 86%, which exceeds the performance of existing methods. The results demonstrate the effectiveness of the approach for non-invasive assessment of psycho-emotional state, opening up prospects for application in psychological support, remote medicine, educational analytics and security systems.

Стрес розглядається як універсальна фізіологічна й психологічна реакція організму на вимоги, що перевищують можливості адаптації [1, 2]. Він супроводжується активацією симпатичної нервової системи, змінами серцевого ритму, дихання, тону м'язів і впливає на роботу мозкових структур, зокрема амігдали, що відповідає за емоційну регуляцію [3]. Тривалий стрес підвищує ризик розвитку тривожних і депресивних розладів, порушень сну та соматичних проявів.

Важливими зовнішніми маркерами стресу є мімічні зміни: напруження щелепи, розширені зіниці, підняття брів, неприродна посмішка чи відкритий рот. Ці мікровирази пов'язані з гормональними реакціями та механізмом швидкої

мобілізації «бийся або тікай». Вони можуть бути використані як індикатори раннього виявлення надмірного психоемоційного навантаження [4].

В українському суспільстві рівень стресу значно зріс під впливом війни, економічної нестабільності та соціальних трансформацій. Дослідження показують, що основні джерела знервованості пов'язані з воєнними подіями, фінансовими труднощами, здоров'ям і безробіттям, а молодь частіше реагує на професійні та особисті проблеми.

За умов високого психологічного навантаження зростає потреба в об'єктивних і доступних інструментах діагностики. Використання комп'ютерного аналізу мімічних характеристик дає змогу автоматизувати процес виявлення стресу та зменшити залежність від суб'єктивних оцінок, що є важливим для збереження психічного здоров'я та своєчасного реагування на ризики [5]. Актуальність дослідження автоматизованого виявлення стресу за фотозображенням обличчя визначається поєднанням кількох чинників, серед яких зростання психоемоційного навантаження у сучасному суспільстві [6, 7], потреба у неінвазивних інструментах первинної оцінки психологічного стану [8] та активний розвиток інтелектуальних систем підтримки здоров'я [9]. Традиційні методи діагностики стресу – анкетні опитування, психофізіологічні вимірювання або клінічні інтерв'ю – часто потребують участі фахівця, значних ресурсних витрат або спеціального обладнання. На цьому тлі методи комп'ютерного зору [10], зокрема глибинні згорткові нейронні мережі [11], відкривають можливість автоматизованого аналізу мікроознаків, які людина не здатна надійно оцінити без допоміжних інструментів: легких мікровиразів, змін тонуся шкіри, ступеня напруження м'язів, асиметрії погляду чи деформацій у зонах, пов'язаних із мімікою. Поширення смартфонів і камер високої якості робить інструменти візуальної діагностики доступними, що підсилює суспільний інтерес до розробки точних та етичних алгоритмів аналізу обличчя.

Сучасні CNN-моделі демонструють високу ефективність у виокремленні релевантних ознак із зображень [12], що робить їх природним інструментом для задачі виявлення емоційних та психофізіологічних станів [13]. Використання згорткових шарів дозволяє моделі фіксувати як низькорівневі текстурні характеристики – мікровізерунки шкіри, локальні напруження в м'язах навколо очей та рота – так і високорівневі композиційні патерни, пов'язані з глобальною структурою міміки. Це особливо важливо у контексті виявлення стресу, оскільки він рідко проявляється у формі яскраво виражених емоцій, натомість характеризується сукупністю тонких, мультифакторних ознак. Глибинні мережі здатні навчатися на цих складних комбінаціях ознак, що суттєво підвищує точність класифікації порівняно з класичними методами або ручними дескрипторами [14].

У рамках розглянутого дослідження застосування архітектури MobileNetV2 є обґрунтованим рішенням, оскільки такі моделі мають невелику кількість параметрів і оптимізовані для роботи на мобільних та веб-платформах. Це створює передумови для розробки систем реального часу, здатних здійснювати аналіз без необхідності передачі зображень на сервери високої потужності, що важливо як для

продуктивності, так і для захисту персональних даних. Мобільні CNN-моделі також добре піддаються донавчанню на спеціалізованих наборах даних, таких як Stress Faces Dataset, що дозволяє адаптувати фільтри згортки до характерних особливостей облич у стані стресу [15]. Використання аугментацій у цьому процесі сприяє підвищенню стійкості мережі до варіацій умов зйомки, освітлення, ракурсу та природної різноманітності облич, що наближає модель до умов реального використання [16].

Важливою перевагою CNN підходів є можливість інтерпретації результатів за допомогою теплових карт, таких як Grad-CAM, що підвищує довіру користувачів та експертів до системи. Візуалізація зон, що найбільше вплинули на прогноз, надає додатковий аналітичний інструмент для дослідження фізіологічних проявів стресу, формування більш збалансованих вибірок та покращення дизайну моделей. Це також дає змогу виявляти потенційні упередження в навчальних даних і здійснювати їхню корекцію.

Загалом, використання методів комп'ютерного зору та згорткових нейронних мереж у задачі виявлення стресу створює широкі можливості для впровадження інтелектуальних сервісів у галузі психологічного добробуту [17], телемедицини, моніторингу ризикових груп, освітньої аналітики та корпоративних систем охорони праці. Високі показники точності та узагальнювальної здатності, продемонстровані в експериментальних дослідженнях, свідчать про потенціал побудови масштабованих, економічно доступних та етично вивірених рішень, здатних забезпечити неінвазивний аналіз стану людини на основі повсякденних цифрових зображень [18]. Такий підхід розширює можливості сучасних систем підтримки здоров'я та демонструє перспективність подальшого розвитку CNN-архітектур у напрямку афективних обчислень та оцінки психоемоційних станів.

Метою роботи є підвищення ефективності процесу виявлення стресу на основі аналізу візуальних характеристик обличчя за фотозображенням нейромережевими засобами.

Для розпізнавання стресових станів передбачається застосування нейромережі, налаштованої для бінарної класифікації. Модель донавчається на вибірці, що містить два типи зображень обличчя — із проявами стресу та без них. Після навчання система визначає приналежність нового зображення до одного з класів, формуючи висновок про наявність чи відсутність стресових ознак. Такий підхід забезпечує більш точне та швидке виявлення стресу за візуальними параметрами обличчя.

Запропоновано метод, який передбачає три послідовні стадії: підготовку вхідного зображення, класифікацію за допомогою нейромережі та інтерпретацію отриманого прогнозу (рисунок 1). На вхід подається попередньо навчена модель бінарної класифікації та зображення обличчя, що підлягає аналізу. На першому етапі зображення приводиться до формату, сумісного з вимогами моделі глибокого навчання.



Рисунок 1 – Метод виявлення стресу на основі аналізу візуальних характеристик обличчя за фотозображенням

Далі відбувається основний етап – класифікація. Нейромережа порівнює візуальні риси обличчя з шаблонами, засвоєними під час навчання, і визначає ймовірність належності до класів «стрес» або «без стресу». Такий аналіз дає можливість оцінити емоційний стан людини за єдиним фотознімком.

На завершальному етапі здійснюється узагальнення результатів. Висновок формується на основі рівня впевненості моделі у належності зображення до кожного з двох класів. Якщо ймовірність «стресу» перевищує встановлений поріг у 60%, зображення класифікується як таке, що демонструє стресові ознаки. У результаті система повертає рівні впевненості моделі та підсумковий висновок щодо наявності стресу.

Процес отримання нейромережевої моделі на основі архітектури MobileNetV2 для бінарної класифікації стресу представлено у вигляді послідовної схеми навчання (рисунок 2).

Запропонована структура відображає ключові етапи формування моделі, здатної визначати стресові стани за фотозображенням обличчя, і охоплює підготовку даних, навчання та подальшу оцінку ефективності.

На вхід подається набір зображень обличчя, що містить приклади двох класів «стрес» і «без стресу», а також обрана архітектура моделі MobileNetV2,

адаптована до завдання бінарної класифікації. Перший етап включає попередню обробку датасету: всі зображення приводяться до єдиного розміру, нормалізуються та доповнюються методами аугментації. Динамічна генерація модифікованих варіантів зображень у процесі тренування (обертання, масштабування, зсуви, дзеркальне відображення) підвищує стійкість моделі до варіацій даних і запобігає перенавчанню, що є критично важливим у випадку обмеженого набору унікальних прикладів.

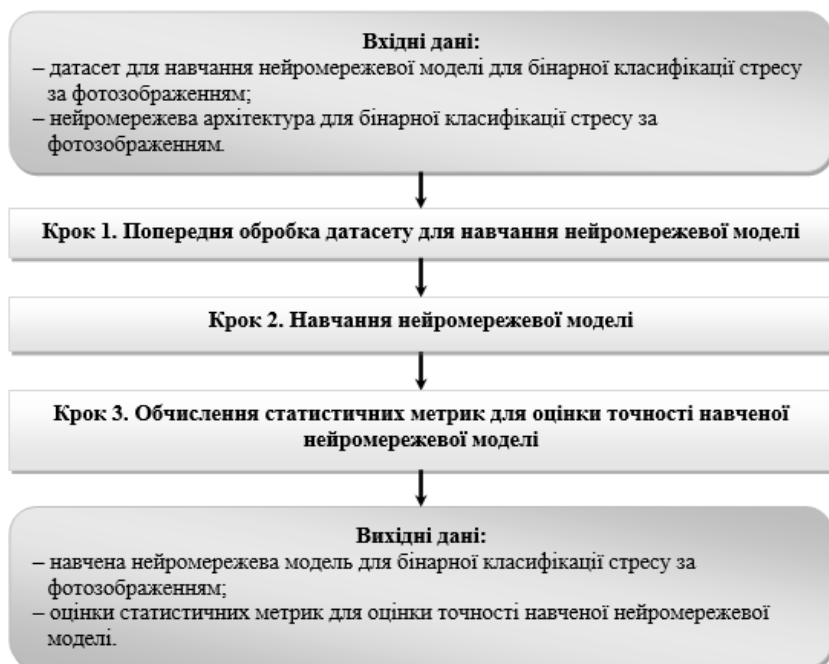


Рисунок 2 – Метод виявлення стресу на основі аналізу візуальних характеристик обличчя за фотозображенням

Після підготовки даних виконується навчання архітектури MobileNetV2. На цьому етапі оптимізуються параметри моделі, що дозволяє їй розпізнавати характерні візуальні ознаки, пов'язані зі стресовими станами, та співвідносити їх з відповідним класом. Формування внутрішніх представлень відбувається на основі аналізу варіативності мімічних особливостей, які модель отримує з тренувального набору.

Завершальною стадією є оцінювання якості навченої нейромережі за допомогою метрик точності, повноти та F_1 -міри. Ці показники дозволяють визначити, наскільки модель коректно розпізнає обидва класи та чи здатна вона

узагальнювати інформацію на нових даних. На виході формується готова до практичного застосування нейромережева модель, що здатна класифікувати зображення обличчя за наявністю або відсутністю ознак стресу.

Для навчання моделі було залучено датасет «Stress Faces Dataset», підготовлений Janith Ukwattage та розміщений на платформі Kaggle. Він орієнтований на бінарну класифікацію станів «stress» і «nostress» та має структуровану організацію у вигляді директорій train і test, кожна з яких містить окремі каталоги для двох класів. Представлені у вибірці зображення відрізняються за якістю та роздільною здатністю, оскільки походять з різних джерел – переважно фотографій і відеокадрів, що забезпечує природну варіативність даних і сприяє підвищенню стійкості моделі до зовнішніх змін.

У тренувальній частині міститься 4 830 зображень класу stress та 4 965 – класу poststress, а тестова вибірка включає відповідно 1 247 і 1 233 зразки. Загальний обсяг даних становить 12 275 прикладів, причому співвідношення між класами є практично симетричним, що забезпечує збалансованість навчального процесу.

Оцінювання точності моделі становить невід'ємний етап її валідації, оскільки дає змогу встановити не лише загальний рівень ефективності, а й виявити специфічні характеристики розподілу помилок. Матриця помилок слугує інструментом структурованого подання результатів класифікації, демонструючи кількість коректних і хибних рішень для кожного класу. Її інтерпретація дає змогу окреслити домінантні типи хибних передбачень та визначити напрями подальшого вдосконалення моделі.

Точність як частка коректних рішень забезпечує загальну характеристику продуктивності. Показник влучності відображає здатність моделі мінімізувати хибнопозитивні рішення та підвищує надійність ідентифікації класу. Показник повноти характеризує спроможність моделі виявляти максимум релевантних зразків, що особливо важливо у задачах, де пропуск цільових об'єктів є критичним. Гармонізоване співвідношення цих двох характеристик задається F1-мірою, яка формує узагальнену оцінку для збалансованого аналізу помилок обох типів.

Узагальнені середні значення метрик, зокрема macro та weighted average, забезпечують цілісну інтерпретацію якості моделі: перше усуває вплив дисбалансу класів, тоді як друге відображає реальну структуру вибірки.

Динаміка функції втрат і точності, відтворена на кривих навчання, дає змогу візуалізувати процес формування параметрів моделі, виявити ознаки перенавчання або недостатнього навчання та своєчасно скоригувати конфігурацію гіперпараметрів. Аналіз цих показників формує підґрунтя для комплексного експериментального підтвердження ефективності моделі та оцінки її здатності до узагальнення.

Розроблена система виявлення стресу складається з інтегрованих модулів, що забезпечують повний цикл обробки зображення – від його подачі до класифікації та формування висновку про результати (рисунк 3).



Рисунок 3 – Розроблена система

Для оцінки точності навченої нейромережі використовувалися статистичні метрики, описані вище, метою яких було визначити здатність моделі коректно класифікувати нові, раніше невідомі зображення за двома класами: «стрес» та «відсутність стресу». Було проведено експериментальне дослідження впливу кількості епох і розміру batch на продуктивність моделі, результати якого наведено в таблиці 1.

Таблиця 1 – Точність класифікації залежно від кількості епох та batch-size

Епохи	batch-size	Accuracy, %
15	16	68
15	32	65
20	16	75
20	32	72
30	16	86
30	32	84
35	16	78
35	32	72

Згідно з даними таблиці 1, точність класифікації підвищується зі збільшенням кількості епох, досягаючи 86% при 30 епохах і batch-size = 16. Збільшення розміру batch до 32 знижує точність на всіх рівнях епох, що свідчить про ефективніше навчання при менших batch. Водночас, перевищення 35 епох призводить до ознак перенавчання моделі. Під час навчання будувалися графіки

динаміки точності та функції втрат на кожній епосі, що дозволяло оцінити стабільність навчання та своєчасно виявити потенційне перенавчання. Результуючі криві точності та втрат наведено на рисунку 4.

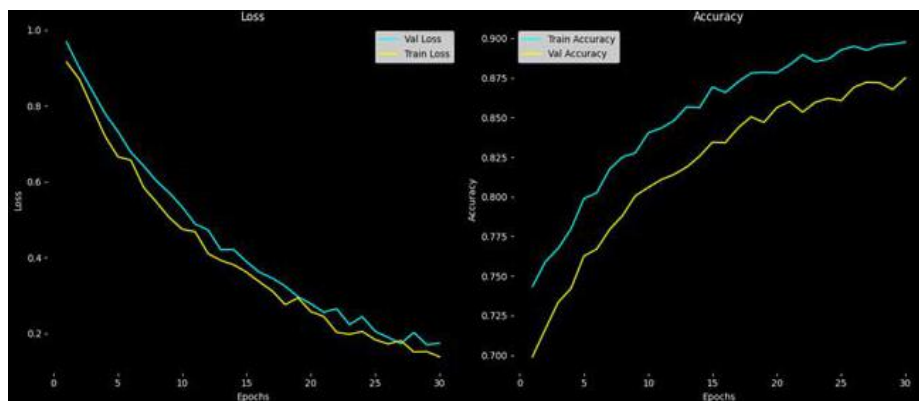


Рисунок 4 – Графіки точності та втрат

На графіку відображено зміну функції втрат і точності протягом 30 епох навчання. Результати демонструють стабільну роботу моделі: тренувальна точність перевищує 90 %, а валідаційна досягає 86 %, що свідчить про відсутність перенавчання. Функція втрат поступово зменшується для обох наборів даних, підтверджуючи покращення узгодженості моделі.

Для детальнішого аналізу ефективності класифікації було використано матрицю помилок, яка відображає відповідність між реальними та передбаченими класами (рисунком 5).

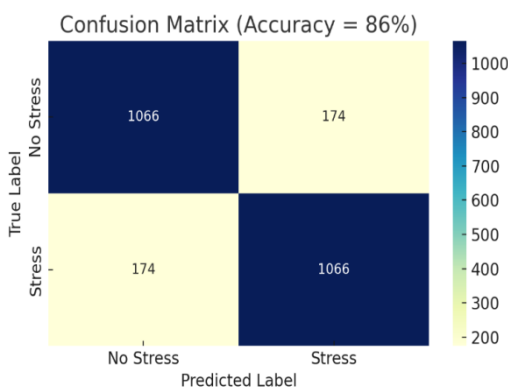


Рисунок 5 – Матриця сплутувань

Для детальної оцінки точності моделі застосовано метрики влучності, повноти та F_1 -міри (рисунок 6). Отримані результати демонструють, що модель ефективно класифікує зображення за ознаками стресу та їх відсутністю. Значення влучності і повноти на рівні 86 % свідчать про збалансовану продуктивність для обох класів.

F_1 -міра, також становлячи 86 %, підтверджує узгодженість між влучністю та повнотою. Таким чином, навчена модель MobileNetV2 досягає точності 86 % на валідаційній вибірці для задачі класифікації «стрес» та «без стресу».

Розробка та дослідження нейромережевої моделі на основі архітектури MobileNetV2 для виявлення стресових станів за фотозображеннями обличчя показали високу ефективність запропонованого підходу та обґрунтованість використання методів глибокого навчання у задачах автоматизованого визначення емоційного стану людини. Проведений аналіз включав послідовну обробку вхідних даних, початкову підготовку та аугментацію датасету, навчання моделі з оптимізацією параметрів нейронної мережі, а також оцінку результатів за допомогою комплексного набору статистичних метрик, що включав точність, влучність, повноту, F_1 -міру, а також візуалізацію процесу навчання через криві втрат і точності.

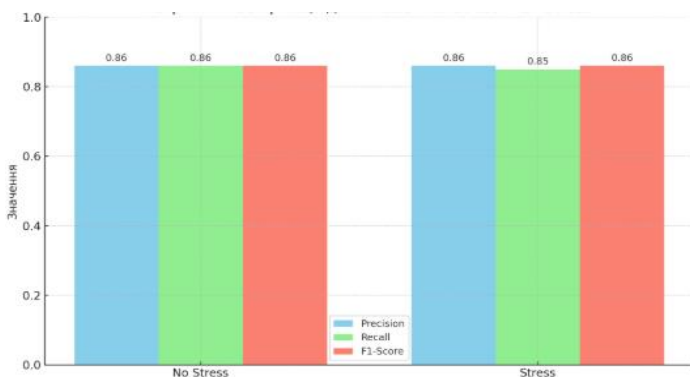


Рисунок 6 – Метрики влучності, повноти та F_1 -міри моделі

Експериментальні дослідження продемонстрували, що модель здатна узагальнювати знання на нових, раніше невідомих зображеннях, забезпечуючи точність класифікації на рівні 86 % при оптимальних параметрах навчання. Високі показники влучності та повноти для обох класів підтверджують збалансовану продуктивність, а узгодженість цих характеристик, зафіксована через F_1 -міру, свідчить про ефективність та стабільність роботи нейромережі. Аналіз матриці помилок дозволив виявити мінімальні дисбаланси в класифікації та підтвердив

переваги запропонованого підходу для розпізнавання як наявності, так і відсутності ознак стресу на обличчі.

Завдяки використанню аугментації даних та належного попереднього опрацювання зображень, модель виявила високу стійкість до різних варіацій фотозображень, що включали зміни роздільної здатності, ракурсів, освітлення та інших умов зйомки. Це забезпечує її практичну придатність для використання у реальних умовах, де вхідні дані можуть мати високу мінливість і нерівномірність.

Отримані результати свідчать про те, що застосування нейромережових методів для виявлення стресу за фотозображеннями є доцільним та ефективним. Запропонований підхід дозволяє автоматизувати процес оцінки емоційного стану людини, знижує суб'єктивність традиційних методів спостереження та дає змогу швидко реагувати на прояви стресу, що має важливе значення для профілактики психічного перенавантаження, покращення психологічного комфорту та підвищення продуктивності в різних сферах діяльності.

Таким чином, розроблена інтелектуальна система може виступати надійним інструментом для ранньої діагностики стресових станів, сприяє вдосконаленню існуючих методів моніторингу психоемоційного стану та відкриває перспективи для подальшого впровадження штучного інтелекту у психологічну практику, охорону здоров'я та соціальні дослідження. Отримані результати підкреслюють значущість поєднання нейромережових технологій і аналізу візуальних характеристик обличчя для створення ефективних і доступних рішень у сфері емоційної діагностики та моніторингу стресу.

Перелік посилань

1. Altered Functional Connectivity of the Default Mode Network in Patients with Uncontrolled Hypertension / J. Zhou et al. Brain Sciences. 2023. Vol. 13, no. 2. P. 310.
2. ПТСР: все, що необхідно знати - причини, симптоми та лікування. ГМКА. 2023. URL: <https://gmka.org/uk/articles/ptsr-vse-shho-neobhidno-znaty-prychyny-symptomy-ta-likuvannya/>
3. Physiological Responses to Stress. EBSCO. URL: <https://www.ebsco.com/research-starters/health-and-medicine/physiological-responses-stress>
4. García Q., Barbas A., Lázaro M. Neuroinflammation and neurodegeneration: A two-way road. Nature Reviews Neuroscience. 2010. Vol. 11, no. 3. P. 259–262.
5. Smith J., Jones M. The effects of X on Y: A comprehensive study. Journal of Research. 2006. Vol. 34, no. 2. P. 123–130.
6. Mazurets O., Vit R. Practical Application of Method of Thematic Classification of Text Information Using LDA. Information Technology and Implementation (Satellite). Proceedings 11th International Conference. November 21, 2024. Kyiv, Ukraine. 2024. Pp. 151-152.
7. Віт Р.В., Мазурець О.В. Тематична класифікація текстової інформації засобами обробки природної мови. Збірник наукових праць XXIII Міжнародної наукової конференції «Нейромережні технології та їх застосування НМТіЗ-2024». 11-12 грудня 2024. Краматорськ-Тернопіль, ДДМА. 2024. с. 63-66.
8. Овчарук О.М., Мазурець О.В. Нейромережеве діагностування проявів ПТСР у текстовому контенті з використанням помилко-орієнтованого навчального набору даних. Науковий

- журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2024. №6, Т.1 (343). С. 195-200.
9. Крак Ю.В., Дідур В.О., Молчанова М.О., Мазурець О.В., Собко О.В., Залуцька О.О., Бармак О.В. Метод виявлення політичної пропаганди в інтернет-контенті нейромережевими засобами обробки природної мови. Науковий журнал «Проблеми програмування». Київ, 2024, №2-3. с. 288-295.
10. Овчарук О.М., Мазурець О.В. Нейромережева архітектура з квантовим шаром для аналізу текстових повідомлень на прояви посттравматичного стресового розладу. Науковий журнал «Наука і техніка сьогодні». Київ, 2024. №13 (41). С. 1192-1204.
11. Мазурець О.В., Тимофіїв І.А., Кліменко В.І., Тищенко О.О. Метод виявлення депресивного стану пов'язаного із навчанням у закладах освіти із використанням нейромережі дуальної архітектури. Науковий журнал «Вісник Херсонського національного технічного університету». 2024. №4 (91). С. 311-318.
12. Біт Р.В., Мазурець О.В. Підхід до тематичної класифікації текстової інформації засобами обробки природної мови. Науковий журнал «Наукові праці Донецького національного технічного університету», серія «Проблеми моделювання та автоматизації проектування». 2025. №1 (21). С. 94-99.
13. Овчарук О.М., Мазурець О.В. Нейромережевий метод діагностування психологічних розладів за аналізом повідомлень на основі роздільного підходу до класифікації. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». № 1, 2025. с. 210-216.
14. Murava V., Zalutska O., Didur V., Mazurets O. Software architecture of information system for exchanging LLM thematic prompts. Global Trends in the Development of Information Technology and Science. Proceedings IV International Scientific and Practical Conference. June 25-27, 2025. Stockholm, Sweden. Pp. 121-127.
15. Юрченко Д.Ю., Овчарук О.М., Мазурець О.В., Шевчук П.О. Метод використання нейромережі гібридної архітектури для визначення емоційної тональності текстових повідомлень. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». № 2, 2025. с. 136-141.
16. Мазурець О.В., Козенко О.В., Собко О.В. Метод автоматизованого підбору відповідей на користувацькі запитання за семантичною подібністю. Матеріали XII Всеукраїнської науково-практичної конференції «Глушковські читання». Київ – 2023. с. 106-109.
17. Shevchuk P., Molchanova M., Mazurets O. Software for Text Messages Reliability Analysis Based on the Machine Learning Models Ensemble. Proceedings of IV International Scientific and Practical Conference «Innovative research and perspectives of the development of science and technology». January 29-31, 2024. Stockholm, Sweden. 2024. Pp. 347-354.
18. Молчанова М.О., Мазурець О.В., Собко О.В., Біт Р.В., Назаров В.В. Алгоритм виявлення аб'юзивного вмісту в україномовному аудіоконтенті для імплементації в об'єктно-орієнтовану інформаційну систему. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2024. №1 (331). С. 101-106.
19. Mazurets O.V., Sobko O.V., Molchanova M.O., Zalutska O.O., Yurchak A.V. Practical Implementation of Neural Network Method for Stress Features Detection by Social Internet Networks Posts. Global Science: Prospects and Innovations. Proceedings of the II International Scientific and Theoretical Conference «Scientific Review of the Actual Events, Achievements and Problems». May 31, 2024. Berlin, Federal Republic of Germany: International Center of Scientific Research. 2024. Pp. 160-167.

УДК 004.4

Шуневич В.І., Павлова О.О.

Хмельницький національний університет

СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ ПЕРСОНАЛЬНИХ КОМП'ЮТЕРІВ

Розглянуто прикладні аспекти розвитку апаратного забезпечення персональних комп'ютерів, спрямовані на підвищення продуктивності, енергоефективності та багатозадачності систем. Запропоновані підходи дозволяють забезпечити оптимальне співвідношення швидкодії, надійності та вартості компонентів, що робить сучасні ПК більш доступними для широкого кола користувачів. Розроблені рішення сприяють зниженню енергоспоживання та тепловиділення, що підвищує стабільність роботи й продовжує термін служби обладнання.

Applied aspects of the development of personal computer hardware aimed at improving system performance, energy efficiency, and multitasking capabilities are considered. The proposed approaches ensure an optimal balance between speed, reliability, and cost of components, making modern PCs more accessible to a wide range of users. The developed solutions contribute to reducing power consumption and heat generation, increasing system stability and extending hardware lifespan.

Персональний комп'ютер в наш час є ключовим інструментом у сучасному світі, що використовується для роботи у різних сферах таких як навчання, розваги та наукові дослідження. Розвиток апаратного забезпечення визначає швидкість, надійність і функціональні можливості персонального комп'ютера. На сьогодні відбувається швидка еволюція процесорів та графічних прискорювачів, а також оперативної пам'яті та систем зберігання даних, якими забезпечується зростання продуктивності та одночасне зниження енергоспоживання [1]. Водночас розвиток ПК супроводжується проблемами такими як збільшення тепловиділення компонентів, зростанням енергоспоживання і підвищенням вартості сучасних рішень, що робить апгрейд системи дорожчим для середнього користувача.

Дослідження демонструють перехід до багатоядерних і багатопотокових архітектур процесорів (прикладом є Intel Core 14-го покоління [2], AMD Ryzen 7000 [3]), що дозволяє ефективно виконувати паралельні обчислення даних одночасно. Проблемаю при цьому залишається те, що не всі програми здатні ефективно використовувати багатоядерність, що обмежує потенційну продуктивність [1, 3]. У сфері відеоадаптерів зростає роль штучного інтелекту, що розширює застосування відеокарт не лише для ігор, а й для машинного навчання [1], але це призводить до зростання енергоспоживання і тепловиділення, що потребує складних систем охолодження. Оперативна пам'ять переходить на стандарт DDR5, який забезпечує вищу пропускну здатність та енергоефективність порівняно з DDR4 [4], але ціна

модулів DDR5 значно вища, що має великий вплив на бюджетність зборки ПК. Також активно впроваджуються твердотільні накопичувачі SSD з інтерфейсом NVMe, які дають значний приріст швидкості роботи системи [5], проте SSD швидше зношуються при інтенсивних навантаженнях, що може стати проблемою для серверних або робочих систем.

Усе ж ще на шляху розвитку залишаються проблеми з високим енергоспоживанням продуктивних компонентів, якими є процесор та графічний процесор [1]. Додатково важливими проблемами є зростання ціни на нові платформи (DDR5, PCIe 5.0), через складність модернізації та короткий життєвий цикл материнських плат є також поява нових уразливих систем безпеки, які знижують надійність роботи системи. Також не всі завдання можуть підтримувати масштабування на багатоядерних процесорах [1, 3], що накладає обмеження на ефективність використання ресурсів компонентів. Питання охолодження залишається критичним, адже збільшення потужності дає більший приріст температури та вимагає складніших і дорожчих систем відведення тепла.

Вивчення тенденцій розвитку апаратної частини забезпечення персонального комп'ютера є актуальним, оскільки дозволяє обирати оптимальні рішення для роботи комп'ютера, зменшувати витрати на його апгрейд і підвищувати ефективність використання ресурсів. Особливу актуальність мають питання енергоефективності, охолодження та доступності нових технологій для масових користувачів. Це дозволить розробляти системи, які не лише продуктивні, а й екологічні, економічні та безпечні у використанні.

Отже сучасний розвиток апаратного забезпечення персональних комп'ютерів спрямований на підвищення продуктивності, енергоефективності та багатозадачності. Основними тенденціями є збільшення кількості ядер у процесорах [2, 3], поширення твердотільних накопичувачів (SSD) [5], удосконалення технологій відеокарт [1] і впровадження швидшої оперативної пам'яті DDR5 [4].

Разом із цим існують проблеми, що потребують вирішення: високе тепловиділення, підвищена вартість компонентів, короткий життєвий цикл платформ і нові ризики безпеки. Подальші дослідження мають бути спрямовані на зниження тепловиділення компонентів, зменшення вартості нових рішень і розробку більш доступних технологій для масового користувача.

Перелік посилань

1. Hennessy, J. L., Patterson, D. A. Computer Architecture: A Quantitative Approach. 6th ed. Morgan Kaufmann, 2019.
2. Intel. 14th Gen Intel® Core™ Desktop Processors [Електронний ресурс]. – Режим доступу: <https://www.intel.com>
3. AMD. Ryzen 7000 Series Desktop Processors [Електронний ресурс]. – Режим доступу: <https://www.amd.com>
4. Kingston Technology. DDR5 Memory Overview [Електронний ресурс]. – Режим доступу: <https://www.kingston.com>
5. Western Digital. NVMe SSD Technology Brief [Електронний ресурс]. – Режим доступу: <https://www.westerndigital.com>.

УДК 004.8

Шурипа М.О., Мазурець О.В.

Хмельницький національний університет

НЕЙПРОМЕРЕЖЕВЕ КОРОТКОСТРОКОВЕ ПРОГНОЗУВАННЯ ТРАЄКТОРІЙ БПЛА У ВІДЕОПОТОЦІ НА ОСНОВІ ТРАНСФОРМЕРНОЇ АРХІТЕКТУРИ

Розглянуто задачу короткострокового прогнозування траєкторій малоформатних безпілотних літальних апаратів у потоках відеоспостереження. Досягнута продуктивність у сотні кадрів за секунду на CPU підтверджує придатність запропонованого рішення до використання в системах моніторингу повітряного простору реального часу на вбудованих платформах. Обговорено обмеження методу (двовимірне прогнозування, фіксована камера, детерміністичний характер передбачень) та окреслено напрями подальшого розвитку, зокрема врахування невизначеності та розширення до багатоагентних сцен.

The paper addresses the problem of short-term trajectory prediction for small unmanned aerial vehicles (UAVs) in video surveillance streams. The achieved throughput of several hundred frames per second on a CPU confirms the feasibility of deploying the proposed solution in real-time airspace monitoring systems on embedded or industrial platforms. The study discusses current limitations, including 2D image-coordinate prediction, assumption of a static camera, and deterministic outputs, and outlines future work directions such as uncertainty-aware modelling and extension towards multi-agent scenarios.

Розширення сфери застосування безпілотних літальних апаратів охоплює сьогодні цивільну, промислову та оборонну інфраструктуру: від моніторингу довкілля, інспекції енергетичних об'єктів і агровиробництва до логістики малих вантажів, пошуково-рятувальних операцій та підтримки військових місій [1, 2]. Разом із цим стрімко зростає потреба у засобах автоматизованого спостереження за повітряним простором, здатних не лише зафіксувати присутність БПЛА, а й оперативно оцінити їх подальшу траєкторію руху для підтримки рішень щодо супроводу, уникнення загроз або перехоплення [3].

Класичні засоби контролю повітряного простору – радіолокаційні станції та акустичні сенсори – виявляють обмежену ефективність щодо малогабаритних, малошумних або низькошвидкісних дронів, особливо у щільно забудованому середовищі, в умовах перешкод або за наявності складного рельєфу місцевості. Ці обмеження стимулюють перехід до відеоорієнтованих систем моніторингу, де ключову роль відіграють методи комп'ютерного зору та глибинні нейромережі. Вони дозволяють аналізувати відеопотік у режимі, близькому до реального часу, детектуючи цільові об'єкти та відстежуючи їх у часовій послідовності кадрів [4]. Зростання використання безпілотних літальних апаратів у цивільних і військових

сферах зумовлює потребу у високоточних системах моніторингу та прогнозування їхніх траєкторій у реальному часі. Актуальність задачі короткострокового прогнозування руху БПЛА у відеопотоці зумовлена необхідністю забезпечення безпеки повітряного простору, попередження зіткнень, підвищення ефективності систем протидії, а також удосконалення технологій автономної навігації. У цьому контексті методи комп'ютерного зору [5] та глибокого навчання [6], зокрема згорткові нейронні мережі (CNN) [7] та трансформерні архітектури [8], створюють фундамент для побудови високопродуктивних систем аналізу динамічних сцен.

CNN залишаються ключовими моделями для виявлення та відстеження об'єктів у відеопотоці завдяки своїй здатності вилучати просторові ознаки з високою точністю [9, 10]. У задачах аналізу руху це дозволяє визначати контури, орієнтацію та швидкість об'єкта на кожному кадрі [11]. Однак прогнозування траєкторії потребує не лише просторових [12], але й якісних часових залежностей [13]. У цьому аспекті трансформерні архітектури демонструють значні переваги [14], оскільки здатні моделювати довготривалі залежності у відеоряді та враховувати складні поведінкові патерни БПЛА, включаючи маневри, зміни швидкості чи реакцію на зовнішні стимули. Поєднання CNN як екстрактора ознак із трансформерами як предиктивним механізмом формує потужний гібридний підхід до аналізу відеоданих.

Перспективи розвитку цього напрямку пов'язані з інтеграцією мультимодальних джерел даних – оптичного відео, глибинних карт, тепловізійних сигналів та телеметрії – що дозволить формувати більш стійкі моделі прогнозування у складних умовах [15]. Ці технології формують основу для створення систем спостереження й автономної взаємодії, що здатні оперативно та надійно реагувати на поведінку БПЛА у режимі реального часу [16].

Однак для практичних задач безпеки та ситуаційної обізнаності простого відстеження координат БПЛА недостатньо. Оператору або автономній системі потрібна оцінка того, де саме дрон опиниться через найближчі секунди. Саме тому особливої актуальності набуває задача короткострокового прогнозування траєкторій у відеопотоці, яка поєднує просторовий аналіз поточного кадру з часовим моделюванням історії руху та має працювати в жорстких обмеженнях за затримкою і обчислювальними ресурсами.

У центрі роботи знаходиться задача побудови методу, який за даними відеоспостереження формує послідовність координат позицій БПЛА, а далі, спираючись на цю історію, генерує короткостроковий прогноз траєкторії у межах декількох десятків кадрів уперед. Об'єктом дослідження є рух малорозмірних дронів у складному фоновому середовищі, а предметом – нейромережіві моделі прогнозування траєкторій у координатному просторі відеозображення [17].

Мета полягає у розробленні методу короткострокового прогнозування траєкторій БПЛА у відеопотоці на базі модифікованої трансформерної архітектури з позиційним кодуванням, яка використовує історію руху у вигляді координатних часових рядів і враховує просторові обмеження сцени, забезпечуючи зменшення

середньої та фінальної похибки прогнозу порівняно зі статистичними моделями при збереженні придатності до інтеграції у системи реального часу.

Сучасні методи виявлення об'єктів у відео базуються переважно на згорткових нейронних мережах, які будують багаторівневі просторові ознаки і дозволяють одночасно виконувати локалізацію та класифікацію об'єктів. Найбільш поширені архітектури поділяють на одноетапні та двоетапні. Одноетапні детектори (типу YOLO або SSD) обробляють весь кадр за один прохід, забезпечуючи високу швидкодію, що критично для задач відеомоніторингу. Двоетапні моделі, зокрема Faster R-CNN, спершу формують регіони інтересу, а потім уточнюють їхню класифікацію, досягаючи більшої точності за рахунок додаткових ресурсів.

Для малоформатних повітряних об'єктів особлива увага приділяється адаптації детекторів до малих цілей: розширюються механізми багатомасштабного злиття ознак, удосконалюються FPN-блоки, застосовуються спеціалізовані модифікації YOLO, орієнтовані на дрібні об'єкти та шумний фон. На рівні трекінгу використовують як класичні фільтри Калмана та фільтри частинок, так і сучасні асоціативні трекери (DeepSORT, ByteTrack), що комбінують результати детекції з ідентифікаційними ознаками для підтримання сталої ідентичності об'єктів.

Проблема прогнозування траєкторій у часовій перспективі вирішується двома основними класами методів. Статистичні підходи будують модель динаміки руху (лінійну або кусочно-лінійну) і використовують фільтри типу Калмана чи IMM для екстраполяції майбутніх положень. Нейромережеві моделі натомість розглядають послідовність координат як часовий ряд і навчаються апроксимувати нелінійні патерни руху, зокрема за допомогою LSTM або трансформерів. У низці робіт продемонстровано, що включення додаткового контексту сцени (обмеження траєкторій, наявність перешкод) та поведінкових факторів дозволяє суттєво зменшити помилки прогнозу у короткому горизонті.

Водночас залишається низка відкритих питань: недостатня увага до оцінки невизначеності передбачень, слабка робастність до втрат спостережень у відеопотоці, обмежена адаптивність до раптових маневрів БПЛА та відсутність інтегрованих конвеєрів, де виявлення, трекінг і прогнозування тісно пов'язані між собою в єдиній архітектурі. Саме ці обмеження і стають фокусом запропонованого підходу.

Розроблена система (рисунок 1) моделює повний цикл обробки відеопотоку: від надходження сирих кадрів до візуалізації фактичних і прогнозованих траєкторій руху БПЛА. На вхід можуть податися локальний відеофайл, онлайн-потік або сигнал із камери реального часу. Кожен кадр передається до модуля детекції на базі YOLOv12, який повертає координати обмежувальних рамок і ймовірність належності до класу «дрон».

Набір детекцій для кожного кадру надходить до алгоритму BYTETrack, який виконує асоціативний трекінг: зіставляє детекції з уже відомими траєкторіями, призначає стійкі ідентифікатори та формує історію руху кожного БПЛА. У

результаті для кожного активного треку доступна послідовність координат центру обмежувальної рамки в попередніх кадрах.



Рисунок 1 – Цикл обробки відеопотоку

Ця координатна історія, нормалізована відносно розміру кадру, використовується як вхід трансформного модуля прогнозування. Модуль оцінює майбутній шлях БПЛА у вигляді набору наступних точок траєкторії. Далі фактичні та прогнозовані траєкторії разом із супровідними даними (час виявлення, фрагмент зображення з дроном, ідентифікатор треку) зберігаються у сховищі результатів і паралельно виводяться у двох формах: як накладені на відеокадри рамки та як карта руху на окремі панелі.

Таким чином, система забезпечує єдиний конвеєр, у межах якого детектор, трекер і трансформер тісно взаємодіють: результати одного етапу безпосередньо формують вхід наступного, а кінцевий користувач отримує не лише факт наявності БПЛА, а й оцінку його подальшого переміщення.

Короткострокове прогнозування у роботі реалізовано на основі послідовної трансформерної архітектури, адаптованої до обробки відносно коротких координатних рядів. Для кожного треку формується послідовність із 30 точок, що описують історію руху БПЛА в останню секунду (за частоти 30 кадрів за секунду). На основі цих 30 спостережень модель генерує прогноз ще 60 наступних положень, тобто траєкторію на дві секунди вперед.

На першому етапі кожна координата (x, y) перетворюється лінійним шаром у вектор більшої розмірності (2→128), що дозволяє відобразити просторовий рух у багатовимірному латентному просторі. Далі до цих векторів додається синусоїдальне позиційне кодування, яке фіксує порядок елементів у часовій послідовності й дає змогу моделі розрізняти новіші та давніші спостереження.

Основу архітектури становить енкодер із трьома шарами Transformer Encoder, кожен з яких містить багатоголову самоувагу (4 голови), двошаровий feedforward-блок із розмірністю 256 та dropout-регуляризацию. Така конфігурація дає змогу одночасно аналізувати взаємозв'язки між усіма точками траєкторії: як локальними (невеликі зміни напрямку), так і глобальними (загальний тренд руху). Результатом роботи енкодера є тензор ознак, який агрегується по часовій осі в

компактний контекстний вектор, що узагальнює поведінку об'єкта за історичний інтервал.

Декодер побудовано у вигляді багат шарового перцептрона з нормалізацією, двома прихованими шарами та фінальним лінійним шаром, який формує 120 числових значень – координати 60 точок майбутньої траєкторії. Таким чином, модель безпосередньо перетворює послідовність нормалізованих координат минулого руху на послідовність прогнозованих координат, не потребуючи явного обчислення швидкостей, прискорень чи інших похідних параметрів.

Важливою особливістю підходу є робота у просторі нормалізованих координат кадру, а не у фізичних метрах. Це з одного боку істотно спрощує інтеграцію з відеопотоком з різною роздільною здатністю, а з іншого – вимагає окремого етапу інтерпретації результатів, якщо потрібні оцінки у метричних одиницях.

Експериментальне відпрацювання методу проводилося на основі великомасштабного набору даних Anti-UAV, орієнтованого на задачі виявлення, трекінгу та ідентифікації БПЛА у відеопотоці. Датасет містить сцени з різноманітними типами фону, умовами освітлення та ракурсами зйомки, включаючи випадки низької видимості, швидких маневрів, змін масштабу, часткових перекриттів та тимчасового зникнення об'єктів з поля зору.

У роботі використовувалася підмножина відео у видимому діапазоні спектра. Набір структуровано на тренувальну, валідаційну та тестову частини, що налічують 160, 67 та 91 відеозапис відповідно – загалом 318 відеофрагментів та майже шістьсот тисяч кадрів. Такий обсяг даних забезпечує достатню статистичну базу як для навчання глибинної моделі детекції, так і для оцінювання стабільності трекінгу та точності прогнозування траєкторій у різних сценаріях.

Структура анотацій у наборі Anti-UAV дозволяє паралельно розв'язувати задачі детекції і трекінгу: для кожного кадру задані обмежувальні рамки БПЛА, що у поєднанні з алгоритмом асоціації детекцій дає можливість будувати безперервні траєкторії та формувати координатні часові ряди, необхідні для навчання трансформера.

Програмна система реалізована у середовищі Python із використанням фреймворку Kivu для побудови графічного інтерфейсу. Центральна керуюча сутність відповідає за організацію життєвого циклу застосунку: ініціалізацію модулів, завантаження відеоджерел, синхронізацію обробки кадрів і відображення результатів у реальному часі. Для роботи з відео передбачені класи-джерела, що реалізують читання з локальних файлів, URL-потоків або камер.

Модуль детекції інкапсулює завантажену модель YOLOv12, керує вибором обчислювального пристрою (CPU/GPU), виконує попереднє масштабування кадрів та повертає детекції у стандартизованому форматі. Для трекінгу використано окремий клас, що реалізує алгоритм BYTETrack: виконується асоціація детекцій, підтримання історії треків, скидання стану та відображення траєкторій у зручному для візуалізації форматі.

Сховище результатів накопичує кадри, зображення дронів та як фактичні, так і прогнозовані координати. Інтерфейс користувача складається з двох ключових візуальних компонентів: панелі дронів, де представлено перелік активних об'єктів і базову інформацію про них, та карти руху, яка показує траєкторії БПЛА на координатній сітці з урахуванням масштабування між простором зображення та площиною відображення. Така модульна організація забезпечує простоту модифікації кожного компонента та можливість подальшого розширення функціоналу без зміни базової логіки.

Оцінювання модуля детекції показало, що модель YOLOv12 демонструє стабільно високі значення mAP50 на тренувальній, валідаційній і тестовій вибірках, що вказує на якісне позиціонування обмежувальних рамок дронів навіть за умов шуму, дрібних розмірів об'єкта та складного фону. Значення mAP50-95 підтверджує, що модель зберігає достатню чутливість і при жорсткіших критеріях відповідності. При цьому досягається висока швидкодія як на GPU, так і на CPU, що важливо для інкрементної обробки потоку відеоданих.

Аналіз конфузійної матриці показує, що частина випадків, інтерпретованих формально як помилкове виявлення фону, насправді відповідає об'єктам, подібним за структурою або силуетом до БПЛА. Для практичних систем моніторингу така поведінка моделі є прийнятною, оскільки чутливість до дроноподібних цілей часто важливіша за жорстке розділення «ціль/фон», особливо на ранніх етапах виявлення загроз.

Трекер BYTETrack показав значення MOTA на рівні 0.79 та IDF1 близько 0.64, що свідчить про збереження ідентичності більшості об'єктів упродовж спостереження, навіть за умов часткових перекриттів, змін масштабу та нерівномірної швидкості руху. Швидкодія понад 300 кадрів за секунду на CPU дозволяє позиціонувати обрану конфігурацію як придатну для розгортання в системах реального часу без критичної оптимізації.

Процес навчання трансформерної моделі супроводжувався стабільним зниженням значення функції втрат на тренувальній та валідаційній вибірках. На ранніх епохах спостерігається інтенсивне зменшення похибки, після чого крива поступово виходить на плато, причому розбіжність між тренувальною і валідаційною кривими залишається помірною, що вказує на відсутність явного перенавчання. Нормалізація координат у діапазон $[0;1]$ дає змогу інтерпретувати кінцеві значення втрат як малі відхилення у відносних координатах, тоді як у перерахунку на пікселі абсолютні помилки виглядають більшими, хоч описують той самий рівень точності.

Підсумкові метрики на тестовому наборі засвідчують середню кореневу середньоквадратичну помилку $RMSE \approx 12.66$ пікселів, середню похибку по траєкторії $ADE \approx 14.1$ пікселя та фінальну помилку $FDE \approx 17.4$ пікселя. За типової ширини кадру такі значення відповідають приблизно 1–2 % від розміру зображення, що є прийнятним для короткострокового прогнозування у тактичному горизонті в

дві секунди. Обчислювальна складність моделі становить близько 0.03 GFLOPs, що підтверджує сумісність із пристроями з обмеженими ресурсами.

Порівняння з класичними статистичними підходами (моделі типу IMM/Kalman) показало, що трансформерний предиктор забезпечує істотно менші значення RMSE, ADE та FDE – відносна різниця сягає порядку величини для маневрових траєкторій. Це означає, що модель краще відтворює як напрямок, так і кривину шляху БПЛА, особливо в ситуаціях зі змінною швидкістю та різкими розворотами.

З урахуванням середнього масштабу сцени в наборі Anti-UAV співвідношення «метр – пікселі» оцінюється як 40-60 пікселів на метр. За цього припущення похибка RMSE близько 12.66 пікселів відповідає приблизно 0.25-0.32 м, що співмірно з точністю, наведеною у відомих роботах з траєкторного прогнозування в метричних координатах.

Візуальний аналіз прикладів роботи показує, що модель коректно відтворює як прямолінійні, так і маневрові траєкторії дронів, підтримуючи близькість прогнозованого шляху до фактичного та забезпечуючи плавне зростання розбіжності із збільшенням горизонту передбачення, без різких стрибків або деградації якості. Приклад роботи застосунку наведено на рисунку 2.

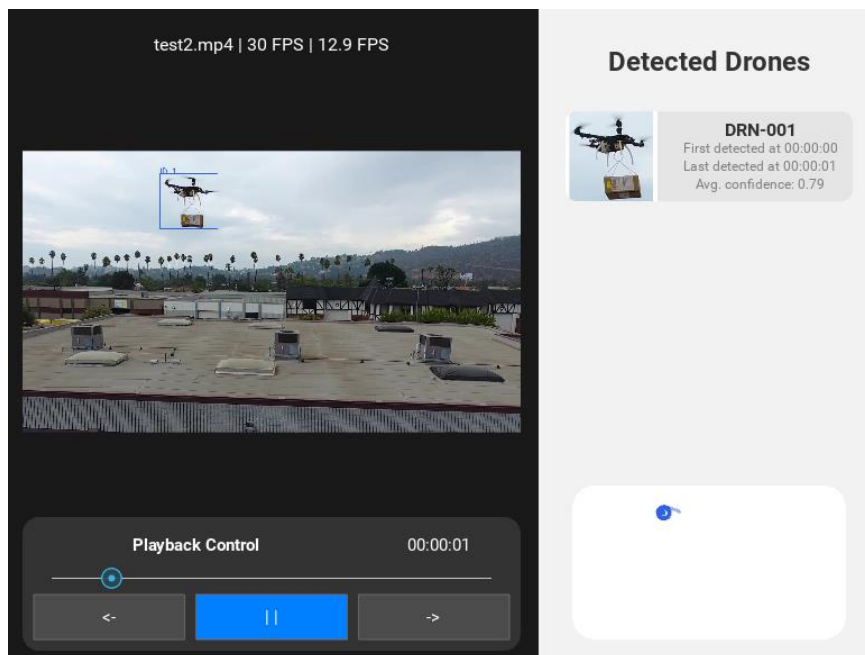


Рисунок 2 – Приклад роботи програмного забезпечення

Отримані результати свідчать, що поєднання сучасного детектора малих об'єктів, асоціативного трекера та трансформерного модуля прогнозування дозволяє побудувати практично орієнтований конвеєр короткострокового прогнозування траєкторій БПЛА з прийнятним балансом між точністю, робастністю та обчислювальною вартістю. Модуль детекції забезпечує достатню чутливість до дрібних дронів на складному фоні, трекер підтримує тяглість ідентичностей навіть за рахунку перекриттів, а трансформер здатний відтворювати як плавні, так і маневрові траєкторії з помилками, які у фізичному просторі не перевищують кількох десятків сантиметрів у короткому горизонті.

Приклад прогнозів розробленим програмним забезпеченням наведено на рисунку 3.

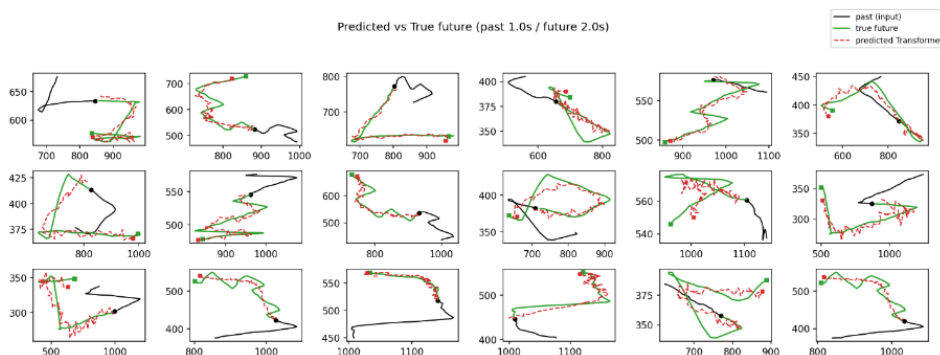


Рисунок 3 – Приклад прогнозування траєкторії

Висока продуктивність (сотні кадрів за секунду на CPU) відкриває можливість інтегрувати запропонований метод у системи моніторингу повітряного простору, які працюють на вбудованих платформах або індустриальних комп'ютерах без потужних GPU. Одночасно модульна архітектура програмної реалізації створює передумови для розширення функціоналу: можна додавати модулі класифікації типів БПЛА, оцінювання рівня загрози, інтегрувати додаткові сенсорні канали (радар, тепловізор) тощо.

Разом із тим робота має низку обмежень. По-перше, прогнозування здійснюється у двовимірних координатах зображення при стаціонарному розміщенні камери, тому переходу до сценаріїв із рухомою платформою спостереження має передувати етап стабілізації відео та переходу до єдиної системи координат. По-друге, розглядається короткий горизонт прогнозування (дві секунди), що є логічним для оперативного реагування, але не охоплює сценарії планування довготривалих траєкторій або уникнення конфліктів між кількома дронами.

По-третє, у роботі не враховано явне моделювання невизначеності передбачень: трансформер повертає одну детерміністичну траєкторію, тоді як для

задач безпеки важливим є оцінювання інтервалів довіри або ймовірнісних «коридорів» руху. Нарешті, не здійснюється попередня класифікація типів траєкторій (наприклад, прямолінійний проліт, кружляння, агресивний маневр), яка могла б підвищити точність прогнозування через вибір спеціалізованих підмоделей для кожного типу динаміки.

Перспективним напрямом подальших досліджень є об'єднання трансформерної архітектури з поведінковими моделями ймовірнісного характеру, навчання окремих предикторів для різних класів траєкторій, розширення набору даних за рахунок сценаріїв із рухомими платформами та багатоагентними сценами, а також інтеграція оцінки невизначеності у процес ухвалення рішень системами протидії БПЛА.

У роботі сформульовано й реалізовано неймережевий підхід до короткострокового прогнозування траєкторій БПЛА у відеопотоці, в основі якого – позиційно-кодований трансформер, що працює з координатними часовими рядами. Метод функціонує у складі інтегрованого відеоаналітичного конвеєра, який поєднує детекцію дронів за допомогою YOLOv12, багатооб'єктний трекінг на базі BYTETrack та трансформерний модуль прогнозування, а результати візуалізуються у вигляді накладених на відео рамок і карти руху з фактичними та прогнозованими траєкторіями.

Перелік посилань

1. Zhan, C., Hu, H., Sui, X., Liu, Z., Wang, J., & Wang, H. (2020). Joint resource allocation and 3D aerial trajectory design for video streaming in UAV communication systems. *IEEE Transactions on Circuits and Systems for Video Technology*, 31(8), 3227-3241
2. Huang, H., Savkin, A. V., & Ni, W. (2021). Online UAV trajectory planning for covert video surveillance of mobile targets. *IEEE Transactions on Automation Science and Engineering*, 19(2), 735-746.
3. binti Burhanuddin, L. A., Liu, X., Deng, Y., Challita, U., & Zahemszky, A. (2022). QoE optimization for live video streaming in UAV-to-UAV communications via deep reinforcement learning. *IEEE Transactions on Vehicular Technology*, 71(5), 5358-5370.
4. Zhong, G., Zhang, H., Zhou, J., Zhou, J., & Liu, H. (2022). Short-term 4D trajectory prediction for UAV based on spatio-temporal trajectory clustering. *IEEE Access*, 10, 93362-93380.
5. Pokhytun A., Mazurets O., Molchanova M., Tyschenko O. Method for Neural Network Detecting Changed Images of People's Faces Using CNN. *New Horizons in Scientific Research: Challenges and Solutions. Proceedings of the 1st International scientific and practical conference. October 21-23, 2024. Marseille, France. 2024. Pp. 35-40.*
6. Zhamovskiy O., Mazurets O., Sobko O. Approach to Identification of Artificial Intelligence-Generated People Images by Means of Machine Learning. *Key Aspects of the Development of Scientific Research in Modern Conditions. Proceedings of the XLV International scientific and practical conference. October 30 – November 1, 2024. Constanta, Romania. 2024. Pp. 69-73.*
7. Мазур Є.В., Мазурець О.В., Кліменко В.І., Собко О.В., Залуцька О.О. Алгоритми та програмна архітектура інформаційної системи неймережевого аналізу постави людини. *Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2025. №3. Т.1. С. 275-284.*

8. Мазурець О.В., Собко О.В., Дидо Р.А., Молчанова М.О., Тищенко О.О. Проектування структури бази даних для інтелектуальної системи нейромережевого виявлення та локалізації на фотозображеннях ділянок із залишками зруйнованих будівель. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №4 (45). С. 1242-1258.
9. Молчанова М.О., Дідур В.О., Мазурець О.В., Тищенко О.О., Залуцька О.О. Інформаційна технологія використання хмарних обчислень для класифікації залишків зруйнованих будівель засобами нейронних мереж за візуальними даними з безпілотних літальних апаратів. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №4 (45). С. 1259-1272.
10. Похитун А.В., Мазурець О.В., Дидо Р.А., Молчанова М.О. Програмна архітектура для нейромережевого виявлення модифікованих фотографій обличчя людей. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2025. №3. Т.2. С. 493-500.
11. Мазурець О.В., Жарновський О.В., Гладун О.В., Собко О.В. Нейромережеве виявлення фейкових зображень людей. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2025. №5. Т.1. С. 416-422.
12. Дідур В.О., Молчанова М.О., Мазурець О.В. Спосіб виявлення та класифікації залишків зруйнованих будівель та будівельного сміття за фотографіями з використанням моделей CNN. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №1 (42). С. 1162-1175.
13. Дидо Р.А., Мазурець О.В. Метод ідентифікації особистості на основі розпізнавання обличчя в реальному часі для систем кібербезпеки. Інформаційна, функційна і кібербезпека СКІФіК2024. Матеріали IV Всеукраїнської науково-технічної конференції. 29-30 листопада 2024. Харків. 2024. с. 36-37.
14. Похитун А.В., Мазурець О.В., Молчанова М.О., Бармак О.В. Підхід до формування датасету для нейромережевого виявлення модифікованих фотографій обличчя людей. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». 15-16 листопада 2024. Хмельницький, 2024. с. 428-433.
15. Собко О.В., Кліменко В.І., Мазурець О.В., Залуцька О.О., Гладун О.В. Особливості програмної інженерії та тестування програмного забезпечення для нейромережевого аналізу фотоданих залишків зруйнованих будівель із роботизованої техніки. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №4 (45). С. 1566-1581.
16. Мазурець О.В., Петровський С.С., Дидо Р.А. Нейромережева модель для ідентифікації особистості за зображенням обличчя у реальному часі Інформаційні технології і автоматизація. Матеріали XVII міжнародної науково-практичної конференції. 31 жовтня – 1 листопада 2024 р. Одеса, ОНТУ. 2024. С.655-658.
17. Молчанова М.О., Мазурець О.В., Шурипа М.О. Об'єктно-орієнтований підхід до нейромережевого виявлення та відстеження БПЛА з використанням хмарних технологій. Науковий журнал «Наука і техніка сьогодні». Київ, 2025. №9 (50). С. 1346-1360.

УДК 004.8

Юрченко Д.Ю., Мазурець О.В.

Хмельницький національний університет

МЕТОД ІНТЕРПРЕТАЦІЇ РЕЗУЛЬТАТІВ НЕЙРОМЕРЕЖЕВОГО ВИЯВЛЕННЯ ОЗНАК МАНІПУЛЯТИВНИХ ТЕХНІК ЗА ЕМОЦІЙНОЮ ТОНАЛЬНІСТЮ ТЕКСТІВ

Запропоновано метод інтерпретації результатів нейромережевого виявлення ознак маніпулятивних технік за емоційною тональністю текстів, який має перевагу у точності на понад 7% у порівнянні з відомими аналогами, та відрізняється використанням гібридної архітектури CNN та BiLSTM, що дозволяє ефективно виділяти локальні патерни та враховувати довгострокові залежності у тексті. Крім того, пропонується застосування моделі LIME для локальної інтерпретації результатів, що підвищує прозорість та інтерпретованість моделі, що сприяє довірі до нейромережесих підходів.

The method for interpreting the results of neural network detection of signs of manipulative techniques by the emotional tone of texts is proposed, which has an accuracy advantage of over 7% compared to known analogues, and is distinguished by the use of a hybrid CNN and BiLSTM architecture, which allows for effective local pattern identification and consideration of long-term dependencies in the text. In addition, the use of the LIME model for local interpretation of the results is proposed, which increases the transparency and interpretability of the model, which contributes to trust in neural network approaches.

Соціальні мережі, форуми та інші платформи стали основними каналами комунікації, де люди обмінюються думками, висловлюють свої емоції та реагують на події [1]. Важливість аналізу емоційної тональності таких повідомлень полягає у можливості виявлення загальних настроїв, тенденцій та потенційних соціальних ризиків [2]. Проте, результати нейромережевого аналізу часто є складними для сприйняття і вимагають додаткового пояснення. Створення ефективного методу візуалізації цих результатів допоможе полегшити розуміння виявлених емоційних станів, сприятиме більш інформованому прийняттю рішень та підвищенню прозорості аналізу [3, 4]. У цьому контексті використання методів візуального пояснення набуває особливого значення, оскільки дозволяє зменшити інформаційне навантаження на користувачів і забезпечити доступність аналітичних даних для широкого кола зацікавлених осіб.

Методи обробки природної мови демонструють значний потенціал у дослідженні маніпулятивних впливів у текстових повідомленнях [5, 6], зокрема

через аналіз емоційної тональності [7, 8]. Розвиток глибинних нейронних мереж [9], трансформерної архітектури [10] та контекстних ембеддингів [11] забезпечив можливість виявляти приховані патерни мовного впливу, які не піддаються фіксації традиційними статистичними підходами [12]. Емоційні індикатори – такі як інтенсивність позитивних чи негативних емоцій, наявність страхових, агресивних або мобілізаційних сигналів – стали окремими маркерами для розпізнавання маніпулятивних стратегій, зокрема залякування [13], емоційного тиску [14], викривлення інформації [15] та створення штучного емоційного контексту [16].

Водночас однією з ключових проблем є обмежена інтерпретованість нейромережових моделей, що ускладнює достовірне пояснення того, які саме мовні ознаки стали підставою для класифікації повідомлення як маніпулятивного [17]. У цьому контексті особливого значення набувають методи Explainable AI (XAI) та інтерпретованого NLP, зокрема такі підходи, як attention-аналіз, оцінювання важливості слів (feature importance), методи LIME та SHAP для текстів, а також візуалізація емоційних патернів. Поєднання цих підходів дає змогу не лише підвищити прозорість моделей, але й виявити сталі мовні конструкції, що слугують індикаторами маніпулятивної риторики.

Проблема непрозорості моделей ШІ часто призводять до непередбачуваних результатів, включаючи упереджені рішення та недостатню інтерпретацію. Зазвичай відсутній блок пояснень результатів, які видає модель машинного навчання. І якщо мова йде про нейромережі – тут задача стає ще більш проблемною. Пропонується підхід на основі візуального пояснення результатів нейромережового аналізу емоційної тональності, наведений на рисунку 1.

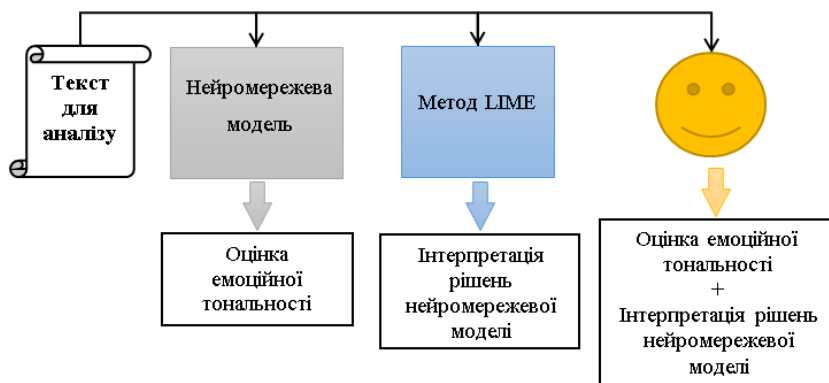


Рисунок 1 – Схема підходу на основі інтерпретації результатів нейромережового виявлення ознак маніпулятивних технік

У межах запропонованого підходу для візуалізації пояснень результатів нейромережевого аналізу емоційної тональності пропонується застосувати модель LIME, яка є локальною моделлю для інтерпретації пояснень, незалежних від конкретної моделі [18].

Отже, такий підхід дозволить зберегти всі переваги нейромережевих рішень, одночасно надаючи користувачеві зрозуміле пояснення, що вплинуло на ці рішення. Це підвищить довіру до результатів нейромережі та дасть змогу виявляти помилки, які вона може допускати.

Метод візуального пояснення результатів нейромережевого аналізу емоційної тональності повідомлень у соціально-орієнтованих сервісах, що базується на використанні гібридної нейронної мережі архітектур CNN та BiLSTM, з локальною інтерпретацією моделлю машинного навчання LIME [19]. Схема та етапи методу наведені на рисунку 2.

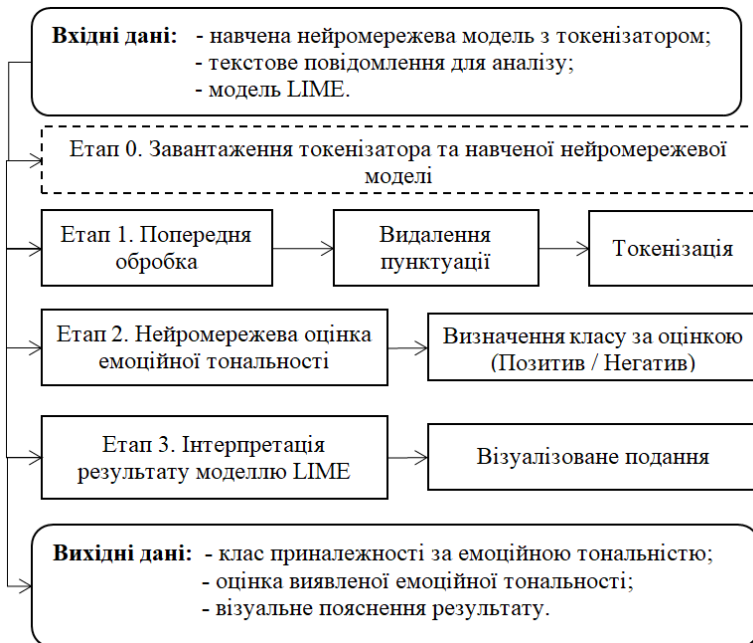


Рисунок 2 – Етапи методу інтерпретації результатів нейромережевого виявлення ознак маніпулятивних технік за емоційною тональністю текстів

Комбінація архітектур CNN та BiLSTM дозволяє ефективно виявляти локальні патерни в тексті (CNN), такі як важливі слова або фрази, що можуть бути

ключовими для визначення емоційної тональності. Bidirectional LSTM, у свою чергу, дає змогу аналізувати довгострокові залежності в тексті з обох напрямків, що сприяє кращому розумінню контексту та підвищує точність прогнозів.

Вхідними даними є попередньо навчена нейромережева модель з токенизатором, текст для аналізу та модель LIME для пояснення результатів. Спочатку необхідно завантажити токенизатор і навчану нейромережеву модель, що дасть змогу надалі подавати текстові повідомлення з соціально орієнтованих сервісів для подальшого аналізу нейронною мережею. На етапі 1 також виконується попередня обробка тексту, яка повинна відповідати тій, що застосовувалась під час навчання моделі. Вона охоплює видалення пунктуації, стоп-слів та виконання токенизації.

Наступним кроком є оцінка емоційної тональності за допомогою нейронної мережі з гібридною архітектурою, що об'єднує CNN та BiLSTM. Ця нейромережа має один вихід, і повідомлення вважається позитивним, якщо показник позитивної тональності перевищує 0,5, в іншому випадку – негативним. Третій етап передбачає інтерпретацію результату за допомогою моделі LIME.

Інтерпретація відбувається у вигляді візуалізації, яка демонструє ключові слова та ознаки, що вплинули на прийняте моделлю рішення, а також оцінку їх важливості.

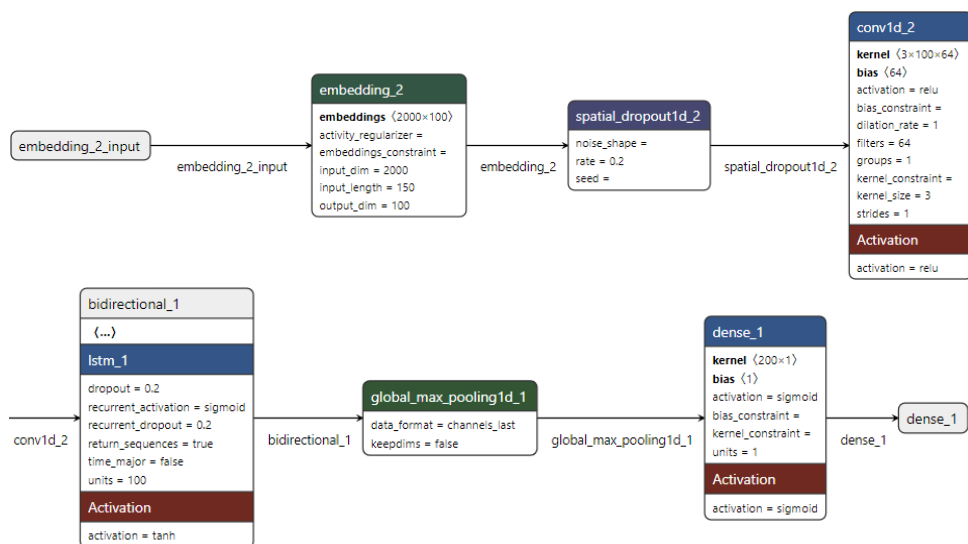


Рисунок 3 – Архітектура нейромережі для виявлення ознак маніпулятивних технік за емоційною тональністю текстів

Вихідними даними методу є клас приналежності за емоційною тональністю, оцінка виявленої емоційної тональності; візуальне пояснення результату.

Для нейромережевого аналізу емоційної тональності повідомлень запропоновано використати нейромережу гібридної архітектури, що поєднує одночасну переваги архітектур CNN та BiLSTM. Архітектура запропонованої нейромережі наведена на рисунку 3.

Модель починається з шару Embedding, який перетворює вхідний текст у числові вектори заданої розмірності. Потім використовується шар SpatialDropout1D, який випадковим чином «відключає» частину нейронів (20%) для запобігання перенавчанню.

Наступним йде шар Conv1D, який застосовує одинарні згортки до вхідних даних, виявляючи локальні патерни. Після цього модель має двонаправлений шар LSTM, який здатний запам'ятовувати інформацію з обох кінців послідовності. Цей шар також має вбудовані механізми випадкового відключення нейронів для кращої узагальнювальної здатності.

Після шару LSTM йде шар GlobalMaxPooling1D, який обирає максимальні значення з усіх отриманих ознак, зменшуючи розмірність даних. Завершує модель щільний шар Dense з одним нейроном та сигмоїдною функцією активації, який видає ймовірність належності вхідного тексту до класу «Позитивна тональність». Для навчання нейромережі необхідно виконати ще підготовчий етап по роботі з датасетом. Схема навчання нейромережі гібридної архітектури наведено на рис. 4.

Вхідними даними для отримання навченої нейромережевої моделі є навчальна вибірка та ненавчена нейромережева модель гібридної архітектури.

Перший етап відповідає за попередню обробку всіх навчальних текстів, що присутні в датасеті. Попередня обробка включає видалення стоп-слів та знаків пунктуації, а також токенизацію тексту.

На другому етапі відбувається поділ навчальної вибірки на тренувальну та валідаційну у співвідношенні 80 на 20, де 80% тренувальні дані та 20 % валідаційні.

Третій етап відповідає за визначення параметрів навчання нейромережі, таких як кількість епох та розмір партії навчальних зразків. Ці параметри змінюються у залежності від результатів метрик, якщо результати навченої нейронної мережі не задовольняють потребам, змінюються дані параметри та повторюється процес навчання. За замовчуванням кількість епох 5, а розмір навчальної партії 32 зразка.

Наступним етапом відбувається тренування нейромережі із визначенням метрик для кожної епохи навчання. Використовуються метрики accuracy та loss. Це дозволяє оцінювати результат і бачити статистику. Якщо по завершенні епох

ассурасу все ще зростає, а loss спадає, це означає що можна спробувати тренування з більшою кількістю епох.



Рисунок 4 – Схема навчання нейромережі гібридної архітектури

П'ятим етапом відбувається збереження навченої моделі та токенизатора, якщо метрики ассурасу та loss показують результат, більше 0.9 для метрики ассурасу та менше 0.1 для метрики loss. Якщо результату не досягнуто, необхідно повернутись на етап 3 та перенавчити нейромережу.

Вихідними даними є збережена нейромережева модель з оцінками ассурасу та loss і токенизатор.

Як показав проведений експеримент, точність нейромережі з гібридною архітектурою CNN та BiLSTM перевищує 97 %, що пояснюється здатністю цієї архітектури ефективно виявляти локальні патерни та враховувати довгострокові залежності в тексті. Графіки статистики навчання використовуваної архітектури наведені на рисунку 5.

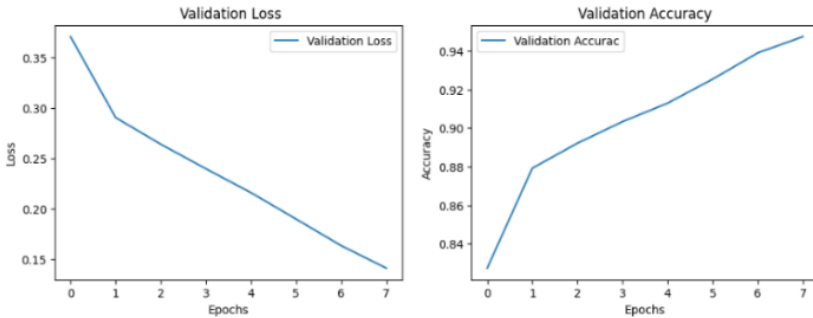


Рисунок 5 – Графіки навчання нейромережі

Окрім високої точності, у порівнянні з реалізованими аналогами (аналоги мають точність 86 – 89 %), протестованими на запропонованому наборі даних, даний метод має надбудову для інтерпретації отриманих рішень. Приклад інтерпретації наведено на рисунку 6.

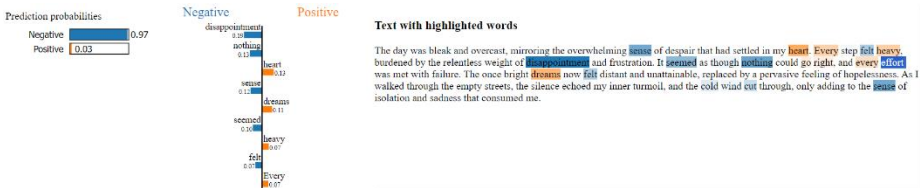


Рисунок 6 – Приклад застосування інтерпретації до результатів нейромережевого виявлення ознак маніпулятивних технік

Як видно з рисунку 6, повідомлення має негативну тональність. Окрім оцінки тональності, представлено слова, які мають вплив на прийняте мережею рішення із вагами. Наприклад, такі слова як «disappointment» (розчарування), «nothing» (нічого), «seemed» (здалося), «felt» (відчувати себе далеким) дійсно мають негативне спрямування.

Отже, запропонований метод візуального пояснення результатів нейромережевого аналізу емоційної тональності повідомлень у соціально-орієнтованих сервісах має перевагу у точності на понад 7% у порівнянні з відомими аналогами, та відрізняється використанням гібридної архітектури CNN та BiLSTM, що дозволяє ефективно виділяти локальні патерни та враховувати довгострокові залежності у тексті. Крім того, пропонується застосування моделі LIME для локальної інтерпретації результатів, що підвищує прозорість та інтерпретованість моделі, що сприяє довірі до нейромережевих підходів

Подальші дослідження будуть спрямовані експерименти з гібридною архітектурою, на кшталт зміни кількості та розмірності шарів, що націлені на підвищення точності ідентифікації. Також планується використання додаткових методів візуалізації з метою підвищення рівня поясненості прийнятих нейромережею рішень.

Перелік посилань

1. Huffaker, J. S., Kummerfeld, J. K., Lasecki, W. S., & Ackerman, M. S. (2020, April). Crowdsourced detection of emotionally manipulative language. In Proceedings of the 2020 CHI conference on human factors in computing systems (pp. 1-14).
2. Leary, R. (2022). Manipulation techniques: Discover covert manipulation techniques to persuade and influence anyone, how to analyze people and Reading body language. BoD–Books on Demand.
3. Bakpokayev, A., Razaque, A., Kalpeeva, Z., & Ayapbergenova, A. (2025). Combating Social Network Manipulations: A Machine Learning Approach to Enhance Digital Literacy and Emotional Awareness. *Computing & Engineering*, 3(1), 1-8.
4. Phirangee, K., & Hewitt, J. (2016). Loving this dialogue!!!!: Expressing emotion through the strategic manipulation of limited non-verbal cues in online learning environments. In *Emotions, technology, and learning* (pp. 69-85). Academic Press.
5. Залуцька О.О., Молчанова М.О., Мазурець О.В., Мельник О.І., Скрипник Т.К. Метод інтелектуального аналізу емоційної тональності текстової інформації для визначення поведінкових намірів нейромережевими засобами. *Науковий журнал «Вісник Хмельницького національного університету»* серія: Технічні науки. Хмельницький, 2023. №5 (325). Т.1. С. 67-73.
6. Мазурець О.В., Козенко О.В., Собко О.В. Метод автоматизованого підбору відповідей на користувацькі запитання за семантичною подібністю. *Матеріали XII Всеукраїнської науково-практичної конференції «Глушковські читання»*. Київ – 2023. с. 106-109.
7. Shevchuk P., Molchanova M., Mazurets O. Software for Text Messages Reliability Analysis Based on the Machine Learning Models Ensemble. Proceedings of IV International Scientific and Practical Conference «Innovative research and perspectives of the development of science and technology». January 29-31, 2024. Stockholm, Sweden. 2024. Pp. 347-354.
8. Молчанова М.О., Мазурець О.В., Собко О.В., Віт Р.В., Назаров В.В. Алгоритм виявлення аб'юзивного вмісту в україномовному аудіоконтенті для імплементації в об'єктно-орієнтовану інформаційну систему. *Науковий журнал «Вісник Хмельницького національного університету»* серія: Технічні науки. Хмельницький, 2024. №1 (331). С. 101-106.
9. Молчанова М.О., Мазурець О.В., Собко О.В., Кліменко В.І., Андрощук В.І. Метод нейромережевого виявлення кібербулінгу з використанням хмарних сервісів та об'єктно-орієнтованої моделі. *Науковий журнал «Вісник Хмельницького національного університету»* серія: Технічні науки. Хмельницький, 2024. №2 (333). С. 200-206.
10. Mazurets O., Sobko O., Vit R., Pasternak V. Practical Approach for Detection by Deep Learning of Target Objects of Subject Area Based on Semantic Connectivity Indicators in Audio Database. Proceedings of XXIV International Scientific and Practical Conference «Modern Scientific

Challenges are the Driving Force of the Development of Scientific Research». May 22-24, 2024. Bruges, Belgium. International Scientific Unity. 2024. Pp. 91-96.

11. Mazurets O.V., Sobko O.V., Molchanova M.O., Zalutska O.O., Yurchak A.V. Practical Implementation of Neural Network Method for Stress Features Detection by Social Internet Networks Posts. Global Science: Prospects and Innovations. Proceedings of the II International Scientific and Theoretical Conference «Scientific Review of the Actual Events, Achievements and Problems». May 31, 2024. Berlin, Federal Republic of Germany: International Center of Scientific Research. 2024. Pp. 160-167.

12. Sobko O., Mazurets O., Didur V., Chervonchuk I. Recurrent Neural Network Model Architecture for Detecting a Tendency to Atypical Behavior Of Individuals by Text Posts. Theoretical and Practical Aspects of Modern Research. Proceedings of XXVI International scientific and practical conference. June 5-7, 2024. International Scientific Unity. Ottawa, Canada. 2024. Pp. 113-117.

13. Mazurets O., Molchanova M., Klimenko V., Prosvitliuk M Practice Implementation of Neural Network Model BART-Large-CNN for Text Annotation. Prospects of Scientific Research in the Conditions of the Modern World. Proceedings of XXVII International scientific and practical conference. June 12-14, 2024. Rotterdam, Netherlands. 2024. Pp. 97-102.

14. Мазурець О.В., Віт Р.В. Інтелектуальний метод виявлення цільових об'єктів предметної області за показниками семантичної зв'язності для класифікації текстової інформації. Розвитки інформаційно-керуючих систем та технологій.: монографія. Львів-Торунь : Lina-Pres, 2024. – С.223-244.

15. Mazurets O., Vit R. Practical Application of Method of Thematic Classification of Text Information Using LDA. Information Technology and Implementation (Satellite). Proceedings 11th International Conference. November 21, 2024. Kyiv, Ukraine. 2024. Pp. 151-152.

16. Овчарук О.М., Мазурець О.В. Нейромережеве діагностування проявів ПТСР у текстовому контенті з використанням помилко-орієнтованого навчального набору даних. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2024. №6, Т.1 (343). С. 195-200.

17. Yurchenko D., Mazurets O., Didur V., Molchanova M. Approach to Using Cloud Services for Visual Analytics of Neural Network Analysis of Texts Emotional Tonality. The Future of Scientific Discoveries: New Trends and Technologies. Proceedings of the XLVII International scientific and practical conference. November 13-15, 2024. Marseille, France. 2024. Pp. 108-113.

18. Юрченко Д.Ю., Мазурець О.В., Залуцька О.О., Безпрозвана Ю.Г. Підхід до візуального пояснення результатів нейромережевого аналізу емоційної тональності повідомлень у соціальних мережах. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». 15-16 листопада 2024. Хмельницький, 2024. с. 565-571.

19. Юрченко Д.Ю., Овчарук О.М., Мазурець О.В., Шевчук П.О. Метод використання нейромережі гібридної архітектури для визначення емоційної тональності текстових повідомлень. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». № 2, 2025. с. 136-141.

УДК 004.4

Юрчук Р.В., Праворська Н.І.

Хмельницький національний університет

ІНСТРУМЕНТ ВІЗУАЛЬНОГО СТВОРЕННЯ ТА РЕДАГУВАННЯ КОРИСТУВАЦЬКИХ РЕДАКТОРІВ ДЛЯ ІГРОВОГО РУШІЯ UNITY

В сучасній індустрії програмного забезпечення велику роль відіграє сфера розробки комп'ютерних ігор. Ця галузь вже давно перестала бути вузькою та непоширеною серед спеціалістів. Станом на зараз вона має великий вплив у формуванні сучасної інтернет спільноти та розвитку комп'ютерних наук, часто надаючи нові виклики і завдання розробникам як програмних, так і апаратних частин. У зв'язку із цим потреби на спеціалізовані інструменти для розробки ігрового програмного забезпечення інтенсивно зростають. Проте не всі люди причетні до розробки знають кодування на достатньому рівні, щоб створювати чи модифікувати засоби розробки власними силами. Впровадження інструменту для візуального створення користувачьких редакторів дозволить спеціалістам різних профілів полегшувати свою роботу без написання коду.

In the modern software industry, computer game development plays a major role. This industry has long ceased to be narrow and uncommon among specialists. As of now, it has a significant impact on the formation of the modern Internet community and the development of computer science, often presenting new challenges and tasks to developers in both software and hardware. In this regard, the demand for specialized tools for game development software is growing rapidly. However, not all people involved in development know coding well enough to create or modify development tools on their own. The introduction of a tool for the visual creation of user editors will allow specialists of various profiles to facilitate their work without writing code.

Згідно із нещодавніми звітами середньостатистична людина проводить за екранами пристроїв 6 годин та 45 хвилин щодня, із яких за іграми – 1 годину та 46 хвилин, що складає близько 26%. Ринок ігор набирає обертів, розробка ігрових застосунків стає дедалі поширенішою практикою, а попит на інструменти для їхньої розробки зростає з великими темпами. Розробниками ігор тепер можуть бути не тільки програмісти, але й люди творчих спеціальностей. Тому створення візуальних інструментів розробки зможе відкрити шлях багатьом новим людям для прийняття активної участі у розробці ігор, тим самим розширюючи ринок та стираючи межу для входу у цю сферу.

Наразі найбільшим ігровим рушієм за кількістю розроблених ігрових проєктів залишається Unity. При роботі із ним розробники створюють власні керуючі компоненти чи контейнери для даних, а потім мають можливість редагувати властивості їхніх екземплярів через вбудований редактор. Однак деколи виникає потреба у розширенні можливостей цього редактора шляхом додавання

функціональних кнопок, вкладок, груп, або ж зміни його вигляду, наповнення чи конфігурації для покращення та пришвидшення взаємодії. Для цього Unity надає можливість писати власні редактори для класів, щоправда для цього потрібно знати особливості функціонування системи редакторів Unity, а також вміти працювати із бібліотекою, що надає цей функціонал.

У зв'язку із складністю прямої розробки користувацьких редакторів на ринку з'явилися рішення для полегшення та пришвидшення цієї роботи. Найпопулярніші із них, такі як Odin Inspector, NaughtyAttributes та Alchemy покладаються на атрибути полів та класів для зміни вигляду редактору. Метод атрибутів зменшує кількість необхідного коду та знань для реалізації власних редакторів, проте все-таки має декілька нерозв'язаних проблем:

Потреба у розумінні програмування все ще присутня.

Необхідність у знанні наборів атрибутів конкретного рішення та їх правильно використовувати на практиці.

Додавання великої кількості атрибутів погіршує читабельність та розуміння коду.

Можливість побачити результат тільки після компіляції коду, що збільшує кількість необхідного часу для внесення змін та їхньої перевірки у редакторі, що особливо стосується незначних змін.

Неможливість передачі коду для інших розробників, які не мають доступу до відповідного рішення.

Іншим методом розробки власних редакторів є рішення UI Toolkit від Unity. Це вбудований набір інструментів, який надає можливість створювати користувацький інтерфейс, в тому числі редактори, за допомогою візуальних інструментів, беручи за основу засоби веброзробки. У цьому методі є три головних компонента: структура (файл UXML), стилізація (файл USS) та поведінка (файл коду), що в точності повторює будову звичайної інтернет сторінки. Однак навіть для простої зміни порядку елементів необхідно окрім файлу структури створювати файл поведінки з кодом, який буде відмальовувати редактор, а додавання функціональної кнопки не можливе без втручання у код файлу поведінки.

Метою цієї роботи є дослідження методів та розробка інструменту для допомоги у створенні та редагуванні власних користувацьких редакторів, що матиме наступні особливості:

- відсутність потреби у написанні будь-якого коду;
- виключно візуальний підхід до роботи;
- автоматичне оновлення редагованих редакторів у реальному часі без потреби у компіляції коду;
- можливість експортувати створені редактори у самодостатньому вигляді для безшовної передачі іншим розробникам;
- мінімальна конфігурація у одному файлі.

Для кращого розуміння взаємодії інструменту із сутностями можна розглянути діаграму потоків даних (рисунок 1). Із неї видно, що користувач



```
sequenceDiagram
    actor User as Користувач
    participant Logic as Логіка відмальовки
    participant Config as Файл конфігурації
    participant Component as Компонент
    participant Editor as Редактор Unity

    User->>Logic: [1] Відкриває редактор
    Logic->>Config: [2] Читає структуру UI
    Config-->>Logic: [3] Повертає структуру
    Logic->>Component: [4] Запитує поточні дані компонента
    Component-->>Logic: [5] Повертає значення властивостей
    Logic->>Editor: [6] Створює та наповнює UI елементи даними
    Editor-->>User: [7] Відображає готовий кастомний редактор
```

Рисунок 2 – Діаграма послідовності «Відмальовка редактору»

Запропонований інструмент має потенціал стати суттєвим знаряддям у реалізації власних користувацьких редакторів, особливо на фоні тенденцій приходу в ігрову індустрію людей неінженерних спеціальностей, а також поширенню візуальних інструментів розробки. Ключові особливості цього продукту, а саме відсутність необхідності кодування та можливість легкого перенесення компонентів між проектами, зробить його унікальним рішенням проблеми на існуючому ринку.

У подальшому описаний інструмент можна розширити підтримкою власних стилізацій, які можна буде додавати до декількох файлів конфігурації без необхідності перевизначати загальні елементи стилю для кожного із них окремо. Поглиблення модульності задля використання одних конфігурацій усередині інших, а також підтримка вибору конкретної конфігурації серед існуючих, сприятиме ще більшому збільшенню гнучкості системив.

Перелік посилань

1. Average Screen Time Statistics 2025 (By Age, Gender & Region). URL: <https://www.demandsage.com/screen-time-statistics/>
2. The Big Game Engine Report of 2025. URL: https://app.sensortower.com/vgi/assets/reports/The_Big_Game_Engines_Report_of_2025.pdf
3. Gauffin, H. (2022). Additional Unity tool creation for game development using Unity Editor Scripting.

УДК 004.9

Яшина В.А.

Хмельницький національний університет

ПРОЄКТУВАННЯ ПРОГРАМНИХ СИСТЕМ ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ

Розглянуто поняття та можливості проектування програмного забезпечення для Інтернету речей (IoT). Вказано особливості та специфіку такого проектування з точки зору сучасних аспектів використання можливостей IoT-систем.

The concept and possibilities for designing software for the Internet of Things (IoT) are considered. The features and specifics of such design are indicated from the point of view of modern aspects of using the capabilities of IoT systems.

Інтернет речей або IoT – це поєднання звичайних фізичних предметів, які оснащені вбудованими обчислювальними потужностями, сенсорними чи актуаторними модулями та засобами комунікації, що дозволяють їм ідентифікуватися, збирати дані та обмінюватися інформацією з іншими системами та сервісами через стандартизовані або спеціалізовані протоколи, незалежно від людського втручання. Суть дуже проста і полягає в тому, що кожен предмет – від годинника до холодильника чи навіть вуличного ліхтаря – має вбудований сенсор, який збирає інформацію, і передавач, який може надсилати ці дані в мережу.

Ці зібрані дані, наприклад, яка температура в кімнаті, чи відчинені двері, чи скоро зламається мотор на заводі надходять у хмару, де аналізуються спеціальними програмами та завдяки цьому аналізу «речі» можуть приймати рішення. Наприклад, якщо датчик руху бачить, що господар будинку зайшов додому, система автоматично вмикає світло та обігрів.

Головна цінність Інтернету речей – це автоматизація та ефективність, що дозволяє компаніям запобігати поломкам до того, як вони трапляться або містам оптимізувати світлофори, щоб зменшити затори. IoT створює розумну екосистему, де фізичний світ постійно обмінюється інформацією з цифровим.

Проектування IoT-систем суттєво відрізняється від традиційної розробки, оскільки необхідно керувати великою кількістю географічно розподілених, ресурсно обмежених пристроїв, що генерують великі обсяги даних. Це завдання вимагає інтеграції знань із вбудованих систем, хмарних технологій, безпеки та архітектури розподілених систем.

Внутрішня природа систем IoT характеризується надвеликою масштабільністю, високодинамічними топологіями, високою гетерогенністю та міждоменністю з точки зору сценаріїв застосування [3]. Ці характеристики, разом з

іншими, створюють нові виклики для життєвого циклу розробки програмного забезпечення IoT, включаючи фазу проектування.

Попит на дані з боку цифрових аборигенів у поєднанні з величезним обсягом даних, що генеруються мобільними пристроями, датчиками та застосунками, призвів до нової програмної кризи [2].

Проектування для Інтернету речей (IoT) інтегрує зв'язок та можливості інтелекту у фізичні об'єкти, змінюючи взаємодію людини із навколишнім середовищем. Впровадження IoT дозволяє пристроям автономно спілкуватися, забезпечуючи при цьому значне підвищення ефективності. Центральним елементом IoT є взаємозв'язок збору, аналізу та використання даних, що вимагає продуманого проектування для забезпечення зручності використання, надійності та масштабованості. Щоб досягти успіху в динамічному ландшафті IoT, проектування повинно передбачати різноманітні потреби та адаптуватися до постійно зростаючих технологічних можливостей [1].

Разом з тим, зростання кількості підключених до мережі Інтернет пристроїв з обчислювальними можливостями, повпливало на складність та поширеність програмних систем. Іншим фактором успішності IoT є вибір найактуальнішого способу безперешкодного з'єднання великої кількості доступних пристроїв та послуг. Загалом, розробка програмних систем є складною через складну природу цих систем та так званий «людський фактор».

Отже, системи на основі Інтернету речей (IoT) підтримують обчислення в будь-який час і в будь-якому місці, з'єднуючи людей, системи, сервіси, пристрої та речі, що дозволяє автономним системам формувати оцифроване середовище. Саме тому проектування таких програмних систем є достатньо складним завданням та вимагає інтеграції та взаємодії знань та досвіду з різних областей галузі інформаційних технологій.

Перелік посилань

1. How to Design for the Internet of Things: Key Principles for IoT Development. – URL: <https://profiletree.com/design-for-the-internet-of-things-iot/> (дата звернення 16.09.2025 р).
2. Glaroudis D. et al. Survey, comparison and research challenges of IoT application protocols for smart farming. Comput. Netw. 2020.
3. Ray P. P. A survey of IoT cloud platforms Future Comput. Inf. J. 2016.



АКТУАЛЬНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК 2025

ЗБІРНИК НАУКОВИХ ПРАЦЬ

Комп'ютерна верстка: **Мазурець О. В.**

Підписано до друку 15.11.2025.

Версія друку «APKN2025_CorpusPaper v5mod93 Final».

Е-mail: apkt.khnu@gmail.com

ХНУ. м. Хмельницький, вул. Інститутська, 11.