

Міністерство освіти і науки України  
Хмельницький національний університет



**ЗБІРНИК НАУКОВИХ ПРАЦЬ**  
за матеріалами XV Всеукраїнської науково-практичної конференції  
«Актуальні проблеми комп'ютерних наук АПКН-2023»

*17-18 листопада 2023*

Хмельницький 2023

УДК 004:37:001:62

Збірник наукових праць за матеріалами XV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2023». Хмельницький. 2023. 345с.

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. При макетуванні можливі незначні зміни компоновки контенту авторських оригіналів.

Участь у конференції та складові всіх її етапів (розгляд праць, 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](mailto:apkt.khnu@gmail.com)

**АКТУАЛЬНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК - 2023**

*XV Всеукраїнська науково-практична конференція*

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

**СЕКЦІЇ КОНФЕРЕНЦІЇ:**

1. Комп'ютерні науки 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.

Робочі мови конференції: українська, англійська

**ОРГКОМІТЕТ:**

**Олег СИНЮК** – голова оргкомітету, проректор Хмельницького національного університету з наукової роботи, доктор технічних наук, професор

**Олег САВЕНКО** – заступник голови оргкомітету, декан факультету Інформаційних технологій ХНУ, доктор технічних наук, професор

**Олександр БАРМАК** – заступник голови оргкомітету, завідувач кафедри Комп'ютерних наук ХНУ, доктор технічних наук, професор

**Тетяна ГОВОРУЩЕНКО** – завідувач кафедри Комп'ютерної інженерії та інформаційних систем ХНУ, доктор технічних наук, професор

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

**Євгеній ЛАВРОВ** – доктор технічних наук, професор (Сумський державний університет)

**Людмила ТИМОФЄЄВА** – відповідальна за студентську науково-дослідну роботу ХНУ

**Олександр МАЗУРЕЦЬ** – секретар конференції, к.т.н., доцент кафедри Комп'ютерних наук ХНУ

**Марина МОЛЧАНОВА** – секретар конференції, викладач кафедри Комп'ютерних наук ХНУ

**КОНТАКТНА ІНФОРМАЦІЯ:**

e-mail для листування: [apkt.khnu@gmail.com](mailto:apkt.khnu@gmail.com)

## ЗМІСТ

### **Аскеров В.В.**

Метод покращення перевірок AML шляхом зміни парадигми ставлення системи до кожної окремої транзакції..... 12

### **Атаман В.О.**

Огляд технологій двофакторної аутентифікації та їх впровадження у мобільних додатках ..... 16

### **Башта А.Р.**

Способи побудови детектингу об'єктів у реальному світі..... 19

### **Білінська А.Є.**

Дослідження підсистеми визначення безпечної відстані під час водіння автомобіля за допомогою комп'ютерного зору ..... 22

### **Біньковський Я.В.**

Підсистема розпізнавання світлових сигналів світлофора ..... 27

### **Бойчук А.І., Данчук С.В., Нічепорук А.О.**

Оцінка доступності SaaS систем в контексті аналізу впливу несправностей в ІТ інфраструктурі..... 31

### **Бохонько О.О., Бондарук О.В.**

Дослідження методів підтримки та керування життєвим циклом хмарних середовищ ..... 35

### **Бохонько О.О., Лисенко С.М.**

Метод виявлення кібер-атак на основі соціальної інженерії ..... 38

### **Бугайчук В.О.**

Сумаризація тексту за допомогою рекурентних нейронних мереж та трансформерів ..... 41

### **Ваховська В.М.**

Мобільний додаток «GymRat» – віртуальний фітнес тренер..... 43

### **Владовська А.О., Продеус М.С., Нічепорук А.О.**

Адаптивне прогнозування та розпізнавання поведінки мешканців у розумних будинках ..... 47



**Воробійов В.С., Лисенко С.М.**

Дослідження методів ідентифікації атак типу фішинг у корпоративних мережах..... 51

**Галицький О.С.**

Підвищення якості керування квадрокоптером за допомогою використання ретранслятора..... 54

**Гардиш Д.О., Кліменко В.І.**

Прикладні аспекти автоматизованого оцінювання відповідності кейса тестових завдань семантичній складовій навчальних матеріалів..... 57

**Головатюк А.О.**

Дослідження підсистеми розпізнавання та аналізу дорожніх знаків методами комп'ютерного зору ..... 64

**Денисенко Б.О., Молчанова М.О., Кліменко В.І.**

Підхід до автоматизованого вирішення задач лінійного програмування ..... 68

**Денисюк Д.О.**

Методи виявлення вразливостей в графічних об'єктах ..... 77

**Домбровський Н.С., Скрипник Т.К., Вознюк Л.О.**

Метод ідентифікації подій в україномовних текстах засобами обробки природної мови ..... 80

**Дуда К.М., Кустовський Р.С.**

Метод генерації тестів програмного забезпечення з пошуком певних дій..... 84

**Дудар Ю.М.**

Метод компенсації термодинамічної складової нестабільності частоти кварцових резонаторів..... 88

**Єршова С.А., Мельников О.Ю.**

Додавання модуля пошуку асоціативних правил до інтелектуальної системи прийняття рішень аналізу даних аптечної мережі ..... 91

**Єфремов М.С., Ляшко А.В., Крак Ю.В.**

Візуалізація та попередній аналіз даних ЕКГ..... 95

**Закабула О.Ю., Мельников О.Ю.**

Аналіз моделей і методів прогнозування можливості аварій в системі водопостачання ..... 99

<b>Залуцька О.О., Молчанова М.О., Віт Р.В., Мазурець О.В.</b> Конфігурування нейронної мережі для класифікації емоційної тональності текстової інформації за показниками семантичної зв'язності .....	102
<b>Запорожець М.В., Молчанова М.О., Скрипник Т.К.</b> Метод виявлення патологій мозку за зображеннями магнітно-резонансної терапії нейромережевими засобами .....	108
<b>Карлечук Д.Т., Багрій Р.О., Скрипник Т.К., Тищенко О.О.</b> Метод структурування тексту оголошень для об'єктів нерухомості засобами NLP	111
<b>Карпович В.В., Дрозд А.І., Жуковський П.О., Мельник В.В.</b> Методи вирішення проблем пропускну здатності дисків для застосунків з інтенсивним обсягом даних .....	116
<b>Каушан. С.О., Лисенко С.М.</b> Дослідження інформаційних систем електронного рекрутингу персоналу .....	118
<b>Качур А.В., Лисенко С.М.</b> Виклики в розвитку технології віртуальної реальності: оптимізація архітектури VR .....	121
<b>Качур О.І.</b> Перспективні напрямки розвитку сучасного антивірусного захисту мереж та роль методів на основі генетичних алгоритмів .....	124
<b>Кирилюк О.О., Онишко О.Г.</b> Дослідження використання інструменту Elasticsearch для оптимізації вебдодатків, розроблених з використанням фреймворку Laravel .....	128
<b>Кльоц Ю.П., Петляк Н.С., Чвалов А.А.</b> Технології тестування безпеки вебресурсів .....	130
<b>Коберник Д.С.</b> Мобільний додаток для читання книг з Google Books: методології програмної інженерії та архітектурні рішення .....	133
<b>Козакевич В.А., Собко О.В., Тищенко О.О., Вознюк Л.О., Медведчук В.Ю.</b> Метод автоматизованої генерації текстових повідомлень заданої семантичної спрямованості з використанням лексичних n-грам .....	136
<b>Козельський О.В.</b> Методи та засоби створення мультикомп'ютерних систем з подвійною автентифікацією потоків даних в корпоративних мережах .....	142

**Козенко О.В., Мазурець О.В., Молчанова М.О., Собко О.В.**

Використання метрик косинусної схожості та індексу Жаккара для інтелектуального аналізу семантичної подібності текстових документів ..... 146

**Комін А.С., Бойко О.В.**

Архітектурне рішення для підсистеми підтримки управління гібридною енергосистемою з використанням машинного навчання на мобільних пристроях ..... 148

**Кузьмін А.А.**

Концепція інформаційної системи для автоматизованої генерації цифрового контенту на основі штучного інтелекту ..... 153

**Кучменко К.Ю., Праворська Н.І.**

Ігровий застосунок у жанрі «платформер» з інтерфейсом управління на основі голосової взаємодії з використанням технологій Unity ..... 157

**Лантєв М.П., Лисий А.М., Сергєєв Є.В., Віжевський П.В.**

Метод криптографічного захисту протоколів в засобах комунікації інтернету речей ..... 161

**Левандовський А.О., Муляр І.В.**

Метод аналізу трафіку з метою виявлення атак на комплексні системи захисту інформації ..... 163

**Лигун О.О.**

Методи та засоби виявлення зловмисних дроперів в комп'ютерних системах ..... 166

**Мазур К.Р., Пасічник О.А., Скрипник Т.К.**

Метод виявлення боєприпасів, що не розірвались, за зображенням з тепловізора засобами глибокого навчання ..... 168

**Малицький Т.Б., Чешун О.В., Чешун В.М.**

Математична інтерпретація концепції захисту інформаційних ресурсів корпоративної мережі із застосуванням імовірнісних критеріїв довіри ..... 172

**Мандрик А.І., Лисенко С.М.**

Метод оптимізації планування проєктів та формування команд з використанням генетичного алгоритму ..... 177

**Манзюк Е.А.**

Застосування розпаралелювання для криптографії з використанням губчастої структури ..... 181

**Мантур В.А.**

Використання кодування зображень у форматі Base64 для вебзастосунків з використанням реляційних баз даних ..... 184

**Медведєва К.С., Антипенко В.П.**

Web-орієнтована система автоматизації процесу аналізу якості програмного продукту..... 187

**Мельник В.М., Сорочинський О.Ю., Глухенький О.А., Семенюк Б.В.**

Метод створення безпечної кіберфізичної системи для автоматизації приміщень підприємств з використанням операційних систем на основі мікроядра ..... 190

**Миронюк К.Г.**

Задача транспортування ресурсів споживачам ..... 193

**Міроник М.В., Праворська Н.І.**

Ігровий застосунок в жанрі «Rogue-lite» з використанням технології Unity..... 197

**Морський О.О., Лукманов Т.К., Манзюк Е.А.**

Виявлення забруднень навколишнього середовища методами штучного інтелекту з використанням супутникових зображень ..... 201

**Муляр Е.Р., Багрій Р.О., Пасічник О.А., Манзюк Е.А.**

Метод виявлення ознак насильства у відеоматеріалах нейромережевими засобами..... 203

**Наймитенко С.І., Подорожняк А.О.**

Розробка та дослідження сервісу для розумного протезу ..... 209

**Нечепорук О.А., Ващенко С.М., Івашова Н.В.**

Рекомендаційні системи контенту різного типу ..... 213

**Ничік Є.О., Мельников О.Ю.**

Система підтримки прийняття рішень для оптимізації розподілу посівних площ аграрного підприємства..... 216

**Новак Я.В., Мазурець О.В.**

Дослідження ефективності методу автоматизованої ідентифікації особи за відбитками пальців ..... 221

**Новацький О.В., Сороколіт В.О., Яшина О.М.**

Метод підтримки якості програмного коду на основі автоматичного тестування..... 225

**Овчарук О.М., Мазурець О.В.**

Прогнозування значень параметрів за їх часовими рядами рекурентною темпоральною нейронною мережею ..... 227

**Олійник П.О.**

Удосконалений метод роботи з метриками покриття коду для забезпечення ефективного оцінювання результатів тестування програмного забезпечення ..... 233

**Онікієнко С.С., Глухов В.Ю., Манзюк Е.А.**

Детектування об'єктів на зображеннях з невеликою роздільною здатністю ..... 236

**Охота В.В., Міхалевський В.Ц., Скрипник Т.К.**

Метод здійснення річкової переправи транспортних засобів за мурашиним алгоритмом ..... 239

**Павлова О.О., Рудик І.В.**

Пост-обробка сигналів тривоги систем відеоспостереження за допомогою нейромережі YOLOv8 ..... 242

**Побережна А.Ю.**

Кіберфізична система моніторингу стану рослин в режимі реального часу ..... 245

**Присяжнюк О.О.**

Дослідження та проектування комп'ютерних систем штучного інтелекту ..... 250

**Рижий Я.О., Мельник М.М., Чешун О.В., Орленко В.С.**

Класифікація атрибутів особи і формування цифрового підпису на їх основі ..... 252

**Ровінчук Д.Ю.**

Метод та програмні засоби виявлення метаморфних комп'ютерних вірусів ..... 257

**Родін О.О., Яшина О.М.**

Метод спектральних характеристик звукового сигналу для визначення рівня психологічного стану людини за допомогою глибинного навчання ..... 260

**Савчук А.В.**

Розробка бібліотеки для побудови та обчислень електричних кіл ..... 264

**Сверба А.А.**

Удосконалення методу роботи з метрикою середнього часу між відмовами для забезпечення ефективного оцінювання результатів тестування програмного забезпечення ..... 266

**Свистун С.О., Мельниченко О.В., Скрипник Т.К.**

Проектування робочої місії безпілотних літальних апаратів в тривимірному просторі ..... 269

<b>Слутяк Є.І., Радельчук Г.І., Балицький Б.І.</b> Удосконалення передачі даних у мережі інтернет з використанням алгоритму верифікації повідомлень.....	274
<b>Смірнов О.П., Поплавський С.Ю., Ковальчук В.К., Лутюк Л.І.</b> Удосконалений метод та засоби криптографічного захисту від вразливостей в апаратному забезпеченні.....	278
<b>Смолієнко Д.В., Петровський С.С.</b> Метод прогнозування забруднення громадських доріг на основі підходу глибокого активного навчання .....	280
<b>Собко В.В.</b> Метод поєднання технологій Redux-Toolkit та Redux-Saga для роботи з API веб-ресурсів .....	284
<b>Собкова Ю.В., Міхалевський В.Ц., Скрипник Т.К.</b> Метод автоматизованого підбору тимчасового житла для категорій споживачів за генетичним алгоритмом.....	286
<b>Стецюк Ю.В.</b> Методи обробки даних з обмеженим доступом в мультикомп'ютерних системах із застосуванням хмарних технологій їх зберігання .....	289
<b>Тоцький О.П.</b> Методи обробки кардіограм .....	293
<b>Уваров В.С., Чабан О.Р., Манзюк Е.А.</b> Метод діагностики захворювань серця на основі аналізу зображень, отриманих методом магнітно-резонансної томографії.....	296
<b>Федоренко В.В., Пасічник О.А., Скрипник Т.К.</b> Технологія блокчейн у сфері реєстрації майнових прав .....	300
<b>Хміль О.О., Праворська Н.І.</b> Веб-сайт біржі фрілансу.....	304
<b>Швайко В.К., Ільчишина Ю.В.</b> Метод вибору виду спорту на основі морфофункціональних показників людини.....	308
<b>Шебетко О.В., Кліменко В.І., Мазурець О.В.</b> Метод адаптивного тестування з використанням продукційних правил.....	311

**Шевчук П.О., Молчанова М.О., Собко О.В.**

Система керування продажами товарів комп'ютерної техніки з використанням об'єктно-орієнтованого підходу ..... 323

**Якимчук Г.Б., Праворська Н.І.**

Програмний застосунок для керування проектами..... 329

**Ялик В.І., Праворська Н.І.**

Програмний застосунок для навчання математиці учнів початкових класів з використанням інтерактивних ігор ..... 333

**Яресько А.Ю.**

Розвиток цифрових підписів ..... 337

**Яшина В.А.**

Дизайн мобільних застосунків..... 340

**Alpashkin M.I., Dmytriiev V.G., Romaniuk O.V.**

Usability testing as an important factor in the development of a successful software product ..... 343

УДК 004.4

Аскеров В.В.

*Хмельницький національний університет*

## **МЕТОД ПОКРАЩЕННЯ ПЕРЕВІРОК AML ШЛЯХОМ ЗМІНИ ПАРАДИГМИ СТАВЛЕННЯ СИСТЕМИ ДО КОЖНОЇ ОКРЕМОЇ ТРАНЗАКЦІЇ**

*Розглянуто результати статистичних досліджень щодо актуальності та дослідження AML-процедури. Запропоновано підхід до покращення перевірок AML шляхом зміни парадигми ставлення системи до кожної окремої транзакції.*

*The results of statistical studies on the relevance and research of the AML procedure are considered. An approach to improving AML checks by changing the paradigm of the system's attitude to each individual transaction is proposed.*

AML-процедури та законодавство в Україні базуються на міжнародних стандартах та рекомендаціях Фінансової діяльності та боротьби з відмиванням грошей (FATF). Основним законом, що регулює боротьбу з відмиванням грошей в Україні, є Закон України «Про запобігання та протидію відмиванню доходів, одержаних злочинним шляхом, та фінансуванню тероризму» від 14.10.2014 р. № 1702-VII» [1].

Згідно з цим законом, банки та інші фінансові установи зобов'язані проводити AML-процедури, такі як клієнтська перевірка та моніторинг фінансових транзакцій, та співпрацювати з органами державної влади в цій сфері. Як відомо, головним завданням систем AML (Anti-Money Laundering)[2,3] у сфері криптовалют є своєчасне виявлення та запобігання можливостям використання електронних активів у протизаконних операціях, що можуть нашкодити світові загалом та людству зокрема. Одним із факторів, що можуть істотно покращити процес протидії, є використання машинного навчання (ML) — реалізації сценаріїв поведінки комп'ютерних систем на основі попереднього вивчення однотипних ситуацій. Станом на зараз, методологічна база знаходиться на етапі становлення, оскільки достеменно не відомі усі можливості ML, що практично із кожним днем розширюються стараннями великої кількості науковців та ентузіастів. Однак станом на зараз, уявлення сучасників про ML знаходяться у парадигмі природи людського мислення – раціональний пошук можливих варіантів, заснований на дедукції. У нашому науковому пошукові ми намагаємося відійти від шаблонних методів, що наразі привалюють в царині AML та поглянути на ситуацію під розгорнутим кутом,



що може якісно вплинути на вдосконалення методів протидії деструктивним тенденціям у світі криптовалют.

У ході дослідження було проведено аналіз ситуації з розвитком децентралізованих мереж (відповідно до даних, систематично зібраних з відкритих джерел), результати якого представлено на рисунках 1 та 2.

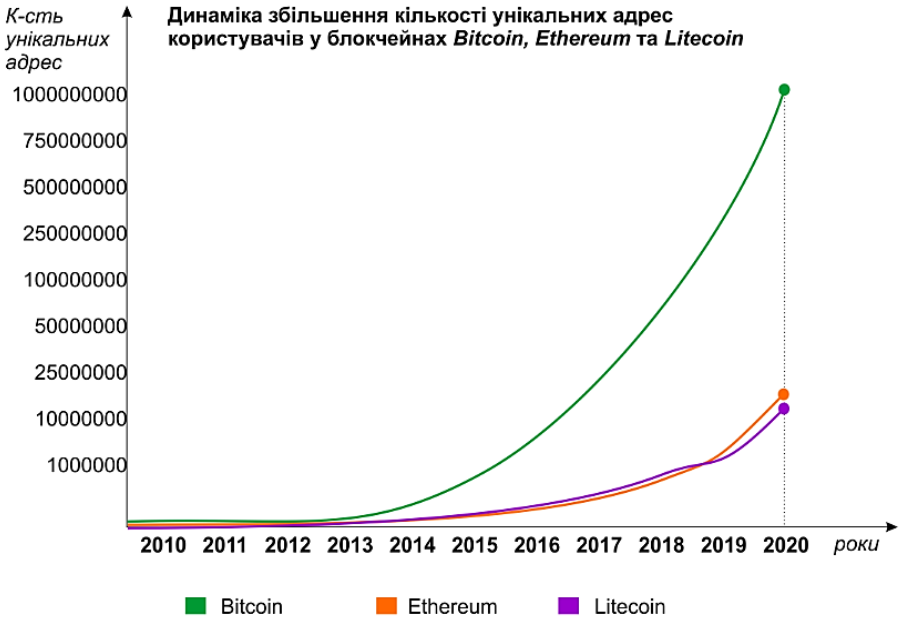


Рисунок 1 – Динаміка збільшення кількості унікальних адрес користувачів

Як можна побачити з рисунку 1, на рубежі 20-х років XXI століття розвиток блокчейнів переживає бурхливий сплеск. Наразі для нашого дослідження не так важливі абсолютні показники, як динаміка їхнього збільшення. Також варто сказати, що саме після 2020-го року відбулися фундаментальні зміни в роботі блокчейну Ethereum, що значно розширило можливості мережі та привабило ще більшу кількість користувачів та розробників. Оскільки більшу цінність для даного дослідження становить інформація саме про перевірку транзакцій, необхідно звернутися до відповідних даних. На жаль, отримати статистичні дані практично неможливо з ряду причин:

- перевірки надаються різними провайдерами, кожен з яких збирає статистику окремо;

–кожен провайдер зацікавлений у покращенні власного сервісу, тому стежить за збереженням внутрішньої інформації;

–неможливо узагальнити дані, оскільки кожна перевірка використовує унікальні підходи та алгоритми.

Однак буде корисним поглянути на динаміку збільшення кількості активних крипто-гаманців у світі, що дає приблизне розуміння обсягів транзакцій. Адже якщо гаманець активний, це означає, що транзакції відбуваються, що передбачає їхню перевірку. Станом на 2022-й рік динаміка виглядає наступним чином:

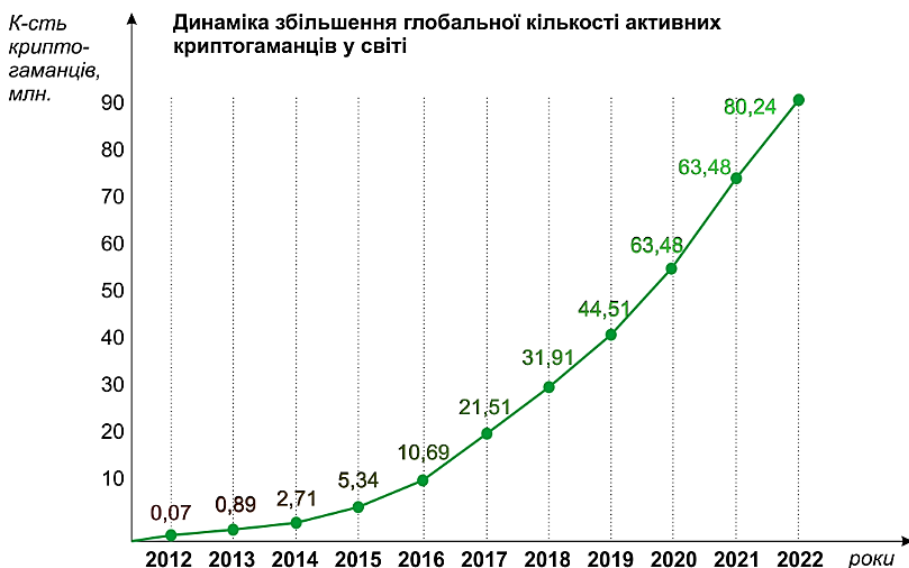


Рисунок 2 – Динаміка збільшення кількості активних крипто гаманців у світі

Як можна побачити з рисунку 2, станом на сьогодні у світі одночасно функціонує більше 90 мільйонів крипто гаманців. На кожен з них припадає від 1 до нелімітованої кількості транзакцій за одиницю часу. Це дає поверхнєве уявлення про обсяг масивів інформації, що з'являються після обробки транзакцій та можуть бути використані для аналізу та застосування у ML.

Тому тематика покращення якості AML-перевірок є наразі актуальними для безпечного керування фінансовими даними.

У наших попередніх роботах було запропоновано алгоритм формування вартості перевірок AML, головна відмінність якого полягає у зміні парадигми ставлення системи AML до кожної наступної транзакції. Якщо раніше попередня оцінка була основою для застосування подальших механізмів, зараз вона виконує цілком протилежну роль - заборону транзакції та попередньої оцінки на предмет можливості, а не заборони. Для цього штучний інтелект розглядає транзакцію з різних боків та приймає рішення про послаблення негативної оцінки.

Однозначними лишаються маркери причетності криптовалюти до сумнівних та небажаних операцій:

– маркер “брудної” криптовалюти, відмічених у попередніх “шкідливих” транзакціях;

– залишковий маркер, у випадку спроб приховання слідів після використання блендерів для криптовалют;

– інші явні причини заборонити транзакцію на основі попередньо встановлених обставин.

Варто розуміти, що всі ці дані — вже доступні та не потребують встановлення, лише перевірки. Таким чином витрати ресурсів для обчислень на цьому етапі мають бути заздалегідь меншими, ніж якби кожне подібне дослідження потрібно було робити окремо.

Надалі алгоритм звертається до результатів машинного навчання, що базується на основі розгляду типових виявлених та попередження випадків шахрайства. Як вже було встановлено раніше, кількість “шкідливих” транзакцій становить меншість, в порівнянні з “корисними”. Таким чином, для підвищення заздалегідь низької оцінки, слід опрацювати менший масив даних, ніж для зниження високої оцінки.

### **Перелік посилань**

1. Закон України «Про запобігання та протидію відмиванню доходів, одержаних злочинним шляхом, та фінансуванню тероризму» від 14.10.2014 р. № 1702-VII» URL: <https://www.president.gov.ua/documents/2258-vi-11305> (Доступ 25.10.2023)
2. Що таке AML? URL: <https://blog.whitebit.com/uk/what-is-anti-money-laundering/#heading-text-0-8> (Доступ 25.04.2023)
3. AML Anti Money Laundering URL: <https://finap.com.ua/category/aml/> (Доступ 01.11.2023)

УДК 004.056

Атаман В.О.

*Хмельницький національний університет*

## **ОГЛЯД ТЕХНОЛОГІЙ ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ ТА ЇХ ВПРОВАДЖЕННЯ У МОБІЛЬНИХ ДОДАТКАХ**

*Розглянуто технології двофакторної аутентифікації та їх впровадження у мобільних додатках для забезпечення безпеки та захисту особистих даних, оскільки це є нагальною потребою в інформаційній епохі, де цифрові технології проникають у кожен сферу життя. Особливу увагу привертають мобільні додатки, які стали частиною життя для більшості людей, надаючи можливість виконувати найрізноманітніші завдання в онлайн-середовищі.*

*The technologies of two-factor authentication and their implementation in mobile applications to ensure the security and protection of personal data have been discussed, as this is an urgent need in the information age, where digital technologies permeate every aspect of our lives. Mobile applications, in particular, have garnered significant attention, as they have become an integral part of life for most people, offering the capability to perform a wide range of tasks in the online environment.*

Згідно зі статистикою, в 2021 році мобільні програми були завантажені на пристрої користувачів більше 200 мільярдів разів. За даними Marketing Land, 57% часу, проведеного в цифровому просторі, - це час, витрачений на програми у смартфонах чи планшетах. Мобільні пристрої міцно увійшли в життя: месенджери, банкінг, бізнес-додатки, особисті кабінети стільникових операторів - за сучасного ритму життя використовуються додатки щодня. За даними Juniper Research, загальна кількість користувачів мобільних банківських програм наближається до двох мільярдів, що становить близько 40% всього дорослого населення. Мобільним банком користується кожен третій (34%) віком від 18 років.

Метою роботи є аналіз існуючих сучасних технологій двофакторної аутентифікації та їх можливе впровадження в мобільних додатках, з метою збільшення рівня безпеки та захисту особистих даних користувачів.

Безпека в мобільних додатках є надзвичайно важливою, оскільки вона впливає на захист особистих даних користувачів, довіру споживачів, законність та стійкість бізнес-операцій, а також на репутацію та успіх розробників мобільних додатків.

Ризики виникають не тільки через окремі вразливості на клієнті або сервері; часто загрози обумовлені кількома, здавалося б, незначними недоліками в різних частинах мобільного додатка, які в сукупності можуть призводити до серйозних

наслідків, аж до фінансових збитків для користувачів та репутаційних втрат для виробника.

Двофакторна аутентифікація (2FA) відіграє критичну роль у забезпеченні безпеки в різних онлайн-системах, включаючи мобільні додатки. Переваги 2FA:

1. Підвищення рівня безпеки
2. Захист від фішингу
3. Зменшення ризику атаки з використанням витоку паролів
4. Додаткова безпека при втраті пристрою
5. Захист від брутфорс-атак
6. Захист конфіденційності особистих даних
7. Відповідність законодавству про захист даних

Існує декілька методів двофакторної аутентифікації, які можна впровадити в мобільних додатках. Кожен з них має свої переваги і недоліки.

**SMS-повідомлення (OTP).** Переваги: Цей метод досить простий та зручний для користувачів. OTP-коди надходять через sms і можуть бути швидко введені для підтвердження ідентичності. Недоліки: SMS-повідомлення можуть бути підтверджені перехопленню або не надходити в разі відсутності мобільного зв'язку. Також є ризик, що SIM-карту можуть взяти в заручники для отримання OTP-кодів.

**Генерація OTP в мобільному додатку.** Переваги: Мобільні додатки, як Google Authenticator або Authy, генерують OTP-коди без підключення до мережі, що робить їх більш надійними в порівнянні з sms-повідомленнями. Вони також можуть бути використані офлайн. Недоліки: В разі втрати або пошкодження смартфона, доступ до OTP-кодів може бути втрачено. Також, резервні копії кодів повинні зберігатися безпечно.

**E-mail-підтвердження.** Переваги: Користувач отримує електронний лист із посиланням для підтвердження доступу. Це досить зручно та забезпечує додатковий рівень безпеки. Недоліки: E-mail може бути вразливий на атаки фішингу або перехоплення листів. Також, цей метод може бути повільним у порівнянні із способами, які вимагають лише введення коду.

**Біометричні дані (відбитки пальців, розпізнавання обличчя).** Переваги: Біометричні дані надають високий рівень зручності, оскільки користувачам не потрібно запам'ятовувати паролі або OTP-коди. Недоліки: Біометричні дані можуть бути скомпрометовані або використані без дозволу користувача. Також не завжди доступні на всіх пристроях.

**Фізичний ключ (пристрій для двофакторної аутентифікації).** Переваги: фізичні ключі дуже надійні, оскільки їх фактично неможливо підробити в онлайн-середовищі. Недоліки: вони можуть бути втрачені або пошкоджені; користувачам потрібно мати фізичний ключ при собі, що може бути не дуже зручно.

При виборі методу двофакторної аутентифікації в мобільних додатках користувач повинен враховувати низку конкретних потреб та загроз, щоб забезпечити оптимальний баланс між безпекою та зручністю.

Зручність та використання. Користувачі віддають перевагу методам, які є зручними та легкими у використанні. Важливо, щоб метод двофакторної аутентифікації не мешкав звичному користуванню додатком.

Рівень безпеки. Рівень безпеки методу повинен відповідати характеру інформації та даних, які зберігаються в додатку. Для дуже конфіденційної інформації можуть вимагатися сильніші методи аутентифікації.

Вартість та доступність. Користувачі можуть враховувати вартість впровадження та обслуговування методом двофакторної аутентифікації. Деякі методи можуть бути дорожчими або вимагати спеціального обладнання.

Відновлення доступу. Важливо мати механізм відновлення доступу до облікового запису у разі втрати одного з факторів аутентифікації або інших непередбачуваних ситуацій.

Загрози безпеці. Користувачі повинні враховувати потенційні загрози безпеці, які можуть виникнути у конкретному сценарії використання додатку. Наприклад, атаки на облікові записи, крадіжка пристрою чи перехоплення sms-повідомлень.

Біометричні дані. Використання біометричних даних (відбитки пальців, розпізнавання обличчя) може зробити аутентифікацію більш зручною, але варто розглянути можливість витоку цих даних.

Резервні методи. Користувач повинен мати можливість вибору резервних методів аутентифікації, які можна використовувати у випадках, коли основний метод недоступний.

Час та місце. В залежності від ситуації, користувач може віддавати перевагу певним методам аутентифікації в залежності від часу та місця використання додатка.

Інтеграція з іншими службами. Деякі методи двофакторної аутентифікації можуть легше інтегруватися з іншими службами та додатками, що може бути важливим фактором вибору.

Отже, впровадження двофакторної аутентифікації в мобільні додатки є важливим кроком у підвищенні безпеки в онлайн-середовищі. Користувачі повинні враховувати індивідуальні потреби та загрози, що стосуються їх облікових записів та даних у мобільних додатках, при виборі методу двофакторної аутентифікації. Тільки зрозумівши ці аспекти, користувач може вибрати найбільш відповідний та ефективний метод для забезпечення безпеки своїх даних. Це допомагає захистити особисті дані та конфіденційні інформаційні ресурси користувачів, забезпечуючи їм більший рівень впевненості у безпеці використання мобільних додатків. У майбутньому розробники мобільних додатків повинні продовжувати досліджувати та вдосконалювати методи двофакторної аутентифікації, щоб відповідати зростаючим вимогам безпеки в цифровому світі.

### Перелік посилань

1. Двофакторна аутентифікація для бізнесу: як захистити облікові записи співробітників. URL: <https://cutt.ly/4wE7IUIV>. Дата звернення 5.09.2023.
2. Детально про 4 типи двофакторної автентифікації в інтернеті. URL: <https://www.imena.ua/blog/two-factor-authentication-guide/>. Дата звернення 8.09.2023.
3. Двофакторна автентифікація для безпеки облікового запису — що це, її види та як використовувати. URL: <https://ssl.com.ua/blog/ukr/what-is-2fa/>. Дата звернення 10.09.2023.

УДК 004.4

Башта А.Р.

*Хмельницький національний університет*

## **СПОСОБИ ПОБУДОВИ ДЕТЕКТИНГУ ОБ'ЄКТІВ У РЕАЛЬНОМУ СВІТІ**

*Розглянуто методи створення джерела даних для детектора об'єктів та продемонстровано реальні програми, доступні в App Store і Google Play, що використовують технологію виявлення об'єктів. Запропоновано підхід до створення детектора об'єктів у реальному світі.*

*The methods of creating a data source for object detector are considered and real programs available in the App Store and Google Play are demonstrated using object detection technology. An approach to creating object detector in the real world is proposed.*

Виявлення об'єктів є фундаментальним завданням у галузі комп'ютерного зору та штучного інтелекту. Це знаходить застосування у різних галузях і сферах, сприяючи інноваціям та покращенню безпеки, ефективності та користувацького досвіду. Наразі виявлення об'єктів є завданням, яке ставиться у багатьох галузях. У таблиці 1 наведені галузі, де найчастіше застосовуються розпізнавачі об'єктів.

Розуміння конкретних галузей та застосунків виявлення об'єктів допомагає дослідникам, розробникам та фахівцям налаштовувати свої підходи та методи збору даних, щоб вирішити унікальні виклики та вимоги для кожного випадку використання. Якість та актуальність навчальних даних є вирішальними для досягнення точних та ефективних систем виявлення об'єктів у різних застосунках. Справжнім ключем до успіху систем виявлення об'єктів є якість та актуальність навчальних даних. Для створення ефективної системи виявлення об'єктів потрібно виконати кілька етапів, які представлені схематично на рисунку 1.

Отже, перший етап – це збір даних. Збір великого обсягу зображень або відео, на яких реальні об'єкти показані в різних умовах та точках зору. Для навчання моделі важливо мати різноманітність в навчальних даних. Наступний етап – позначення даних. Після збору даних слід розмітити об'єкти на зображеннях чи відео. Ця розмітка містить інформацію про місцезнаходження та клас об'єкта на кожному зображенні. Цей процес може вимагати багато часу та труднощів, але він важливий для навчання точної моделі виявлення об'єктів. Підготовка даних потребує підготувати для навчання моделі, включаючи їх масштабування, обрізку та нормалізацію. Це допомагає моделі навчатися ефективніше та швидше.

Для навчання моделі можна використовувати різні алгоритми машинного навчання та глибокого навчання. Після навчання моделі важливо оцінювати її

точність та вдосконалювати за потреби. Також потрібно забезпечувати підтримку та оновлення моделі, оскільки середовище та умови можуть змінюватися з часом.

Таблиця 1 – Галузі застосування розпізнавачів об'єктів

<b>Галузь застосування</b>	<b>Опис</b>
Автономні автомобілі	У галузі автономних автомобілів виявлення об'єктів відіграє ключову роль у забезпеченні можливості самостійного руху автомобілів, їх сприйняття навколишнього середовища та прийняття рішень у реальному часі. Здатність виявляти пішоходів, транспортні засоби, дорожні знаки та перешкоди є критичною для забезпечення безпечного та надійного автономного руху
Спостереження та безпека	Системи спостереження широко використовують виявлення об'єктів для моніторингу та ідентифікації підозрілих дій, зловмисників чи потенційних загроз у реальному часі
Доповнена реальність	Виявлення об'єктів є ключовою технологією у застосунках розширеної реальності (AR). Розпізнавши та відстеживши об'єкти у реальному світі, системи AR можуть накладати віртуальні об'єкти чи інформацію безперешкодно, збагачуючи користувацький досвід у галузях гри, освіти та маркетингу
Електронна торгівля та роздрібна торгівля	У сфері електронної торгівлі та роздрібно торгівлі виявлення об'єктів допомагає виконувати візуальний пошук та управління запасами
Інклюзивність	Технології виявлення об'єктів також використовуються для покращення доступності для осіб з візуальними порушеннями. Ідентифікуючи та описуючи об'єкти в реальному часі, ці застосунки допомагають користувачам ефективно орієнтуватись у середовищі
Медичне зображення	У медичному зображенні виявлення об'єктів використовується для ідентифікації та локалізації аномалій чи конкретних структур на медичних зображеннях, сприяючи діагностиці та плануванню лікування. Застосування включає виявлення пухлин на MRI-знімках та ідентифікацію клітин на мікроскопічних зображеннях



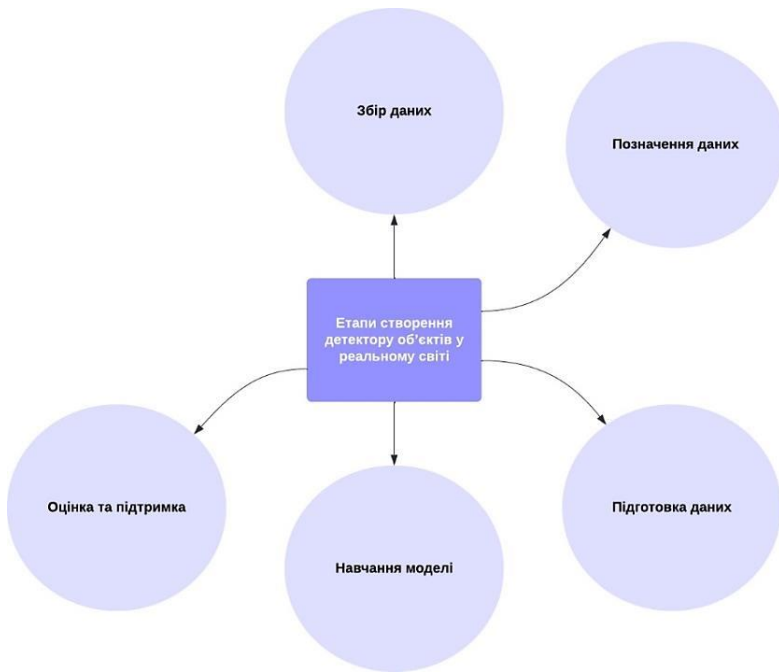


Рисунок 1 – Етапи створення детектора об'єктів у реальному світі

Щоб реалізувати розпізнавач на мобільних платформах, а конкретно на iOS, використовується фреймворк Apple Create ML[1,2] - це інструмент, який надає зручний інтерфейс для створення моделей виявлення об'єктів на платформах Apple, таких як iOS та macOS. Він дозволяє розробникам легко створювати та навчати моделі з використанням наявних даних або власних наборів даних.

Подальші зусилля будуть спрямовані на розробку методів та алгоритмів застосування для роботи зі збором даних для створення моделі, ML-фреймворком для її тренування та поліпшення відсотку успішного розпізнавання об'єктів, та подальшої інтеграції у практичну реалізацію.

### Перелік посилань

1. Create ML. Create machine learning models for use in your app. URL: <https://developer.apple.com/documentation/createml> (дата звернення: 27.09.2023)
2. Create ML Tutorial: Getting Started URL: <https://www.kodeco.com/5653-create-ml-tutorial-getting-started> (дата звернення: 28.09.2023)
3. Башта А.Р., Павлова О.О., Метод практичної побудови розпізнавача об'єктів у реальному світі, «Комп'ютерні ігри і мультимедіа як інноваційний підхід до комунікації - 2023», 28-29 вересня 2023, Одеса, Україна, с. 160-162

УДК 004.89: 004.3

Білінська А.Є.

*Хмельницький національний університет*

## **ДОСЛІДЖЕННЯ ПІДСИСТЕМИ ВИЗНАЧЕННЯ БЕЗПЕЧНОЇ ВІДСТАНІ ПІД ЧАС ВОДІННЯ АВТОМОБІЛЯ ЗА ДОПОМОГОЮ КОМП'ЮТЕРНОГО ЗОРУ**

*У статті розглянуто етапи створення однієї з підсистем системи попередження дорожньо-транспортних пригод, а саме визначення безпечної відстані між автомобілями, яка б допомогла зменшити трагічну статистику на дорозі. Дані про кількість ДТП спричинених недотриманням дистанції показують актуальність даної тематики. У даній статті було здійснено огляд різних варіантів вирішення поставленої задачі, проведено моделювання підсистеми, а також описано алгоритм дії майбутньої підсистеми.*

*The article discusses the stages of creating one of the subsystems of the road traffic accident prevention system, namely, determining the safe distance between cars, which would help reduce tragic statistics on the road. The data on the number of traffic accidents caused by failure to maintain the distance shows the relevance of this topic. This article reviews various options for solving this problem, models of subsystem and describes the algorithm of the future subsystem.*

З кожним роком зростає кількість транспортних засобів на дорогах, а разом із ними збільшується кількість трагічних ситуацій. За перше півріччя 2021 року сталося понад 86 тисяч ДТП. Однією з основних причин є недотримання дистанції, за даний період було зафіксовано 14 675 випадків. За даною причиною офіційні дані фіксують 709 постраждалих та 27 загиблих [1]. Тому система визначення безпечної відстані під час водіння автомобіля за допомогою комп'ютерного зору є актуальною для реалізації.

Для початку розробки підсистеми було проведено огляд наукових статей за схожою тематикою. Для виявлення транспортних засобів з різними характеристиками автомобіля (довжина/висота) використовують створення нейронної мережі [2]. Ця система є досить простою, але водночас демонструє значну точність вимірювань. Інші вчені [3] представили інноваційний підхід, використовуючи згорткову нейронну мережу (CNN) та маску R-CNN для вирішення проблеми виявлення та розпізнавання дорожніх знаків. Система вимірювання відстані між транспортними засобами може розроблятися за допомогою застосування двох камер [4]. Відстань між автомобілями обчислюється за допомогою зображення положення автомобіля на обох камерах, відстані між камерами та кута поля зору камер.

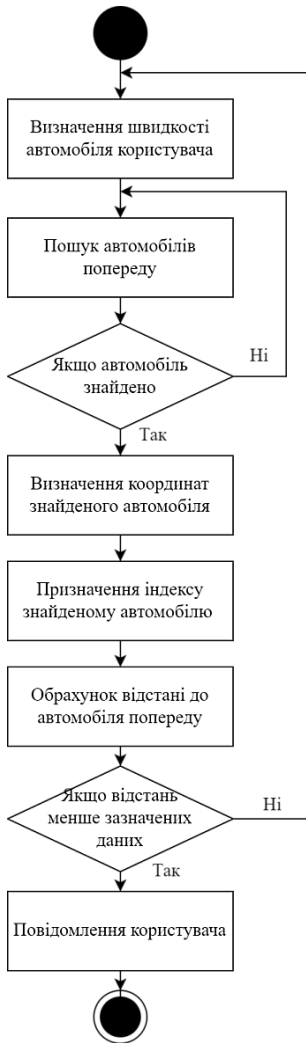


Рисунок 1 – Діаграма станів системи

У іншій статті [5] застосовується алгоритм, що комбінує згорткову нейронну мережу (CNN) з методами комп'ютерного зору, що дозволяє розпізнавати на малопотужних платформах малої форми. Ці платформи є легкими, портативними та можуть бути встановлені на автономних транспортних засобах при денному освітленні.

Наступним кроком є розроблення діаграми станів системи, яку зображено на рисунку 1. Перед початком основного алгоритму, система отримує вхідні дані у вигляді відеопотоку. Кожен кадр цього потоку аналізується з використанням алгоритмів обробки зображень, таких як методи комп'ютерного зору, для визначення автомобілів попереду. Перш ніж розпочати аналіз, визначається швидкість автомобіля, де встановлена система. Від даного показника на пряму залежить визначення безпечної відстані, згідно зазначеним нормам.

Далі система розпочинає пошук автомобіля попереду. За допомогою алгоритмів визначення об'єктів на кадрах, вона встановлює наявність автомобіля та його координати. При цьому кожному автомобілю присвоюється порядковий номер для подальшого запису та використання даних. Якщо дорожній транспорт не був визначений, то пошук продовжується.

Після визначення координат автомобіля попереду система обчислює відстань від користувача до цього автомобіля. Це може бути здійснено на основі визначених координат та інших параметрів, таких як розмір автомобіля на зображенні.

Завершальним етапом є порівняння отриманих даних зі списком відповідності швидкості до безпечної відстані. Якщо відстань менше зазначених значень, система вважає, що існує ймовірність небезпеки. Користувач повідомляється про це за допомогою відповідного повідомлення або сигналу, попереджаючи його про можливу небезпеку на дорозі.

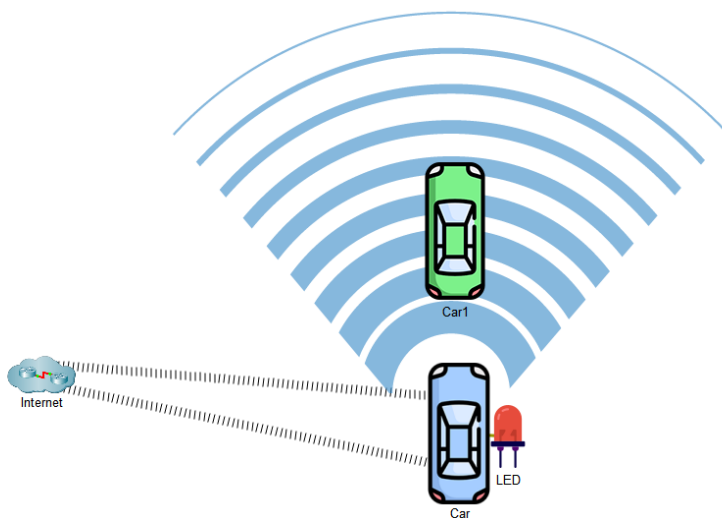


Рисунок 2 – Моделювання системи

Наступним кроком було проведено моделювання роботи системи за допомогою програмного забезпечення Cisco Packet Tracer. На рисунку 2 представлено її виконання в дії. Але у даному випадку не було враховано швидкість руху автомобілів, безпечна та небезпечна відстані між автомобілями, які є сталими в даній ситуації. Акцент було зроблено саме на програмну складову, яка б повідомляла користувача про небезпеку, у вигляді світлодіода. А також на те, чи потрапляє автомобіль попереду в небезпечну зону, для того щоб не сталася ДТП.

У реальній системі для визначення безпечної відстані потрібно знати швидкість автомобіля користувача. За загальнодоступними даними виділяють три випадки співвідношень швидкості до відстані [6], які представлені на рисунку 3.

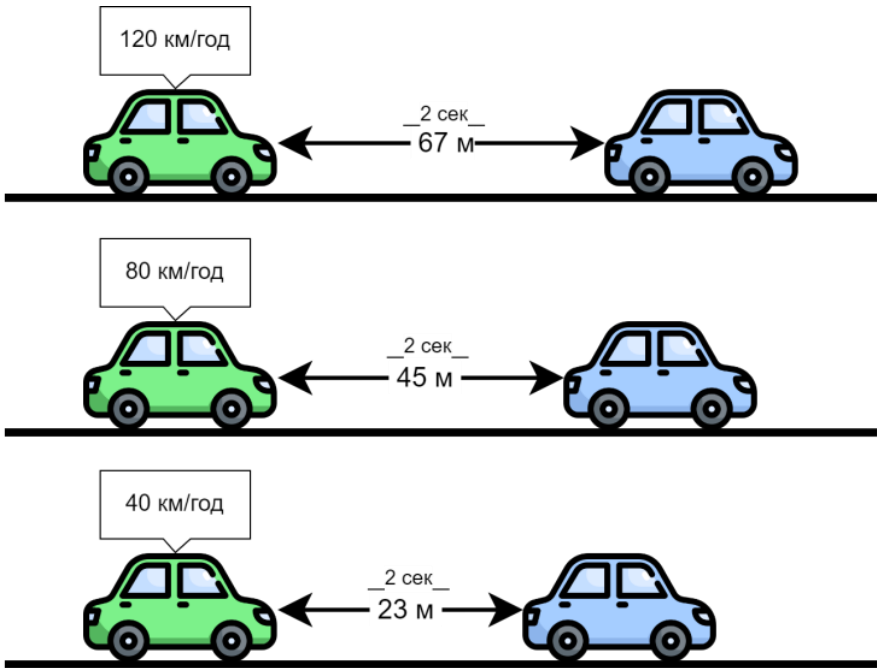


Рисунок 3 – Випадки співвідношень швидкості користувача до відстані між автомобілями

Якщо користувач їде зі швидкістю 120 км/год, тоді безпечною відстанню вважається 67 метрів. Під час другого випадку швидкість становить 80 км/год, тому безпечною відстанню вважається 45 метрів. Якщо швидкість користувача 40 км/год, то відстань має становити 23 метри.

Але дані випадки є загальними, таких ситуацій може бути безліч. Також на визначення відстані може впливати погодні умови такі, як дощ, туман та сніг. Ще однією з умов впливу є вид транспорту попереду. Адже перед автомобілем користувача можуть бути вантажні автомобілі такі, як вантажівка, трактор, тощо.

Тому в подальшому планується розширити список випадків співвідношення швидкості автомобіля до відстані, а також додати до нього залежність від виду транспорту та погодних умов. Для отримання додаткових значень у планах провести моделювання руху транспортних засобів за допомогою мови програмування Python з використанням бібліотеки SimPy.

Отже, у процесі дослідження було проведено огляд наукових статей схожої тематики та розроблено діаграму станів системи. Набуті знання будуть застосовані для розробки тестової системи визначення безпечної відстані під час водіння автомобіля.

### Перелік посилань

1. Названо найчастіші причини ДТП в Україні: кількість аварій у 2021 році різко зросла. URL: <https://www.rbc.ua/ukr/styler/nazvany-samye-chastye-prichiny-dtp-ukraine-1627463985.html> (дата звернення: 19.10.2023).
2. X. Hu, X. Xu, Y. Xiao, H. Chen, S. He, J. Qin, P. A. Heng, "SINet: A Scale-Insensitive Convolutional Neural Network for Fast Vehicle Detection," in IEEE Transactions on Intelligent Transportation Systems, 2018. vol. 20, no. 3, pp. 1010-1015, doi: 10.1109/TITS.2018.2838132.
3. D. Tabernik and D. Škočaj, "Deep Learning for Large-Scale Traffic-Sign Detection and Recognition," in IEEE Transactions on Intelligent Transportation Systems, 2020. vol. 21, no. 4, pp. 1427-1429, doi: 10.1109/TITS.2019.2913588.
4. A. Zaarane, I. Slimani, W. Al Okaishi, I. Atouf, A. Hamdoun, Distance measurement system for autonreferenceomous vehicles using stereo camera. Array, 2020. pp. 1-3.
5. G. Golcarenarenji, I. Martinez-Alpiste, Q. Wang, J. M. Alcaraz-Calero, Robust real-time traffic light detector on small-form platform for autonomous vehicles. Journal of Intelligent Transportation Systems, 2023. pp. 1-4. doi: 10.1080/15472450.2023.2205018.
6. Safe Following Distance Guide. URL: <https://www.dubizzle.com/blog/cars/safe-following-distance/> (дата звернення: 19.10.2023).

УДК 004.4

Біньковський Я.В.

*Хмельницький національний університет*

## **ПІДСИСТЕМА РОЗПІЗНАВАННЯ СВІТЛОВИХ СИГНАЛІВ СВІТЛОФОРА**

*Було реалізовано підсистему розпізнавання сигналів світлофора за допомогою OpenCV, а також конвертування зображення світлофора в простір кольорів HSV та визначення діапазонів для червоного, жовтого та зеленого кольорів. Запропонована підсистема дозволяє використовувати її в транспортних засобах задля запобігання ризиків виникнення дорожньо-транспортних пригод.*

*A subsystem for recognizing traffic signals using OpenCV was implemented, as well as converting the traffic light image to the HSV color space and defining ranges for red, yellow, and green. The proposed subsystem can be used in vehicles to prevent the risk of road accidents.*

Постійний розвиток технологій дозволяє удосконалювати такі системи та забезпечувати їх доступність для широкого кола автомобілістів. Забезпечення безпеки на дорогах є пріоритетом для суспільства, оскільки це впливає на життя та здоров'я мільйонів людей щодня.

Було проаналізовано дотичні системи, які працюють за допомогою штучного інтелекту, використовуються для розпізнавання зображень та мають великий потенціал в майбутньому.

В статті [1] система об'єднує потужність глибокого виявлення, базованого на навчанні з попередніми картами, яке використовується на автомобільній платформі IARA. Вона дозволяє розпізнавати відповідні світлофори на попередньо визначених маршрутах. Процес складається з двох етапів: офлайн-етапу для побудови карт та анотації світлофорів та онлайн-фази для розпізнавання та ідентифікації світлофорів під час руху автомобіля.

Стаття [2] присвячена аналізу різних методів та інструментів для створення розумних парковок з доказами переваги методу на основі використання камер, та спрямована на розпізнавання зображень для камерної системи розумного паркування з використанням згорткових нейронних мереж.

Тому, актуальність даної теми полягає в необхідності впровадження нових систем, які забезпечують запобігання аварійним ситуаціям на дорозі та покращують безпеку дорожнього руху. Це сприятиме зниженню аварійності, збереженню життів та здоров'я людей, а також зменшенню матеріальних збитків, пов'язаних з аваріями на дорогах.

Підсистема завантажує зображення світлофора з файлу "traffic.jpg" за допомогою функції "cv2.imread()" і зберігає його в змінній "image", конвертує

зображення з простору кольорів BGR (використовуваного в OpenCV) в простір кольорів HSV за допомогою функції `cv2.cvtColor()` і зберігає його в змінній `“hsv_image”`, визначає діапазони кольорів для червоного, жовтого та зеленого кольорів у просторі HSV за допомогою об'єктів `“np.array()”`. Наприклад, для червоного кольору задається нижня межа `“red_lower = np.array([0, 120, 70])”` і верхня межа `“red_upper = np.array([10, 255, 255])”`, створює бінарні маски для областей, що відповідають червоному, жовтому та зеленому кольорам за допомогою функції `“cv2.inRange()”`. Ця функція порівнює значення кожного пікселя зображення з відповідними межами кольору і встановлює значення 255 в масці, якщо піксель потрапляє в заданий діапазон, і 0 в іншому випадку, а також рахує кількість ненульових пікселів (білих пікселів) в кожній з масок червоного, жовтого та зеленого кольорів за допомогою функції `“cv2.countNonZero()”` і зберігає їх в змінних `“red_pixel_count”`, `“yellow_pixel_count”` і `“green_pixel_count”`.

На рисунку 1 зображено процес розпізнавання червоного сигналу світлофора з фотографії.

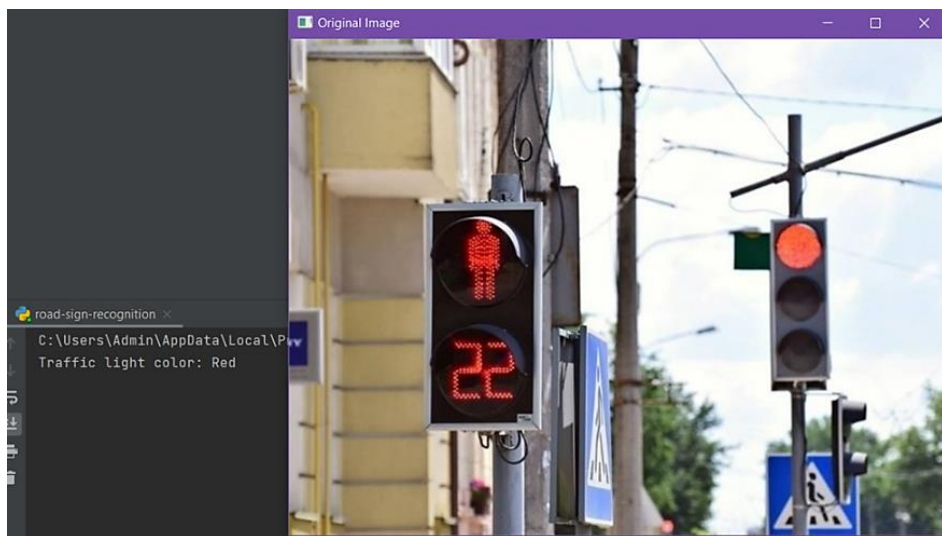


Рисунок 1 – Розпізнавання червоного сигналу з фотографії

Дана підсистема також визначає колір світлофора визначається на основі кількості пікселів у кожній з областей (червоної, жовтій і зеленій). Ось принцип роботи, по якому працює підсистема:

1. Якщо кількість червоних пікселів більша за кількість жовтих пікселів і більша за кількість зелених пікселів, то колір світлофора встановлюється як "Червоний"



2. У випадку, якщо кількість жовтих пікселів перевищує кількість червоних пікселів і кількість зелених пікселів, тоді колір світлофора буде встановлений як "Жовтий".

3. Якщо кількість зелених пікселів перевищує кількість червоних пікселів і кількість жовтих пікселів, то колір світлофора буде встановлений як "Зелений".

4. У всіх інших випадках, коли не виконується жодна з умов, колір світлофора буде позначений як "Невідомий".

Ці формули порівнюють кількість пікселів у кожній області і встановлюють значення "traffic\_light\_color" відповідно до найбільшої кількості пікселів у певній області. Наприклад, якщо кількість червоних пікселів більша за жовті та зелені, то встановлюється значення 'Red' для "traffic\_light\_color" і результат зберігається у змінній "traffic\_light\_color", також виводить колір світлофора на екран за допомогою функції "print()", відображає оригінальне зображення та області, які відповідають червоному, жовтому та зеленому кольорам, за допомогою функції "cv2.imshow()".

На рисунку 2 зображено процес розпізнавання жовтого сигналу.

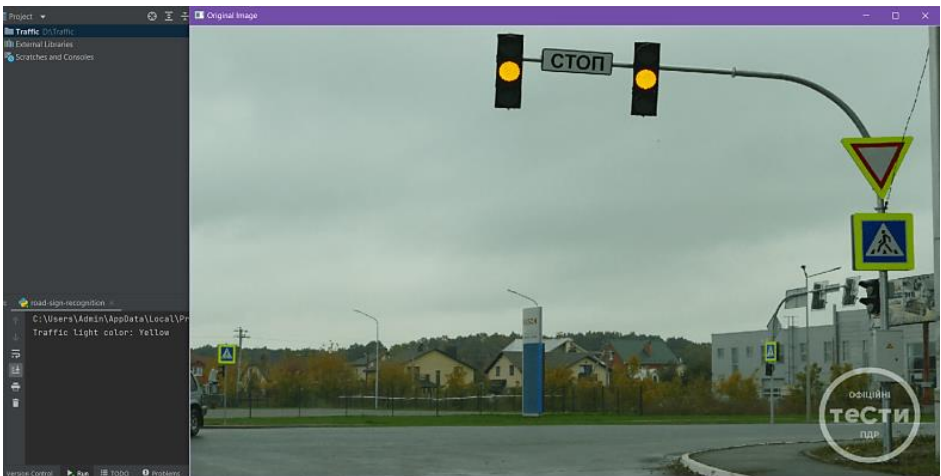


Рисунок 2 – Розпізнавання жовтого сигналу з фотографії

На рисунку 3 зображено процес розпізнавання зеленого сигналу світлофора з фотографії.

Зображення областей виводяться за допомогою побітового "І" ("cv2.bitwise\_and()") з оригінальним зображенням та відповідною маскою. Далі програма очікує натискання будь-якої клавіші для закриття вікон зображень за допомогою функції "cv2.waitKey(0)", а потім закриває всі вікна зображень за допомогою функції "cv2.destroyAllWindows()".

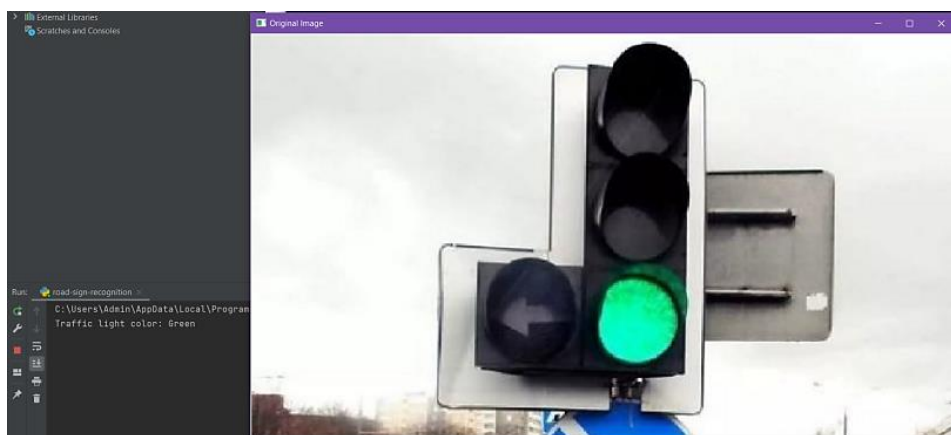


Рисунок 3 – Розпізнавання зеленого сигналу з фотографії

Отже, зважаючи на наведені вище факти та дослідження, можна зробити висновок, що дана система є надзвичайно значущим кроком у поліпшенні безпеки дорожнього руху, однак, важливо зазначити, що система не може замінити відповідальність та увагу водія. Призначення системи полягає в допомозі та підтримці водіїв моніторингу ситуації на дорозі, але керування автомобілем та прийняття рішень залишається тільки у руках водіїв. В подальшому планується розширити функціонал системи, що додатково збільшить ефективність та її корисність. Також буде додатково проведено ряд тестувань задля виправлення непомічених раніше помилок та збільшення надійності системи.

### Перелік посилань

1. L. C. Possatti, R. Guidolini, V. B. Cardoso, R. F. Berriel, T. M. Paixão, C. Badue, T. Oliveira-Santos, Traffic light recognition using deep learning and prior maps for autonomous cars. In 2019 international joint conference on neural networks (IJCNN), 2019. pp. 1-4, doi: 10.1109/IJCNN.2019.8851927.
2. O. Pavlova, V. Kovalenko, T. Hovorushchenko, V. Avsiyevych. Neural network based image recognition method for smart parking, 2021. pp. 49-51.

УДК 004.052.2

Бойчук А.І., Данчук С.В., Нічепорук А.О.

*Хмельницький національний університет*

## **ОЦІНКА ДОСТУПНОСТІ SAAS СИСТЕМ В КОНТЕКСТІ АНАЛІЗУ ВПЛИВУ НЕСПРАВНОСТЕЙ В ІТ ІНФРАСТРУКТУРІ**

*Розглянуто прикладні аспекти оцінки доступності SaaS систем в контексті аналізу впливу несправностей в ІТ інфраструктурі. Приведено приклади показників які можна розраховувати для аналізу стану інформаційних систем.*

*The practical aspects of assessing the availability of SaaS systems in the context of fault analysis in IT infrastructure have been discussed. Examples of metrics that can be calculated to analyze the state of information systems are provided*

Протягом багатьох років в ІТ індустрії зберігається тренд на використання розподілених систем, оскільки він забезпечує краще масштабування незалежних компонентів, швидкість відповіді, роботу з великою кількістю запитів, а також надає можливість незалежної роботи багатьох команд над проектом з мінімізацією координації на нижніх рівнях. Усі ці характеристики дозволяють підтримувати модульну структуру ПЗ, підтримувати належну якість коду та забезпечувати свободу вибору при розробці компонентів системи оскільки підхід є технологічно неупередженим. Ця тенденція призвела до популяризації сервісів які надають послуги з продажу елементів ІТ інфраструктури і ПЗ для забезпечення роботи кінцевого продукту, а також засобів за допомогою яких здійснюється створення та налаштування ПЗ та інфраструктури. Такі сервіси створюють додатковий рівень абстракції та збільшують складність і розширеність системи, при цьому відстежування помилок на кожному з рівнів інфраструктури набуває високого пріоритету, оскільки напряму впливає на якість надання послуг такими компаніями

Програмне забезпечення як послуга (SaaS) – це модель розподілу програмного забезпечення, в якій хмарний провайдер розміщує програми та надає до них доступ кінцевим користувачам через Інтернет. У цій моделі незалежний постачальник програмного забезпечення (ISV) може укласти угоду з стороннім хмарним провайдером для розміщення програми. Або, у великих компаній, таких як Microsoft чи Amazon, хмарний провайдер також може бути постачальником програмного забезпечення.

SaaS – одна з трьох основних категорій хмарних обчислень, поряд з інфраструктурою як послугою (IaaS) і платформою як послугою (PaaS). Широкий спектр ІТ-фахівців, бізнес-користувачів і особистих користувачів використовують SaaS-застосунки. Продукти варіюються від особистого розвагового контенту,

наприклад, Netflix, до високотехнологічних ІТ-інструментів. У відміню від IaaS і PaaS, продукти SaaS часто маркетингові і доступні як для користувачів B2B, так і для користувачів B2C.

При проектуванні SaaS систем важливо забезпечити функціонування інформаційної системи 24/7/365, оскільки послуги які надають можуть мати критично важливі елементи для кінцевих продуктів і навіть бути їх основною складовою.

Доступність, середній час відновлення (MTTR) і середній час між відмовами (MTBF) є важливими поняттями в операціях обслуговування та у практиці інженерії надійності сайту(SRE). Вони можуть використовуватися для отримання уявлення про продуктивність сервісу, але вони мають певні обмеження. У організації SaaS обчислення MTTR і MTBF базуються на показниках часу безвідмовної роботи та часу простою, зареєстрованих протягом певного періоду часу. Ці сирі дані також використовуються для обчислення показника доступності - безперечно, найбільшого і найважливішого показника рівня обслуговування (SLI). Це важливий момент, оскільки в інженерії надійності, визначення простою базується на часі, необхідному для виправлення несправності в системі. У інженерії надійності сайту простій базується на тому, скільки часу несправність мала вплив на кінцевого користувача. Помилки і простой – пов'язані поняття, але розрізнення між ними важливе. Помилки в системі доволі поширене явище, але вони не завжди призводять до простою.

Доступність визначається як співвідношення часу роботи системи до суми часу простою і часу роботи системи, формула виглядає наступним чином[1]:

$$Availability = \frac{Uptime}{Uptime + Downtime}$$

Показник описаний вище дає лише узагальнену картину того що відбувається в системі і не може бути єдиним маркером для оцінки стану інформаційної системи. Для кращого розуміння ситуації потрібно збирати інформацію про середній час між системними помилками (MTBF) та середній час простою (MDT) і додаткові показники які необхідні для їх розрахунку. Для розрахунку операційної доступності, необхідно розрахувати показники зазначені вище для кожного з елементів системи за формулою[2]:

$$MBTF = \frac{T_{mean}}{F_{mean}}$$

$$MDT = T_d + T_i + T_r + T_{rc}$$

$$A_o = \frac{MBTF}{MBTF + MDT}$$

де MBTF – середній час між помилками,  $T$  – операційний час,  $mean F mean$  – середня кількість помилок, MDT – середній час простою,  $T$  – час  $d$  виявлення,  $T$  – час інтервенції, – час відновлення, – час  $i T r T rc$  повернення сервісу,  $A$  – операційна доступність.

Формула, яка показана вище, використовується для розрахунку показників в одному з компонентів інформаційної системи, але відповідний розрахунок необхідно проводити для кожного з них, щоб краще розуміти в якому стані вони знаходяться, і який з елементів може призводити до виникнення проблем. Для кращого розуміння розглянемо абстрактну інформаційну систему, яка складається з  $N$  компонентів на Рисунок 1.

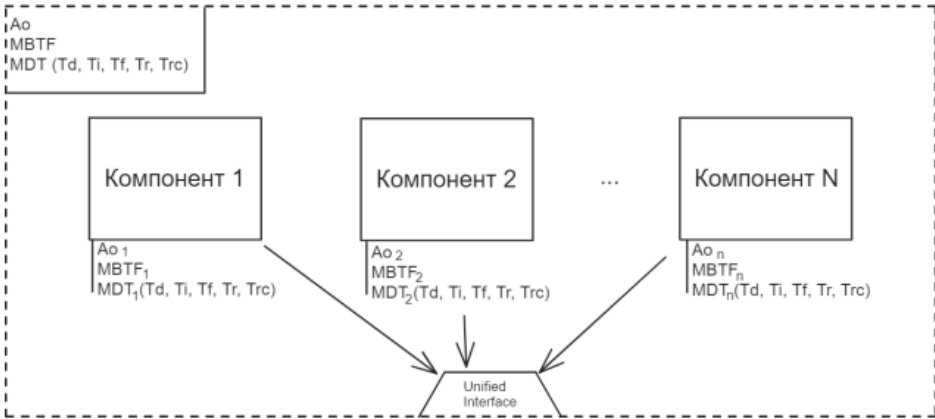


Рисунок 1 – Схема абстрактної інформаційної системи з  $N$  компонентів

Згідно схеми видно, що інформаційна система складається з  $N$  внутрішніх елементів які доступні кінцевому користувачу через певний абстрактний, уніфікований інтерфейс (метод взаємодії користувача та системи в даному випадку не суттєвий) і кожен компонент, має власні показники  $A$ ,  $MBTF$  та  $MDT$ . Окрім цього сама  $o$  платформа має власні показники, які вже необхідно обчислити за наступною формулою, враховуючи середні значення показників усіх її компонентів:

$$MBTF_{avg} = \frac{\sum_{i=1}^n MBTF_i}{n}$$

$$MDT_{avg} = \frac{\sum_{i=1}^n MDT_i}{n}$$

$$A_{o(avg)} = \frac{\sum_{i=1}^n A_{o(i)}}{n}$$

Після проведення розрахунків можна оцінити загальний стан інформаційної системи і окремо кожного з її компонентів, що дозволяє, в подальшому, аналізувати існуючі проблеми та приймати рішення для покращення її стану для забезпечення максимальної доступності.

Слід зазначити, що операційна доступність не єдиний компонент на основі якого потрібно аналізувати стан інформаційної системи в контексті наявних та потенційних несправностей, а лише один з показників які необхідно враховувати при аналізі. Оцінка стану вимагає комплексу заходів по збору інформації і її програмного аналізу, що включає наступні елементи: моніторинг та аналіз журналу подій (Event Log Monitoring and Analysis), моніторинг продуктивності (Performance Monitoring), тестування системи при великих навантаженнях (Load Testing), тестування аварійного переходу (Failover Testing), моделювання впливу (Impact Modeling), автоматизовану систему моніторингу (Automated Monitoring System) та оцінку рівня обслуговування (SLA Assessment). На основі отриманих результатів, можна провести комплексний аналіз метрик згідно якого вже можна приймати більш обґрунтований висновок про поточний стан інформаційної системи.

Інформаційні системи постійно розвиваються і їх ускладнення є логічним еволюційним процесом який створює нові виклики пов'язані з ускладненням ІТ інфраструктури і використанням розподіленої архітектури.

Аналіз SaaS систем на основі доступності внутрішніх компонентів у системах з розподіленою архітектурою дозволяє отримати високорівневе представлення про стан інформаційної системи, її вузькі місця та потенційні проблемні зони. Операційна доступність, як один показників відіграє важливу роль, оскільки його досить легко вирахувати і впровадити в існуючі проекти, що дозволяє покращити прозорість та видимість стану інформаційної системи, а аналіз та оптимізація елементів з існуючими проблемами дозволить покращити якість надання послуг SaaS платформ.

### Перелік посилань

1. How to design a network architecture using availability. URL: [https://www.researchgate.net/publication/359814855\\_How\\_to\\_design\\_a\\_network\\_architecture\\_using\\_availability](https://www.researchgate.net/publication/359814855_How_to_design_a_network_architecture_using_availability)
2. Availability, MTTR, and MTBF for SaaS Defined <https://medium.com/@daveowczarek/availability-mtrr-and-mtbf-for-saas-defined-66b618ac1533>
3. Ролік А.І. Управління корпоративною ІТ-інфраструктурою / А.І. Ролік, С.Ф. Теленик, М.В. Ясочка // К.: Наукова думка, 2018. – 576 с

УДК 004.7.056.5

Бохонько О.О., Бондарук О.В.

*Хмельницький національний університет*

## **ДОСЛІДЖЕННЯ МЕТОДІВ ПІДТРИМКИ ТА КЕРУВАННЯ ЖИТТЄВИМ ЦИКЛОМ ХМАРНИХ СЕРЕДОВИЩ**

*Дослідження зосереджене на проблемі розробки та управління хмарними додатками з критичними за часом характеристиками, такими як системи передчасного сповіщення про небезпеки та трансляція даних в реальному часі. Виявлено, що на сьогоднішній день відсутні системи та інструменти для динамічної оркестровки та адаптації, які б забезпечували відповідну підтримку для розробки критичних за часом хмарних додатків на протязі їхнього життєвого циклу.*

*The research focuses on the challenge of designing and managing cloud applications with time-critical features such as early warning systems and real-time data streaming. It was found that today there are no systems and tools for dynamic orchestration and adaptation that would provide appropriate support for the development of time-critical cloud applications throughout their life cycle.*

### **Вступ**

Критичні за часом хмарні додатки, такі як системи раннього попередження про катастрофи та трансляція відео в реальному часі, можуть отримати вигоду від моделі хмарних обчислень і (у випадку останньої) використовувати Інтернет речей (IoT), який може отримувати величезну кількість даних від датчиків і виконавчих механізмів. Такі додатки можуть бути повністю функціональними, лише якщо вони відповідають очікуванням користувачів, наприклад, швидке реагування на події в реальному часі для забезпечення покращеної якості обслуговування (QoS) і якості досвіду (QoE).

Наразі бракує систем та інструментів динамічної оркестровки та адаптації, які б забезпечили відповідну підтримку для розробки критичних за часом хмарних додатків протягом усього їхнього життєвого циклу, беручи до уваги різноманітні фактори, такі як атрибути QoS, SDN та попит на обчислювальні ресурси, пропонувані хмарними постачальниками. Крім того, є обмежені дослідження специфікацій оркестровки.

### **Дослідження методів підтримки та керування життєвим циклом хмарних середовищ**

Найдосконалішою мовою хмарної оркестровки є Topology and Orchestration Specification for Cloud Applications (TOSCA) [1], яка служить схемою для моделювання логіки рішень, визначення опису програмного забезпечення та

мережевих компонентів, топології та політик тощо. Її можна використовувати для автоматизації процесу розгортання, самоадаптації та автомасштабування. TOSCA забезпечує статичний опис логіки програми в її проектному стані та не залежить від постачальників хмарних технологій.

За допомогою динамічних відображень QoS, QoE та атрибутів часу виконання, пов'язаних із програмою та її базовою архітектурою, можна забезпечити виконання компонентів розподіленої програми разом із їхніми залежностями та зв'язками всередині хмарного середовища, маючи можливість миттєво змінювати конфігурацію обчислювальних ресурсів та базової інфраструктури відповідно до критичних часових обмежень. Тому QoS хмарних додатків із критичними часовими обмеженнями необхідно покращувати [2].

Також необхідним є створення багаторівневої архітектури з асоційованою моделлю спільного програмування та спільного керування, яка може підтримувати динамічний формат обміну TOSCA, забезпечуючи необхідну модульність, програмованість і керованість як додатків, так і інфраструктури за допомогою робочого середовища та методології для виконання додатків, задовольняючи їх суворим вимогам до часу.

Оцінка основних характеристик і можливостей таких мов/специфікацій та інструментів оркестровки хмари подано в Таблиці 1.

Таблиця 1 – Оцінка основних характеристик і можливостей мов/специфікацій та інструментів оркестровки хмари: SWITCH IDE, ARIA TOSCA, CAMEL, Cloudify, Heat Translator

	ARIA TOSCA	CAMEL	Cloudify	Heat Translator	SWITCH IDE
<b>Інтерфейс</b>	Засоби CLI	Засоби CLI	Blueprint Composer (GUI)	Засоби CLI	SIDE GUI
<b>Режим створення ПЗ</b>	Консольний режим	Консольний режим	Графічний режим	Скрипти Python	Графічний режим
<b>Мова оркестрації</b>	ARIA TOSCA	CAMEL	TOSCA	згенерований засобами TOSCA	TOSCA
<b>Оркестратор</b>	Двигун ARIA Workflow	Платформа PaaSage	Платформа Cloudify	Двигун Heat	Менеджер DRIP
<b>Атрибути специфікації QoS/QoE</b>	Консольний режим	Консольний режим	Консольний режим	TOSCA	TOSCA
<b>Моніторинг додатків</b>	ARIA	Платформа Needs PaaSage	Grafana	Kibana	ASAP, JCatascopia
<b>Само-адаптивність</b>	Підтримка моделей @runtime	Платформа Needs PaaSage	немає	немає	Адаптив-ність
<b>Здатність до реконфігурації</b>	Немає	Немає	Немає	Updated TOSCA template, static	Динамічне оновлення QoS
<b>Рівень дружності інтерфейсу</b>	низький	низький	середній	низький	високий



Для реалізації поставлених завдань можуть бути виконані, засоби SWITCH IDE (Software Workbench для інтерактивних, критичних до часу та високосамоадаптивних хмарних програм), які через свій графічний інтерфейс користувача дозволяють здійснювати опис додатків та інфраструктури а також маніпулювання атрибутами QoS, їх відображення в топологію TOSCA та через оркестровку та самоадаптацію, реконфігурацію QoS і атрибутів часу виконання шляхом генерації нової топології TOSCA під час виконання програми.

### **Висновок**

Результати досліджень показали що для того, щоб забезпечення підвищення QoS для хмарних додатків і задоволення їх критичних часових обмежень вимагає розроблення нових методів та засобів підтримки та керування життєвим циклом хмарних середовищ.

### **Перелік посилань**

1. Aria, Apache ARIA TOSCA, 2019, <http://ariatosca.incubator.apache.org/>, (Accessed September 2023).
2. Anser Y., Gaber C., Wary J. -P., García S. N. M., Bouzefrane S. TRAILS: Extending TOSCA NFV profiles for liability management in the Cloud-to-IoT continuum. *2022 IEEE 8th International Conference on Network Softwarization (NetSoft)*, Milan, Italy, 2022, pp. 321-329, doi: 10.1109/NetSoft54395.2022.9844027.

УДК 004.7.056.5

Бохонько О.О., Лисенко С.М.

*Хмельницький національний університет*

## **МЕТОД ВИЯВЛЕННЯ КІБЕР-АТАК НА ОСНОВІ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ**

*Визначено проблематику технічних видів кібер-атак на основі застосування методів соціальної інженерії. Авторами представлено метод виявлення кібер-атак соціальної інженерії. Підхід виявлення кібер-атак використовував чотири алгоритми машинного навчання (decision tree, random forest, K-nearest neighbor, та extreme gradient boosting). Аналіз зосереджено на даних, зібраних з хостів мережі, які можуть служити індикаторами потенційної атаки соціальної інженерії. Емпіричні результати продемонстрували високу точність визначення.*

*The problems of technical types of cyber-attacks based on the use of social engineering methods are defined. The authors present a method for detecting social engineering cyber attacks. The cyber attack detection approach used four machine learning algorithms (decision tree, random forest, K-nearest neighbor, and extreme gradient boosting). The analysis focuses on data collected from network hosts that can serve as indicators of a potential social engineering attack. The empirical results demonstrate high accuracy of the identification.*

### **Вступ**

Сьогодні кібер-атаки соціальної інженерії можуть завдавати значної шкоди суспільству. Потенційними наслідками, які можуть виникнути в результаті кібер-атак соціальної інженерії є фінансові втрати, скомпрометовані системи, крадіжка даних, шкода репутації, збої в роботі, правові наслідки, психологічний вплив, поширення шкідливих програм [1-3]. Мета дослідження полягає в тому, щоб зосередитися на новому методі виявлення атак соціальної інженерії.

### **Аналіз відомих рішень**

У дослідженні [4] автори висувають стратегії та тактики кампанії охорони здоров'я для протидії атакам соціальної інженерії. Дослідження [5] вивчало зв'язок між рисами особистості та її сприйнятливістю до соціальної інженерії в контексті соціальних мереж. Під час дослідження [6] було створено Framework людини як датчика безпеки, яка була практично реалізована через CogniSense, прототип програми для Microsoft Windows, і має на меті надати користувачам можливість проактивно виявляти атаки семантичної соціальної інженерії, націлені на них, і повідомляти про них. Автори [7] розробили метод вилучення даних, необхідних для здійснення ефективних фішингових атак із відкритих наукових джерел. При цьому

запропонували використовувати автоматизовані скрипти для перевірки автентичності зібраних даних перед розгортанням і для автоматизації процесу розсилки, минаючи алгоритми виявлення спаму. У роботі [8] представлено модель виявлення кібер-атак з використанням методів машинного навчання, яка передбачала поділ набору даних на набори для навчання та тестування, що дозволило охопити внутрішні риси тексту електронної пошти та інші функції, забезпечивши ефективну класифікацію на фішингові та нефішингові категорії. У роботі [9] представлено метод виявлення метаморфічних вірусів на основі аналізу ознак їх обфускації.

### **Метод виявлення кібер-атак на основі соціальної інженерії**

Запропоновано новий метод виявлення кібер-атак соціальної інженерії. Дослідження включає етапи навчання та виявлення. Етапи навчання: формування знань шляхом аналізу характеристик, які можуть вказати на існування атаки соціальної інженерії на хостах мережі; представлення інформації про атаки у вигляді набору векторів ознак.

Етапи виявлення: моніторинг системних подій в хостах мережі; збір ознак і виділення функцій з хосту мережі, які потенційно можуть вказати на існування атаки соціальної інженерії на цей хост, і побудова вектора ознак з цих ознак; формування векторів ознак з використанням даних, отриманих від хостів мережі; виконання класифікації об'єктів з використанням алгоритмів машинного навчання шляхом використання отриманих векторів ознак для призначення досліджуваного об'єкта конкретним класам атак; локалізація хоста мережі, який піддається атаці.

Для прийняття рішення використовуються MLA: decision tree, random forest, K-nearest neighbor, та extreme gradient boosting.

### **Експерименти**

Для оцінки ефективності методу було проведено експерименти, де використовувалися набори даних [9], що містять приклади зловмисної поведінки. У експериментах було залучено 50 хостів, а також 15 типів атак. Експеримент тривав 24 години.

### **Висновок**

Представлено інноваційний метод виявлення атак соціальної інженерії. Цей метод передбачає використання алгоритмів машинного навчання. Перевірка зосереджена на даних, зібраних з мережевих хостів, які можуть вказувати на наявність атаки соціальної інженерії. Емпіричні результати виявили вражаючу точність виявлення приблизно 99% у поєднанні з частотою помилкових позитивних результатів приблизно 6%.

### Перелік посилань

1. Лисенко С. М., Харченко В.С., Бобровнікова К.Ю., Щука Р. Резильєнтність комп'ютерних систем в умовах кіберзагроз: Онтологія та таксономії. *Радіoeлектронні і комп'ютерні системи*. 2020. №1. С. 17-28.
2. Wang Z., Sun L., Zhu H., Defining Social Engineering in Cybersecurity. *IEEE Access*. 2020, vol. 8, no. 1, pp. 85094–85115, doi: 10.1109/ACCESS.2020.2992807.
3. Abe N., Soltys M., Deploying health campaign strategies to defend against social engineering threats, in *Procedia Comput. Sci.*, 2019 vol. 159, p. 824–831.
4. Albladi S.M., Weir G.R.S, Predicting individuals' vulnerability to social engineering in social networks, in *Cybersecur 2020*, 3, 7, <https://doi.org/10.1186/s42400-020-00047-5>.
5. Heartfield R., Loukas G., Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework, in *Computers & Security*, 2018, vol. 76, p. 101-127, ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2018.02.020>.
6. Марусенко Р., Соколов В., Богачук І., Методика отримання даних з відкритих наукових джерел та симуляція атак соціальної інженерії / Штучні системи для логістичної інженерії. *ICAILE 2022. Конспект лекцій з інженерії даних і комунікаційних технологій*, 2022, том. 135. Springer, Cham, [https://doi.org/10.1007/978-3-031-04809-8\\_53](https://doi.org/10.1007/978-3-031-04809-8_53).
7. Mughaid A., AlZu'bi S., Hnaif A., An intelligent cyber security phishing detection system using deep learning techniques, in *Cluster Comput.* 25, 3819–3828, 2022, <https://doi.org/10.1007/s10586-022-03604-4>.
8. Марковський Г., Савенко О., Лисенко С., Нічепорук А., Методика виявлення метаморфічних вірусів на основі аналізу ознак обфускації // *CEUR-WS*, ISSN: 1613–0073, 2018, том. 2104, стор. 680–687.
9. Miyamoto D., Hazeyama H., Kadobayashi Y., An evaluation of machine learning -based methods for detection of phishing sites, 2009, doi: 10.1007/978 -3-642-02490-0\_66.

УДК 004.4

Бугайчук В.О.

*Київський національний університет імені Тараса Шевченка*

## **СУМАРИЗАЦІЯ ТЕКСТУ ЗА ДОПОМОГОЮ РЕКУРЕНТНИХ НЕЙРОННИХ МЕРЕЖ ТА ТРАНСФОРМЕРІВ**

*Розглянуто різні підходи сумаризації тексту за допомогою рекурентних нейронних мереж та трансформерів, які забезпечують аналіз та вилучення необхідної інформації з тексту. Запропонований підхід дозволяє здійснювати зручну та точну сумаризацію текстів різної природи та структури.*

*Various approaches to annotating the text using recurrent neural networks and transformers, which provide analysis and extraction of the necessary information from the text, are considered. The proposed approach allows you to conveniently and accurately annotate texts of different nature and structure.*

З бурхливим зростанням збору та зберігання текстових даних потреба в аналізі та вилученні інформації з цієї маси стає все більш актуальною. Крім того, розвиток моделей глибокого навчання для обробки природньої мови полегшив використання текстових даних. Важливою частиною останніх досліджень є розробка уваги та механізмів вибору, які допомагають моделям зосереджуватися на ключових частинах тексту для здійснення точної та конкретної сумаризації. Крім того, деякі дослідники вивчають можливості комбінування рекурентних нейронних мереж та трансформерів для досягнення кращих результатів у сумаризації тексту, використовуючи переваги обох підходів. Однак існують невирішені проблеми. Одна з них полягає у покращенні якості сумаризації тексту з різними структурами, такими як технічні документи, новини, наукові статті тощо. Іншою важливою проблемою є розв'язання проблеми адаптації моделей до різних мов та культурних контекстів, оскільки сумаризація тексту повинна бути ефективною незалежно від мови чи жанру тексту.

Метою роботи є розробка моделі для сумаризації новинних текстів українською мовою за допомогою рекурентних нейронних мереж та трансформерів. Основною постановкою завдання є створення ефективної моделі, яка здатна аналізувати та розпізнавати ключові інформаційні елементи у новинах. Дослідження спрямоване на оптимізацію якості сумаризації для новинних матеріалів з урахуванням особливостей української мови та жанрових особливостей новинарських текстів.

Задачу резюмування тексту можна перетворити на контрольовану або напівконтрольовану задачу машинного навчання. Використовується архітектура рекурентних нейронних мереж seq2sequence, яка складається з кодувальника та декодера, з'єднаних послідовно, щоб генерувати підсумок для заданого тексту [1]. Ці кодери та декодери додатково складаються з LSTM (Long Short-Term Memory), як розширена функціональність простої рекурентної нейронної мережі. У

рекурентних нейронних мережах новий вихід залежить від попереднього. Завдяки цій властивості текст узагальнюється більш людяно. Рекурентні нейронні мережі дозволяють моделі враховувати контекст тексту, використовуючи попередні інформаційні стани для генерації наступних слів [2]. Трансформери дозволяють уважно аналізувати великі текстові обсяги паралельно, що полегшує роботу з довільно довгими текстами та покращує швидкість навчання. Для вирішення проблеми короткострокових залежностей простої рекурентної нейронної мережі використовується архітектура LSTM, яка здатна вивчати довгострокові залежності. Кодер та декодер є двома компонентами архітектури рекурентної нейронної мережі sequence2sequence, які в основному використовуються, коли вхідні та вихідні дані мають різну довжину. Кодер – кодує весь вхідний файл у форму, придатну для обробки. Декодер – декодує оброблений вхідний сигнал у необхідний вихід. Одне слово за раз надається як вхідні дані кодеру з його міткою часу. Потім це слово обробляється LSTM шляхом відновлення інформації, присутньої в послідовному введенні. За ним іде декодер, який декодує вхідну послідовність у більш читабельний і бажаний вихідний формат. Далі створюється резюме, використовуючи модель, яка передбачає наступне релевантне слово, враховуючи попередню послідовність слів.

В якості датасету використовується набір даних, який включає в себе різноманітні новинні тексти українською мовою. Модель вдосконалюється шляхом оптимізації параметрів та навчання на великій кількості даних, щоб забезпечити її здатність до адаптації до різних стилів та жанрів новин.

Отримані наукові результати вказують на високу ефективність моделі у завданні сумаризації текстів. Ефективність моделі вимірювалася за допомогою метрик якості сумаризації, таких як ROUGE (Recall-Oriented Understudy for Gisting Evaluation) [3]. Застосування механізму LSTM дозволяє уникнути проблеми з довготерміновими залежностями у тексті, що забезпечує більш точні та змістовні результати сумаризації. Модель демонструє здатність генерувати конкретні та змістовні сумаризації для різних новинних матеріалів. Отримані результати відкривають нові перспективи для застосування моделей сумаризації тексту у сфері автоматизованих новинних порталів, допомагаючи користувачам швидко здобувати необхідну інформацію, що є важливим кроком у напрямку покращення доступу до знань та інформації для громадськості. Запропонований підхід має свої переваги та недоліки. Серед переваг: створює більш людське резюме, точність зростає зі збільшенням розміру даних. Серед недоліків можна виділити складність моделі, повторення слів не перевіряється, повільна робота моделі.

### Перелік посилань

1. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L., & Polosukhin, I. Attention is All You Need. 2017. С. 2-3.
2. Subha Shini R., Ambeth Kumar V. D. An Effective Analysis for Text Summarization by Word Sequence Generation. 2021. С. 1-2.
3. Two minutes NLP – Learn the ROUGE metric by example. URL: <https://medium.com/nlplanet/two-minutes-nlp-learn-the-rouge-metric-by-examples-f179cc285499>

УДК 004.4

Ваховська В.М.

*Хмельницький національний університет*

## **МОБІЛЬНИЙ ДОДАТОК «GYMRAT» – ВІРТУАЛЬНИЙ ФІТНЕС ТРЕНЕР**

*Досліджено прикладні аспекти розробки мобільного додатку, який виступає в ролі віртуального фітнес тренера. Додаток надає користувачам можливість переглядати різноманітні фітнес-вправи та проходити тренування. Основний акцент робиться на створенні користувачами власних тренувань у спеціальному редакторі, та шляхом надсилання запиту до попередньо натренованої моделі. Запропонований додаток надає користувачам зручний та ефективний інструмент для досягнення спортивних цілей.*

*The applied aspects of developing a mobile application functioning as a virtual fitness trainer have been studied. This application allows users to view diverse fitness exercises and participate in workout sessions. The primary emphasis is placed on users creating their own customized workouts using a specialized editor, and by sending requests to a pre-trained model. The proposed application offers users a convenient and efficient tool for achieving their fitness goals.*

Здоровий спосіб життя та фітнес – одна з найактуальніших ключових тем сучасного світу. Згідно зі статистичними даними, все більше людей починають стежити за своїм здоров'ям і підтримувати хорошу форму, займаючись спортом. Фітнес індустрія стрімко розвивається в усьому світі завдяки комерційній орієнтації, а тенденції у сфері фітнесу швидко змінюються.

Не всі мають можливість відвідувати спортивні заклади через різні обставини, такі як зайнятість або віддаленість. У зв'язку з цим, актуальним стає пошук альтернативних способів тренувань, не виходячи з дому. З появою смартфонів та розвитком технологій, таку роль на себе взяли мобільні фітнес додатки. Вони надають можливість тренуватися де завгодно і коли завгодно, а також стежити за прогресом в тренуваннях та раціональному харчуванні.

Ще один пік популярності мобільних додатків почався з пандемією COVID-19, так як більшість фітнес-клубів тимчасово зачинилися та стало складно відвідувати спортивні майданчики та тренуватися з професійними тренерами через карантинні обмеження.

Аналіз останніх досліджень і публікацій, які розглядають рішення даної проблеми, вказує на популярність та актуальність мобільних фітнес-додатків як інструменту для підтримання здорового способу життя. Для визначення вимог та недоліків було проведено порівняльний аналіз двох відомих додатків: Nike Training Club та Jefit.

У Nike Training Club неможливо користуватися додатком без авторизації, окремо переглядати вправи та створювати власні тренування. Проходження тренувань відбувається у формі перегляду відео, що може бути незручним, оскільки відсутня можливість легко переключити вправу або повернутися до попередньої. Додаток також не надає опцію встановлення індивідуальних інтервалів відпочинку між вправами.

У випадку Jefit також спостерігається відсутність можливості користування додатком без авторизації, проте на відміну від Nike Training Club, Jefit надає більший вибір вправ, які розділені на категорії відповідно до груп м'язів. Проте користувачам не надається можливість створення власних тренувань з нуля; замість цього їм надається можливість редагувати наявні тренування за допомогою обмежених опцій. Важливим недоліком є поява нав'язливої реклами, значна частина функцій є платними, інтерфейс може викликати плутанину для користувачів.

Отже, додаток GymRat повинен вирішувати ці проблеми, надаючи користувачам свободу вибору. Він дозволить користувачам персоналізувати свої тренування, вибираючи вправи, які відповідають їхнім потребам та цілям. Користувачі зможуть створювати власні тренування, змінювати вправи та налаштовувати час виконання та відпочинку між ними. При проходженні тренування користувач бачитиме анімацію виконання вправи та зможе стежити за таймером, який відліковує час до завершення вправи. Крім того, користувач матиме можливість пропустити або повернутися до попередньої вправи, якщо така потреба виникне. Після кожної вправи надається відпочинок на спеціальному екрані з релаксуючою анімацією та таймером, який за бажанням можна пропустити. Після успішного проходження тренування виникає екран привітання.

Метою цього додатку є надання користувачам зручного та простого інструменту для здійснення фітнес тренувань. Додаток дозволяє користувачам переглядати вправи, проводити тренування, створювати список улюблених вправ та створювати власні тренування з використанням вже доданих вправ. Додаток буде побудований на React Native Expo, з використанням RapidAPI для надання вправ та Firebase для зберігання персоналізованих даних користувачів.

На рисунку 1 зображено загальну діаграму мобільного фітнес додатку.

У результаті дослідження було обрано React Native Expo та Redux для розробки мобільного фітнес-додатку.

React Native – відкрите програмне забезпечення, що використовується для розробки мобільних додатків. React Native базується на бібліотеці React, що дозволяє розробникам використовувати JavaScript для створення компонентів інтерфейсу користувача, які можуть бути перенесені на різні мобільні платформи. Також використано набір інструментів Expo (React Native), що допомагає прискорити розробку мобільних додатків на основі React Native. Ці технології виявилися оптимальними для створення переносних додатків для Android і iOS з



однією спільною кодовою базою, що спрощує процес розробки і зменшує витрати часу та ресурсів.

Додаток буде взаємодіяти з Firebase сервісами:

1. Firebase Authentication для автентифікації користувачів;
2. Firestore Database для зберігання персоналізованих даних;
3. Cloud Storage для зберігання статичних даних.

Цей вибір технології обґрунтовується їхньою здатністю до забезпечення безпеки і доступності даних, а також можливістю синхронізації даних у режимі реального часу.

Firebase Firestore обрано як базу даних для додатку так як ця документно-орієнтована база даних дозволяє зберігати дані у вигляді колекцій документів, забезпечуючи гнучкість та синхронізацію даних в режимі реального часу. Важливою перевагою є підтримка роботи в офлайн режимі та автоматична синхронізація з сервером.

Також обрано RapidAPI ExerciseDB для отримання даних про фітнес-вправи, що розширює можливості додатку щодо надання розширеного переліку вправ та їх категорій. Кожна вправа має докладний опис, включаючи назву та GIF-анімацію виконання, час виконання та відпочинку, що дозволяє користувачам правильно та ефективно виконувати вправи під час своїх тренувань. Інтеграція з цим API обґрунтовується бажанням додати варіативності для різного кола користувачів.

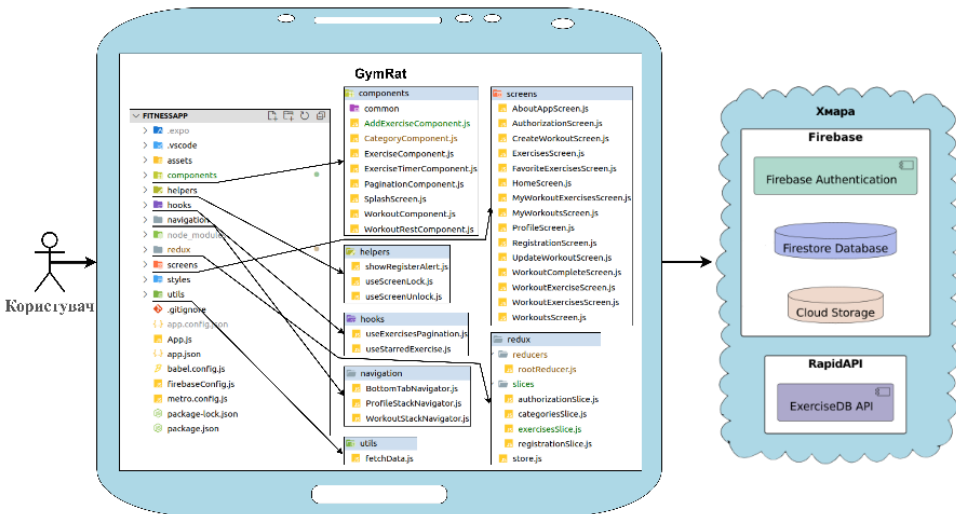


Рисунок 1 – Загальна діаграма структури та взаємодії

Особливістю додатку також є потенційне використання передових технологій у сфері машинного навчання, зокрема методу тонкого налаштування (fine-tuning) попередньо натренованих моделей, для створення власних персоналізованих тренувальних планів. Цей підхід дасть користувачам змогу отримати персоналізоване тренування, просто вказавши свої тренувальні цілі. Ця інноваційна можливість підвищить конкурентоспроможність додатку на ринку фітнес-додатків, надаючи користувачам унікальний та індивідуалізований підхід до тренувань.

Отже, запропонований мобільний фітнес додаток, який виступає в ролі віртуального фітнес тренера, є потужним інструментом для покращення фізичної активності користувачів. Він надає зручний доступ до великого розмаїття фітнес-вправ та тренувань, а також дозволяє користувачам створювати та проходити власні тренування. Ця можливість дає користувачам вибір і контроль над своєю фітнес-програмою, забезпечуючи персоналізований підхід до досягнення спортивних цілей. Подальші дослідження спрямовані на використання штучного інтелекту (наприклад fine-tuned Llama 2) для створення персоналізованих тренувальних програм для користувачів.

### **Перелік посилань**

1. Alexander Benedikt Kuttig. Professional React Native: Expert techniques and solutions for building high-quality, cross-platform, production-ready apps – Birmingham: Packt Publishing, 2022 – 268 p.
2. M. Holmes He. Creating Apps with React Native: Deliver Cross-Platform – New York: Apress, 2022 – 449 p.
3. Shashank Mohan Jain. Introduction to Transformers for NLP: With the Hugging Face Library and Models to Solve Problems – New York: Apress, 2022 – 183 p.
4. Lewis Tunstall, Leandro von Werra, Thomas Wolf. Natural Language Processing with Transformers: Building Language Applications with Hugging Face – California: O'Reilly Media; 1st edition, 2022 – 406p.

УДК 005.21:005.8:004.8

Владовська А.О., Продеус М.С., Нічепорук А.О.

*Хмельницький національний університет*

## **АДАПТИВНЕ ПРОГНОЗУВАННЯ ТА РОЗПІЗНАВАННЯ ПОВЕДІНКИ МЕШКАНЦІВ У РОЗУМНИХ БУДИНКАХ**

*Розглянуто масштабований метод, що забезпечує гнучке моделювання та ідентифікацію діяльності в розумних будинках, орієнтоване на велику кількість видів діяльності та здатне адаптуватися до різноманітних умов і предметів.*

*Considered is a scalable method that provides flexible modeling and identification of activities in smart homes, is focused on a large number of activities and is able to adapt to a variety of conditions and subjects.*

Часто «розумні будинки» розглядаються як ідеальне рішення для побутових проблеми. Автоматизація може бути реалізована лише за умови виявлення активності мешканців. Це дає змогу «розумним сервісам» працювати автономно, щоб відслідковувати її активність. Технології досягли вражаючого прогресу в цій галузі, проте більшість існуючих сервісів покладаються на заздалегідь запрограмовані дії, які не завжди задовольняють потреби користувачів. Крім того, вони зазвичай мають обмежену масштабованість отже – не підходять для практичного застосування в реальних умовах за межами лабораторії. Щоб відповідати потребам користувачів пропонується нова структуру для розпізнавання дій і прогнозування поведінки людини. Ця система складається з трьох етапів: розпізнавання, виявлення та прогнозування активності, бонусом є використання RFID-міток, що суттєво знижує її вартість. Експеримент показує, що запропонований підхід добре ідентифікує і прогнозує дії, демонструючи чудову масштабованість.

Цей метод є масштабованим та підтримує велику кількість видів діяльності, легко адаптується для різних будинків, навіть якщо в них є різні предмети (наприклад стільці) та пристрої (наприклад лампи), і ця гнучкість виходить за межі обмежень традиційних моделей. Крім того, моделювання прогнозованої активності дозволяє покращити Human Activity Recognition (HAR) в розумних будинках, і незабаром може дозволити створювати повністю автоматизовані розумні будинки. Ще одна перевага полягає в тому, що треступеневий підхід дозволяє розбити завдання ідентифікації на основі даних сигналів, та забезпечує надзвичайну універсальність.

Кожен етап можна оптимізувати окремо, або замінити іншими. Одним із прикладів може бути заміна LSTM-моделі на третьому етапі на будь-який інший алгоритм інтелектуального аналізу часових рядів і використання маркованих даних з першого етапу. Оскільки метод має три етапи, потрібно оцінити ефективність та продуктивність кожного. Мета першого етапу полягає в тому, щоб визначити дії які виконувались. Є два ключові фактори, які значною мірою визначають ефективність цього етапу. Перший фактор – це те, чи можна правильно визначити використання об'єкта, а другий – чи можна правильно позначити діяльність. На другому етапі набір даних використовується для навчання та тестування відповідно. Ідентифікатори дій 1-10 представляють 10 дій: вихід, туалет, душ, сон, сніданок, вечеря, обід, перекус, вільний час/телебачення та догляд за собою. Наприклад, такі дії, як туалет і душ, можуть бути розпізнані точно (таблиця 1).

Таблиця 1 – Матриця помилок визнаних видів діяльності

№ активності	1	2	3	4	5	6	7	8	9	10
1	37	0	0	0	0	0	0	0	0	2
2	0	91	0	0	0	0	0	0	0	0
3	0	0	11	0	0	0	0	0	0	0
4	0	0	0	28	0	0	0	0	0	0
5	0	0	0	0	22	0	0	0	1	0
6	0	0	0	0	0	11	3	0	0	0
7	0	0	0	0	0	3	13	1	0	0
8	0	0	0	0	0	1	1	45	0	0
9	1	0	0	0	0	0	0	2	98	1
10	2	0	0	0	0	0	0	0	0	92

Згідно з розрахунками, середня точність на другому етапі становить 85,0%, а середня розпізнаваність дій – 87,9%. Дії № 6 і № 7 помилково ототожнюються тричі, вони представляють "обід" та "вечерю". У наборі даних дії "сніданок", "обід" і "вечеря" розглядаються як три різні дії. Хоча вони відрізняються в часовому

просторі, репрезентативні об'єкти, пов'язані з цими діями, є схожими. Однак несправедливо ділити такі чутливі до часу види діяльності лише за часом, оскільки мешканці мають різний розпорядок дня – наприклад, якщо час обіду з 11:00 до 13:00, то, крім того, мешканець може просто встати об 11:00 і поспідати. Якщо судити лише за часом, то це має бути "обід". Однак "сніданок" – це перший прийом їжі впродовж дня, який спричиняє конфлікт. У дослідженні планується об'єднати активності, які чутливі до часу, це допоможе краще розпізнавати такі види діяльності. Третій етап у процесі прогнозування спочатку потрібно відкоригувати та очистити вихідні дані. Розглядається та сама активність, яка повторюється через короткий проміжок часу, як псевдозапис і об'єднується разом. Крім того, видаляються деякі помилкові записи. Потім потрібно нормалізуємо дані, щоб використовувати їх для навчання LSTM-моделі. На відміну від другого етапу, на третьому етапі початкові 70% даних використовуються для навчання, а решта 30% – для тестування.

Мешканці виконують різні дії у відносно фіксованій послідовності. Наприклад, згідно з журналом активності, є мешканець, який завжди дивиться телевизор після вечері. Отже, якщо виявлено, що в даний момент він вечеряє, то його наступною активністю, швидше за все, буде перегляд телевізора. Таку проблему з прогнозуванням наступного стану на основі поточного стану можна вирішити за допомогою класичного підходу машинного навчання. Проте, наступна активність пов'язана не лише з поточною, але й з попередніми.

Це означає, що модель може передбачити наступну дію, використовуючи не лише поточну дію, але й декілька минулих дій. Це узгоджується з припущенням, що дії не відбуваються випадково, і що мотивація наступної дії - це те, що мешканець зробив в даний момент. Таким чином, точність прогнозування LSTM вища, ніж у класичного підходу машинного навчання; як і у випадку з першим підходом, для моделювання звичок мешканців враховується більше знань ( рисунок 1).

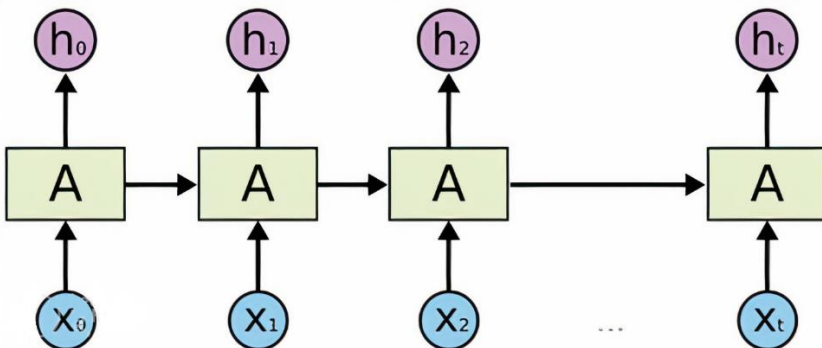


Рисунок 1 – Послідовність дій та модель рекурентної нейронної мережі (RNN)

Отже, система RF-ARP, яка створена для "розумних" будинків і використовується для визначення та розпізнавання дій людей всередині. Система використовує трьохетапний метод, який допомагає вирішити проблеми, пов'язані з розпізнаванням активності мешканців. Оскільки для цього методу не потрібен зворотній зв'язок, його можна буде використовувати у різних будинках, також має низьку вартість та мінімальне споживання енергії. Система була верифікована, використовуючи набір даних ADL з відкритим кодом з двома мешканцями, отримавши точність розпізнавання 85,0% і точність прогнозування 78,3%.

Тим не менш, поточна архітектура не позбавлена обмежень. Оскільки система розпізнавання активності в основному залежить від просторових знань, вона страждає від активності, яка має тимчасове семантичне значення. В майбутньому планується включити часові знання в цей метод, щоб виправити цей недолік.

### **Перелік посилань**

1. Feng, S.; Setoodeh, P.; Haykin, S. Smart home: Cognitive interactive people-centric Internet of Things. *IEEE Commun. Mag.* 2017, 55, 34–39.
2. Pradhan, S.; Chai, E.; Sundaresan, K.; Qiu, L.; Khojastepour, M.A.; Rangarajan, S. Rio: A pervasive rfid-based touch gesture interface. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking, Snowbird, UT, USA, 16–20 October 2017*; pp. 261–274.
3. Liu, Y.; Nie, L.; Liu, L.; Rosenblum, D.S. From action to activity: Sensor-based activity recognition. *Neurocomputing* 2016, 181, 108–115.
4. Du, Y.; Lim, Y.; Tan, Y. Activity Recognition Using RFID Phase Profiling in Smart Library. *IEICE Trans. Inf. Syst.* 2019, 102, 768–776.

УДК 004.7.056.5

Воробйов В.С., Лисенко С.М.

*Хмельницький національний університет*

## **ДОСЛІДЖЕННЯ МЕТОДІВ ІДЕНТИФІКАЦІЇ АТАК ТИПУ ФІШИНГ У КОРПОРАТИВНИХ МЕРЕЖАХ**

*Було проведено аналіз відомих методів виявлення кібератак типу фішинг, і виявлено, що існуючі підходи мають свої обмеження. Специфічно, ці методи не ефективно запобігають раннім атакам і лише обмежено блокують окремі інциденти, не охоплюючи всі можливі реальні атаки. Крім того, хоча існують певні інструменти, які можуть вирішити ці проблеми, наукові дослідження виділили інші недоліки, включаючи обмежений доступ до веб-сервісів і набору даних, що робить складним порівняння їхніх результатів з власними методами.*

*An analysis of known methods for detecting phishing attacks was conducted, and it was found that existing approaches have their limitations. Specifically, these methods are not effective in preventing early attacks and only block individual incidents to a limited extent, not covering all possible real attacks. In addition, while there are certain tools that can address these issues, research studies have highlighted other shortcomings, including limited access to web services and data sets, making it difficult to compare their results with our own methods.*

### **Вступ**

Фішингові атаки – це спроби зловмисників отримати конфіденційну інформацію, таку як паролі, номери кредитних карток та інші конфіденційні дані, видаючи себе за надійні джерела або осіб. Розглянемо функціональні особливості фішингових атак. [1-2].

Мета дослідження полягає в тому, щоб здійснити аналіз відомих методів виявлення атак типу фішинг та окреслити недоліки, які необхідно виправити засобами розроблення нових методів, що підвищать достовірність та ефективність ідентифікації атак типу фішинг.

### **Дослідження методів ідентифікації кібератак типу фішинг**

На відміну від традиційного підходу, заснованого на чорних списках, успіх інтелектуального підходу до виявлення фішингових сайтів значною мірою ґрунтується на виділенні загальних ознак веб-сайтів для ефективного навчання моделей машинного навчання з метою розпізнавання фішингових веб-сайтів [!!!!].

Так, у роботі [3] автори виділили чотири категорії релевантних ознак фішингових веб-сайтів: ознаки на основі HTML та JavaScript, ознаки на основі

адресного рядка, ознаки на основі домену та ознаки на основі аномалій. В [4] досліджено 51 401 унікальний фішинговий веб-сайт. Ця статистика доводить, що існуючі антифішингові рішення та зусилля не є по-справжньому ефективними. У роботі [5] було представлено новий метод для виявлення фішингових сайтів, який був названий як динамічний алгоритм прийняття рішень за категоріями (DCDA), в якому запропонований і використаний підхід багатовимірного виявлення фішингу за ознаками (MFPD).

У роботі [6] було вдосконалено алгоритм асоціативної класифікації за кількома мітками (Multi-Label Class асоціативної класифікації (MCAC) шляхом врахування особливості на основі контенту.

Метод в [7] є гібридизацією еволюційного алгоритму та глибокої нейронної мережі. еволюційного алгоритму та глибокої нейронної мережі. В якості еволюційного алгоритму в їхній дослідницькій роботі був використаний генетичного алгоритму (ГА), який був використаний для пошуку високоінформативні ознаки з вихідних наборів ознак.

Автори [8] запропонували систему на основі навчання для вибору порівнянності дизайну сторінок, яка використовується для розрізнення сторінок фішингових атак. Для ефективного визначення особливостей макета сторінки вони охарактеризували рекомендації та побудували класифікатор фішингових сторінок за допомогою двох традиційних алгоритмів навчання, SVM та DT. Вони протестували методологію на реальних тестах сторінок сайтів phishtank.com та alexa.com.

Автори [9] запропонували порівняння Adaboost та мульти-бустінгу для виявлення фішингових сайтів. Вони використовували набір даних репозиторію машинного навчання UCI, що містить 11 055 екземплярів і 30 ознак. AdaBoost та multi boost - це ансамблеві моделі навчання, запропоновані в цьому дослідженні для покращення представлення розрахунків фішингових атак. Ансамблеві моделі покращують представлення класифікаторів з точки зору точності, F-міри та області ROC. Експериментальні результати показують, що за допомогою ансамблевих моделей можна розпізнавати фішингові сторінки з точністю 97,61%.

Автори [10] запропонували новий підхід, в якому URL-адреса надсилається як вхідні дані, а URL-адреса, а також ознаки, пов'язані з HTML, витягуються. Після вилучення ознак використовується модель стекування для об'єднання класифікаторів. Вони провели експерименти на різних наборах даних: Перший був отриманий з Phishtank і містив 2000 веб-сторінок (1000 легальних і 1000 фішингових).

Автори [11] використовували різні класифікатори, такі як C4.5, IBK, NB та SVM.

Аналогічно, автори в [12] використовували RF для того, щоб відрізнити фішингові атаки від оригінальних веб-сторінок.



## Висновок

З'ясовано, що існуючі підходи до виявлення кібератак типу фішинг мають обмеження, оскільки вони не ефективно протистоять раннім атакам і блокують лише окремі інциденти, а не всі реальні атаки. Додатково, хоча є певні засоби, які можуть компенсувати ці недоліки, наукові дослідження виокремили деякі інші недоліки, включаючи обмежений доступ до веб-сервісів та набору даних, що ускладнює порівняння їхніх результатів із власним методом. Отже, існує актуальна науково-практична задача по вдосконаленню методів виявлення кіберзагроз типу "фішинг" з метою підвищення їхньої надійності та ефективності.

## Перелік посилань

1. Ali, W., & Malebary, S. (2020). Particle swarm optimization-based feature weighting for improving intelligent phishing website detection. *IEEE Access*, 8, 116766–116780.
2. Patel, P., Sarno, D. M., Lewis, J. E., Shoss, M., Neider, M. B., Bohil, C. J. (2019). Perceptual Representation of Spam and Phishing Emails. *Applied Cognitive Psychology*, асп.3594. <https://doi.org/10.1002/acp.3594>
3. Cybercrime Protection: Phishing and How to Avoid it? <https://www.bocasay.com/cybercrime-protection-phishing-avoid/>
4. C. C. Inez and F. Baruch, "Setting Priorities in Behavioral Interventions: An Application to Reducing Phishing Risk," *Risk Anal.*, vol. 38, no. 4, pp. 826-838, Apr. 2019.
5. Jakobsson, M. The Rising Threat of Launchpad Attacks. *IEEE Secur. Priv.* 2019, 17, 68–72.
6. Abdelhamid, Neda & Ayyesh, Aladdin & Thabtah, Fadi. (2014). Phishing detection based Associative Classification data mining. *Expert Systems with Applications*. 41. 5948–5959. 10.1016/j.eswa.2014.03.019.
7. W. Ali and A. A. Ahmed, "Hybrid intelligent phishing website prediction using deep neural networks with genetic algorithmbased feature selection and weighting," *IET Inf. Secur.*, vol. 13, no. 6, pp. 659–699, 2019.
8. Mao, J.; Bian, J.; Tian, W.; Zhu, S.; Wei, T.; Li, A.; Liang, Z. Phishing Page Detection via Learning Classifiers from Page Layout Feature. *EURASIP J. Wirel. Commun. Netw.* 2019, 43. Available online: <https://jwcn-urasipjournals.springeropen.com/articles/10.1186/s13638-019-1361-0> (accessed on 27 September 2021). [CrossRef]
9. S. Rao and A. R. Pais, "Jail-Phish: An improved search engine based phishing detection system," *Comput. Secur.*, vol. 83, pp. 246–267, 2019.
10. Li, Y., Yang, Z., Chen, X., Yuan, H., & Liu, W. (2019). A stacking model using url and html features for phishing webpage detection. *Future Generation Computer Systems*, 94, 27–39.
11. S. Wang, X. Jiang, W. Cui, T. Huang, B. Li, and Y. Qian, "Robust detection of web phishing using RBF based on an improved extreme learning machine," *Expert Systems with Applications*, vol. 42, no. 21, pp. 7374-7382, 2019.
12. A. Agresti, "Foundations of Linear and Generalized Linear Models," John Wiley & Sons, 2019.

УДК 004.4

Галицький О.С.

*Хмельницький національний університет*

## **ПІДВИЩЕННЯ ЯКОСТІ КЕРУВАННЯ КВАДРОКОПТЕРОМ ЗА ДОПОМОГОЮ ВИКОРИСТАННЯ РЕТРАНСЛЯТОРА**

*Розглянуто проблему накладання відеосигналів при роботі з дронами на однаковій частоті. Запропоновано рішення у вигляді ретранслятора сигналів та розроблено платформу-тримач ретранслятора для БПЛА типу Mavic.*

*The problem of overlapping video signals when working with drones at the same frequency was considered. A solution in the form of a signal repeater is proposed and a repeater-holding platform for Mavic-type UAVs is developed.*

Проблема, яку розглянуто, полягає у тому, що при роботі оператора з дроном, іноді інші команди, які знаходяться неподалік, вмикають дрон і працюють на тій самій частоті відеосигналу. Через це відеосигнали обох команд накладаються один на одного і цим самим створюють перешкоди одна для одної. Пілот 1 замість зображення з дрону 1 бачить картинку дрону 2 чи навпаки пілот 2 бачить картинку дрону 1. Було розглянуто ймовірні варіанти вирішення цієї проблеми:

1. Створити загальну систему оповіщень, хто з операторів на якій частоті працює і в який час.

Труднощі реалізації: дану систему треба вводити на всю лінію фронту, що є довгим та бюрократичним процесом. В реаліях бойових дій дане рішення не є доцільним і потребує набагато нагальніших варіантів.

2. Створити індивідуальну систему, для пілота, щоб у разі співпадіння частот пілот міг швидко переключити канал відеозв'язку.

В протоколі Crossfire є можливість переключити канал відео з пульта. Для цього до Vtx порта в дроні потрібно встановити IRCTramp(Zeus pro) або Tbs smart audio(rush solo tank) протокол.

Дана задача є можливою для вирішення, але для перемикання каналу пілоту треба зняти окуляри, і зайти в меню пульта щоб здійснити операцію. Так само потрібно змінити канал прийому на окулярах. Дана операція досить є повільною і займе до хвилини часу. За цей період інший дрон ймовірно все втрутиться.

З даної ідеї випливає наступне завдання: пришвидшити час перемикання каналу на приймачі і передавачі до кількох секунд.

Дана задача без проблем реалізується на FC-коптері за допомогою тонких налаштувань відеопередавача і пульта. Тобто на одному з аналогових каналів пульта, наприклад auh4 (3 позиційний стік) встановити перемикання між собою 3-х

каналів відео. Проблемою залишається перемикання каналів на окулярах, адже прямого зв'язку окулярів та пульта немає.

Варіантом рішення є винести приймач відео сигналу окремо, та використати ретранслятор, як показано на рисунку 1.

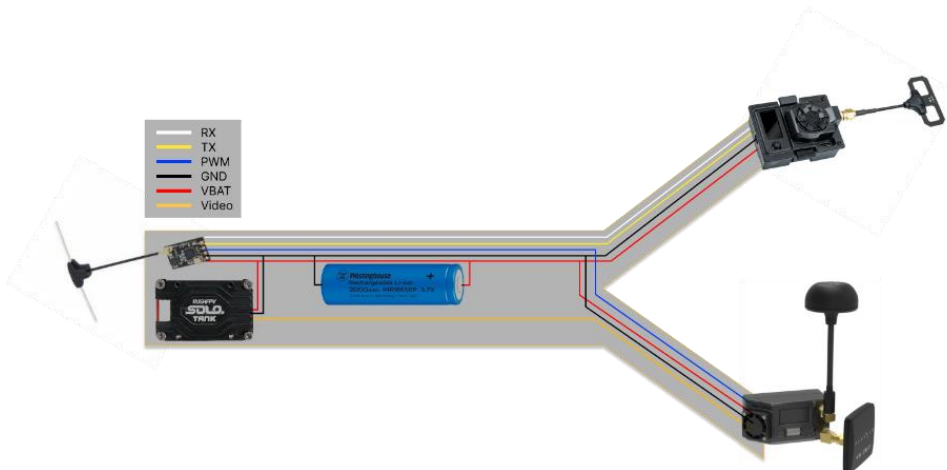


Рисунок 1 – Схема перемикання каналів за допомогою ретранслятора

Принцип роботи, який зображено на схемі на рисунку 1 наступний: у підота є пульт керування з каналом 2.4ггц. На БПЛА типу мавік є приймач керування на 2.4ггц. Даний приймач передає сигнал на 2 об'єкти: передавач 900мгц, який вже приймає коптер 900мгц, та керування платою приймача відео на 5.8ггц. На приймачі 2.4, один із виходів можна запрограмувати на роботу того ж самого аналогового сигналу пульта аух4. На відео приймачі запрограмувати зміну параметру аух4 відповідає за зміну каналу приймання. Відео приймач за допомогою кабеля чи за допомогою іншого відеопередавача з нижчим сигналом, скажімо 1.2ггц передає сигнал на окуляри пілота.

Для проведення експерименту з текстоліту було виготовлено тримач ретранслятора на Mavic (рисунок 2). Також було використано наступні комплектуючі:

1. Передавач відео RushFPV TANK SOLO VTX
  2. Приймач відео Skyzone steadyview x receiver with IPS screen (STVX)
  3. Антена TrueRC 5.8 МК II SMA RHCP
  4. Приймач керування з додатковими pwm виходами HappyModel ExpressLRS ELRS EPW6 TCXO 2.4GHz
  5. Передавач керування BETA FPV ELRS Micro TX Module 915MHZ
  6. Перетворювачі напруги типу DC-DC
- Для унівесалізації живлення використано елементи типу 18650.



Рисунок 2 – Платформа-рогатка з текстоліту для кріплення до БПЛА типу Mavic

У результаті було отримано перемикач на пульті, який одночасно перемикає канал на передавачі відеосигналу дрона та на приймачі відеосигналу на ретрансляторі. Недоліком є те що перемикання каналів обмежене кількістю перемикачів в аналоговому тумблері пульта, а саме 3 канали, на tx12. Але для екстрених ситуацій дана схема дієздатна та може врятувати дрон та продовжити місію.

### Перелік посилань

1. Зубрецька І. С., Афонін І. В., Зубрецька Н. А. Дослідження технічних та метрологічних характеристик засобів радіопеленгації. Наукові розробки молоді на сучасному етапі : тези доп. XVII Всеукр. наук. конф., Київ, 26–27 квітня 2018 р. С. 347–348.
2. Калашніков Д.С., Тимченко В.В., Шутько В.О. Огляд методів радіопеленгування наземної РЕБ. Ольвійський форум – 2023: стратегії країн Причорно-морського регіону в геополітичному просторі. Технічні на-уки. Сталий розвиток університетської системи освіти: XVII Міжнар. наук. конф. 15–18 черв. 2023 р., с. 31-34.

УДК 004.4

Гардиш Д.О., Кліменко В.І.

*Хмельницький національний університет*

## **ПРИКЛАДНІ АСПЕКТИ АВТОМАТИЗОВАНОГО ОЦІНЮВАННЯ ВІДПОВІДНОСТІ КЕЙСА ТЕСТОВИХ ЗАВДАНЬ СЕМАНТИЧНІЙ СКЛАДОВІЙ НАВЧАЛЬНИХ МАТЕРІАЛІВ**

*Розглянуто прикладні аспекти програмної реалізації застосунку для автоматизованого оцінювання відповідності кейса тестових завдань семантичній складовій навчальних матеріалів. Також наведено особливості роботи відповідного методу, що базується на інтелектуальному аналізі текстового контенту тестових і навчальних матеріалів.*

*The applied aspects of software implementation of application for automated assessment of compliance of the case test tasks with the semantic component of educational materials are considered. Features of corresponding method based on intellectual analysis of textual content of test and educational materials are also given.*

В сучасному освітньому процесі велика увага зосереджена на вдосконаленні якості та ефективності навчальних матеріалів, зокрема, тестових завдань, які є цінним інструментом для оцінки знань та розуміння учнів. Проте, варто не забувати, що звичайні методи оцінювання зазвичай обмежені тільки перевіркою правильності відповідей без урахування семантичного зв'язку та контексту [1, 2]. В результаті чого це може призвести до мало об'єктивних результатів та неефективного використання навчальних матеріалів.

Метод автоматизованого оцінювання відповідності кейса тестових завдань семантичній складовій навчальних матеріалів базується на інтелектуальному аналізі текстового контенту цих матеріалів. Він використовує комп'ютерні алгоритми та техніки обробки природної мови для визначення семантичного зв'язку між тестовими завданнями та навчальними матеріалами [3]. Цей метод дозволяє автоматично визначати, наскільки відповіді на тестові завдання відповідають змісту та семантиці навчальних матеріалів. На рисунку 1 зображений метод оцінювання відповідності кейса тестових завдань семантичній складовій навчальних матеріалів.

На вхід метод приймає обраний текст інформаційно-навчальних матеріалів, а також кейс тестових завдань, який відповідає обраній темі. Для відповідних цілей у застосунку було створено спеціальний редактор навчальних матеріалів (рисунк 2). Після того як весь вміст навчальних матеріалів та тестових завдань було виведено на форму, користувач може їх редагувати. Тобто, вносити зміни в текст навчальних матеріалів та зберігати ці зміни. Також можна редагувати тестові запитання.



Рисунок 1 – Схема методу оцінювання відповідності кейса тестових завдань семантичній складовій навчальних матеріалів

Після прийому вхідних даних, починається їх обробка. Спершу йде фільтрація ІНМ. Фільтрація включає в себе видалення знаків пунктуації та цифр, а також перетворення всього тексту в нижній регістр. Після чого відбувається векторизація контенту ІНМ, тобто перетворення на масив слів. Для кейса тестових запитань застосовуються ті ж етапи, що й до навчальних матеріалів.

Отримавши два переліки слів, метод приступає до їх семантичного аналізу. Тобто, відбувається формування множини ключових слів для ІНМ за допомогою методу DE [4].

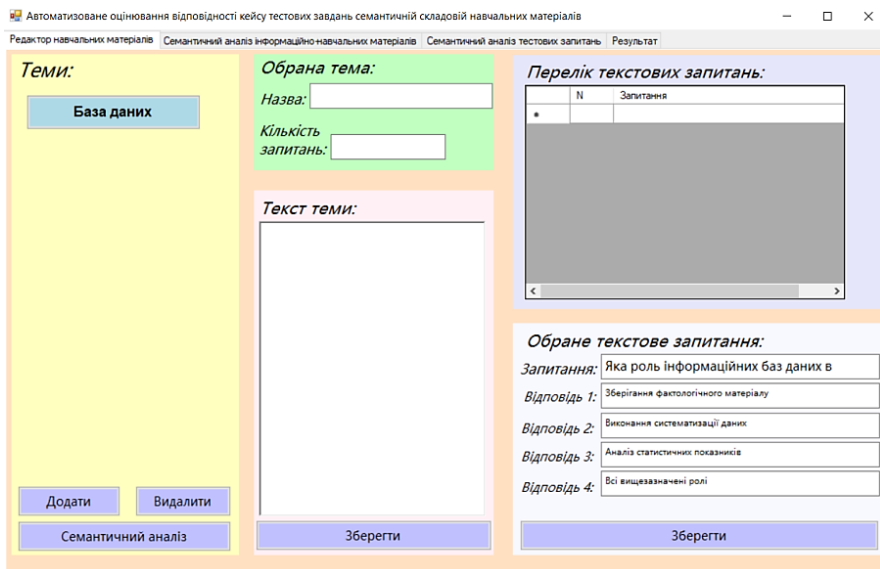


Рисунок 2 – Знімок екрану першої вкладки застосунку

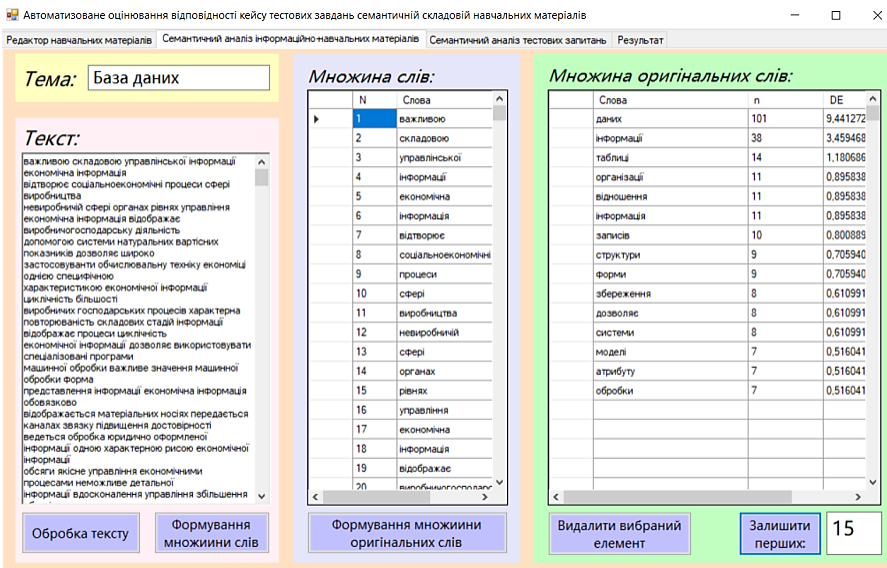


Рисунок 3 – Результат семантичного аналізу ІНМ

Першим етапом йде формування множини оригінальних слів. Після чого, з тексту видаляються стоп-слова, такі як прийменники, займенники, числівники та сполучники. Далі для ІНМ обраховуються відстані між словами та обрахунок важливості за допомогою DE (рисунок 3), а для КТЗ йде обрахунок кількості оригінальних слів (рисунок 4). Після чого йде формування множини ключових слів.

Автоматизоване оцінювання відповідності кейсу тестових завдань семантичній складовій навчальних матеріалів

Редактор навчальних матеріалів Семантичний аналіз інформаційно-навчальних матеріалів Семантичний аналіз тестових запитань Результат

**Тема:** База даних

**Текстовий контент тестових запитань:**

складова управлінської інформації важливою відтворює соціально-економічні процеси таблиці таблиця технологічна інформаційна економічна інформація соціологічна інформація політична інформація які показники використовуються відображення виробничого господарської діяльності допомогою економічної інформації записів записів тільки натуральні показники тільки вартісні показники натуральні вартісні показники фінансові показники управління економічними процесами неможливі характеристики економічної інформації системи системи система достовірність об'єктивність систематичність актуальність програми можна використовувати машинної обробки циклічної економічної інформації моделі моделі редакторів операційні системи текстові редактори економічна інформація передається допомогою натуральних показників допомогою вартісних показників завантаженою інформацією комунікації підлягають обробці підвищення достовірності економічної інформації юридично оформлена інформація фактологічний матеріал статистичні показники фінансові звітника економічної інформації описує обсяги деталізація комплексність циклічність об'ємність інформацію зазвичай включають

**Множина слів:**

N	Слова
1	складова
2	управлінської
3	інформації
4	важливою
5	відтворює
6	соціально-економічні
7	процеси
8	таблиці
9	таблиця
10	таблиця
11	технологічна
12	інформацій
13	економічна
14	інформація
15	соціологічна
16	інформацій
17	політична
18	інформаційні
19	показники
20	виключити

**Множина оригінальних слів:**

Слова	n
даних	11
вищезазначені	9
кадровий	5
інформації	5
допомогою	5
фінансові	5
склад	5
економічної	5
даних	4
працівників	4
тільки	4
даних	4
вимоги	4
інформацію	4
організації	3
даних	3
дозволяє	3
збереження	3
характеризують	3
львів	1

Обробка тексту    Формування множини слів    Формування множини оригінальних слів    Видалити вибраний елемент

Рисунок 4 – Результат семантичного аналізу КТЗ

Після того як метод отримає ключові терміни ІНМ та ключові терміни КТЗ він переходить до останнього етапу – співставлення відповідності кейса тестових завдань семантичній складовій навчальних матеріалів. Метод перевіряє чи усі важливі терміни, які містяться у навчальних матеріалах наявні у тестових запитаннях.

Вихідними даними даного методу є цифрова оцінка відповідності кейса тестових завдань семантичній складовій навчальних матеріалів за інтелектуальним аналізом їх текстового контенту. Також користувач також може отримати експертний висновок програми з рекомендацією, які ключові терміни з навчальних матеріалів варто включити в зміст тестових запитань. Для цього йому необхідно



натиснути на кнопку «Згенерувати висновок» (рисунок 5). Після чого кінцевий результат застосунку набуде наступного вигляду.

Автоматизоване оцінювання відповідності кейсу тестових завдань семантичній складовій навчальних матеріалів

Редактор навчальних матеріалів Семантичний аналіз інформаційно-навчальних матеріалів Семантичний аналіз тестових запитань Результат

Тема:

Оцінка відповідності: 80%

N	Термін	Важливість	Кількість завдань
1	дані	9,44127211747572	11
2	інформації	3,45946890134739	3
3	таблиці	1,1806867237747	0
4	організації	0,895838951578111	3
5	відношення	0,895838951578111	1
6	інформація	0,895838951578111	1
7	записів	0,800889694179248	0
8	структури	0,705940436780386	1
9	форми	0,705940436780386	1
10	збереження	0,610991179381523	3
11	дозволяє	0,610991179381523	3
12	системи	0,610991179381523	0
13	моделі	0,516041921982661	0
14	атрибути	0,516041921982661	2

**Висновок:**

Проаналізувавши вхідні дані за допомогою застосунку автоматичної оцінки відповідності кейсу тестових завдань семантичній складовій навчальних матеріалів було виявлено, що не усі ключові слова, які містяться в навчальних матеріалах є наявними в тестових запитаннях. Тому задля кращого оцінювання по даній темі користувачу варто додати запитання, в яких будуть наявні наступні терміни:

таблиці  
записи  
системи  
моделі

Рисунок 5 – Результат аналізу відповідності КТЗ до ІНМ

Розробивши застосунок з реалізацією методу автоматичного оцінювання відповідності кейса тестових завдань семантичній складовій навчальних матеріалів за інтелектуальним аналізом їх текстового контенту, було отримано діаграму класів (рисунок 6). З рисунку можна побачити що основними класами в даному застосунку є клас «Form1», «Text Processor», «Read Text», «Semantic».

Клас «Form1» є основним в даному застосунку, та містить в собі методи багатьох компонентів форми. Клас містить приватне поле folder Path, яке відповідає за збереження шляху до папки з файлами. У даному класі реалізовані методи ReadText() та LoadDataIntoDataGridView(), які реалізують виведення даних на відповідні компоненти DataGridView. Також клас містить методи, які викликаються при натисканні на кнопку, ці методи відповідно виконують ті функції за які відповідає кожна з кнопок.

Клас «ReadText» відповідає за методи зчитування даних з текстових файлів. Перший метод – readINM(), відповідає за зчитування тексту інформаційно-навчальних матеріалів. Отримує ім'я файлу, далі створює шлях до нього та повертає його вміст у вигляді рядка. Метод LoadDataIntoDataGridView() відповідає за

зчитування тексту кейса тестових завдань. Тобто метод зчитує дані з файлу по рядках та повертає їх масив.

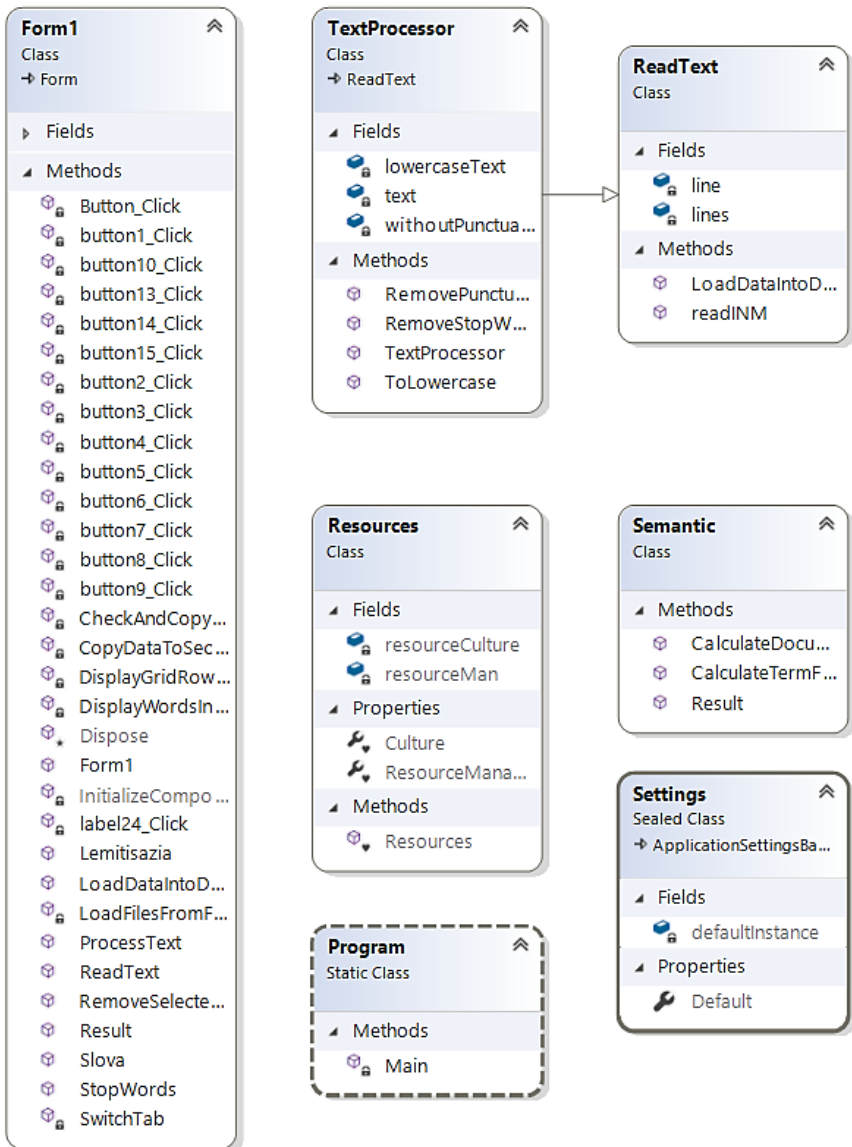


Рисунок 6 – Діаграма класів застосунку для аналізу відповідності КТЗ до ІНМ

Клас «TextProcessor» загалом використовується для обробки вхідного тексту. Метод RemovePunctuation() видаляє всі знаки пунктуації, ToLowercase() – перетворює текст у нижній регістр, а RemoveStopWords() відповідає за видалення стоп-слів з тексту.

Останній клас – «Semantic», він містить у собі два методи для обчислення TF та DE. Перший метод «CalculateTermFrequency» перебирає кожне слово методу та для нього обраховує частотну оцінку. Метод «CalculateDocumentImportance» також перебирає кожне слово тексту та вираховує його важливість за допомогою дисперсійної оцінки.

Отож, розроблена система може мати великий потенціал під час її використання у навчальних закладах та організаціях, де важливо оцінювати відповідність тестових завдань навчальним матеріалам. Вона дозволить автоматизувати процес оцінювання та забезпечить об'єктивність результатів.

Для вдосконалення системи, можна розглянути наступні напрямки розробки: покращення алгоритмів семантичного аналізу за допомогою більш спеціалізованих методів, більш точний алгоритм для порівняння тексту з тестовими запитаннями та розробка більшої функціональності системи.

### Перелік посилань

1. Myownconference. Онлайн тестування та анкетування. URL: <https://myownconference.com/blog/uk/onlajn-testuvannya-ta-ankety/>
2. Stud. Дисперсійна оцінка. URL: [https://stud.com.ua/50291/psihologiya/dispersiya\\_otsinka](https://stud.com.ua/50291/psihologiya/dispersiya_otsinka)
3. Бармак О. В., Мазурець О. В. Інформаційна модель семантичної структури навчального курсу Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2018. №6. Т.1. С.92-97.
4. 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 004.8

Головатюк А.О.

*Хмельницький національний університет*

## **ДОСЛІДЖЕННЯ ПІДСИСТЕМИ РОЗПІЗНАВАННЯ ТА АНАЛІЗУ ДОРОЖНІХ ЗНАКІВ МЕТОДАМИ КОМП'ЮТЕРНОГО ЗОРУ**

*В даній статті було розглянуто підсистему розпізнавання та аналізу дорожніх знаків методами комп'ютерного зору. Під час дослідження було проаналізовано пропозиції інших розробників у даній тематиці, описано алгоритм роботи підсистеми та проведено її тестування.*

*In this article were considered a subsystem for recognizing and analyzing road signs using computer vision methods. The research analyzed the proposals of other developers in this area, described the algorithm of the subsystem and tested it.*

Згідно з повідомленням від Департаменту патрульної поліції України, за період 2022 року в Україні сталось понад 18 тисяч дорожньо-транспортних пригод. При цьому близько 23 тис. людей отримали поранення, 2791 особа загинула. Основними причинами ДТП виділяють: перевищення безпечної та встановленої швидкості руху, порушення правил маневрування, порушення правил проїзду пішохідних переходів та перехресть, недотримання дистанції [1]. В більшості ситуацій, їх можна було уникнути, якщо б учасники дорожнього руху були пильніше та приділяли увагу дорожнім знакам. Тому, після перегляду статистик ДТП було прийнято рішення розробити підсистему розпізнавання та аналізу дорожніх знаків за допомогою методів комп'ютерного зору.

Під час проведення досліджень було розглянуто декілька статей інших науковців на дану тему.

В одній з проаналізованих статей [2] пропонується використовувати двоетапну каскадну систему виявлення об'єктів на дорозі на основі регресії. Система одночасно використовує одноступеневі методи виявлення об'єктів, які є надзвичайно швидкі, та двоетапні методи, які мають високий показник точності виявлення, але мають обмеження в швидкості роботи. Розпізнавання кадрів і виявлення дорожніх знаків може бути виконано за допомогою сегментації на основі кольорів і виявлення за допомогою перетворення Гафа (Hough) з подальшою класифікацією за допомогою капсульної нейронної мережі [3].

Для виявлення дорожніх знаків пропонують також використати техніку глибокого навчання на основі згорткових нейронних мереж [4]. А також, вдосконалений алгоритм SSD (Single Shot Detector) з використанням

багатоканального злиття та покращення ознак, позначений як MF-SSD, для розпізнавання дорожніх знаків [5].

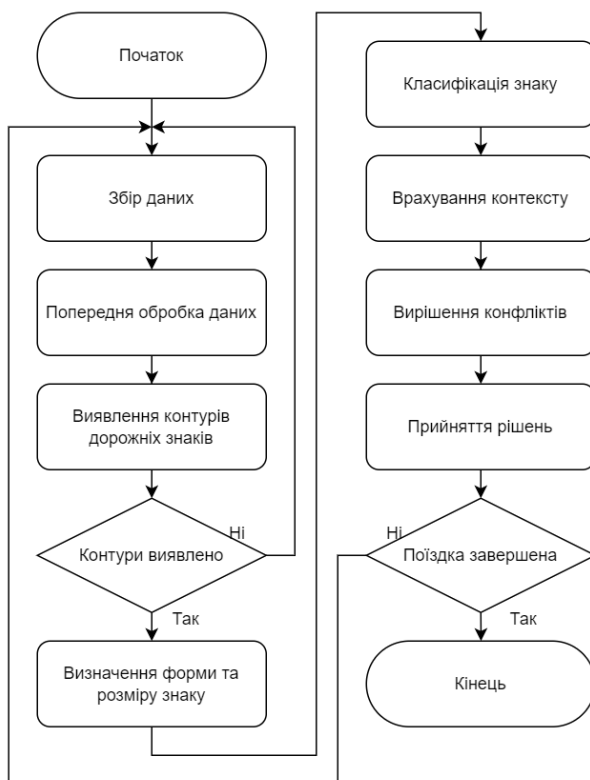


Рисунок 1 – Алгоритм розпізнавання дорожніх знаків

Алгоритм розпізнавання дорожніх знаків зображено на рисунку 1. Він включає наступні кроки:

1. Збір даних: Спочатку використовується спеціальне обладнання, таке як камера, для збору візуальних даних з навколишнього середовища автомобіля.

2. Попередня обробка: Отримані візуальні дані можуть бути зашумленими або містити надмірну інформацію. Попередня обробка включає у себе такі етапи, як зменшення шуму, фільтрація, збільшення контрастності тощо.

3. Виявлення контурів: Спеціальні алгоритми аналізують оброблене зображення, щоб виявити можливі контури дорожніх знаків. Цей етап дозволяє виділити області, де можливо розташовані знаки.

4. Визначення форми та розміру: На основі виявлених контурів алгоритм намагається визначити форму та розмір потенційного дорожнього знаку. Це включає в себе аналіз кутів, відстаней між точками та ін.

5. Класифікація знаку: Одразу після визначення форми та розміру, система пробує класифікувати знак за його образом. Це включає в себе порівняння розпізнаного зображення з базою даних знаків для визначення його значення.

6. Врахування контексту: Деякі ситуації можуть вимагати врахування контексту. Наприклад, якщо два знаки мають схожий образ, система використовує інші дані, такі як місцезнаходження, тип дороги, час доби тощо.

7. Ви рішення конфліктів: Якщо два або більше знаків можуть бути застосовані до поточної ситуації, система використовує різні евристичні або аналізує додаткові параметри для визначення найбільш ймовірного варіанту.

8. Прийняття рішення: На основі класифікації та контексту, система приймає рішення про те, як реагувати на розпізнаний знак. Це включає в себе надсилання водію попередження та відображення інформації на панелі приладів.

За даним алгоритмом було створено тестову версію програмного забезпечення. Реальна система буде включати в себе камеру для зчитування ситуації на дорозі, екран на панелі керування для виведення інформації для водія, динамік для програвання деяких попереджувальних сигналів та сам автомобіль. Тестова версія функціонує в програмному середовищі та працює наступним чином: в програму завантажуються фотографії на яких присутні (іноді відсутні, для тестування адекватності системи) дорожні знаки. Програма аналізує фото, знаходить на ньому дорожній знак, окреслює зону, де його було знайдено, та виводить повідомлення про значення знайденого знаку.

Результати тестування показано на рисунках 2 та 3.

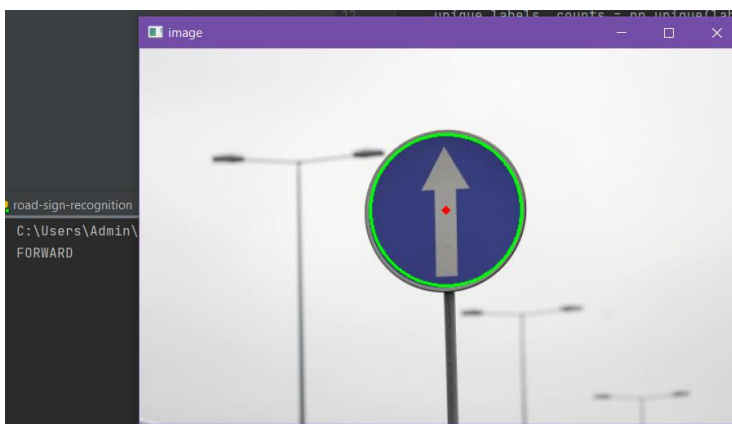


Рисунок 2 – Тестування підсистеми розпізнавання дорожніх знаків на фотографії з одним знаком

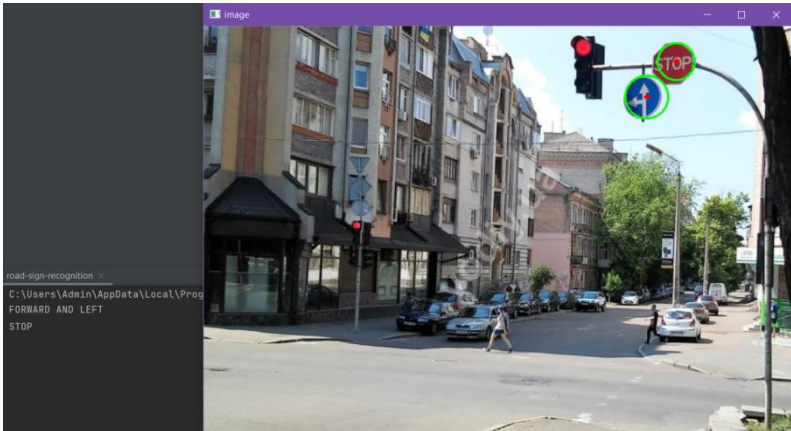


Рисунок 3 – Тестування підсистеми розпізнавання дорожніх знаків на фотографії з двома знаками

Отже, була розглянута актуальна проблема дорожньо-транспортних пригод в Україні та наголошено на необхідності уваги до дорожніх знаків для запобігання подібним ситуаціям. Дослідження включило аналіз різних методів розпізнавання дорожніх знаків, включаючи каскадну систему виявлення об'єктів та використання нейронних мереж для цієї мети. У майбутньому планується розробка реальної системи, яка включатиме камеру для моніторингу дорожньої ситуації, екран для відображення інформації для водія, динамік для програвання сигналів та інших елементів. Також, під час розгляду цієї теми було наведено алгоритм роботи такої підсистеми та протестовано її пробну версію без залучення реальних автомобілів. Цей крок є важливим у покращенні безпеки дорожнього руху та запобіганні ДТП.

### Перелік посилань

1. Найпоширеніші причини ДТП у 2022 році: поліція показала статистику. URL: <https://glavcom.ua/techno/auto/dtp-907624.html> (дата звернення: 21.10.2023).
2. X. Dai. HybridNet: A fast vehicle detection system for autonomous driving. Signal Processing: Image Communication, 2019. pp. 79-88.
3. M. H. Koresh. Computer vision based traffic sign sensing for smart transport. Journal of Innovative Image Processing, 2019. pp. 11-19.
4. Y. Jin, Y. Fu, W. Wang, J. Guo, C. Ren, X. Xiang, (2020). Multi-feature fusion and enhancement single shot detector for traffic sign recognition. IEEE access, 8, 38931-38940.
5. Ayachi, R., Afif, M., Said, Y., & Atri, M. (2020). Traffic signs detection for real-world application of an advanced driving assisting system using deep learning. Neural Processing Letters, 51, 837-851.

УДК 004.4

Денисенко Б.О., Молчанова М.О., Кліменко В.І.

*Хмельницький національний університет*

## **ПІДХІД ДО АВТОМАТИЗОВАНОГО ВИРІШЕННЯ ЗАДАЧ ЛІНІЙНОГО ПРОГРАМУВАННЯ**

*Розглянуто підхід до автоматизованого вирішення задач лінійного програмування та розглянуто прикладні аспекти відповідного програмного застосунку. Забезпечено можливість розв'язувати різні типи завдань лінійного програмування, обробку великого обсягу вхідних даних, підтримку різноманітних типів задач лінійного програмування, відтворення для знаходження результату.*

*The approach to automated solution of linear programming problems is considered and the applied aspects of corresponding software application are considered. The ability to solve various types of linear programming tasks, processing of large volume of input data, support for various types of linear programming tasks, reproduction to find the result is provided.*

Ефективність роботи сучасних підприємств, які є складними системами, залежить від якості організаційного управління. Процеси прийняття рішень лежать в основі будь-якої цілеспрямованої діяльності. При формуванні стратегічних і тактичних рішень керівник повинен враховувати безліч часом суперечливих міркувань, спиратися на складні критерії ефективності шляхів досягнення кінцевих цілей. У зв'язку з цим виникла необхідність застосовувати для аналізу і синтезу економічних ситуацій і систем математичні методи і сучасну обчислювальну техніку. Такі методи об'єднуються під загальною назвою – математичне програмування [1].

Завдання математичного програмування знаходять застосування в різних областях людської діяльності, де необхідний вибір одного з можливих варіантів дій, наприклад при вирішенні багаточисельних проблем управління і планування виробничих процесів, в задачах проєктування та перспективного планування, при організації функціонування та розвитку соціальних процесів, їх координації з господарськими та економічними процесами [2]. Оптимальні (ефективні) рішення дозволяють досягати мети при мінімальних витратах трудових, матеріальних і сировинних ресурсів.

Ефективність автоматизації за допомогою інформаційних технологій полягає у швидкості та точності самих обчислень. До того ж за допомогою комп'ютера ми матимемо змогу обробляти дійсно великі обсяги даних і проводити складні оптимізаційні розрахунки, що дозволить нам значно економити велику кількість часу і та зберегти наші ресурси.



Метою роботи є розробка підходу до автоматизованого вирішення задач лінійного програмування і його апробація. Має бути забезпечена підтримка різноманітних типів задач лінійного програмування, включаючи мінімізацію, максимізацію та цілочисельне програмування.

Для полегшення проєктування підходу було створено декілька діграм. На рисунку 1 подано діаграму варіантів використання [3].



Рисунок 1 – Діаграма варіантів використання застосунку

Зміна кількості «стовбців» чи «рядків» викликає за собою оновлення матриці вхідних даних. «Вхідні дані» містять в собі цільову функцію задачі лінійного програмування, обмеження, а також її тип (максимізація чи мінімізація). Вибір алгоритму включає в себе додаткові покращення для оптимізації, як от цілочисельна оптимізація та інші.

Задля запуску розв'язку обов'язковою умовою є «ініціалізація вхідних даних».

На рисунку 2 за допомогою «Activity diagram»[14] представлено хід розв'язку задачі.

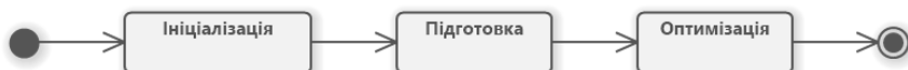


Рисунок 2 – Діаграма активності ходу розв’язування ЗЛП

Процес ініціалізації включає в себе заповнення цільової функції, обмежень, а також типу задачі (мінімум/максимум). Підготовку ж у свою чергу можна розбити на декілька етапів. Перший – приведення задачі до коректного типу (задачу на мінімум перетворити на задачу на максимум) (рисунок 3).



Рисунок 3 – Діаграма активності дочірнього процесу підготовки вхідних даних ЗЛП. Приведення задачі до коректного типу

Наступним кроком буде перетворення обмежень за допомогою внесення додаткових змінних. Схематично зображено на рисунку 4.



Рисунок 4 – Діаграма активності дочірнього процесу підготовки вхідних даних ЗЛП. Корегування обмежень

Останнім кроком слід перевірити, чи можливо виділити в задачі базис, і якщо ні, додати штучні змінні (рисунок 5).



Рисунок 5 – Діаграма активності дочірнього процесу підготовки вхідних даних ЗЛП. Введення штучного базису

Після підготовки даних можна приступати до розв'язку задачі, алгоритм чого зображено на наступній «activity diagram» (рисунок 6).

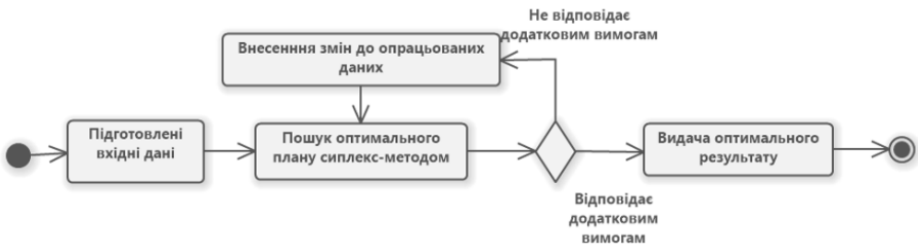


Рисунок 6 – Діаграма активності процесу оптимізації ЗЛП

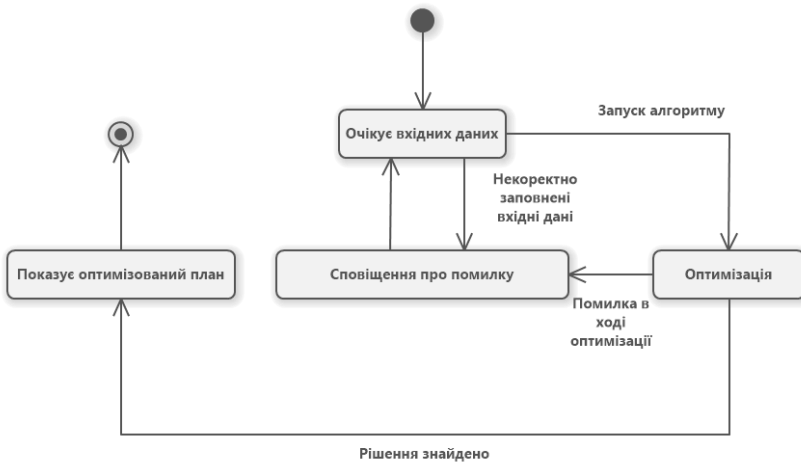


Рисунок 7 – Діаграма станів

Варто звернути увагу на те, що приховано під «додатковими умовами» та «внесенням змін до опрацьованих даних». Якщо взяти, до прикладу, алгоритм розв'язування ЗЛП в цілих числах, то за другим буде сховано додавання нового обмеження, а за першим – перевірка на те, чи можливо взагалі додати те обмеження.

На рисунку 7 зображено діаграму станів розв'язку задачі. Помилками у вхідних даних можуть бути, до прикладу, пусті, або не правильно поля даних (цільова функція, обмеження). У разі їх коректності буде можливо запустити алгоритм оптимізації. У його роботі також можуть статися помилки: не перехоплені на етапі заповнення, або ж викликані в ході роботи (план не можливо оптимізувати). Коли рішення буде все ж таки знайдено, показати його користувачу.

Для того, щоб показати взаємодію деяких об'єктів у динаміці, побудовано діаграму послідовностей (рисунк 8).

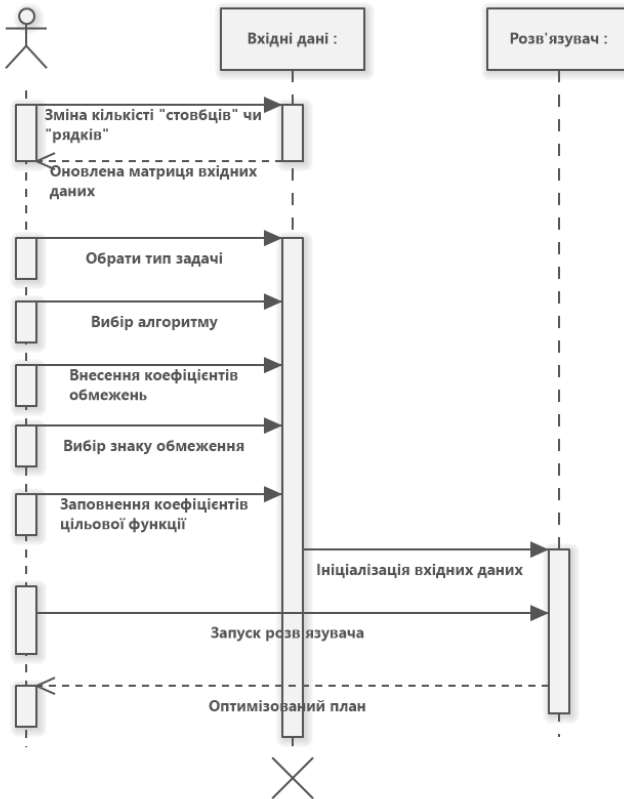


Рисунок 8 – Діаграма послідовностей розв'язування ЗЛП

Серед можливих архітектур для розробки була обрана «компонентна» [4], коли кожен компонент відповідає за конкретну функціональність або аспект застосунку. Така декомпозиція дозволяє логічно групувати функції та розділяти відповідальність. Вибір компонентної архітектури з фокусом на розподілі компонентів по категоріях є хорошою стратегією. Це дозволяє зберегти чіткість, модульність та розширюваність застосунку, а також забезпечити зручний спосіб взаємодії з користувачем.

Для ще більшої упорядкованості, компоненти додатково розподіляються на дві логічні категорії – для власноруч розробленої бібліотеки для вирішення ЗЛП та для взаємодії з користувачем.

Компоненти бібліотеки будуть містити необхідні алгоритми та методи для розв'язання задач, як от симплекс-алгоритм, метод Гоморі [5], введення штучного базису, тощо. Проведені тут розрахунки будуть передаватися іншим компонентам ІС. Компоненти для взаємодії з користувачем будуть відповідати за зовнішній вигляд, включаючи введення даних та відображення результатів. Включає в себе графічний інтерфейс (GUI).

На основі розробленої структури програми було створено діаграму класів, що буде використовуватися при створенні проекту. Розроблена діаграма зображена на рисунку 9.



Рисунок 9 – Діаграма класів інформаційної системи

«SimplexMethod» – клас, що відповідає за систему оптимізації задачі лінійного програмування. Також зберігає в собі історію оптимізацій. «GomoryMethod» – його клас-нащадок. Для вирішення задачі в цілих числах.

«TableauSimplex» – являє собою таблицю оптимізацій. «TableauCreator» – конвертує канонічну форму задачі до стандартної. Готує її для «TableauSimplex». «ProblemData» – вхідні дані для таблиці.

«StructuresCreator» – статичний «Generic» клас. Дає змогу створювати масиви різної розмірності з визначеними для них стандартними значеннями від «IDefault», також дає можливість конвертувати масив, елементи якого наслідують інтерфейс «IParsable».

«ComplexVariable» та «Fraction» структури, що відповідають за подання комплексних чисел та дробів відповідно. Обо'є наслідують три інтерфейси: «IDefault», «IParsable» та «INumber». Останній необхідний для порівняння значень в «Generic» методах.

У класі «Utils» містяться методи для комфортного представлення таблиці будь-якої таблиці в вигляді тексту.

«NamedFraction» та «NamedFractionList» відповідають за подання дробів з їх ідентифікаторами як елементів обмежень або цільової функції.

«Problem» та «Constraints» використовуються при прямому зверненні до бібліотеки. Забезпечують правильний парсинг стрічкових даних для подальшої їх обробки в «TableauCreator» та «TableauSimplex».

Перелічуванні типи даних «ProblemType», «SimplexMethodType» та «ConstraintsSign» використовуються задля визначення типу поставленої задачі, виду екстремумів та знаку обмеження відповідно.

Класи, які на діаграмі розташовані після інтерфейсів та перелічуваних типів даних відповідають за правильне відображення помилок в ході роботи програми. Як от: «TableauException» – загальний клас для помилок в ході обробки (оптимізації) таблиці. «InvalidTableauInitDataException» – некоректно задані вхідні дані таблиці. «CannotFindPivotElementException» – не можливо знайти елемент відносно якого буде здійснюватися оптимізація. «OptimalPlanFoundedException» – не можливо покращити результуюче рішення, оскільки оптимальне вже знайдено. «DoesNotHaveOptimalPlanException» – не можливо знайти оптимальний план. «SimplexMethodException» – загальний клас, що описує помилки, котрі можуть виникнути в ході оптимізації симплексним-методом. «GomoryException» – помилки похідного класу (цілочисельна оптимізація). «GomoryDoesNotHaveIntegerSolutionException» – не можливо знайти цілочисельне рішення задачі. «GomoryDoesAlreadyHaveIntegerSolutionException» – пошук цілочисельного рішення не можливий, оскільки воно вже знайдено. «ProblemDataException» – помилка вхідних даних таблиці. «InvalidProblemDataInitialParametersException» – некоректно задані вхідні параметри. «CannotFindBasisException» – не може віднайти базис. Показує також кількість знайдених, та кількість необхідних векторів до утворення базису. Використовується

здля майбутнього конвертування вхідних даних задачі з внесенням штучного базису. «InvalidConstraintException» – некоректні вхідні дані обмеження. «ConstraintHasInvalidBValueException» – помилки в задані обмеження. «ConstraintHasInvalidSignException» – помилковий знак в обмеженні. «NamedFractionException» – загальний клас для помилок виявлених в ході конвертування числа з ідентифікатором. «NamedFractionNumberException» – некоректно задано число. «NamedFractionNameException» – некоректний ідентифікатор. «NamedFractionNameIsAlreadyExistsException» – у одному й тому ж самому обмежені ідентифікатор не може зустрічатися більше двох разів. «NamedFractionListException» – помилка конвертування стрічки чисел з їх ідентифікатором.

«MainForm» – основне вікно програми. Задаються всі вхідні дані. «ResultForm» – необхідний для виводу результату оптимізація з усіма пройденими кроками. «ConstraintsList», «CellPairList», «FractionInput», «ConstraintsRow» та «CellPair» користувацькі компоненти, значно полегшують розробку.

В усіх вище згаданих реченнях стосовно помилок, ідентифікатор слід сприймати як унікальну змінну, що стоїть біля числа.

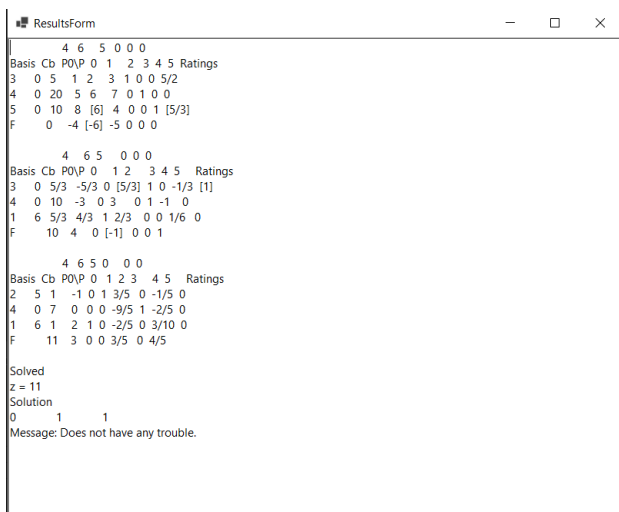
Після введення початкових даних та натискання кнопки «Solve» програма вирішує задану йому задачу лінійного програмування (рисунок 10). Далі розв'язок виводиться на екран користувача (рисунок 11).

Рисунок 10 – Головний екран застосунку

У результаті виконання завдання було розроблено підхід і відповідний застосунок для вирішення задач лінійного програмування, який виконує всі необхідні функції. Система може ефективно розв'язувати різні типи завдань лінійного програмування, працює офлайн, обробляє велику кількість вхідних даних, підтримує різноманітні типи задач лінійного програмування та показує кроки до знаходження результату.

Щодо перспектив та ступеня впровадження розробленої системи – його можливості і переваги, дають йому потенціал для широкого використання в

академічних дослідженнях, промисловості та інших галузях, де потрібно розв'язувати задачі лінійного програмування.



```

ResultsForm
|
| 4 6 5 0 0 0
| Basis Cb P0/P 0 1 2 3 4 5 Ratings
| 3 0 5 1 2 3 1 0 0 5/2
| 4 0 20 5 6 7 0 1 0 0
| 5 0 10 8 [6] 4 0 0 1 [5/3]
| F 0 -4 [-6] -5 0 0 0
|
| 4 6 5 0 0 0
| Basis Cb P0/P 0 1 2 3 4 5 Ratings
| 3 0 5/3 -5/3 0 [5/3] 1 0 -1/3 [1]
| 4 0 10 -3 0 3 0 1 -1 0
| 1 6 5/3 4/3 1 2/3 0 0 1/6 0
| F 10 4 0 [-1] 0 0 1
|
| 4 6 5 0 0 0
| Basis Cb P0/P 0 1 2 3 4 5 Ratings
| 2 5 1 -1 0 1 3/5 0 -1/5 0
| 4 0 7 0 0 0 -9/5 1 -2/5 0
| 1 6 1 2 1 0 -2/5 0 3/10 0
| F 11 3 0 0 3/5 0 4/5
|
| Solved
| z = 11
| Solution
| 0 1 1
| Message: Does not have any trouble.

```

Рисунок 11 – Результат виконання програми

У майбутньому планується розширення функціональності: додавання нових типів задач лінійного програмування, підтримки різних алгоритмів розв'язування, вдосконалення інтерфейсу користувача тощо; аналіз та вдосконалення алгоритмів і структур даних для покращення швидкості розв'язування задач та зменшення використання ресурсів; додавання налаштувань та параметрів, які дозволять користувачам налаштовувати програмний застосунок для виконання конкретних завдань. Ці можливості та шляхи до вдосконалення сприятимуть подальшому успіху та використанню розробленої системи.

### Перелік посилань

1. О. О. Ємець, О. С. Пічугіна, О. Б. Маций, К. П. Коробчинський. Лінійне програмування. Навчальний посібник. Х. : ХНАДУ, 2019. 102 с.
2. А. А. Яровий, Л. М. Ваховська, Л. В. Крилик. Математичні методи дослідження операцій. Лінійне програмування. Частина 1. Навчальний посібник. Вінниця: ВНТУ. 2020. 86 с.
3. eMathHelp. Simplex Method Calculator. URL: <https://www.emathhelp.net/en/calculators/linear-programming/simplex-method-calculator>.
4. What is Component-Based Architecture? URL: <https://www.mendix.com/blog/what-is-component-based-architecture/>
5. Метод Гоморі (метод відсікаючих площин). URL: <https://www.mathros.net.ua/metod-gomori-metod-vidsikajuchyh-ploshhyn.html>



УДК 004.9

Денисюк Д.О.

Хмельницький національний університет

## МЕТОДИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В ГРАФІЧНИХ ОБ'ЄКТАХ

*Розробка програмного забезпечення та обробка графічних об'єктів стали невід'ємною частиною сучасних інформаційних технологій. Графічні формати, такі як PNG, JPG та JPEG, широко використовуються в різних галузях, проте разом із популярністю зростає і вразливість до різноманітних атак та зловмисного використання. Відображення картинок на програмному рівні включає зчитування, декодування та відображення графічних файлів. Для різних форматів використовуються різні методи декодування. Зловмисники можуть використовувати стеганографію для приховування шкідливого коду в зображеннях. Для виявлення таких змін використовуються різні методи аналізу, такі як візуальний аналіз, аналіз гістограм та статистичні методи. Це сприяє підвищенню рівня безпеки системи та виявленню нових загроз.*

*Software development and processing of graphic objects have become an integral part of modern information technology. Graphic formats such as PNG, JPG, and JPEG are widely used in various industries, but along with their popularity, their vulnerability to various attacks and misuse is growing. Image display at the software level involves reading, decoding, and displaying graphic files. Different decoding methods are used for different formats. Attackers can use steganography to hide malicious code in images. Various analysis methods are used to detect such changes, such as visual analysis, histogram analysis, and statistical methods. This helps to increase the security level of the system and detect new threats.*

Розробка програмного забезпечення та обробка графічних об'єктів стали невід'ємною частиною сучасних інформаційних технологій. Зокрема, графічні формати, такі як PNG, JPG та JPEG, знаходять широке застосування в різних сферах, але разом з їхньою популярністю зростає і вразливість до різноманітних атак та зловмисного використання.

Відображення картинок у форматах PNG, JPG та JPEG на програмному рівні включає в себе ряд операцій, які забезпечують зчитування, декодування та відображення графічних файлів у вікні або на екрані. Процес зчитування файлу включає в себе операцію, під час якої програмне забезпечення отримує доступ до даних, що містяться в файлі або іншому ресурсі, що відповідає відомим форматам, таким як PNG, JPG та JPEG. Це дає можливість подальшої обробки та декодування графічної інформації, що міститься в цих файлах. Для різних форматів, таких як PNG та JPG або JPEG, використовуються різні методи декодування. У випадку формату PNG (Portable Network Graphics), який славиться своєю здатністю стискувати зображення без втрат, застосовується алгоритм стиснення zlib[1]. Цей алгоритм дозволяє ефективно стиснути графічні дані, зменшуючи їх розмір без втрати якості. Формати JPG або JPEG (Joint Photographic Experts Group) призначені

для фотографій та подібних зображень, вони використовують послідовність дій з кількох алгоритмів для декодування графічних даних[2]. Ці алгоритми включають в себе стиснення з втратами, що дозволяє зменшити розмір файлу, але може призвести до втрати деякої якості зображення. Отже, можна прийти до висновку, що спроби запустити зловмисне програмне забезпечення, використовуючи саму картинку як вектор атаки, найімовірніше будуть невдалими. Це пояснюється тим, що графічні формати, які використовуються для зображень, такі як PNG, JPG та JPEG, не містять в собі вбудованих механізмів для виконання вірусів або команд. Вони призначені для представлення зображень і не мають можливості виконувати код. Однак важливо враховувати, що навіть у випадку, коли сам формат зображення не може виконувати команди, зловмисне програмне забезпечення все одно може бути передано через зображення шляхом використання технології стеганографії.

Стеганографія [3] - це метод, який дозволяє приховувати інші дані всередині зображення так, що це приховане повідомлення не може бути помічене при звичайному перегляді. Зловмисники можуть використовувати цей метод для внесення шкідливого коду в зображення, при цьому зовнішній вигляд зображення залишається незмінним. Загроза полягає у тому, що, використовуючи стеганографічні зображення та додаткові скрипти, можна проводити атаки, що залишаються непомітними і не піддаються ідентифікації антивірусними програмами. Головна проблема полягає в тому, що більшість додаткових скриптів не містять в собі напряду відомих команд, а отримують їх через приховане стеганографічне зображення, яке було змінено без видимих змін. Така техніка може дозволити зловмисникам виконувати шкідливі дії, такі як розповсюдження вірусів чи атаки на систему, обходячи захисні механізми. Через те, що скрипти відправляють запити та отримують команди, які вбудовані в стеганографічне зображення, вони можуть залишатися невиявленими антивірусними програмами, які не виявляють конкретних загроз або аномалій в поведінці програм. Отже, виникає потреба в використанні методів, які дозволяють проводити перевірку зображень на наявність стеганографічних змін.

Найпростіші методи аналізу контейнерів зображень включають в себе візуальний підхід. Візуальний аналіз спрямований на виявлення стеганографічних вкраплень за допомогою візуального контролю (за допомогою звичайного погляду) або використання автоматизованих процесів. Візуальний контроль, проведений звичайним оком, може бути успішним, особливо коли стеганографічні дані приховані в однотонних областях зображення.

Для автоматизованого аналізу зображень використовують комп'ютерні програми, які дозволяють розкласти зображення на окремі бітові площини. Кожна бітова площина представляє собою послідовність бітів пам'яті, які відповідають кожному пікселю на зображенні. Зазвичай інформацію, приховану за допомогою стеганографічних програм, зберігають на площинах молодших бітів. Якщо виникають підозри стосовно незвичайних артефактів на площинах молодших бітів, це може вказувати на наявність стеганографічних даних в зображенні.

Існує кілька поширених методів для виявлення стеганографії в графічних зображеннях:

1. Метод оцінки числа переходів значень молодших бітів в сусідніх елементах контейнера. Цей метод спрямований на аналіз переходів між значеннями найнижчих бітів сусідніх пікселів у зображенні.

2. Метод аналізу гістограм, побудованих за частотами елементів зображення. Цей метод включає в себе аналіз гістограм, які відображають розподіл інтенсивності пікселів у зображенні.

3. Метод аналізу розподілу елементів зображення на площині. Цей метод досліджує розміщення та розподіл пікселів у площині зображення.

4. Статистичні методи аналізу. Цей підхід використовує різні статистичні методи та метрики для виявлення аномалій в графічних даних.

5. Метод аналізу розподілу пар значень на основі критерію. Цей метод оцінює розподіл пар значень пікселів та застосовує певний критерій для визначення аномалій.

6. Метод оцінки частот появи  $k$ -бітових серій у потоці НЗБ елементів контейнера. Цей підхід аналізує частоту виникнення послідовностей  $k$ -бітових даних у найменш значущих бітах контейнера.

7. Метод оцінки числа переходів значень молодших бітів в сусідніх елементах контейнера. Цей метод також спрямований на аналіз переходів між значеннями найнижчих бітів пікселів у зображенні.

Ці методи допомагають виявити підозрілі зміни в графічних даних, які можуть свідчити про наявність стеганографії, тобто прихованих повідомлень у зображеннях.

Таким чином, можна зробити висновок, що для підвищення рівня безпеки системи важливо впроваджувати механізми перевірки зображень не лише на наявність шкідливого коду, але також на наявність стеганографічних змін. Це може бути ключовим кроком у запобіганні можливим загрозам, оскільки зміни в зображеннях можуть вказувати на наявність схованих вказівок для інших програмних продуктів з метою виконання певних дій. Такий комплексний підхід може виявити нові види загроз та поліпшити загальну безпеку системи.

#### **Перелік посилань**

1. CHEN, Jianyu; DAVERVELDT, Maurice; AL-ARS, Zaid. Fpga acceleration of zstd compression algorithm. In: 2021 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW). IEEE, 2021. p. 188-191.
2. HUSSAIN, Abdullah A.; AL-KHAFI, Ghadah K.; SIDDEQ, Mohammed M. Developed JPEG Algorithm applied in image compression. In: IOP Conference Series: Materials Science and Engineering. IOP Publishing, 2020. p. 032006.
3. RAJVANSHI, Srishiti, et al. Image Steganography. Int. J. Res. Appl. Sci. Eng. Technol, 2019, 7.11: 408-411.
4. KUMAR, Singamaneni Kranthi, et al. Image Transformation Technique Using Steganography Methods Using LWT Technique Image Transformation Technique Using Steganography Methods Using LWT Technique. 2019.
5. RAHMAN, Shahid, et al. A novel approach of image steganography for secure communication based on LSB substitution technique. Computers, Materials & Continua, 2020, 64.1: 31-61.

УДК 004.4

Домбровський Н.С., Скрипник Т.К., Вознюк Л.О.

*Хмельницький національний університет*

## **МЕТОД ІДЕНТИФІКАЦІЇ ПОДІЙ В УКРАЇНОМОВНИХ ТЕКСТАХ ЗАСОБАМИ ОБРОБКИ ПРИРОДНОЇ МОВИ**

*В даному дослідженні проводиться оцінка, наскільки текст тестового документа відповідає введеним користувачем ключовим токенам з урахуванням оцінки важливості слів у тексті. Для визначення цієї важливості можуть використовуватися два підходи: дисперсійна оцінка та метод VM-25. Передбачається автоматизований процес формування синонімічних рядів до введених користувачем токенів з метою розширення можливостей методу.*

*In this study, we evaluate the extent to which the text of the test document corresponds to the key tokens entered by the user, taking into account the importance of words in the text. To determine this importance, two approaches can be used: variance estimation and the VM-25 method. An automated process of forming synonymous series to the user-entered tokens is envisaged to expand the capabilities of the method.*

Обробка природної мови (Natural Language Processing, NLP) – це міждисциплінарна галузь інформатики та мовознавства, що вивчає та розробляє методи та технології для взаємодії між комп'ютерами та людьми через природну мову. Вона включає в себе комплексний аналіз та обробку тексту та мови з метою автоматизації розуміння та генерації текстової інформації [1].

Метод ідентифікації подій в україномовних текстах засобами обробки природної мови є актуальною задачею в галузі обчислювальної лінгвістики та штучного інтелекту. Цей метод спрямований на автоматичне визначення подій, які відбуваються в тексті, зокрема, діяльності, подій, процесів та їхніх атрибутів. Ідентифікація подій є важливою для багатьох застосувань, включаючи аналіз новин, моніторинг соціальних мереж, розробку систем автоматичного розуміння тексту, аналізу семантики та багато інших областей [2].

Для специфічних задач NLP іноді використовуються поєднання декількох методів та моделей, а також аналіз контексту та зв'язків між словами та фразами. Застосування цих математичних методів дозволяє здійснювати складний аналіз текстів і виявляти події та інформацію, пов'язану з ними, що може бути корисним в різних додатках, включаючи аналітику соціальних медіа, пошукові системи, моніторинг новин тощо [3].

Для поставленого завдання було обрано метод дисперсійної оцінки, це статистичний метод для визначення різноманітності та варіабельності даних у

вибірці. Дисперсія грає важливу роль у багатьох аналітичних задачах, включаючи оцінку важливості слів у текстових документах для подальшого використання в методах обробки природної мови, таких як ідентифікація подій.

Дисперсійна оцінка базується на обчисленні середнього квадратичного відхилення (стандартного відхилення) даних від їхнього середнього значення. Вона вимірює, наскільки дані розподілені відносно середнього значення. Вища дисперсія вказує на більшу розкиданість даних, тоді як нижча дисперсія вказує на менший розкид [4].

Формула для обчислення дисперсії наведено у формулі:

$$\sigma^2 = \frac{\sum (x_i - \mu)^2}{N}$$

де  $\sigma^2$  – дисперсія,  $x_i$  – кожне окреме значення вибірки,  $\mu$  – середнє значення (середнє арифметичне) вибірки,  $N$  – кількість значень вибірки.

Основна ідея полягає в тому, що дисперсія вимірює, наскільки середнє значення відхиляється від кожного окремого значення вибірки. Велика дисперсія вказує на те, що дані мають великий розкид, тоді як мала дисперсія означає, що значення вибірки майже однакові.

Дисперсійна оцінка може бути важливим інструментом в контексті ідентифікації подій в текстах. Вона може використовуватися для визначення важливості слів у текстових документах, які можуть вказувати на ключові терміни або інформацію, що вказує на певні події чи теми [5]. Розрахунок дисперсійної оцінки може допомогти виокремити найбільш значущі слова, які слід аналізувати подальше в контексті ідентифікації подій.

При розробці методу ідентифікації подій в україномовних текстах за допомогою обробки природної мови, одним з важливих виборів є вибір підходу для оцінки важливості слів та токенів у текстах. У контексті поставленої задачі, дисперсійна оцінка виявляється більш вдалою стратегією. Дисперсійна оцінка більше урахує різноманітність слів та токенів у тексті. Це означає, що вона надає важливість словам, які вносять різноманітність та багатогранність в текст, що є важливим аспектом ідентифікації подій. Таким чином, дисперсійна оцінка відображає різноманітність тексту, що може допомогти виокремити ключові слова та фрази, пов'язані з подіями.

Для реалізації методу ідентифікації подій в україномовних текстах необхідно чітко окреслити послідовність його виконання. Схема роботи методу наведена на рисунку 1.

Вхідні дані. На цьому кроці вхідні дані включають текстовий документ, який піддається обробці, і список токенів, які вводить користувач. Текстовий документ представляє собою послідовність слів або фраз, які містять інформацію про події.

Токенізація тексту. Токенізація – це процес розбиття тексту на окремі токени (слова, фрази, символи тощо). Цей процес виконується для підготовки

тексту до подальшого аналізу. Токени представлені як послідовність символів, і кожен токен має свій внутрішній ідентифікатор.

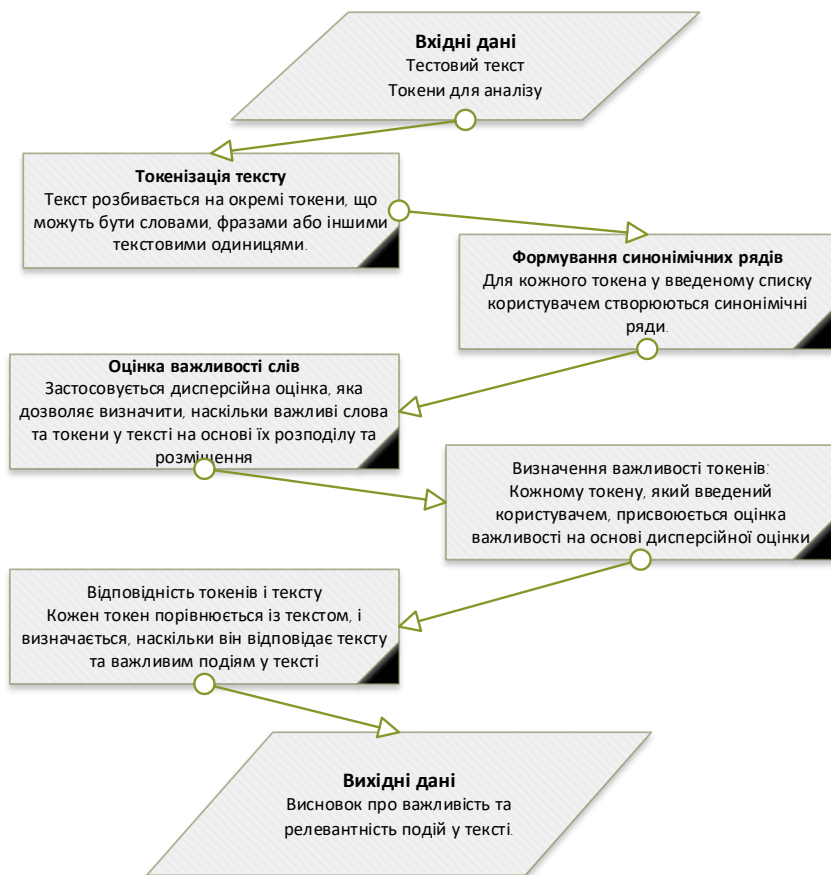


Рисунок 1 – Схема методу ідентифікації подій в україномовних текстах засобами обробки природної мови

Формування синонімічних рядів. Після токенізації для кожного токена, введеного користувачем, формуються синонімічні ряди. Синонімічний ряд - це набір інших слів або фраз, які мають схожий семантичний зміст або пов'язані за контекстом. Формування синонімічних рядів допомагає розширити можливості аналізу тексту.

Оцінка важливості слів. Для оцінки важливості слів у тексті використовується дисперсійна оцінка. Дисперсійна оцінка визначає, наскільки

слова розподілені у тексті та як вони пов'язані між собою. Ця оцінка допомагає визначити, які слова є ключовими для подій у тексті.

Визначення важливості токенів. Кожному токenu, введеному користувачем, присвоюється оцінка важливості на основі дисперсійної оцінки. Оцінка важливості враховує розташування токenu в тексті та його семантичний зв'язок з іншими словами. Токени, які мають високий рівень важливості, вважаються ключовими для подій у тексті.

Відповідність токенів і тексту. Кожен токен порівнюється із текстом з використанням отриманих оцінок важливості та дисперсійної оцінки. Це допомагає визначити, наскільки токен відповідає тексту і наскільки важливий для подій, які відображені в тексті.

Результати та висновок. На основі оцінок важливості та відповідності токенів тексту введеним користувачем токенам генерується висновок про важливість та релевантність подій у тексті. Ця інформація допомагає ідентифікувати та аналізувати події та їх контекст у тексті.

Отже, метод ідентифікації подій в україномовних текстах засобами обробки природної мови полягає в складному аналізі тексту та оцінці важливості токенів на основі дисперсійної оцінки. Цей метод дозволяє точно ідентифікувати та аналізувати події в тексті.

Таким чином, було проведено дослідження в галузі аналізу тексту, зокрема ідентифікації подій в україномовних текстах, запропоновано структуру методу, що може бути втілено в програмних реалізаціях.

### **Перелік посилань**

1. An improved text mining approach to extract safety risk factors from construction accident reports
2. AL-NASSERI, Alya; ALI, Faek Menla; TUCKER, Allan. Investor sentiment and the dispersion of stock returns: Evidence based on the social network of investors. *International Review of Financial Analysis*, 2021, 78: 101910.
3. Text preprocessing for text mining in organizational research: Review and recommendations HICKMAN, Louis, et al. Text preprocessing for text mining in organizational research: Review and recommendations. *Organizational Research Methods*, 2022, 25.1: 114-146.
4. KONONOVA, Olga, et al. Opportunities and challenges of text mining in materials research. *Iscience*, 2021, 24.3. NA, X. U., et al. An improved text mining approach to extract safety risk factors from construction accident reports. *Safety science*, 2021, 138: 105216.
5. GRIES, Stefan Th. A new approach to (key) keywords analysis: Using frequency, and now also dispersion. *Research in Corpus Linguistics*, 2021, 9.2: 1-33.

УДК 004.4

Дуда К.М., Кустановський Р.С.

*Хмельницький національний університет*

## **МЕТОД ГЕНЕРАЦІЇ ТЕСТІВ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ПОШУКОМ ПЕВНИХ ДІЙ**

*Розглянуто основні аспекти розробки методу генерації тестів на основі пошуку певних дій. Даний метод здійснює генерацію коду для тестування на основі введених даних користувачем які вказують які дії необхідно протестувати, цим самим забезпечує збільшує продуктивність та якість процесу тестування програмного забезпечення.*

*The main aspects of the development of the test generation method based on the search for complete actions are considered. This method generates code for testing based on the data entered by the user, which indicates which actions need to be tested, thereby increasing the productivity and quality of the software testing process.*

Тестування програмного забезпечення відіграє надзвичайно важливу роль у розробці та підтримці сучасних програм і застосунків. В процесі постійного зростання комп'ютеризації і залежності від програм, функціональність та надійність стали критичними факторами для задоволення потреб користувачів та досягнення бізнес-цілей.

На сьогоднішній день є два основних види тестувань[1]:

- ручне тестування;
- автоматизоване тестування.

Ручне тестування – це процес, в якому тестувальники вручну перевіряють програмне забезпечення на наявність помилок, відповідність вимогам та забезпечують якість продукту. Це включає в себе створення тестових сценаріїв, виконання їх, аналіз результатів та документування виявлених проблем. Ручне тестування використовується для перевірки аспектів, які важко автоматизувати, а також для тестування користувацького інтерфейсу та інших аспектів, які потребують людського інтуїтивного розуміння. Ручне тестування може бути ефективним, але воно ресурсозатратне, і тому автоматизація тестування стає важливою для покращення ефективності та точності процесу тестування.

Автоматизоване тестування – це процес використання спеціальних програмних інструментів та сценаріїв для автоматичного виконання тестів програмного забезпечення. Його головна мета – зменшити ручне тестування, полегшити і прискорити процес виявлення помилок та забезпечити більшу надійність програмного продукту.



Загалом принцип тестування полягає в тому, щоб порівнювати фактичний та очікуваний результат певного функціоналу. Перед початком тестування складається тест-план в якому описується функціонал, що тестується при певних умовах, очікуваний та фактичний результат після виконання функції (таблиця 1). Очікуваний результат – це результат який після виконання певної функції видає дані згідно сценарію. Фактичний результат – це той результат або стан, який спостерігається після виконання тесту чи функції. Якщо фактичний і очікуваний результат співпадають – тест пройдений, якщо не співпадають – тест не пройдений[3].

Таблиця 1 – Приклад тест-плану.

№	Очікуваний результат	Фактичний результат	Статус
Тест 1	При натисканні «кнопки1» має завантажуватись текстовий файл.	При натисканні «кнопки1» текстовий файл НЕ завантажується.	Тест не пройдений
Тест 2	При натисканні «кнопки2» має закриватись «блок1».	При натисканні «кнопки2» закривається «блок1».	Тест пройдений

Загалом процес тестування є важким, масивним процесом життєвого циклу програмного забезпечення, але в першу чергу є надзвичайно важливим для його розробки.

Метою роботи є розробка методу генерації тестів з пошуком певних дій який перед усім дозволить спростити та пришвидшити процес тестування програмного забезпечення.

Постановка завдання складається з наступних етапів:

- проаналізувати сферу тестування програмного забезпечення;
- дослідити наявні підходи та концепції генерації тестів;
- виконати проектування програмної системи на основі розробленого алгоритму генерації тестів;
- проаналізувати та обрати засоби реалізації даного методу;
- виконати програмну реалізацію методу генерації тестів з пошуком певних дій;
- провести тестування та практичну апробацію отриманих результатів;
- проаналізувати отримані результати та сформувавши рекомендації щодо доцільності і впровадження результатів дослідження.

Найпопулярнішим методом автоматизованого тестування є метод тестування чорної скриньки [2]. Метод чорних скриньок (Black Box Testing) - це метод тестування програмного забезпечення, при якому тестувальник не має знань

про внутрішню структуру чи реалізацію програми. Тестувальник працює з програмою як із "чорною скринькою", де він бачить лише вхідні дані та очікувані результати, але не знає, як саме програма обробляє дані. Тобто основним принципом полягає в тому, що не важливо як програма виконує ту чи іншу дію, а важливо який результат вона має виводити. Саме цей вид тестування підходить для методу генерації тестів.

Генетичне програмування – це потужний підхід для генерації коду тестування чорних скриньок та автоматизації тестування. Воно використовує принципи еволюції та відбору для створення оптимальних тестових сценаріїв. Приклад алгоритму генетичного програмування наведено на рисунку 1.

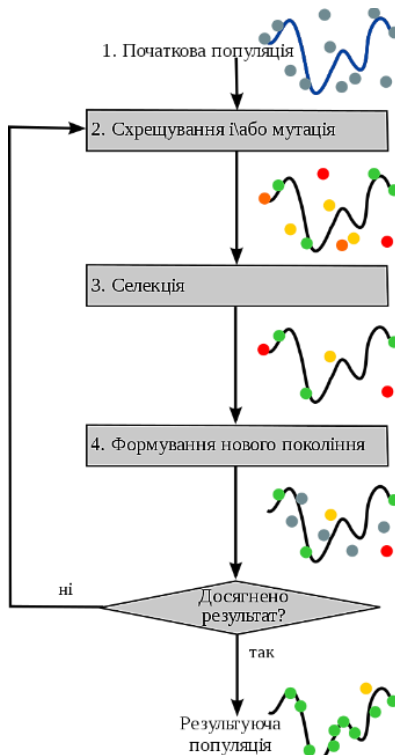


Рисунок 1 – Приклад алгоритму генетичного програмування

Загальний опис процесу використання генетичного програмування [4]:

– **Створення початкової популяції:** генерується велика кількість початкових тестових сценаріїв або хромосом, кожна з яких представляє собою можливий тест.

– **Оцінка пристосованості:** кожен тест оцінюється за допомогою функції пристосованості, яка визначає, наскільки добре він виконує свою роботу.

– **Схрещування:** тестові сценарії об'єднуються (схрещуються) для створення нових тестів, які можуть успадковувати корисні характеристики батьківських тестів.

– **Мутація:** деякі тестові сценарії піддаються випадковим змінам, щоб розширити різноманітність тестів.

– **Відбір:** вибираються кращі тестові сценарії на основі їхньої пристосованості, і вони використовуються для створення наступного покоління тестів.

– **Повторення:** процес схрещування, мутації та відбору повторюється протягом кількох поколінь.

Метод генерації тестів з використанням алгоритму генетичного програмування зосереджується на створенні тестових випадків для програмного забезпечення з точки зору зовнішньої поведінки (метод чорної скриньки). Основною метою є визначення, як програма взаємодіє з вхідними даними і генерує вихідні результати, без необхідності знань про її внутрішню структуру.

В результаті, генетичне програмування може створити оптимальні тестові сценарії, які відповідають вимогам тестування. Цей підхід особливо корисний для автоматизованого тестування складних програмних систем.

Дослідження у галузі генерації тестів для програмного забезпечення з використанням генетичного програмування свідчить про важливість та актуальність цього напрямку в розробці програм. Застосування методів штучного інтелекту для генерації тестів може полегшити процес тестування, покращити якість програм та зменшити трудомісткість тестування. Це дослідження слугує основою для подальших робіт у цій галузі та розвитку більш складних методів генерації тестів.

### Перелік посилань

1. Загальні принципи тестування ПЗ URL: <https://www.browserstack.com/guide/learn-software-application-testing>
2. Оформлення тест-планів URL: <https://softwaretestingfundamentals.com/test-plan/>.
3. Sadeeq Jan, Annibale Panichella, Andrea Arcuri, and Lionel Briand. Search-based multi-vulnerability testing of xml injections in web applications. Empirical Software Engineering, pages 1–34, 2019.
4. Алгоритм генетичне програмування URL: <https://www.geeksforgeeks.org/>

УДК 621.373

Дудар Ю.М.

Хмельницький національний університет

## МЕТОД КОМПЕНСАЦІЇ ТЕРМОДИНАМІЧНОЇ СКЛАДОВОЇ НЕСТАБІЛЬНОСТІ ЧАСТОТИ КВАРЦОВИХ РЕЗОНАТОРІВ

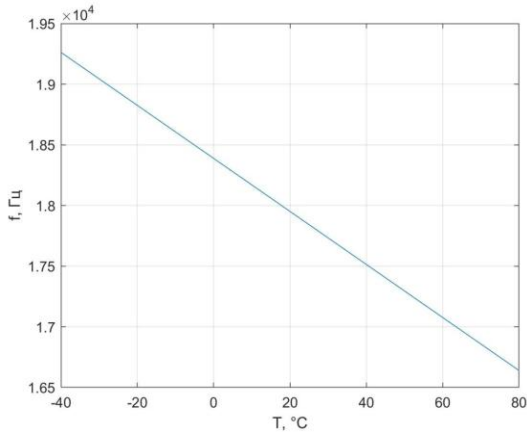
*Показна необхідність та доцільність застосування термодинамічної компенсації нестабільності частоти кварцових резонаторів за рахунок використання двочастотного режиму збудження. Запропонований метод дозволяє здійснювати ідентифікацію стану кварцового резонатора, що також може знайти розвиток у вимірювальній техніці. Результати моделювання показують доцільність застосування термодинамічного компенсатора для радіотехнічних пристроїв, які працюють в широкому діапазоні зміни робочої температури.*

*The necessity and expediency of applying thermodynamic compensation for the frequency instability of a quartz resonator by using a two-frequency excitation mode is demonstrated. The proposed method makes it possible to identify the state of a quartz resonator, which can also be developed in measuring technology. The simulation results show the feasibility of using a thermodynamic compensator for radio engineering devices operating in a wide range of operating temperature changes.*

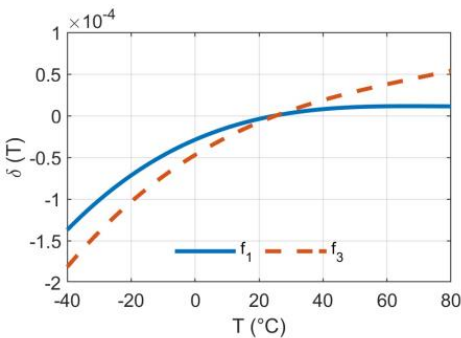
Кварцові резонатори (КР) отримали широкого застосування в радіотехнічних пристроях та засобах телекомунікацій завдяки їхнім характеристикам щодо стабільності частоти, точності, терміну безвідмовної роботи, а також невеликим габаритам та масі [1-3]. Дійсно, генератори опорних коливань, що основані на КР – кварцові генератори (КГ) – дозволяють забезпечити високу стабільність частоти коливань опорного сигналу, а також низький рівень спотворень та власних шумів, що особливо актуально в телекомунікаційних пристроях передачі інформації. Для таких систем та пристроїв будь-який зовнішній вплив на КР (температурний, вібраційний, електромагнітний, спричинений старінням тощо) є дестабілізуючим фактором, що є причиною нестабільності частоти і наслідки якого необхідно мінімізувати повністю або частково. З іншого боку, у вимірювальній техніці КР може використовуватись як чутливий елемент, в такому разі фактори зовнішнього впливу несуть інформативний характер [1], а девіація частоти сигналу КГ несе інформацію про об'єкт вимірювання для подальшого оброблення вимірювальним перетворювачем [1, 4].

З огляду на вищесказане, актуальною задачею є розробка нових та удосконалення існуючих методів контролю та компенсації впливу зовнішніх факторів на стабільність частоти сигналу КГ.

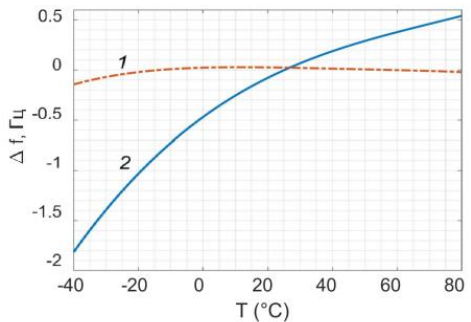
В даному дослідженні розглядається термодинамічний (температурний) вплив зовнішнього середовища на КР, який використовується в якості опорного джерела гармонічних коливань для радіотехнічних пристроїв та мікропроцесорних систем, а також метод компенсації нестабільності частоти коливання за рахунок використання двочастотного режиму збудження КР. Метою роботи є підвищення стабільності вихідної частоти КГ за рахунок застосування методу компенсації термодинамічного впливу середовища.



(а)



(б)



(в)

Рисунок 1 – Залежність різницевої частоти від температури КР (а); температурно-частотні характеристики першої та третьої гармоніки КР (б); результати імітаційного моделювання КГ з термокомпенсатором та без нього (в, криві 1 та 2 відповідно)

Структурна схема імітаційної моделі термодинамічного компенсатора нестабільності частоти ГК показана на Рисунку 1. Центральним елементом моделі є двочастотна підмодель КГ, який збуджений на 1-й та 3-й гармоніках відповідно.

Зміна температури КР відбувається шляхом лінійно зростаючого параметру в межах від -45 до 80 °С. Модель також передбачає візуалізацію сигналів в часовій області. За рахунок виведення КГ в двочастотний режим збудження, за наявності температурно-частотних характеристик (ТЧХ) обох робочих частот резонатора (1-ша та 3-тя гармоніки в даному випадку, див. Рисунок 1, б), з використанням подільника частоти 1:3, змішувача, та фільтра нижніх частот (ФНЧ), можливим є виділення сигналу різницевої частоти  $f_d$ . Залежність частоти цього сигналу та фактичної температури КР є практично лінійною (рисунок 1, а) [4].

Результати моделювання розробленого термокомпенсатора показані на Рисунку 2. Залежність температури від різницевої частоти, що була отримана в результаті лінійної апроксимації, показана на Рисунку 1, а.

Результати моделювання для лінійно наростаючої температури із застосуванням термокомпенсатора і без нього показані на Рисунку 1, в, з якого видно суттєве зниження відхилення частоти  $\Delta f$  – майже на один порядок для діапазону низької температури.

Отже, результати моделювання показують доцільність застосування термодинамічного компенсатора для КГ для широкого діапазону зміни робочої температури – від -45 до +80 °С, що відповідає допустимим нормам для КР [5]. До недоліків методу можна віднести необхідність вимірювання ТЧХ для кожного конкретного екземпляру КР, однак знаючи тип зрізу, а також інші характеристики, можливим є використання усередненої ТЧХ замість реальної з мінімальним погіршенням результату, що буде розвинуто в подальших дослідженнях.

### Перелік посилань

1. Підченко С. К. Теорія і реалізаційні основи інваріантних п'єзорезонансних коливальних систем / Ф. Ф. Колпаков, С. К. Підченко. – Харків: Нац. аерокосм. ун-т «Харьк. авіац. ін-т», 2011. – 327 с.
2. Підченко С. К. Ідентифікація теплового стану кварцового резонатора на етапі встановлення коливальності / С. К. Підченко, А. А. Таранчук // Радіоелектронні і комп'ютерні системи. – 2004. – № 3 (7). С.36-42.
3. Таранчук А. А. Модель кварцового опорного генератора систем синхронізації цифрового телебачення / Вісник Хмельницького національного університету. – 2018. – № 5 (265). С.160-166.
4. Таранчук А. А. Аналіз методів поліпшення температурних характеристик прецизійних кварцових генераторів // Вимірювальна та обчислювальна техніка в технологічних процесах. – Хмельницький. – 2000. – № 3 – С.196-199.
5. Підченко С. К. Температурно-динамічні характеристики кварцових п'єзорезонаторів АТ-та SC-зрізів / С. К. Підченко, А. А. Таранчук, О. А. Лаба // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2003. - № 2. С. 49 – 55.

УДК 004.42:519.6

Єршова С.А., Мельников О.Ю.

Донбаська державна машинобудівна академія

## ДОДАВАННЯ МОДУЛЯ ПОШУКУ АСОЦІАТИВНИХ ПРАВИЛ ДО ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ПРИЙНЯТТЯ РІШЕНЬ АНАЛІЗУ ДАНИХ АПТЕЧНОЇ МЕРЕЖІ

*Розглянуто можливість використання методів інтелектуального аналізу даних для покращення ефективності роботи аптеки. Описано наявну систему підтримки прийняття рішень для прогнозування обсягів продажів груп лікарняних товарів та шляхи її перетворення на інтелектуальну систему прийняття рішень. Наведено опис першого етапу цього процесу – додавання розв'язання задачі пошуку асоціативних правил, аналіз транзакцій для кращого розуміння оптимального сполучення товарів; приклади роботи нового модуля системи.*

*The possibility of using methods of intelligent data analysis to improve the efficiency of the pharmacy was considered. The existing decision-making support system for forecasting sales volumes of groups of hospital goods and the ways in which it can be transformed into an intelligent decision-making system are described. The description of the first stage of this process is provided – adding the solution to the task of finding associative rules, analyzing transactions for a better understanding of the optimal combination of goods; work examples of the new system module.*

Інтелектуальний аналіз даних (ІАД) може допомогти аптечній мережі краще зрозуміти потреби клієнтів, оптимізувати керування запасами та збільшити ефективність бізнес-процесів. Можна навести декілька можливих прикладів ІАД в аптечній мережі: аналіз транзакцій (щоб розуміти, які ліки купуються разом), аналіз цін на продукти в аптечній мережі та конкурентів; аналіз купівельної історії; аналіз соціальних медіа тощо [1].

Наявна аптечна мережа, згідно з її «Статутом», може здійснювати такі види діяльності, як придбання, транспортування, перероблювання, зберігання і реалізація лікарських засобів, предметів медичного призначення і медичної техніки тощо [2]. Було поставлено та розв'язано задачу створення системи підтримки прийняття рішень для прогнозування обсягів продажів груп лікарняних товарів [3–4]. Далі для підвищення ефективності бізнес-процесів наявну СППР треба розвинути до системи інтелектуального аналізу даних – інтелектуальної системи прийняття рішень.

Першим етапом буде додавання розв'язання задачі пошуку асоціативних правил (аналіз транзакцій для кращого розуміння оптимального сполучення товарів) [5].

В наявності є дані щодо придбання покупцями товарів (ліків):

– номер;

- дата та час;
- номер чека;
- назва товару;
- кількість одиниць;
- код об'єкта.

Вочевидь, для розрахунків потрібний номер чека (як ідентифікатор транзакції) та назва товару (як її наповнення).

Форму завантажених початкових даних наведено на рисунку 1.

N:	Чек	Товари	Кількість	Скороч.	Цифр*скор.	N:	Чек	Товари	N:	Чек	Товари
1	0000903	АЛМАГЕЛЬ СУСП ОРАЛЬНІ 10МЛ N20 I	1	бад	г						
2	0000903	ЛЬНА СЕМЕНА 200Г I	1	ейг	нг						
3	0000904	ШПРИЦ BD DISCARDIT II 2МЛ I	7	гель	нгг						
4	0000904	ШПРИЦ BD DISCARDIT II 10МЛ I	7	жидк	нггл						
5	0000905	ШПРИЦ МЕДИСАРЕ ІНЬЕКЦ ОДНОРАЗ 3Х КС I	1	кап	ме						
6	0000906	БЕТАСЕРК ТАБ 16МГ N30 I	1	капс	мес						
7	0000906	БАД ДЕКРИСТОЛ D3 ТАБ 4000МЕ N30 НДС I	1	крем	мер						
8	0000908	КАПТОПРЕС 12,5 -ДАРНИЦА ТАБ N20 I	1	кта	ни						
9	0000908	АСКОРБИНКА-КВ С САХ АПЕЛЬС ТАБ 0.025Г N1	1	мазь	нм						
10	0000908	АСКОРБИНКА-КВ С САХ МЯТА ТАБ 0.025Г N1 I	1	гель	нг						
11	0000912	ДЕТ/ЛИТ МІЦРА РИСОВЫЕ КОРЖИКИ МОР I	1	назал	оральн						
12	0000913	БИСОПРОЛ ТАБ 10МГ N50 /Z/ N1 I	1	пара	спрей						
13	0000914	LA ROCHE ROSAY РЕДЕРМИК Р КОНЦ ИНТ D1	1	сусп	сусп						
14	0000915	АТФ-ЛОНГ ТАБ 20МГ N40 I	1	таб	таб						
15	0000915	ФУЦИН (ФЛУКОНАЗОЛ) ТАБ 150МГ N1 /N1 I	1	туба	туба						
16	0000909	НАЗВИН КАП НАЗАЛ 0.01% 5МЛ I	1								
17	0000909	ЖЕЛЛЕКС АНТИКОЛД НЕО ПОР ІМБІРЬ 4Г Г2	1								
18	0000911	РИНТ СПРЕЙ НАЗАЛ ЧВЛАЖ 0.5МГ/Г С НАСС I	1								
19	0000911	ЗЛИДЕЛ КРЕМ Д/НАР ПРИМ 1% ТУБА 15Г I	1								
20	0000911	ЗЛОКОМ КРЕМ 0.1% ТУБА 15Г I	1								
21	0000911	ЖЕЛЛЕКС АНТИКОЛД НЕО ПОР ІМБІРЬ 4Г Г2	1								
22	0000911	ПАКЕТ П/З 24x40 20МКР НДС I	1								
23	0000911	АНАЛЬГІН-ДАРНИЦА ТАБ 500МГ N10 I	1								
24	0000911	АНАЛЬГІН-ДАРНИЦА ТАБ 500МГ N10 I	1								

Рисунок 1 – Завантажені початкові дані

Далі система здійснює попередню обробку даних таким шляхом:

- видалення спеціальних символів;
- видалення скорочень назв;
- видалення цифрових скорочень.

Перелік скорочень назв та цифрових скорочень наводиться на формі додатку та може редагуватися користувачем.

Користувач по черзі обирає пункти контекстного меню (рисунок 2): «Скоротити назви», «Впорядкувати за чеком», «Об'єднати дублікати» та «Зберегти у файлі».

Оскільки перелік товарів ще має достатньо зайвих даних, система вибирає «головне слово», і пункт «Створити ID-таблиці» здійснює створення саме транзакцій, які містять одне визначення з кожного товару (рисунок 3).



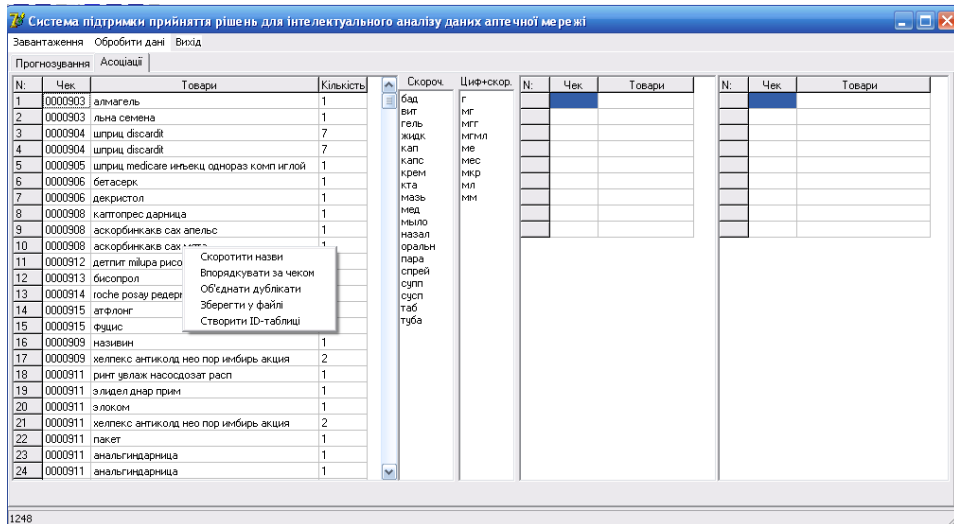


Рисунок 2 – Контекстне меню

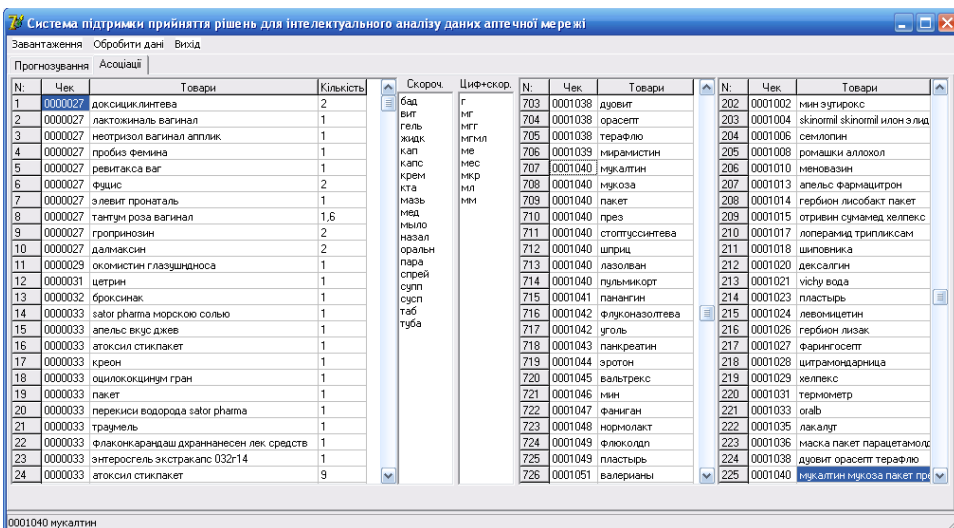


Рисунок 3 – Таблиці для роботи алгоритму

Далі користувач зберігає таблиці у текстовому файлі та залучає алгоритм пошуку асоціативних правил Apriori. Це можна зробити або в аналітичному пакеті Deductor Studio Lite (рисунко 4), або із залученням мови програмування Python чи мови програмування та аналізу даних R.

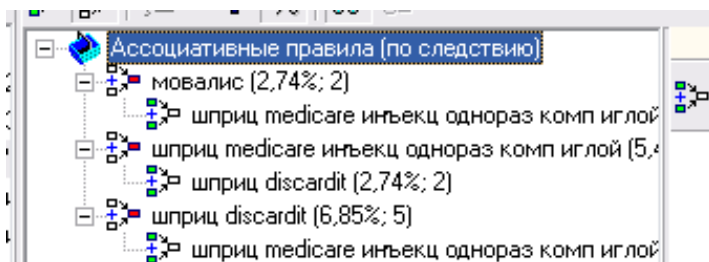


Рисунок 4 – Приклад реалізації у системі Deductor Studio Lite

Використання створеної системи дозволить підвищити ефективність бізнес-процесів, зробити подальше вдосконалення процесу прийняття управлінських рішень.

### Перелік посилань

1. Мельников О. Ю., Єршова С. О. Постановка задачі створення інтелектуальної системи прийняття рішень для аналізу даних аптечної мережі // Інформаційні технології в культурі, мистецтві, освіті, науці, економіці та бізнесі: матеріали VIII Міжнародної науково-практичної конференції / М-во освіти і науки України; Київ. нац. ун-т культури і мистецтв. Київ: Видавничий центр КНУКіМ, 2023. – Ч.1. – С.52–53.
2. ТОВ «Аптечний Будинок». [Електронний ресурс]. – Режим доступу: [https://youcontrol.com.ua/catalog/company\\_details/39264175/](https://youcontrol.com.ua/catalog/company_details/39264175/)
3. Мельников О. Ю., Єршова С. А. Система підтримки прийняття рішень для інтелектуального аналізу даних аптечної мережі // Інформаційні технології та цифрова економіка: матеріали Міжнародної науково-практичної конференції / М-во освіти і науки України; Державний університет інфраструктури та технологій. – Київ: Видавничий центр ДУІТ, 2022. – С. 58-60.
4. Єршова С. А., Мельников О. Ю. Інтелектуальний аналіз даних аптечної мережі із використанням системи підтримки прийняття рішень власної розробки // Матеріали V Всеукраїнської науково-практичної інтернет-конференції студентів, аспірантів та молодих вчених за тематикою «Сучасні комп'ютерні системи та мережі в управлінні»: збірка наукових праць / Під редакцією А.А. Григорової. – Херсон: Видавництво ФОП Вишемирський В. С., 2022. – С.127-129.
5. Чубукова И. А. Data Mining: учебное пособие. – М.: ИНУИТ, 2006. – 382 с.
6. BaseGroup Labs: офіційний сайт. [Електронний ресурс]. – Режим доступу: <https://basegroup.ru/deductor/>.

УДК 004

Єфремов М.С., Ляшко А.В., Крак Ю.В.

*Київський національний університет імені Тараса Шевченка*

## **ВІЗУАЛІЗАЦІЯ ТА ПОПЕРЕДНІЙ АНАЛІЗ ДАНИХ ЕКГ**

*Розглянуто основні аспекти для візуалізації та попереднього аналізу даних ЕКГ, що дозволить виявляти хвороби серцево-судинної системи на ранніх стадіях для постановки більш точного діагнозу, та призначенню ефективного лікування, що в деяких випадках може запобігти летальності. Створене програмне забезпечення реалізує повний цикл попереднього аналізу, починаючи з передачі даних, і закінчуючи виділенням їх окремих відведень, з можливістю подальшої обробки, візуалізації, збереженням та створенням проміжного висновку.*

*The main aspects of visualizing and preliminary data analysis of ECG data have been considered. This enables the early detection of cardiovascular diseases for a more accurate diagnosis and the prescription of effective treatment, which, in some cases, can prevent fatalities. The developed software implements the complete cycle of preliminary analysis, starting with data acquisition and ending with the extraction of individual leads, allowing for further processing, visualization, storage, and the creation of intermediate conclusions.*

Захворювання серцево-судинної системи є однією з наймасовіших причин смертності у всьому світі, зокрема й в Україні [1]. Особливо гостро це проявляється останнім часом, коли з'являється все більше збудників хвороби, які безпосередньо впливають на здоров'я серця [2].

На даний момент одним з найкращих методів моніторингу показників серцево-судинної системи вважається моніторинг ЕКГ за Холтером [3]. Методи виявлення серцевих аномалій на початкових стадіях захворювання є дуже важливим завданням, адже в цьому випадку можна відслідкувати та локалізувати хворобу до її переходу в більш важку стадію, що дозволить призначити ефективне лікування без хірургічного втручання, або навіть запобігти смерті.

Сучасні дослідження в галузі ЕКГ та штучного інтелекту для аналізу результатів Холтер-моніторингу ставлять перед собою завдання покращення точності та ефективності діагностики серцевих аномалій [4]. У роботі запропоновано систему для аналізу та візуалізації ЕКГ знятих з Холтера на різних його етапах для допомоги лікарям завчасно виявляти наявність аритмій чи інших серцевих патологій та можливість ефективної взаємодії лікаря з пацієнтом використовуючи теле-медицину.

Метою роботи є аналіз та покращення сучасних методів моніторингу даних серцевого ритму пацієнта та розробка готової до розгортання системи, що реалізує повний цикл попереднього аналізу, від передачі даних до виділення їх окремих відведень, з можливістю подальшої обробки, візуалізації, збереженням та створенням проміжного висновку [5].

Якщо порівнювати з іншими популярними методами, то ЕКГ за Холтером має суттєві переваги, але й містить незначні недоліки. Одна з характерних відмінностей – дані збираються протягом значно довшого проміжку часу. Так як найбільша кількість захворювань серцево-судинної системи припадає на аритмію, одним з різновидів якої є фібриляція передсердь [6], то саме прилад Холтера зможе показати більш точну картину хвороби.

Найчастіше дані, що збираються за допомогою Холтера, отримуються протягом доби, або ж декількох у випадках, коли в цьому є потреба, що дає можливість відслідковувати аномалії, навіть якщо вони можуть проявляти себе лише в вузькому часовому діапазоні. Також варто зазначити, що дані сигналів збираються з декілька ділянок тіла одночасно, для можливості вибору найкращих даних та їх подальшого аналізу. Проте в цього методу моніторингу є й деякі недоліки, які в основному пов'язані з кількістю даних, які потрібно зберегти та обробити. Саме тому потрібно мати ефективні засоби, які зможуть працювати з великими обсягами даних.

На даний момент створено програмне забезпечення, що реалізує поставлені задачі. На рисунку 1 можна побачити головне меню програми.

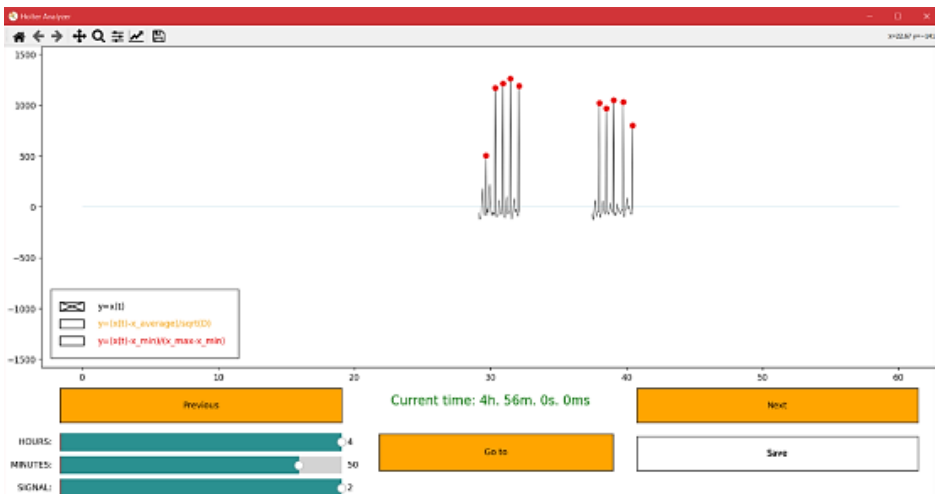


Рисунок 1 – Візуалізація і розмітка фрагментів ЕКГ

Загальний алгоритм роботи програми можна розділити на декілька етапів, першим з яких є розшифрування файлів Холтера, адже всі дані зберігаються у бінарному форматі. Більшість Холтерів кодують дані у загальноприйнятих форматах – такі як edf /edf+/bdf+ [7] Але деякі клініки використовують й власні. У програмі наявний модуль, який в залежності від формату обирає алгоритм декодування. Зазвичай такі формати містять дані про пацієнта у першій частині, а сигнал у другій. Для роботи вся закодована інформація про пацієнта видаляється, а залишені дані декодуються у матриці розмірністю [кількість датчиків x кількість часу], після чого вся інформація розділяється за даними кожного відведення(дані кожного відведення отримуються окремим датчиком) і зберігаються у відповідних файлах. На наступному етапі виконання програми виділені дані передаються на подальшу обробку. Варто зазначити, що розшифрування відбувається лише один раз тільки для нових даних, що дозволяє значно скоротити час в момент кожного наступного запуску. Наступним етапом є виділення важливої інформації шляхом видалення незначущої, що дозволяє не тільки виявляти підозрілі фрагменти ЕКГ, але й зменшити обсяг даних для подальшого перегляду, а також скоротити час повторного запуску до секунд. Перевагою наведеної програми є її універсальність, адже для ввімкнення певного алгоритму аналізу даних не потрібно її перероблювати, достатньо лише ввімкнути необхідний метод, який для вхідних даних буде ставити у відповідність певні вихідні дані, отримані бажаним алгоритмом.

Для подальшого аналізу для кожного відділення застосовується фільтрація, після якої застосовується обробка до менших частин даних. Застосовуючи порогові алгоритми, на проміжках до 10-15 тисяч точок у сигналі знаходимо RR інтервали, та аналізуємо кожен з них на наявність екстрасистолій, для подальшого маркування таких частин аномальними, щоб лікарі які мають доступ до нашої програми звертали на такі елементи ЕКГ увагу в першу чергу.

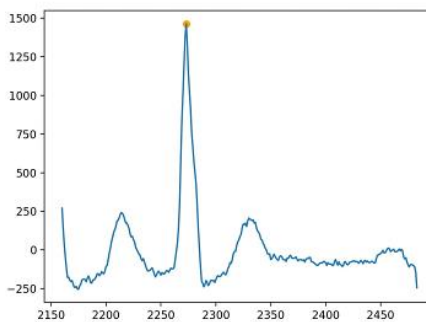


Рисунок 2 – Візуалізація знаходження екстрасистої на RR інтервали

Екстрасистолії є індикатором аномального скорочення серця, що може викликати порушення ритму та погіршити кровопостачання для органів, що представляє загрозу для нормальної серцевої функції. Наявність більше трьох екстрасистолій під час одного циклу вже несе у собі смертельні наслідки для пацієнта.

Нижче наведено приклад, як алгоритми у програмі знаходять екстрасистолію на одному RR інтервалі.

Отже, дослідження цього напрямку в сфері медицини є актуальним та дуже важливим, що в найближчому майбутньому може допомогти виявляти хвороби серцево-судинної системи на їх початковій стадії, що в свою чергу може значно покращити світову тенденцію захворюваності. Розробка нових алгоритмів пошуку підозрілих фрагментів дозволить більш точно виявляти ту чи іншу поведінку, що в свою чергу покращить точність постановки діагнозу. А програми що їх використовують можуть значно покращити сферу теле-медицини, яка стрімко розвивається у наш час. Використання більш сучасних способів збереження та обробки інформації призведе до покращення зручності як для лікарів, так і для пацієнтів.

### **Перелік посилань**

1. Сіренко Ю. М. Стан проблеми серцево-судинної захворюваності та смертності в Україні № 2 (258) додаток 1. 2022: с. 11-14.
2. I. Vosko, A. Zirlík, H. Bugger, Impact of COVID-19 on Cardiovascular Disease //Review, 11 February 2023: <https://www.mdpi.com/1999-4915/15/2/508>, p. 1-31.
3. V. Paudel, K. Paudel, The Diagnostic Significance of the Holter Monitoring in the Evaluation of Palpitation//Original Article, 01 march 2013: p. 480-483.
4. IEEE TRANSACTIONS ON BIOMEDICAL ENGINEERING, VOL. 55, NO. 2, FEBRUARY 2008 //Analysis of First-Derivative Based QRS Detection Algorithms p. 478-484.
5. Ляшко А., Єфремов М. Візуалізація та розмітка даних ЕКГ для ефективного виявлення складових електрокардіограм. II Міжнародна науково-практична інтернет-конференція «FUTURE HEALTHCARE: INNOVATIONS, ADVANCES AND PROGRESS», м. Дніпро, 15-16 червня 2023, с. 102-104.
6. J. G. Andrade, L. Macle, A. Verma, Atrial Fibrillation Guidelines// Canadian Cardiovascular Society, 2018, p. 1-31.
7. Bob Kemp, Jesus Olivan, European data format 'plus' (EDF+), an EDF alike standard format for the exchange of physiological data // Clinical Neurophysiology (Volume 114, Issue 9) 2003 , p. 1755-1761.

УДК 004.42:519.8

Закабула О.Ю., Мельников О.Ю.

*Донбаська державна машинобудівна академія*

## **АНАЛІЗ МОДЕЛЕЙ І МЕТОДІВ ПРОГНОЗУВАННЯ МОЖЛИВОСТІ АВАРІЙ В СИСТЕМІ ВОДОПОСТАЧАННЯ**

*Зазначено важливість систем водопостачання для сучасного світу та забезпечення надійності та безперервності функціонування цих систем. Проведено розгляд наявних методів та моделей прогнозування аварій, визначено низку факторів, які приводять до їхнього виникнення: знос трубопроводів, корозія, нерівномірний тиск, вплив ґрунту тощо. Сформульовано задачу розробки системи підтримки прийняття рішень для прогнозування надійності водопостачання.*

*The importance of water supply systems in the modern world and ensuring their reliability and uninterrupted functioning of these systems is noted. The available methods and models for predicting accidents have been reviewed, and a number of factors that lead to their occurrence have been identified: wear and tear of pipelines, corrosion, uneven pressure, soil influence, etc. The task of developing a decision support system for predicting the reliability of water supply is formulated.*

Системи водопостачання в сучасному світі відіграють надзвичайно важливу роль у забезпеченні життєвої активності населення та різних галузей економіки. Забезпечення надійності та безперервності функціонування цих систем є критично важливим завданням для забезпечення життєво важливих потреб. Аварії в системах водопостачання можуть призвести до серйозних наслідків, включаючи припинення подачі води населенню та забруднення навколишнього середовища. Тому прогнозування можливих аварій стає важливим завданням для забезпечення надійності цих систем.

З метою підвищення рівня безпеки та забезпечення надійності систем водопостачання було проведено аналіз наявних методів та моделей прогнозування аварій. Це передбачає розгляд причин виникнення аварій, їх наслідків та розробку методів та моделей для передбачення можливих аварійних ситуацій.

Модель ризику аварійного витоку [1] враховує такі фактори, як стан трубопроводів, тиск у системі, матеріал труб, якість земельного ґрунту тощо. Формула для ризику має вигляд:

$$\text{Ризик} = (P1 * K1) + (P2 * K2) + \dots \quad (1)$$

Модель прогнозування зносу трубопроводів [2] враховує ступінь зносу матеріалу трубопроводу з плином часу, температуру та рівень корозії. Формула для зносу має вигляд:

$$\text{Знос} = (K1 * t) - (K2 * \% \text{корозії труб}) \quad (2)$$

Модель прогнозування внутрішніх тисків [3] передбачає можливі зміни внутрішнього тиску в системі водопостачання в залежності від споживання води, роботи pomp та інших факторів. Формула виглядає:

$$\Delta P = (\text{Робочий тиск} - \text{Тиск зміни}) / V_{\text{води}} \quad (3)$$

Модель прогнозування ступеня корозії трубопроводів [4] дозволяє визначити ступінь корозії матеріалів трубопроводів в залежності від таких параметрів, як склад води, температура та матеріал труби. Формула має вигляд:

$$\text{Корозія} = (K1 * (t1 - t0)) / \text{Концентрація розчинених солей} \quad (4)$$

Модель прогнозування впливу зовнішніх факторів [5]:

$$\begin{aligned} \text{Вплив} = & (\text{Коефіцієнт погоди} * \text{Зміна тиску повітря}) \\ & + (\text{Коефіцієнт катастроф} * \text{Ймовірність катастрофи}) \end{aligned} \quad (5)$$

Модель прогнозування технічних зламів [6]:

$$\begin{aligned} \text{Технічні злами} = & (\text{Коефіцієнт зламів} * \text{Кількість історичних зламів}) + \\ & (\text{Коефіцієнт стану} * \text{Стан обладнання}) \end{aligned} \quad (6)$$

Модель прогнозування роботи pomp та компресорних систем [7]:

$$\text{Робота pomp} = (\text{Потужність pomp} * \text{Час роботи pomp}) / (\text{Тиск перед} \\ \text{pomпами} * \text{Витрата води}) \quad (7)$$

Авторами було створено модель прогнозування тривалості ремонтних робіт під час пошкодження водопроводу за наявності статистичних даних про аварії, що сталися раніше на водопроводі даного міста, і тривалості ремонтних робіт у кожному випадку [8]. Цю модель було розраховано методом штучних нейронних мереж [9], але можливість її практичного застосування викликає деякі сумніви.

Аналіз наявних моделей та методів показав, що причини виникнення аварій в системах водопостачання можуть бути різними: знос трубопроводів, корозія, нерівномірний тиск, вплив ґрунту тощо. Прогнозування аварій має враховувати ці фактори та бути спрямованим на передбачення можливих ризиків та аварійних ситуацій.

Потрібно створити інтегральну модель прогнозування безперебійності функціонування водопостачання та увести її до наявної системи підтримки прийняття рішень [10].

### Перелік посилань

1. Завгородня Г.А., Корнага Я.І., Мухін В.С., Завгородній В.В., Базака Ю.А. Моделювання сценаріїв аварійних ситуацій на автомобільних газозаправних станціях // URI: [https://www.tech.vernadskyjournals.in.ua/journals/2019/5\\_2019/part\\_1/16.pdf](https://www.tech.vernadskyjournals.in.ua/journals/2019/5_2019/part_1/16.pdf)
2. Біблік І.В., Аврамов К. В., Русанов Р. А. Прогнозування ерозійно-корозійного зносу елементів трубопроводів атомних електростанцій методом нейромережевого моделювання // Journal of Mechanical Engineering – Problemy Mashinobuduvannia. – URI: <https://journal-me.com/archive-ukr/vol21-2018-iss3-paper2/>



3. Мартинов С.Ю. Конспект лекцій з навчальної дисципліни «Імітаційне моделювання у системах водопостачання і водовідведення» для здобувачів вищої освіти другого (магістерського) рівня за спеціальністю 192 «Будівництво та цивільна інженерія» освітньо-професійною програмою «Водопостачання та водовідведення» та заочної форм навчання. – Рівне: НУВГП, 2019. – 90 с. – URI: <https://ep3.nuwm.edu.ua/14306/1/03-06-84%20%281%29.pdf>
4. Пирський Ю. К., Барсуков В. З., Лінючева О. В. Методи захисту обладнання від корозії та захист на стадії проектування [Електронний ресурс]: підр. для студ. спеціальності 161 «Хімічні технології», спеціалізації «Електрохімічні технології неорганічних та органічних матеріалів». – Київ : КПІ ім. Ігоря Сікорського, 2018. – 318 с. – URI: [https://ela.kpi.ua/bitstream/123456789/23891/3/Metody\\_zahystu\\_obladn\\_vid\\_korozii.pdf](https://ela.kpi.ua/bitstream/123456789/23891/3/Metody_zahystu_obladn_vid_korozii.pdf)
5. Черниш З. С. Математичні моделі нелінійних нестационарних процесів на фондовому ринку: дисертація на здобуття ступеня магістра за спеціальністю 124 Системний аналіз; Інститут прикладного системного аналізу Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». – Київ, 2021. – 111 с. – URI: [https://ela.kpi.ua/bitstream/123456789/46544/1/Chernysh\\_magistr.pdf](https://ela.kpi.ua/bitstream/123456789/46544/1/Chernysh_magistr.pdf)
6. Клименко І.В. Моделі та методи оцінки, прогнозування та управління діяльністю підприємств залізничного транспорту в умовах невизначеності – URI: [http://ndch.diit.edu.ua/upload/Защиты/Клименко\\_Иван/Дисертація%20Клименко%20І.В.%20%202021.04.21.pdf](http://ndch.diit.edu.ua/upload/Защиты/Клименко_Иван/Дисертація%20Клименко%20І.В.%20%202021.04.21.pdf)
7. Шевченко Н.Г., Шудрик О.Л., Фатєєва Н.М., Фатєєв О.М., Пономарьов В.А., Прогнозування режиму роботи багатоступеневого відцентрового насоса при реальних умовах експлуатації нафтогазових свердловин – URI: <http://gm.khpi.edu.ua/article/view/226794/226277>
8. Мельников О. Ю., Закабула О. Ю. Постановка задачі прогнозування тривалості ремонтних робіт у випадку пошкодження водопроводу в невеликому місті // «ТАК»: телекомунікації, автоматика, комп'ютерно-інтегровані технології: зб. доповідей Всеукр. наук.-практ. конф. молодих вчених, 1–2 грудня 2021 р. / відп. ред. М.В. Ступак. – Покровськ: ДВНЗ «ДонНТУ», 2021. – С. 95-97
9. Мельников О. Ю., Закабула О. Ю. Застосування нейронних мереж для прогнозування тривалості ремонтних робіт під час пошкодження водопроводу в невеликому місті // Нейромережні технології та їх застосування НМТіЗ-2021: збірник наукових праць ХХ Міжнародної наукової конференції «Нейромережні технології та їх застосування НМТіЗ-2021» / за заг. ред. С.В.Ковалевського. – Краматорськ: ДДМА, 2021. – С. 99-102.
10. Мельников О. Ю., Закабула О. Ю. Моделювання рівня незадоволення потреб мешканців малих міст у системі підтримки прийняття рішень для водопостачання в екстремальних випадках // Вісник Національного технічного університету «ХПІ». Серія: Системний аналіз, управління та інформаційні технології : зб. наук. пр. / Нац. техн. ун-т «Харків. політехн. ін-т». – Харків : НТУ «ХПІ», 2023. – № 1 (9). – С.49–53. – DOI: <https://doi.org/10.20998/2079-0023.2023.01.07>

УДК 004.4

Залуцька О.О., Молчанова М.О., Віт Р.В., Мазурець О.В.

*Хмельницький національний університет*

## **КОНФІГУРУВАННЯ НЕЙРОННОЇ МЕРЕЖІ ДЛЯ КЛАСИФІКАЦІЇ ЕМОЦІЙНОЇ ТОНАЛЬНОСТІ ТЕКСТОВОЇ ІНФОРМАЦІЇ ЗА ПОКАЗНИКАМИ СЕМАНТИЧНОЇ ЗВ'ЯЗНОСТІ**

*Описано результати досліджень з конфігурування нейронної мережі класу трансформер для класифікації емоційної тональності текстової інформації за показниками семантичної зв'язності. Обґрунтовано вибір оптимальних параметрів, необхідних для ефективної класифікації емоційної тональності текстів.*

*The results of research on the configuration of a transformer-class neural network for the classification of the emotional tonality of text information based on indicators of semantic connectivity are described. The choice of optimal parameters necessary for effective classification of the emotional tonality of texts is substantiated.*

Класифікація емоційної тональності текстової інформації є методом вилучення та розпізнавання оцінок користувачів щодо продуктів і моделей та має різні підходи з використанням алгоритмів машинного навчання для класифікації емоцій, що стоять за цим текстом [1]. До прикладу, аналіз настроїв твітів для розуміння сприйняття людьми певних новин, оцінка взаємодії людини з роботом, формування системи рекомендації у виборі товарів тощо.

Розв'язання завдання класифікації емоційної тональності україномовних текстів на прикладі відгуків сервісів електронної комерції може застосовуватись як для розуміння сприйняття людьми певних новин, так і для комерційних цілей як то оцінки роботи менеджера тощо.

У напрямку класифікації емоційної тональності текстової інформації більшість публікацій присвячено саме роботі з англійськими текстами, оскільки є достатня кількість розмічених наборів даних, на кшталт IMDB (набір розмічених даних, що містить понад 50 000 оглядів фільмів) та набір розмічених за емоційним забарвленням відгуків з інтернет-магазину «Amazon». Що ж стосується досліджень української мови, перша проблема з якою зіштовхуються науковці, стосується експериментальних даних [2]. В основному науковці такі дані збирають самі, що є трудомістким процесом, та зазвичай такі дані не є розміченими, їх потрібно розмічувати «вручну».

Для класифікації емоційної тональності текстової інформації використано варіацію нейронної мережі RoBERTa (скорочення від «Надійно оптимізований підхід BERT»), яка є варіантом моделі BERT (Bidirectional Encoder Representations

from Transformers), яку розробили дослідники Facebook AI [3]. Як і BERT, RoBERTa є мовною моделлю на основі трансформера, яка використовує самоувагу для обробки вхідних послідовностей і створення контекстуалізованих представлень слів у реченні.

Однією з ключових відмінностей між RoBERTa та BERT є те, що RoBERTa навчався на значно більшому наборі даних і з використанням ефективнішої процедури навчання. Під час навчання RoBERTa використовує техніку динамічного маскування, що допомагає моделі вивчати більш надійні та узагальнені представлення слів.

Так як класифікація емоційної тональності текстової інформації за показниками семантичної зв'язності на основі нейромережевого підходу є сьогодні актуальним напрямом наукових досліджень, для української мови на сьогодні також є деякі напрацювання. Одними з яких є попередньо навчена мультимовна модель препроцесингу, що працює також і з українською мовою та ще з понад 50 іншими мовами [4], та входить до складу моделей бібліотеки Tensorflow\_hub мови Python. На базі цих моделей пропонується створити модель, що буде донавчено на вищеописаній вибірці експериментальних даних. Вибір мультимовних моделей обумовлено тим, що як вже було вище наведено, тексти можуть містити текст не тільки літературною українською мовою.

Конфігурація нейронної мережі для класифікації емоційної тональності текстової інформації на базі обраного типу нейромережі має наступну структуру. На вхідному шарі відбувається перетворення вхідної текстової інформації на тензор Keras, тобто символічний тензороподібний об'єкт, який доповнюється атрибутами, які дозволяють побудувати модель Keras за вхідним та вихідними даними моделі. Надалі тензор подається на вхід шару попередньої обробки, яка включає в себе обгортку об'єкта, що викликається, для використання як шару Keras на базі попередньо навченої моделі попередньої обробки тексту [4]. Дана модель використовує SentencepieceTokenizer [5], що токенизує тензор рядків UTF-8 та є неконтрольованим токенизатором і детокенизатором тексту.

Наступним шаром є RoBERTa енкодер. Цей шар працює на основі попередньо навченої моделі «xlm\_roberta\_multi\_cased\_L-12\_H-768\_A-12» [6], що є результатом неконтрольованого крос-мовного репрезентативного навчання в масштабі (XLM-RoBERTa), та попередньо навчена на 2,5 ТБ відфільтрованих даних CommonCrawl, що містять 100 мов.

Наступним шаром є шар dropout, що випадково встановлює одиниці введення на 0 із частотою швидкості на кожному кроці під час навчання, що допомагає запобігти перенавчанню. Вхідні дані, для яких не встановлено значення 0 масштабуються таким чином, щоб сума всіх вхідних даних не змінювалася.

Останнім кроком в моделі є безпосередньо класифікація, що здійснюється з використанням функції Dense та видає результат від 0 до 1, що є мірою позитиву в україномовних відгуках електронної комерції. Де 0 – негативний текст, а 1 – позитивний текст.

Далі запропонована модель проходить донавчання під вищеописану вибірку. Донавчання проводилось із різною комбінацією кількісних показників параметрів, таких як: кількість епох навчання, Seed, Batch size [7].

Кількість епох навчання показує, скільки разів модель підлягає навчанню. Параметр Seed буде взято 42, з огляду на те, якщо не встановити для random\_state значення 42, щоразу, коли знову буде запускатись програмний код, він створюватиме інший тестовий набір. Batch size – кількість навчальних прикладів, що використовуються в межах однієї ітерації. Дуже важко відразу визначити, який ідеальний розмір партії для потріб конкретної задачі, тому даний параметр буде підібрано експериментальним шляхом.

Відповідно до обраних параметрів, визначались показники оцінки функціональності моделі класифікації емоційної тональності текстової інформації, такі як: час навчання в секундах, точність та втрати. У якості функції втрат використовувалась бінарна крос-ентропічна функція. Точність для проведеного дослідження визначається як ділення кількості правильних відповідей на загальну кількість відповідей.

Враховувались одержані показники оцінки функціональності (час навчання, точність та втрати) різних параметрів моделей налаштування (кількість епох навчання, seed, batch size) нейромережевого класифікатора. Оскільки досліджувана версія RoBERTa є мультимовним трансформером, донавченим на білінгвістичних даних, в цілому нейромережа не має проблем з ідентифікацією настрів.

При дослідженні текстів, яких немає в навчальній та тестовій вибірках показано високу ефективність запропонованої архітектури. Навчальна вибірка не чистилась «вручну», тому допускається, що може бути певний відсоток хибно-класифікованих текстів, проте це не дає значного впливу на кінцеву точність класифікації емоційної тональності текстової інформації, що написані не лише чистою українською мовою, а й містять суржик та білінгвістичні дані. На Рисунку 1 графік ілюструє зміни параметра точності в залежності від пройдених епох, а Рисунку 2 – зміни функції втрат для комбінації параметрів навчання: 3 епохи, 64 розмір батча.

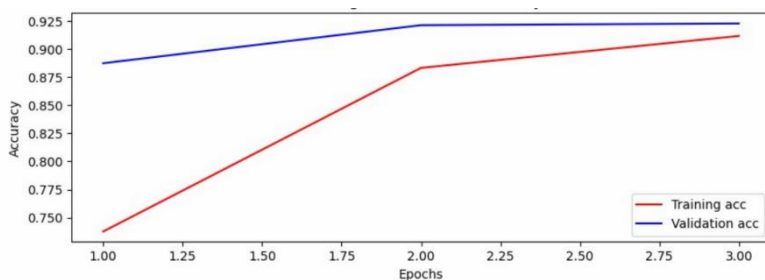


Рисунок 1 – Ілюстрація процесу навчання за епохами за показником точності в залежності від кількості епох навчання 3

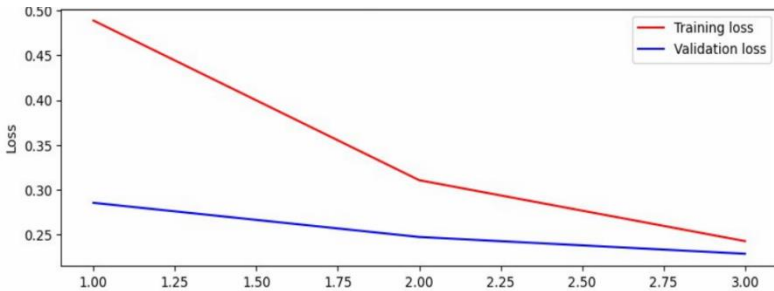


Рисунок 2 – Ілюстрація процесу навчання за епохами за показником функції втрат за кількості епох навчання 3

Графік на Рисунку 1 свідчить про недостатню кількість епох навчання для стабілізації результату, оскільки показник Ассигасу мав тенденцію до зростання, а показник функції втрат – до спадання, не застигнувши на одному рівні.

Проте, продовживши експеримент, змінивши кількість епох навчання до 10, були отримані результати, проілюстровані на Рисунках 3 та 4.

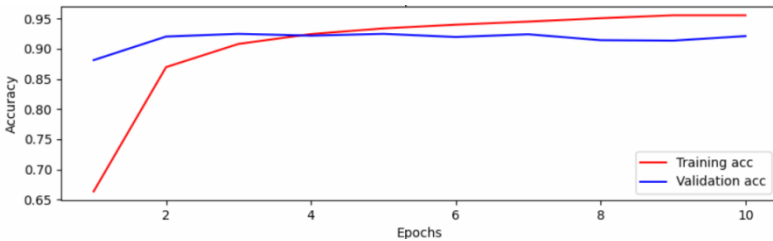


Рисунок 3 – Ілюстрація процесу навчання за епохами за показником точності за кількості епох навчання 10

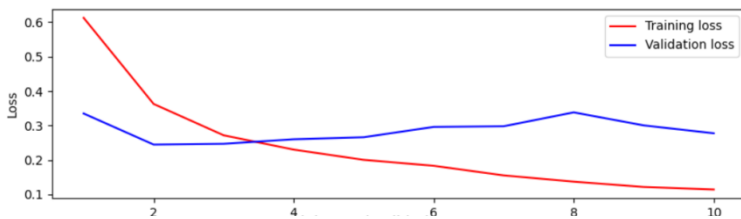


Рисунок 4 – Ілюстрація процесу навчання за епохами за показником функції втрат за кількості епох навчання 10

Отримані результати свідчать, що при використанні вибірки для валідації точність класифікації не росте. А функція втрат взагалі після 3ї ітерації для вибірки

для валідації мала тенденцію до незначного зростання. Проте, такі результати можуть свідчити про те, що вибірки недостатньо відфільтровані. Оскільки перевірка нейромережі на текстах, що не містяться в базі дала практично безпомилкові результати для 40 текстів, які дійсно містили емоцію. Графік ілюстрації проходження процесу донавчання по епохам показано на Рисунках 5 та 6.

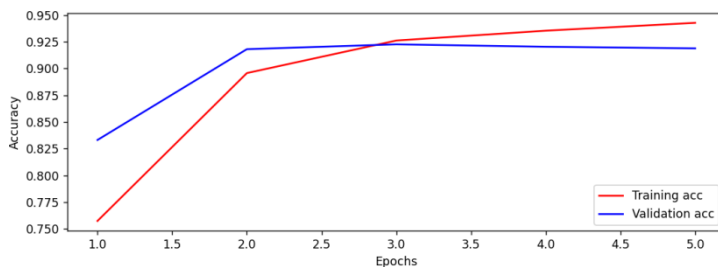


Рисунок 5 – Ілюстрація процесу навчання за епохами за показником точності з донавчанням

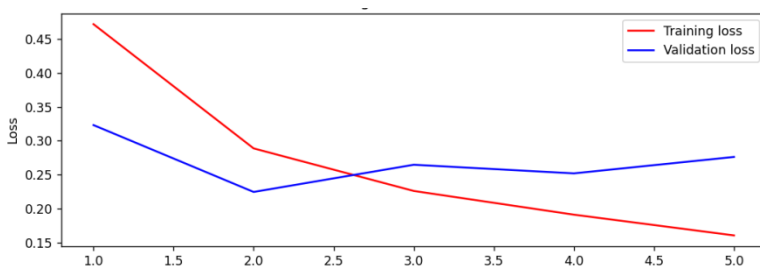


Рисунок 6 – Ілюстрація процесу навчання за епохами за показником функції втрат з донавчанням

Результати даного експерименту з класифікації емоційної тональності текстової інформації свідчать про те, що вибірка як вже було вище сказано, не була очищена вручну. Тому, зі зростом кількості епох нейромережа починає просто «запам'ятовувати», які тексти куди належать, про що свідчить червона лінія на графіках 3-4 та 5-6. Так як для навчальної вибірки функція втрат значно менша, а точність – значно вища. Проте, отримані показники функції втрат та точності пов'язані з тим, що вибірка не була відфільтрована «вручну», і містила тексти, які включали беземоційні коментарі, часто з одного слова або фрази. До того ж, проведений аналіз оцінки тональності показав на практиці з 40 фраз, яких не має ні в навчальній, ні в тестовій вибірках, і які були попередньо оцінені експертом, що нейронна мережа справляється з завданням безпомилково, при чому тексти містили як стилістичні, так і орфографічні помилки та були представлені мультимовними даними.

Отже, було розглянуто сучасний стан напряму семантичної обробки тексту, а саме класифікації емоційної тональності текстової інформації. Однією із найбільш точних нейромереж визначили архітектуру BERT, проте для аналізу коротких документів краще себе показала її модифікація – RoBERTa. Для оцінки роботи запропонованої архітектури для класифікації емоційної тональності текстової інформації було використано точність та функцію втрат. Для комбінованих мультимовних текстів вдалося отримати точність 0.92, в той час як функція втрат мала значення 0.29.

Запропонований підхід до класифікації емоційної тональності текстової інформації має певні обмеження. Доцільно його застосовувати до визначення тональності коротких текстових текстів (довжиною до 500 слів), представлених на українській мові та можуть містити суржик та іншомовні вкладки слів. Зміна вмісту навчальної вибірки впливає на результат навчання нейронної мережі, і відповідно впливає на ефективність класифікації емоційної тональності текстової інформації. З часом в побутовій мові можуть відбуватися зміни, які також впливають на хід та результати класифікації емоційної тональності текстової інформації.

### Перелік посилань

1. Mann, S., Arora, J., Bhatia, M., Sharma, R., Taragi, R, Twitter Sentiment Analysis Using Enhanced BERT, in: Kulkarni, A.J., Mirjalili, S., Udgata, S.K. Intelligent Systems and Applications. Lecture Notes in Electrical Engineering, vol 959. Springer, Singapore, 2023, pp. 263-271.
2. Panchenko, D., Maksymenko, D., Turuta, O., Yerokhin, A., Daniil, Y., Turuta, O., Evaluation and Analysis of the NLP Model Zoo for Ukrainian Text Classification, in: Information and Communication Technologies in Education, Research, and Industrial Applications. ICTERI 2021, Communications in Computer and Information Science, vol 1698. Springer, Cham.
3. Ai.Facebook.Com., RoBERTa: An optimized method for pretraining self-supervised NLP systems. URL: <https://ai.facebook.com/blog/roberta-an-optimized-method-for-pretraining-self-supervised-nlp-systems>.
4. Tfhub.Dev., Text preprocessing model xlm\_roberta\_multi\_cased\_preprocess. URL: [https://tfhub.dev/jeongukjae/xlm\\_roberta\\_multi\\_cased\\_preprocess/1](https://tfhub.dev/jeongukjae/xlm_roberta_multi_cased_preprocess/1).
5. Tensorflow.Org., Text.SentencepieceTokenizer. URL: [https://www.tensorflow.org/text/api\\_docs/python/text/SentencepieceTokenizer](https://www.tensorflow.org/text/api_docs/python/text/SentencepieceTokenizer).
6. Tfhub.Dev., Unsupervised Cross-lingual Representation Learning at Scale. xlm\_roberta\_multi\_cased\_L-12\_H-768\_A-12. URL: [https://tfhub.dev/jeongukjae/xlm\\_roberta\\_multi\\_cased\\_L-12\\_H-768\\_A-12/1](https://tfhub.dev/jeongukjae/xlm_roberta_multi_cased_L-12_H-768_A-12/1).
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.

УДК 004.4

Запорожець М.В., Молчанова М.О., Скрипник Т.К.

*Хмельницький національний університет*

## **МЕТОД ВИЯВЛЕННЯ ПАТОЛОГІЙ МОЗКУ ЗА ЗОБРАЖЕННЯМИ МАГНІТНО-РЕЗОНАНСНОЇ ТЕРАПІЇ НЕЙРОМЕРЕЖЕВИМИ ЗАСОБАМИ**

*Розглянуто аспекти розробки методу для аналізу зображення магнітно-резонансної терапії, яка дозволяє ефективно знаходити різні види патологій на ділянках головного мозку та в подальшому правильно організувати лікування. Запропонований метод забезпечує пошук патології мозку по зображенню магнітно-резонансної терапії.*

*The article deals with the aspects of developing a method for analyzing magnetic resonance imaging, which allows to effectively find various types of pathologies in the brain and subsequently organize treatment correctly. The proposed method provides a search for brain pathology by magnetic resonance imaging.*

В сучасній медицині важливим є виявлення патологій мозку для ранньої діагностики та ефективного лікування. Один із перспективних напрямків - використання нейромереж для аналізу зображень магнітно-резонансної терапії (МРТ) мозку. Цей підхід може забезпечити точну та швидку діагностику, а також поліпшити планування лікування. Аналіз медичних зображень вимагає уважності та професіоналізму фахівця, а також витрати часу. Швидке та вчасне встановлення діагнозу може значно полегшити процес відновлення пацієнта. Використання нейромереж для аналізу МРТ може також виявляти сигнали патології, які можуть бути непомітними для людського ока. Це допомагає виявляти патології на ранніх стадіях, коли лікування найбільш ефективно та може запобігти подальшому прогресу хвороби. Аналіз медичних зображень є важливим методом діагностики для численних захворювань.

Тему нейромережових засобів для аналізу МРТ зображень на сьогоднішній день досліджує досить велика кількість людей. Дехто з них, завдяки результатам своїх досліджень – відкривають щось нове або покращують в загальному роботу цього методу. Для прикладу:

У роботі [1] представлено систему виявлення пухлин головного мозку на основі згорткових нейронних мереж (CNN). Система складається з двох основних компонентів:

1) Архітектура CNN: Автори використовували модифіковану архітектуру VGG16, яка складається з 13 шарів згортки, 3 шарів повного з'єднання та 1 шару класифікатора.

2) Методи обробки зображень: Для підготовки даних для навчання CNN автори використовували такі методи обробки зображень, як нормалізація, фільтрування шуму та сегментація.



Система протестована на наборі даних BRATS 2022, який містить 325 МРТ-зображень мозку з пухлинами. Тестові результати показали, що система може досягти точності 95,3% для виявлення пухлин головного мозку.

У роботі [2] представлені результати дослідження, в якому було розроблено нову модель штучного інтелекту для виявлення пухлин головного мозку на магнітно-резонансних зображеннях (МРТ). Модель заснована на згорткових нейронних мережах (CNN). У статті провели експерименти на наборі даних з 1000 МРТ-зображень головного мозку, на яких були позначені пухлини. Результати експериментів показали, що розроблена модель досягла точності виявлення пухлин головного мозку на рівні 95%.

Якщо порівняти ці дві статті, то можна зробити висновок, перша стаття, використовує набір даних з 1000 МРТ-зображень головного мозку, а друга стаття, використовує набір даних з 2000 МРТ-зображень головного мозку. Це означає, що друга стаття має більшу вибірку, що може призвести до більш точних результатів.

Тому метою проведення дослідження є реалізувати метод виявлення патологій мозку за зображеннями магнітно-резонансної терапії нейромережевими засобами з використанням згорткової нейромережі CNN.

На рисунку 1 представлена архітектура запропонованого методу.

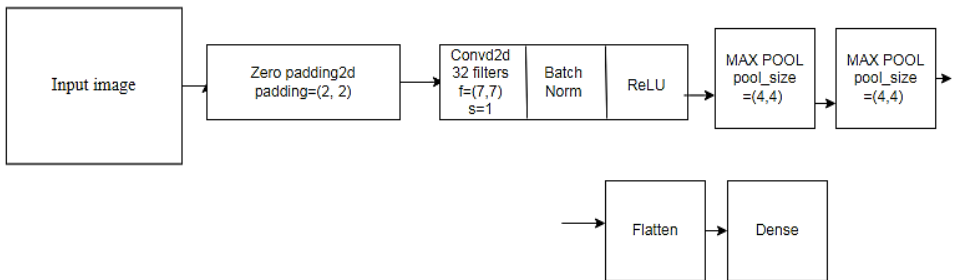


Рисунок 1 – Архітектура методу

Спочатку потрібно надати входні дані у вигляді зображення МРТ і після цього це зображення подається на вхід до нейронної мережі. Після цього, ці данні проходять через наступні шари:

- Починаючи з нульового заповненого шару з розміром пулу (2,2), ми додаємо нульові значення навколо вхідного зображення, щоб зберегти його розміри та розширити його.

- Наступною структурною одиницею є згортковий шар з фільтрами, які мають розмір фільтра і крок 1. Цей шар призначений для виділення різних ознак та особливостей з вхідного зображення. Фільтри переміщуються по всьому вхідному зображенню, шукаючи певні особливості, такі як горизонтальні або вертикальні лінії, кути, текстові шаблони тощо.

- Наступним етапом є шар пакетної нормалізації, який служить для нормалізації значень пікселів з метою прискорення обчислень.

– Після цього в мережі використовується шар активації, який застосовує операцію активації до вихідних значень згорткових та інших шарів.

– Два наступних шари призначені для підсумовування і виділення найбільших значень з певних областей вхідних зображень.

– Після цього слідує шар для перетворення тривимірної матриці в одновимірний вектор.

– Завершальним етапом є щільний (вихідний) повністю зв'язаний шар з одним нейроном, який використовує сигмоїдну активацію.

Для оцінки ефективності роботи методу, проведено експерименти з певною кількістю набору даних в 24 цикла. Результат зображено на рисунку 2-3. По закінченню експерименту отримуємо результат, що найкраща точність була отримана на 23 циклі і становить 91%.

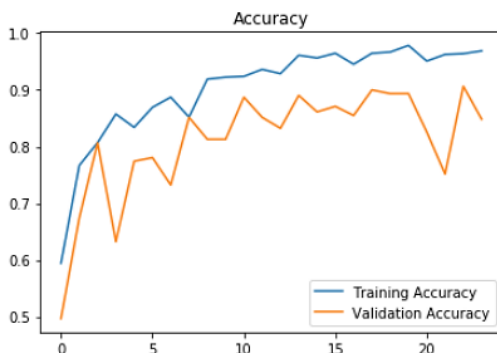


Рисунок 2 – Результат

Отже, результатом роботи є розробка методу виявлення патологій мозку на основі аналізу магнітно-резонансних зображень за допомогою нейромережі. Цей метод дозволяє ефективно аналізувати МРТ-зображення та виявляти різноманітні види патологій головного мозку. Більш того, цей підхід може бути постійно вдосконалюватись для адаптації до нових вимог та виявлення нових видів захворювань мозку, які досі не були відкриті або не мають належних методів виявлення на ранній стадії, коли лікування є найбільш ефективним.

### Перелік посилань

1. Md Abdullah Nasim, Md Shahriar Alam, "Brain Tumor Detection Using Convolutional Neural Network". URL: [https://www.researchgate.net/profile/Md-Abdullah-Nasim/publication/337768246\\_Brain\\_Tumor\\_Detection\\_Using\\_Convolutional\\_Neural\\_Network/links/5eddf25a45851529454462b3/Brain-Tumor-Detection-Using-Convolutional-Neural-Network.pdf](https://www.researchgate.net/profile/Md-Abdullah-Nasim/publication/337768246_Brain_Tumor_Detection_Using_Convolutional_Neural_Network/links/5eddf25a45851529454462b3/Brain-Tumor-Detection-Using-Convolutional-Neural-Network.pdf)
2. D C Febrianto<sup>1</sup>, I Soesanti<sup>1</sup>, H A Nugroho<sup>1</sup>, "Convolutional Neural Network for Brain Tumor Detection" URL: <https://iopscience.iop.org/article/10.1088/1757-899X/771/1/012031/pdf>

УДК 004.4

Карлечук Д.Т., Багрій Р.О., Скрипник Т.К., Тищенко О.О.

*Хмельницький національний університет*

## **МЕТОД СТРУКТУРУВАННЯ ТЕКСТУ ОГОЛОШЕНЬ ДЛЯ ОБ'ЄКТІВ НЕРУХОМОСТІ ЗАСОБАМИ NLP**

*Розглянуто метод розпізнавання іменованих сутностей, який дозволяє ідентифікувати та класифікувати по категоріях розпізнані дані із текстових оголошень у сфері нерухомості, за допомогою підходів обробки природної мови, тим самим забезпечуючи трансформацію неструктурованих даних в структуровані. Також тут описано алгоритм роботи такого методу, внутрішні процеси зв'язані з ним та результат розпізнавання сутностей*

*A named entity recognition method is proposed that allows one to identify and categorize recognized data from text advertisements in the real estate industry using natural language processing methods, thereby ensuring the transformation of unstructured data into structured ones. The algorithm of this method, the internal processes connected with it and the result of entity recognition are described here*

### **Вступ**

Структуровані дані являють собою високоорганізовану, фактичну та точну інформацію [1]. Вони мають чітко визначений та організований формат, який повинен відповідати стійкій схемі або моделі даних, яка визначає тип та розташування цих елементів у самому наборі даних. Неструктуровані дані являють собою неорганізований набір інформації [2]. Вони не мають певної структури, та представлені у всьому різноманітті форм. Одним з прикладів неструктурованих даних, де може міститися інформація про об'єкти нерухомості являється оголошення.

Оголошення – це короткі текстові повідомлення, котрі містять різну за призначенням інформацію, зазвичай приватного рекламного характеру [3]. Зміст будь-якого оголошення варіюється залежно від його типу, та предметної області яку він представляє. Щоб отримати структуровані дані з неструктурованого тексту оголошень необхідно застосувати методи обробки текстової інформації, чим займається окрема галузь під назвою обробка природної мови (Natural Language Processing) [4].

### **Основна частина**

Перетворення неструктурованих даних з оголошення у структуровані здійснюється за допомогою обробки текстової інформації, що включає в себе різні підходи і техніки з використанням текстових даних. Одним з таких підходів є

розпізнавання іменованих сутностей (NER). Це метод обробки природної мови, що використовується для ідентифікації та класифікації іменованих об'єктів у неструктурованому тексті за заздалегідь визначеними категоріями [5].

Метою роботи є розробка методу розпізнавання іменованих сутностей з текстів оголошень у сфері нерухомості. На рисунку 1 представлено цей процес.



Рисунок 1 – Процес роботи розпізнавання сутностей

Згідно рисунку, можна виділити на два ключових етапи:

1. Попередня обробка тексту. Перший крок включає підготовку текстових даних для аналізу. Він включає такі завдання, як токенізація (розбиття речення на слова), видалення шумів (видалення зайвих сполучних слів), лематизація та стеммінг (спрощення слова до його основного кореня).

2. Ідентифікація та класифікація сутності. Після попередньої обробки тексту алгоритми NER сканують його, щоб визначити послідовності слів, які відповідають об'єктам. Для цього було використано алгоритм розпізнавання сутностей, який може базуватися на підході з учителем, оскільки він дає точніші результати в порівнянні з іншими підходами [5]. Цей алгоритм може аналізувати текст і призначати теги, мітки, та категорії на основі вмісту текстових даних, наприклад, вказавши мітку «1200» як ціна маєтку (рисунок 2)

З рисунка видно, що на початку NER-система приймає вхідне речення про об'єкт нерухомості і розбиває його на окремі слова. Тобто, речення: «*Маєток коштує 1200\$ має 5 кімнат, та знаходиться на Трипільській*» розбивається на список слів  $\langle w_n \rangle$ , де  $w$  – означає слово з речення, а  $n$  – порядковий номер слова.

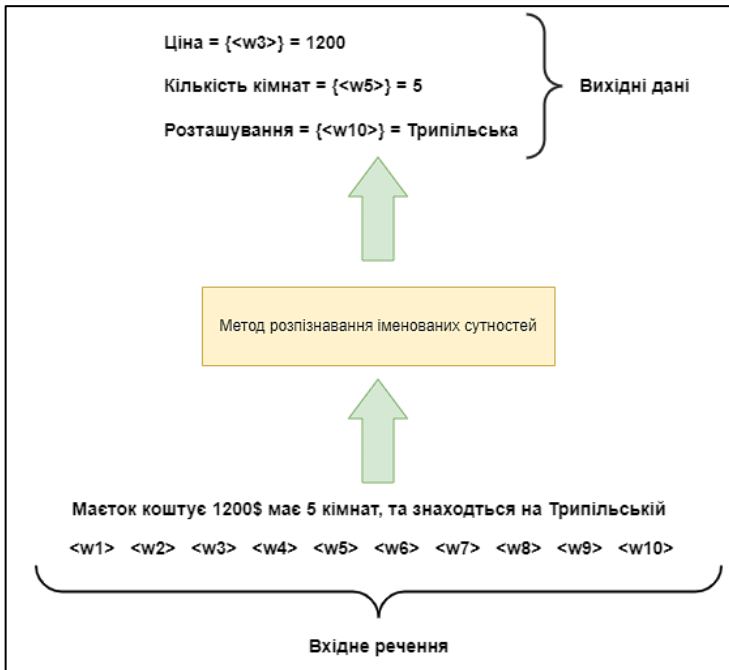


Рисунок 2 – Схема роботи методу розпізнавання сутностей в оголошенні

Отримавши слова з речення до них застосовується метод розпізнавання іменованих сутностей, який всередині являє собою цілий фреймворк ідентифікації та категоризації і має назву «Embed, Encode, Attend, Predict», що стосується концептуальної основи Метью Хоннібала з обробки природної мови [6]. Він зображений на рисунку нижче:

На етапі «*Embed*» кожне слово з речення «*Маєток коштує 1200\$ має 5 кімнат, та знаходиться на Трипільській*» перетворюється в числовий вектор слова, тим самим, збираючи семантичну інформацію із вхідного тексту. Це саме відбувається із словами що позначають готові категорії. Таким чином слова із схожим контекстом стають близько один до одного в числовому просторі.

Після цього відбувається етап «*Encode*» де кодується послідовність числових векторів слів (з попереднього етапу) у матрицю з використанням рекурентних нейронних мереж (RNN). На цьому етапі фіксуються відносини між словами.

Далі етап «*Attend*» – приймає матриці (сформовані на попередньому кроці) та зводить їх до одного єдиного вектора, який буде далі переданий у нейронну мережу прямого поширення для здійснення прогнозування.

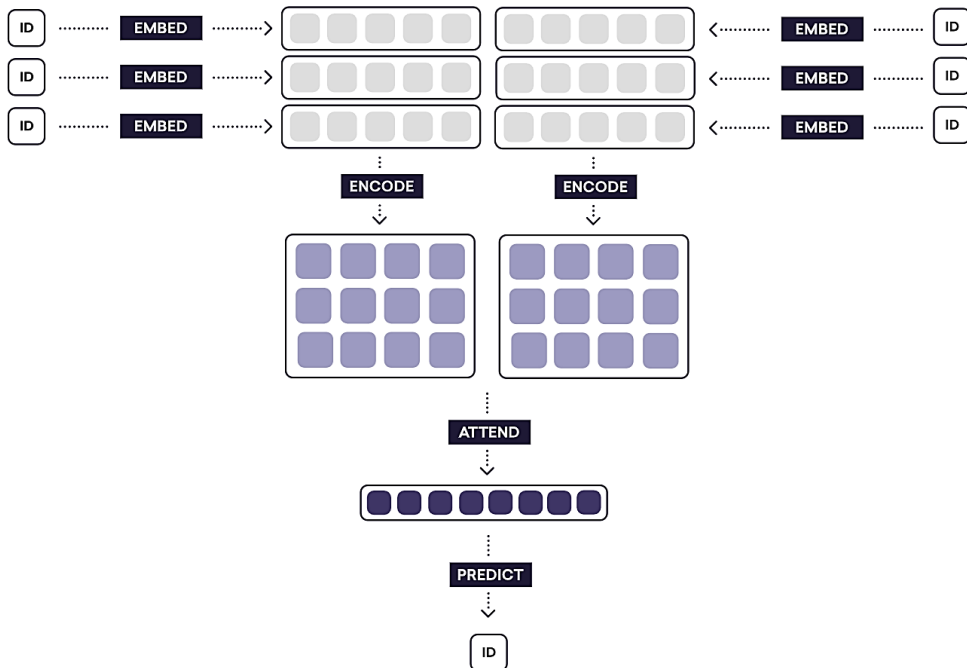


Рисунок 3 – Фреймворк «Embed, Encode, Attend, Predict»

```

text = """
Explore this stunning property in the heart of downtown, boasting a luxurious for sale property, a spacious and elegant mansion property for an attractiv
"""
doc = nlp(text)

spacy.displacy.render(doc, style="ent", jupyter=True)

```

Explore this stunning property in the heart of downtown, boasting a luxurious **for sale** **PROPERTY STATUS** property, a spacious and elegant **mansion** **PROPERTY TYPE** property for an attractive price of **\$1.5 million.** **PRICE** The expansive house size of **5,000 square feet** **HOUSE SIZE** accommodates numerous features and amenities, including a **private pool** **FEATURES/AMENITIES**, **modern kitchen** **FEATURES/AMENITIES**, and a **cozy fireplace.** **FEATURES/AMENITIES** Residents can enjoy the convenience of nearby landmarks like **Central Park** **NEARBY LANDMARKS** and breathtaking views of the city skyline. With its **impeccable condition** **CONDITION** and ample rooms, this **6-bedroom** **BED**, **4-bath** **BATH** gem on **Main Street** **STREET**, nestled in the vibrant city of **New York** **CITY**, is ready to be your new dream home. The property offers essential utilities such as **central air conditioning** **UTILITIES** and **heating** **UTILITIES**, ensuring year-round comfort. Located in the state of New York, this property combines luxury living with urban convenience. If you are interested please contact us at **kidehen@optonline.net** **OWNER EMAIL** or call us at **(206) 342-8631** **OWNER PHONE**

Рисунок 3 – Результат роботи методу з розпізнавання сутностей з текстів оголошень по об'єктах нерухомості

Останній етап «*Predict*» – прогнозує (передає вектор з попереднього кроку) багатозаровому перцептрону для виведення ідентифікатора мітки об'єкта. Саме тут відбувається генерація бажаного результату.

Розібравши роботу розпізнавання іменованих сутностей (NER), важливо відзначити, що практична реалізація NER є значно полегшеною за рахунок уже відомих потужних бібліотек обробки природної мови. Одна з таких комплексних бібліотек, яку було використано в дослідженні має назву SpaCy [7], що забезпечує зручний інтерфейс для NER та значно спрощує процес. На рисунку 3, представлено результат роботи методу розпізнавання сутностей подавши на вхід текст оголошення з нерухомості.

### **Висновки**

Отже, проведено аналіз методів обробки природної мови в структуруванні текстів оголошень для об'єктів нерухомості засобами NLP. Розглянуто та описано основний підхід по ідентифікації та класифікації сутностей у неструктурованому тексті, та аналіз методу з розпізнавання іменованих сутностей. На основі попередньої інформації розроблено та реалізовано метод структурування тексту оголошень. Розроблений метод дозволяє розпізнавати, ідентифікувати, категоризувати та витягувати розпізнану інформацію із звичайних текстів оголошень у сфері нерухомості.

### **Перелік посилань**

1. Структуровані дані. [Електронний ресурс]. – Режим доступу: <https://www.altexsoft.com/blog/structured-unstructured-data/>
2. Неструктуровані дані. [Електронний ресурс]. – Режим доступу: [https://www.researchgate.net/publication/277615592\\_Unstructured\\_Data\\_Analysis-A\\_Survey](https://www.researchgate.net/publication/277615592_Unstructured_Data_Analysis-A_Survey)
3. Різновид оголошень. [Електронний ресурс]. – Режим доступу: [https://en.wikipedia.org/wiki/Classified\\_advertising](https://en.wikipedia.org/wiki/Classified_advertising)
4. Natural Language Processing (NLP). [Електронний ресурс]. – Режим доступу: [https://www.researchgate.net/publication/364302290\\_A\\_Brief\\_Survey\\_on\\_Natural\\_Language\\_Processing\\_Based\\_Text\\_Generation\\_and\\_Evaluation\\_Techniques](https://www.researchgate.net/publication/364302290_A_Brief_Survey_on_Natural_Language_Processing_Based_Text_Generation_and_Evaluation_Techniques)
5. Basra Jehangir, Saravanan Radhakrishnan, Rahul Agarwal, "A survey on Named Entity Recognition": [Електронний ресурс]. – Режим доступу: <https://www.sciencedirect.com/science/article/pii/S2949719123000146>
6. Embed Encode Attend Predict. [Електронний ресурс]. – Режим доступу: [https://github.com/explosion/talks/blob/master/2018-04-12\\_Embed-Encode-Attend-Predict.pdf](https://github.com/explosion/talks/blob/master/2018-04-12_Embed-Encode-Attend-Predict.pdf)
7. Spacy a python library for NLP tasks. [Електронний ресурс]. – Режим доступу: <https://spacy.io/api/entityrecognizer>

УДК 004.7

Карпович В.В., Дрозд А.І., Жуковський П.О., Мельник В.В.

*Хмельницький національний університет*

## **МЕТОДИ ВИРІШЕННЯ ПРОБЛЕМ ПРОПУСКНОЇ ЗДАТНОСТІ ДИСКІВ ДЛЯ ЗАСТОСУНКІВ З ІНТЕНСИВНИМ ОБСЯГОМ ДАНИХ**

*Розглянуто проблеми з пропускнуою здатністю дисків для застосунків з інтенсивним обсягом даних.*

*В роботі пропонується для підвищення ефективності таких операцій, що інтенсивно працюють із даними, розробити нові методи роботи в пам'яті, окрім вирішення нових проблем, пов'язаних із програмами обробки на основі пам'яті, такими як стійкість до відмов і узгодженість. Варіантом вирішення проблеми є обмеження відмовостійкості, щоб дозволити різним програмам із інтенсивним використанням даних продовжувати працювати належним чином у разі збою.*

*Addresses disk bandwidth issues for data-intensive applications.*

*The paper proposes to develop new in-memory techniques to improve the efficiency of such data-intensive operations, in addition to addressing new challenges associated with memory-based processing programs, such as fault tolerance and consistency. A workaround is to limit fault tolerance to allow various data-intensive applications to continue to function properly in the event of a failure.*

Сьогодні «великі дані» стають загальною темою в різних сферах. Таким чином, багато даних застосунків були розроблені для вирішення різних викликів і пов'язаних обмежень з поточним зростанням даних [1-3]. Ці програми використовуються для зберігання, аналізу та керування існуючими великими наборами даних. Одним із головних недоліків [4, 5] існуючих застосунків із інтенсивним використанням даних є відносно повільний доступ до диска. Дисківі програми обробки не можуть запропонувати адекватний відповідний час відповіді через затримку доступу до дисків. Таким чином, ефективні програми з інтенсивним використанням даних повинні підтримуватися обробкою на основі пам'яті замість обробки на основі диска, щоб отримати більшу продуктивність цих програм.

Перспективним напрямом вирішення такої проблеми може бути покращення довгострокових програм, що інтенсивно працюють із даними, шляхом розробки нових методів роботи в пам'яті, окрім вирішення нових проблем, пов'язаних із програмами обробки на основі пам'яті, такими як стійкість до відмов і



узгодженість. Варіантом вирішення проблеми, також, є обмеження відмовостійкості, щоб дозволити різним програмам із інтенсивним використанням даних продовжувати працювати належним чином у разі збою.

Незважаючи на те, що доступ до даних пам'яті є надзвичайно швидким порівняно з доступом до диска, наявна ефективна техніка індексування для підтримки швидких запитів допомагає уникнути інтенсивного сканування пам'яті.

Для вирішення цього завдання розробимо метод індексування, щоб покращити дві складні операції, пов'язані з великими наборами даних – пропуск відсутніх значень і запит просторового з'єднання через створення підходів на основі пам'яті з підтримкою індексування, які можуть обробляти великі обсяги даних.

Застосування розробленого методу дозволить покращити роботу з інтенсивними даними при їх великих обсягах.

Підтвердження результатів роботи здійснено через імплементацію розробленого методу в застосунках і дослідження дискового простору, часу звернень і зміни обсягу.

### **Перелік посилань**

1. Ifeanyi P Egwutuoha, David Levy, Bran Selic, and Shiping Chen. A survey of fault tolerance mechanisms and checkpoint/restart implementations for high performance computing systems. *The Journal of Supercomputing*, 65(3):1302–1326, 2013.
2. Thomas Heinis, Farhan Tauheed, and Anastasia Ailamaki. Spatial data management challenges in the simulation sciences. In *Proceedings of the international conference on Extending Database Technology*, number EPFL-CONF-190522, 2014.
3. Suhasini A Itkar and Uday V Kulkarni. Distributed algorithm for frequent pattern mining using hadoopmap reduce framework. *International Conference on Advances in Computer Science, AETACS*, 2013.
4. K Sunil Kumar, M Laxmaiah, and C Sunil Kumar. A compacted bitmap vector technique to evaluate iceberg queries efficiently. *International Journal*, 3(6):412–418, 2013.
5. Wei-Tee Lin and Chih-Ping Chu. Determining the appropriate number of nodes for fast mining of frequent patterns in distributed computing environments. *International Journal of Parallel, Emergent and Distributed Systems*, (ahead-of-print):1–13, 2014.

УДК 004.7.056.5

Каушан. С.О., Лисенко С.М.

*Хмельницький національний університет*

## **ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ЕЛЕКТРОННОГО РЕКРУТИНГУ ПЕРСОНАЛУ**

*Застосування інформаційних систем в електронному рекрутингу персоналу має велику актуальність у сучасному бізнес-середовищі. Інформаційні системи рекрутингу дозволяють автоматизувати багато рутинних процесів, таких як оголошення вакансій, прийом заявок, сортування резюме, оцінка кандидатів і розсилка запрошень на співбесіди. Це сприяє значному збільшенню продуктивності HR-відділу та заощадженню часу і ресурсів. Електронний рекрутинг дозволяє компаніям привертати таланти з різних регіонів та країн. Кандидати можуть легко знаходити вакансії і надсилати свої резюме через онлайн-платформи, що розширює географічний охоплення. Досліджено інформаційні системи рекрутингу. Виявлено, що вони дозволяють створювати бази даних кандидатів, проводити аналіз даних і використовувати різні методи оцінки для визначення найкращих кандидатів. Виявлено недоліки інформаційні системи електронного рекрутингу персоналу.*

*The use of information systems in the electronic recruitment of personnel is very relevant in the modern business environment. Recruiting information systems allow you to automate many routine processes, such as job postings, receiving applications, sorting resumes, evaluating candidates, and sending invitations to interviews. This helps to significantly increase the productivity of the HR department and save time and resources. Electronic recruiting allows companies to attract talent from different regions and countries. Candidates can easily find jobs and submit their resumes through online platforms, which expands geographic coverage. Researched information systems of recruiting. They have been found to enable the creation of candidate databases, data analysis and the use of various assessment methods to identify the best candidates. The shortcomings of the information system of electronic staff recruitment were revealed.*

### **Вступ**

Однією з найважливіших задач яка стоїть перед компанією як в будь який період її існування є підбір кваліфікованих працівників. Сьогодні в кожній компанії є від 1-2 рекрутерів до цілих окремих відділів рекрутингу, працівники котрих за день можуть провести десятки співбесід - вдалих чи ні [1-3].

Основне рішення при наймі працівника завжди має залишатися за людиною, але все одно існує багато інструментів які так чи інакше полегшують чи пришвидшують цю роботу.

## Дослідження інформаційних систем рекрутингу персоналу

На сьогодні активно розвиваються інформаційні системи рекрутингу персоналу і виконують багато задач, як наприклад упорядкування, виставлення пріоритетів, ведення бази потенційних кандидатів і т.д. Однак одним з найбільш ефективних з точки зору оптимізації робочого процесу рекрутерів бізнес процесів, є сама співбесіда [1-3].

І враховуючи велику кількість етапів співбесід навіть для однієї людини, це є дуже затратною дією .

А для того щоб цей бізнес процес оптимізувати, мабуть найкращим рішенням буде зменшити кількість співбесід за допомогою інформаційної системи яка зможе суттєво зменшити кількість опитуваних кандидатів.

В ході пошуку схожих рішень було виявлено деякі сервіси зі схожою функціональністю:

– All-in-one recruiting software for ambitious companies - програмне забезпечення для рекрутингу штучного інтелекту, призначене для швидшого пошуку та найму кандидатів. Спеціально для команд відділу кадрів, кадрових агентств і хедхантерів, можна переглянути за посиланням [4];

– Rate and compare candidates online - безпечні платформи для онлайн-голосування, які дозволяють легко проводити вибори кандидатів, в джерелі [5];

– Talent Management Software with a Clear Mission for Success - AI допоможе вам скласти набори навичок для посади, заповнити підцілі для посади та підготувати анкети для оцінювання, один з подібих ресурсів можна переглянути в джерелі [6];

– LinkedIn - ми можете швидко знайти вакансію та подати заявки на роботу, що відповідає нашому набору навичок та кар'єрним цілям, можна переглянути за посиланням [7].

Важливий елемент існування команди та запорука її успішності – зворотний зв'язок. Це стосується особливо тих компаній, де є і віддалені команди, і декілька проектів, і амбітні співробітники, а також можлива вірогідність вигорання. Пропонувати колегам заповнити бланки відповідей, а потім щось там рахувати один раз на рік – нелогічно та неінформативно. Хмарні рішення також пропонують функцію опитувань та вимірювання коефіцієнту eNPS.

eNPS – або показник Employee Net Promoter Score – це індекс задоволеності персоналу, що допомагає у вивченні рівня залученості та лояльності [8].

### Висновок

Результати дослідження інформаційні системи електронного рекрутингу виявило ряд недоліків, зокрема: відомі інформаційні системи використовують алгоритми для автоматизованого відбору кандидатів, і ці алгоритми можуть бути

схильні до біасу, що може призвести до недискримінаційного відкидання кандидатів на основі їх статусу, раси, статі тощо; оперування застарілою інформацією; нездатність до оперативної обробки великих даних; неоптимальна архітектура ІТ, що не уможлиблює її оновлення.

Для того, щоб впровадження інформаційних систем рекрутингу було успішним, важливо усунути ці недоліки і забезпечити баланс між автоматизацією та людським підходом у процесі відбору персоналу, що вимагає розроблення нових методів та інформаційні системи електронного рекрутингу.

### **Перелік посилань**

1. <https://review.firstround.com>
2. J. Ba and R. Caruana. Do deep nets really need to be deep? In Advances in neural information processing systems, 2019. (2654-2662)
3. G. Hinton, O. Vinyals, and J. Dean. Distilling the knowledge in a neural network. arXiv preprint, 2021.
4. <https://www.manatal.com>
5. <https://www.opavote.com>
6. <https://www.sloneek.com>
7. <https://www.linkedin.com>
8. <https://business.djia.gov.ua/cases/sistemizacia-biznes-procesiv/ak-avtomatizuvati-upravlinna-personalom-u-2021-roci-ta-comu-ce-neobhidno-biznesu>

УДК 004.7.056.5

Качур А.В., Лисенко С.М.

*Хмельницький національний університет*

## **ВИКЛИКИ В РОЗВИТКУ ТЕХНОЛОГІЙ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ: ОПТИМІЗАЦІЯ АРХІТЕКТУРИ VR**

*Досліджено виклики у розвитку VR, включаючи технічні, фінансові та етичні аспекти. Проблеми включають розробку обладнання та програмного забезпечення, високі витрати та етичні питання. Також розглянуто оптимізацію та потребу у подальших дослідженнях для реалізації потенціалу VR.*

*Research has been conducted on the challenges in the development and application of Virtual Reality (VR) technology. Despite VR's revolutionary potential in various fields, its realization is complicated by technical, financial, and ethical issues. Technical aspects include hardware and software development, high production costs, and ethical concerns, such as addiction and data privacy. Complexity, technological limitations, optimization, testing, and validation of VR have been discussed. An overview of solutions proposed in scientific literature has been presented, emphasizing the need for further research and innovation to unlock the potential of VR technology.*

Віртуальна реальність (VR), яка об'єднує фізичний і цифровий світи, змінює різні галузі, такі як освіта, охорона здоров'я, розваги і навчання. Проте реалізація її потенціалу поставлена під загрозу через технічні, фінансові і етичні виклики [1].

Розробка апаратного та програмного забезпечення для таких систем має свої виклики, включаючи автономність, комфорт, точність слідкування та обробку даних. Високі витрати та етичні дилеми ускладнюють завдання [2].

Оптимізація апаратної частини VR вдосконалює її компоненти для підвищення продуктивності та ефективності користувачів. Покращення одного аспекту може вплинути на інші, ускладнюючи завдання оптимізації. Ця область вимагає міждисциплінарних досліджень, об'єднуючи комп'ютерні науки, інженерію та взаємодію людина-комп'ютер. Розглянемо ці аспекти:

1) **Компромісні рішення.** Оптимізація апаратної частини вимагає збалансування таких цілей, як потужність, ефективність, пам'ять, вартість та надійність [3].

2) **Складність.** Оптимізація апаратної частини враховує взаємозв'язки між компонентами [4].

3) **Технологічні обмеження.** Зменшення розмірів транзисторів створює проблеми, такі як витік сигналу, нестача питомої потужності та перегрівання [5].

4) **Оптимізація апаратно-програмної взаємодії.** Покращення продуктивності передбачає збалансовану взаємодію апаратної та програмної частини [6].

5) **Перспектива.** Прогнозування майбутніх потреб при збереженні балансу між конкретністю і загальністю є викликом [7].

6) **Тестування та перевірка.** Ретельне тестування та програмно-апаратне моделювання забезпечують правильну роботу [8].

7) **Економічна ефективність.** Оптимізація апаратної частини повинна враховувати користь від витрат на виробництво [9].

Ураховуючи складності і міждисциплінарні виклики у оптимізації апаратної частини VR, важливим є системний підхід. Наукова робота має створювати комплексні рішення для їх вирішення.

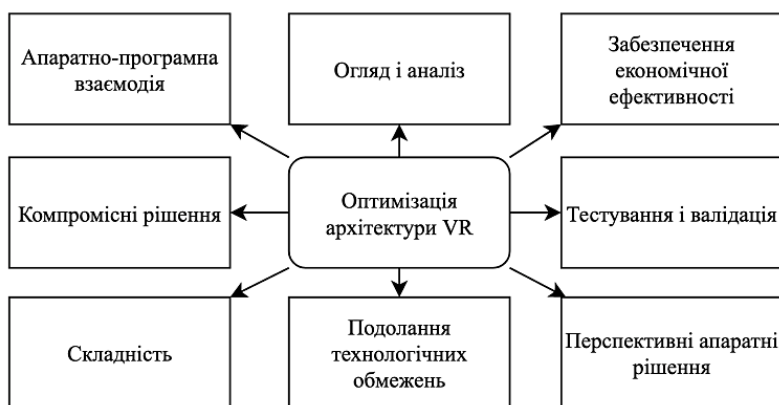


Рисунок 1 – «Дорожня карта» оптимізації архітектури VR

Автори наголошують на важливості оптимізації апаратно-програмної взаємодії в архітектурі VR для досягнення оптимальної продуктивності системи та покращення користувацького досвіду.

Перелік таких викликів служить оглядом основних областей досліджень у сфері VR, який дозволяє визначити актуальні напрямки у вирішенні складної взаємодії апаратного та програмного забезпечення:

- Затримки.
- Витрати енергії.
- Стабільність апаратного забезпечення.
- Зручність для кінцевого користувача.
- Портативність.
- Розробка.

Майбутні дослідження у сфері оптимізації VR повинні фокусуватися на інтегрованих рішеннях, що балансують затримку, споживання енергії та користувацький досвід. Інтеграція VR у різні галузі обіцяє просування, вимагаючи вирішення технологічних викликів та забезпечення безпеки та приватності.

### **Перелік посилань**

1. The Impact of AR and VR on Customer Experience URL: <https://www.forbes.com/sites/forbestechcouncil/2023/04/13/the-impact-of-ar-and-vr-on-customer-experience/?sh=65a908567c3a>
2. Design and Security Challenges for VR. URL: <https://semiengineering.com/design-and-security-challenges-for-vr>
3. J. Chen, M. Manivannan, B. Goel, M. Pericàs, "JOSS: Joint Exploration of CPU-Memory DVFS and Task Scheduling for Energy Efficiency," in Distributed, Parallel, and Cluster Computing (cs.DC), vol. 04615, pp. 1-11, 2023..
4. Z.Wang, W.Mao, P.Yang, Z.Wang, J.Lin, "An Efficient FPGA Accelerator for Point Cloud," in Signal Processing (eess.SP), vol.07803, pp. 1-6, 2023.
5. Y. Wang, Y.Li, Y.Yang, W.Chen, "Hot Carrier Injection Reliability in Nanoscale Field Effect Transistors: Modeling and Simulation Methods. Electronics," in Electronics, vol.11, pp. 1-16, 2022.
6. D.K.Mandal, S.Jandhyala, "Visual Inertial Odometry At the Edge: A Hardware-Software Co-design Approach for Ultra-low Latency and Power," in 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE), Florence, Italy, pp. 960-963, 2022.
7. D.A.Hazelwood, M.G.Pecht, "Life Extension of Electronic Products: A Case Study of Smartphones," in IEEE Access, vol. 9, pp. 144726-144739, 2021.
8. W.Jiang, L.Sun, Y.Chen, H.Ma, S.Hashimoto., "Hardware-in-the-Loop-on-Chip Development System for Teaching and Development of Dynamic Systems," in Electronics, vol.10, pp. 1-15, 2021.
9. A.Dinu, P.L.Ogrutan, "Reinforcement Learning Made Affordable for Hardware Verification Engineers," in Micromachines, vol. 13, pp. 1-28, 2022.

УДК 004.9

Качур О.І.

Хмельницький національний університет

## ПЕРСПЕКТИВНІ НАПРЯМКИ РОЗВИТКУ СУЧАСНОГО АНТИВІРУСНОГО ЗАХИСТУ МЕРЕЖ ТА РОЛЬ МЕТОДІВ НА ОСНОВІ ГЕНЕТИЧНИХ АЛГОРИТМІВ

*Розглянуто проблеми історичних та сучасних загроз у сфері кібербезпеки. Наведений аналіз та класифікація методів детектування комп'ютерних вірусів та шкідливого ПЗ на PC, cloud, mobile та IoT платформах. Наведені сучасні методології аналізу з використанням штучного інтелекту (AI) та генетичних алгоритмів (GA). Наведено приклади використання еволюційних генетичних алгоритмів для захисту від шкідливого ПЗ, та пропонується використання генетичних алгоритмів для розробки методу боротьби з мережевими комп'ютерними вірусами.*

*The scientific work outlines problems of historical and modern threats in the field of cyber security. The analysis and classification of methods for detecting computer viruses and malicious software on PC, cloud, mobile and IoT platforms. Modern analysis of methodologies using artificial intelligence (AI) and genetic algorithms (GA) is provided. Examples of the evolutionary genetic algorithms usage for protection against malicious software are given, and use of the genetic algorithms for the development of a method of network computer viruses detection is proposed.*

У сучасному світі, який швидко розвивається та цифровізується, кібербезпека стала першочерговою проблемою, яка однаково впливає як на окремих осіб так і організації. З розвитком технологій надзвичайно швидкими темпами зростає кількість кіберзагроз та атак націлених на мережеві системи. Для ефективного захисту від цих зловмисників вкрай важливо постійно відстежувати та аналізувати нові загрози кібербезпеці, які становлять значні ризики. Сфера кібербезпеки, що охоплює низку заходів і технологій, спрямована на захист комп'ютерів, серверів, мобільних пристроїв, електронних систем, мереж і даних від цифрових атак і несанкціонованого доступу. Проте постійно зростаючі можливості кіберзлочинців, розвиток технологій і невідоме виявлення нових загроз і вразливостей є постійною проблемою. Історично виділяють ряд епох у появі нових кіберзагроз [1].

Ранні часи (1970-1990 роки): зловмисники почали використовувати вразливості в роботі систем і програмного забезпечення, для отримання неавторизованого доступу. Ці перші загрози були здебільшого поодинокими



інцидентами, а заходи безпеки були мінімальними. Віруси та зловмисне ПЗ (malware) (1990-2000 роки): В цей період зростала популярність вірусних атак, які як правило поширювались за допомогою дискет та електронної пошти з метою отримання несанкціонованого доступу до комп'ютерних систем та викрадення чутливої інформації.

Веб-загрози часів зростаючого Інтернет (2000-2010 роки): Цей період характеризується експоненціальним поширенням інтернету та відповідно новими кіберзагрозами, такими як фішингові атаки та DDoS атаки, на додачу до нових видів вірусних атак.

Сучасна епоха (2010-теперішній час): До всіх вищезазначених загроз додаються цілеспрямовані атаки з метою компрометації конкретних осіб, організацій або галузей. Ці атаки включають поєднання соціальної інженерії, скритного зловмисного програмного забезпечення, мережеских вразливостей, пріоритет на складність детектування. З сучасними трендами додаються Інтернет речей (IoT - Internet of things) та хмарні (Cloud-based) загрози.

Тренди у кібератаках з 2015 по 2022 рік показують постійне зростання кількості атак усіх категоріях, так шахрайство (fraud) - приріст 50%, спам (spam) - 511%, атаки з відмовою доступності (DDoS) - 327%, [1] фішинг (phishing) - 600% [2] Таким чином, тренд на збільшення кількості атак та поява нових типів загроз зберігається, відповідно набувають актуальності сучасні методи детектування та захисту.

Виділяють 2 основні сучасні методології виявлення та аналізу зловмисного програмного забезпечення (malware). MARE (Malware Analysis Reverse Engineering) Загальна стратегія захисту включає наступні етапи: 1) Виявлення 2) ізоляція та вилучення 3) аналіз поведінки 4) аналіз коду та зворотне проектування 5) Розпізнавання шаблонів зловмисного програмного забезпечення 6) лікування Ці кроки мають на меті допомогти аналітикам одержати результат, який є повторюваним, об'єктивним і застосовним, для кращого розуміння аналізованого шкідливого програмного забезпечення. В результаті історичного розвитку через 10 років з'явився підхід SAMA (Systematic Approach to Malware Analysis).

Основні етапи:

1. Початкові дії
2. Класифікація
3. Статичний і динамічний аналіз коду
4. Поведінковий аналіз

Метою нової процедури є створення основи, здатної аналізувати сучасне та складне шкідливе програмне забезпечення, через потребу в ітераційному процесі, який є систематичний, структурований, заснований на надійних і жорстких методах, здатний допомогти аналітикам у отримання необхідних знань про певну шкідливу

програму, для ефективної боротьби з шкідливим ПЗ. Щодо аналізу використовуються такі види, як статичний аналіз (static analysis), динамічний аналіз (dynamic analysis) та гібридний [3].

Статичний аналіз коду відбувається без фактичного виконання коду програми. Приклади інформації що можна отримати шляхом статичного аналізу є послідовності операційних кодів (operation code, opcode) з бінарних файлів, графі потоку керування та інші. Набори такої інформації можуть бути використані як окремо так і в у комбінації для детектування шкідливого коду. Методи машинного навчання також використовуються в контексті статичного аналізу. Перевагою статичного аналізу є низький рівень хибно позитивних детектувань, в той час як неможливість детектування у разі невідомих сигнатур.

Динамічний аналіз вимагає, виконання програми, часто у віртуальному середовищі. Приклади інформації, яку можна отримати за допомогою динамічного аналізу, є: Виклики API, системні виклики, трасування інструкцій, зміни реєстру, записи в пам'ять тощо. В нещодавніх роботах є популярними графові методи, що спираються на динамічні данні. Також популярним є аналіз послідовності API викликів, наприклад з використанням частотного аналізу. Перевагою динамічного аналізу є можливість детектування невідомого шкідливого ПЗ, водночас з високим рівнем хибно позитивних детектувань та повільним виконанням.

Гібридний аналіз включає в себе комбіновані, на певному етапі підходи статичного та динамічного аналізу, з метою поєднати найкращі характеристики обох підходів. До таких підходів відноситься Mal-DNA (Malware-DNA), ROC Analysis (Receiver Operating Characteristic), Precision Recall Analysis (PR) та інші.

Відповідно до різновидів шкідливого ПЗ, різні методи демонструють певний рівень ефективності виявлення, тож найкращою стратегією є поєднання методів з огляду на ресурси та наявні моделі загроз.

З поширенням технологій штучного інтелекту(AI), вони невідворотно входять в сферу кібербезпеки. Були розроблені такі алгоритми штучного інтелекту, як Shallow Learning, Deep Learning and BioInspired Computing під всі види платформ: PC, cloud, mobile та IoT.[4]

Генетичні алгоритми відносяться до біоінспірованих методів пошуку та оптимізацій, що базується на принципах природного відбору та генетики. У сфері кібербезпеки вони набувають використання у створенні нових методів захисту [5] так і побудови нових атак [6]. Прикладом використання є [7]. За допомогою використання еволюційних генетичних алгоритмів для відбору дискримінаційної ознаки. Результатом цього методу стала підмножина функцій, яка пізніше була використана для побудови класифікаторів машинного навчання для виявлення зловмисного програмного забезпечення Android, з точністю 94%.

Мережеві віруси залишаються однією зі зростаючих та найбільш актуальних загроз у сучасній кібербезпеці, тому актуальною є розробка методів їх виявлення згідно еволюційних алгоритмів. Очікуваними перевагами є вища точність та оптимізація використання ресурсів.

### **Перелік посилань**

1. The New Frontier of Cybersecurity: Emerging Threats and Innovations by Daksh Dave, Gauransh Sawhney, Pushkar Aggarwal, Nitish Silswal, Dhruv Khut, pages 1-5, 2023
2. Comparative Review of Malware Analysis Methodologies by Ioannis G. Kiachidis, Dimitrios A. Baltatzis, pages 2-4, 2012
3. A Comparison of Static, Dynamic, and Hybrid Analysis for Malware Detection Anusha Damodaran, Fabio Di Troia, Visaggio Aaron Corrado, Thomas H. Austin, Mark Stamp, pages 2-6, 2022
4. The State-of-the-Art in AI-Based Malware Detection Techniques: A Review, Adam Wolsey, 2022
5. Modified Genetic Algorithm for Feature Selection and Hyper Parameter Optimization: Case of XGBoost in Spam Prediction by Nazeeh Ghatasheh, Ismail Altaharwa, Khaled Aldebei, page 1, 2022
6. Genetic Algorithm-Based Dynamic Backdoor Attack on Federated Learning-Based Network Traffic Classification by Mahmoud Nazzal, Nura Aljaafari, Ahmed Sawalmeh, Abdallah Khreishah, Muhammad Anan, Abdulelah Algozaibi, Mohammed Alnaeem, Adel Aldalbahi, Abdulaziz Alhumam, Conrado P. Vizcarra, Shadan Alhamed, page 1, 2023
7. Android Malware Detection Using Genetic Algorithm based Optimized Feature Selection and Machine Learning by Anam Fatima; Ritesh Maurya; Malay Kishore Dutta; Radim Burget; Jan Masek, page 2, 2019

УДК 004.4

Кирилюк О.О., Онишко О.Г.

*Хмельницький національний університет*

## **ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ ІНСТРУМЕНТУ ELASTICSEARCH ДЛЯ ОПТИМІЗАЦІЇ ВЕБДОДАТКІВ, РОЗРОБЛЕНИХ З ВИКОРИСТАННЯМ ФРЕЙМВОРКУ LARAVEL**

*У даному дослідженні було проведено аналіз можливостей використання інструменту Elasticsearch з метою оптимізації вебдодатків, розроблених на основі фреймворку Laravel, з урахуванням підвищення їхньої продуктивності та ефективності. Основною метою дослідження є створення та інтеграція Elasticsearch у вебдодатки, побудовані на Laravel, з метою надання швидкого та точного механізму пошуку інформації для користувачів. Основний результат дослідження полягатиме в розробці вдосконаленої системи пошуку та фільтрації даних, яка дозволить ефективно взаємодіяти з великим обсягом інформації та покращить користувацький досвід вебдодатків в умовах зростаючого обсягу даних та потреби у реальному часі обробки та пошуку інформації.*

*This research involved an analysis of the possibilities of using Elasticsearch tool to optimize web applications developed based on the Laravel framework, with the aim of improving their productivity and efficiency. The primary goal of the research is to create and integrate Elasticsearch into web applications built on Laravel, in order to provide a fast and precise mechanism for information retrieval for users. The main outcome of the research will be the development of an enhanced data search and filtration system, which will enable effective interaction with a large volume of information and enhance the user experience of web applications in the context of growing data volumes and the need for real-time data processing and retrieval.*

У сучасному світі спостерігається зростання обсягів інформації та даних, які зберігаються та обробляються в мережі. Завдяки цьому, важливість ефективного пошуку та фільтрації цих даних набуває все більшої ваги.

Метою роботи є дослідження використання інструменту Elasticsearch для оптимізації вебдодатків, розроблених з використанням фреймворку Laravel.

Користувачі сучасних вебдодатків очікують миттєвих результатів і реального часу. Для задоволення цих очікувань важливо мати швидкий та точний механізм пошуку та фільтрації даних.

Покращення користувацького досвіду є ключовим завданням для розробників вебдодатків. Ефективний пошук та фільтрація даних допомагають користувачам знаходити потрібну інформацію швидко і зручно.

Elasticsearch є потужним інструментом для створення систем пошуку та аналізу даних, і він надає можливості для оптимізації цих процесів. Об'єднання

Elasticsearch з фреймворком Laravel відкриває нові можливості для розробників у плані підвищення ефективності та швидкодії вебдодатків.

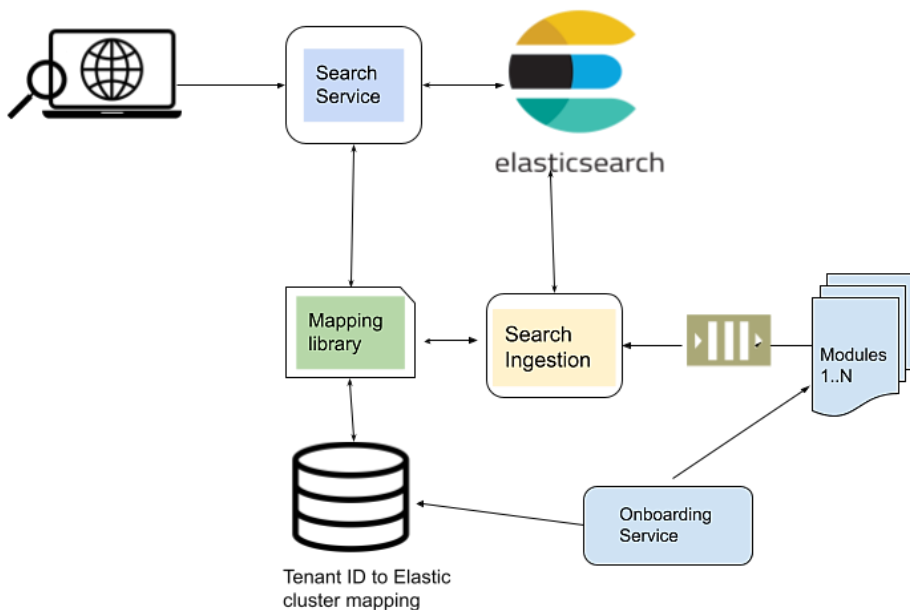


Рисунок 1 – Схема роботи Elasticsearch

Отже, обрана тематика є актуальною і важливою в сучасному світі, оскільки вона відповідає потребам користувачів та бізнесу в оптимізації роботи вебдодатків і покращенні обробки та пошуку даних.

### Перелік посилань

1. Документація з використання Elasticsearch. URL: <http://stmarysguntur.com/wp-content/uploads/2019/04/1021302647.pdf>
2. Wai Tak Wong. Advanced Elasticsearch 7.0: A practical guide to designing, indexing, and querying advanced distributed search engines. 2021. С. 230–239.

УДК 004.056

Кльоц Ю.П., Петляк Н.С., Чвалов А.А.

*Хмельницький національний університет*

## **ТЕХНОЛОГІЇ ТЕСТУВАННЯ БЕЗПЕКИ ВЕБРЕСУРСІВ**

*Кожен веб-ресурс має вразливості. Наявність вразливостей пояснюється здатністю людей допускати помилки, оскільки великі веб-ресурси пише не одна людина, а ціла група. І досить часто вразливості виникають через недостатню перевірку коду, некоректне налаштування серверу та використання неперевірених бібліотек і фреймворків від сторонніх розробників. Однак, для запобігання вразливостям та забезпечення безпеки веб-ресурсів, необхідно впроваджувати технології тестування. В даній роботі проведено порівняння найпоширеніших технологій виявлення вразливостей.*

*Almost any web resource has vulnerabilities. The presence of vulnerabilities is easily explained by the ability of people to make mistakes, because large web resources are written not by one person, but by a whole group. And quite often vulnerabilities occur due to insufficient code verification, incorrect configuration of the server and the use of untested libraries and frameworks from third-party developers. However, to prevent vulnerabilities and ensure the security of web resources, it is necessary to implement testing techniques. This paper compares the most common vulnerability detection techniques.*

Захист веб-ресурсів надзвичайно важливий, особливо в контексті стрімкого розвитку і збільшення залежності сучасного суспільства від технологій та інтернету.

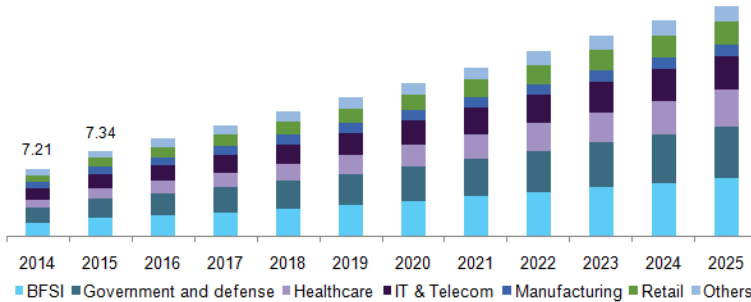
Додатково, важливо враховувати, що високий рівень доступності інтернету і швидкий розвиток технологій призводять до збільшення кількості зловмисників із спеціалізованими навичками, які шукають слабкі місця у веб-ресурсах для незаконного доступу і зловживання. Тому, для забезпечення безпеки веб-ресурсів, необхідно активно застосовувати передові практики та технології, які дозволяють вчасно виявляти і усувати вразливості.

Ринок безпеки також стрімко набирає оберти і ця динаміка особливо помітна з ростом вразливостей і ризиком їх експлуатування зловмисниками. Цей тренд особливо помітний з результатів дослідження Grand View Research [1], що зображений на рисунку 1.

Метою роботи є розгляд найпоширеніших технологій використовуваних на практиці, а саме DAST (Динамічне тестування безпеки додатків)[2] що дозволяє виявити вразливості в реальних умовах експлуатації та SAST (Статичне тестування безпеки додатків)[3] яке спрямоване на виявлення вразливостей на етапі розробки, шляхом аналізу вихідного коду.

DAST – технологія тестування чорної скриньки, яка динамічно перевіряє роботу веб-ресурсу без знання внутрішньої будови та схеми роботи. Даний підхід

використовується для виявлення вразливостей на пізніх стадіях розробки, якими може скористатися зловмисник. Це досягається за допомогою методів введення помилок, а саме передачі шкідливих даних та інструкцій, з метою виявлення поширених вразливостей безпеки, таких як SQL-ін'єкції, міжсайтові сценарії (XSS) та інші, що перераховані в OWASP Top 10[4].



Рисунк 1 – Ринок безпеки додатків у США

SAST –технологія тестування білої скриньки яка існує вже більше десяти років. SAST дозволяє розробникам виявляти вразливості на ранніх стадіях розробки, оскільки в цьому підході аналізується внутрішня структура, будова та вихідний код. Вагомою перевагою є й те що статичний аналізатор точно вказує на вразливий фрагмент в коді та надає рекомендації щодо його усунення.

Обидві технології тестування для виявлення вразливостей та недоліків, використовуються по-різному, але найбільш ефективною практикою є їх використовувати в тандемі. Такий комплексний підхід дозволяє покрити усі аспекти безпеки веб-ресурсів та забезпечити більш повний захист. В таблиці 1 наведені ключові відмінності між DAST і SAST технологіями [5].

Таблиця 1 – Ключові відмінності між DAST і SAST

DAST	SAST
Потрібен працюючий веб-ресурс	Потрібен вихідний код
Підтримує будь яку мову програмування для створення веб-ресурсів	Залежить від використовуваної мови програмування та технологій
Немає можливості точно визначити джерело проблеми	Точно визначає вразливий фрагмент у вихідному коді
Може виявляти проблеми, пов'язані з часом виконання, потоками та середовищем	Не виявляє проблеми що пов'язані з часом виконання, потоками та середовищем
Вразливості можна виявити після завершення циклу розробки	Сканування можна виконати, як тільки код буде вважатися завершеним
Дорогий спосіб усунення недоліків, так як застосовується в кінцевому циклу розробки	Дешевший спосіб усунення недоліків, оскільки виявляються на ранніх стадіях
Не вимагає активної участі розробників у процесі тестування, по закінченню надається звіт з рекомендації для усунення вразливостей	Вимагає участі розробників, оскільки вони повинні аналізувати знайдені вразливості та усувати їх безпосередньо в вихідному коді

Використання обох технологій протягом усього процесу розробки веб-ресурсу, та продовження моніторингу після його випуску – це те, що в кінцевому підсумку забезпечує безпеку веб-ресурсу та бізнесу.

У сучасному цифровому світі, де безпека веб-ресурсів стає дедалі важливішою, використання двох ключових технологій SAST та DAST є надзвичайно важливими. Обидві технології мають свої унікальні переваги і доповнюють одна одну, створюючи комплексну техноогою тестування безпеки, та допомагають виявляти і виправляти вразливості на усіх етапах розробки.

Крім того, важливо пам'ятати про постійний моніторинг безпеки веб-ресурсу, навіть після його випуску. Така практика забезпечить тривалий та ефективний захист, що допоможе уникнути потенційний загроз для бізнесу та користувачів.

### Перелік посилань

1. Application Security Market Size, Share | Industry Trends Report, 2025. URL: <https://www.grandviewresearch.com/industry-analysis/application-security-market>.
2. Static application security testing. URL: [https://en.wikipedia.org/wiki/Static\\_application\\_security\\_testing](https://en.wikipedia.org/wiki/Static_application_security_testing).
3. Dynamic application security testing. URL: [https://en.wikipedia.org/wiki/Dynamic\\_application\\_security\\_testing](https://en.wikipedia.org/wiki/Dynamic_application_security_testing).
4. OWASP Top 10:2021. URL: <https://owasp.org/Top10/>.
5. SAST vs. DAST | Lightrun. URL: <https://lightrun.com/sast-vs-dast/>.



УДК 004.4

Коберник Д.С.

*Хмельницький національний університет*

## **МОБІЛЬНИЙ ДОДАТОК ДЛЯ ЧИТАННЯ КНИГ З GOOGLE BOOKS: МЕТОДОЛОГІЇ ПРОГРАМНОЇ ІНЖЕНЕРІЇ ТА АРХІТЕКТУРНІ РІШЕННЯ**

*Представлені методології програмної інженерії та архітектурні рішення, які були використані для розробки мобільного додатка для читання книг з Google Books. Додаток доступний для пристроїв Android і дозволяє користувачам читати книги з каталогу Google Books.*

*The presented software engineering methodologies and architectural decisions that were used for the development of a mobile application for reading books from Google Books are discussed. The application is available for Android and devices and allows users to read books from the Google Books catalog.*

У сучасному світі книги перестають бути виключно паперовими, перетворюючись на цифрові формати. Google Books є однією з найбільших платформ для цифрового читання, проте потреба в оптимізованому додатку для читання з цього ресурсу лише зростає. Важливість створення ефективного та користувацьки-орієнтованого додатка не може бути недооцінена. Ця стаття розглядає методології програмної інженерії та архітектурні рішення, які були використані при розробці додатка для читання книг з Google Books. Ми зосередимося на виборі методологій, їхній адаптації для конкретного проекту, а також на ключових архітектурних рішеннях, що забезпечують гнучкість, продуктивність та зручність користування додатком.

В останні роки, із швидким ростом цифрових технологій та мобільного Інтернету, споживачі все частіше віддають перевагу читанню в електронному форматі. Google Books, будучи однією з провідних платформ у цьому напрямку, надає доступ до мільйонів видань, але ще залишає простір для покращення користувацького досвіду через спеціалізовані додатки.

Метою роботи є розробка програмного продукту, а саме мобільного додатку, для вільного перегляду та читання книг, що дозволить аудиторії програми відкрити для себе нове заняття чи продовжити займатись приємною справою з комфортом.

При розробці програмного продукту, особливо такого, який взаємодіє із вже існуючою екосистемою, виникає безліч викликів. Це може бути комплексність інтеграції, необхідність оптимізації для різних пристроїв та платформ, а також

забезпечення високої продуктивності та реактивності додатка. Тому правильний вибір методології програмної інженерії та архітектурних підходів є вирішальним.

Ми розглянули, як конкретні методології та підходи допомогли команді розробників створити додаток, який не тільки відповідає технічним вимогам, але і забезпечує відмінний користувацький досвід. Ми також докладно розглянемо архітектурні рішення, прийняті під час розробки, аналізуючи їхні переваги та недоліки в контексті заданих цілей проекту.

Одним з основних етапів розробки додатка є визначення його функціональності та інтерфейсу. Оскільки Google Books має свою унікальну структуру та алгоритми, було важливо розробити додаток, який б не тільки ефективно інтегрувався з цією платформою, але й надавав додаткові функції, які відповідають потребам сучасних користувачів.

Основою розробки стала агільна методологія. Застосування Kanban дозволило команді швидко реагувати на зміни вимог, проводити регулярні ітерації та вдосконалення продукту. Цей підхід сприяв гнучкості розробки та високій взаємодії між членами команди, замовниками та кінцевими користувачами.

Архітектурно, було прийнято рішення використовувати мікросервісну структуру. Це не тільки спростило інтеграцію з Google Books API, але й забезпечило модульність додатка, дозволяючи легко додавати нові функції або вдосконалювати існуючі. Однією з ключових функцій додатка стала можливість персоналізації користувацького досвіду. Використовуючи дані про прочитані книги, інтереси та відгуки користувачів, система пропонує рекомендації та адаптує інтерфейс для кожного користувача індивідуально. Діаграма архітектури мобільного додатка для читання з Google Books наведена на рисунку 1.



Рисунок 1 – Діаграма архітектури мобільного додатка для читання з Google Books

В узагальненому вигляді, цей додаток є результатом поєднання новітніх підходів у програмній інженерії з глибоким розумінням потреб користувачів. Ми розглянули технічні аспекти розробки, а також врахували відгуки користувачів та результати тестування додатка.

### **Перелік посилань**

1. Rubin, K. S. (2012). Essential Scrum: A Practical Guide to the Most Popular Agile Process. Addison-Wesley.
2. Martin, R. (2017). Clean Architecture: A Craftsman's Guide to Software Structure and Design. : Pearson Education.
3. Media, А. Н. (2016). Eric Schmidt and Jonathan Rosenberg's HOW GOOGLE WORKS Summary. (n.p.): CreateSpace Independent Publishing Platform.

УДК 004.4

Козакевич В.А., Собко О.В., Тищенко О.О., Вознюк Л.О., Медведчук В.Ю.

*Хмельницький національний університет*

## **МЕТОД АВТОМАТИЗОВАНОЇ ГЕНЕРАЦІЇ ТЕКСТОВИХ ПОВІДОМЛЕНЬ ЗАДАНОЇ СЕМАНТИЧНОЇ СПРЯМОВАНОСТІ З ВИКОРИСТАННЯМ ЛЕКСИЧНИХ N-ГРАМ**

*Було розглянуто ключові приклади розробки інформаційних систем, які автоматично генерують текстові повідомлення з визначеною семантичною спрямованістю за допомогою лексичних n-грам і були отримані результати роботи цих систем для подальшого аналізу.*

*The key examples of the development of information systems that automatically generate text messages with a defined semantic orientation using lexical n-grams were considered, and the results of the work of these systems were obtained for further analysis.*

Генерація текстових повідомлень – це автоматичне створення або надсилання невеликих обсягів текстової інформації окремим користувачам або групам користувачів з невеликими змінами або без них. Автоматизація такого маркетингу набула популярності серед багатьох брендів, оскільки вона дозволяє їм ефективно взаємодіяти зі своєю новою аудиторією в широкому масштабі. Крім того, автоматична генерація текстових повідомлень часто застосовується в системах сповіщення [1].

У наш час, коли сучасні технології швидко розвиваються і стають все більш інтуїтивно зрозумілими, продуктивними і зручними для користувача, важливо мати засоби ефективного спілкування з ним. Це стає невід'ємною складовою кожного проекту чи роботи. Для підтримки зв'язку з потенційними або постійними клієнтами, укладення контрактів з працівниками компанії та в щоденній робочій атмосфері все частіше використовують засоби для автоматизованої генерації невеликих текстових повідомлень.

Такі системи для автоматичної генерації невеликого обсягу текстових повідомлень застосовуються в різних сферах. Вони можуть бути використані як чат-боти, програми для автоматичного сповіщення користувачів, для модерації активності постійних учасників у групових чатах і соціальних мережах.

Однією з ключових сфер використання є чат-боти. У цьому випадку обмін текстовими повідомленнями між користувачем і сервісом відбувається негайно та нагадує звичайний діалог між двома особами. Однак, з одного боку, одним із учасників є реальна особа, а з іншого - система з автоматизованою генерацією невеликих текстових повідомлень. Також можливий обмін повідомленнями з

більшою кількістю зареєстрованих користувачів. Якщо в бесіді бере участь більше двох осіб одночасно, це вже називається чатом. Також важливою є можливість використання аудіо асистентів [2], які автоматично генерують відповіді у текстовому або аудіо форматі.

Один із прикладів використання цього підходу полягає у використанні типових моделей, який детально розглядається у роботі Лангкільде та Найтта. Задача генерації природної мови [3] є важливою складовою роботи системи автоматичної відповіді користувачу.

Моделі, які ґрунтуються на роботі з конкретними випадками, в даному контексті аналізують вхідні дані як набір порівнюваних ситуацій, які відбуваються у конкретному середовищі. Наприклад, задавши однакові запитання великій кількості людей, можна аналізувати їх відповіді, що в свою чергу утворює групу відповідей з однаковою семантикою та змістом. Grounded theory[4] ґрунтується на цьому підході у своїй роботі. Вони використовували модель HALogen [5], яка представлена на рисунку 1.

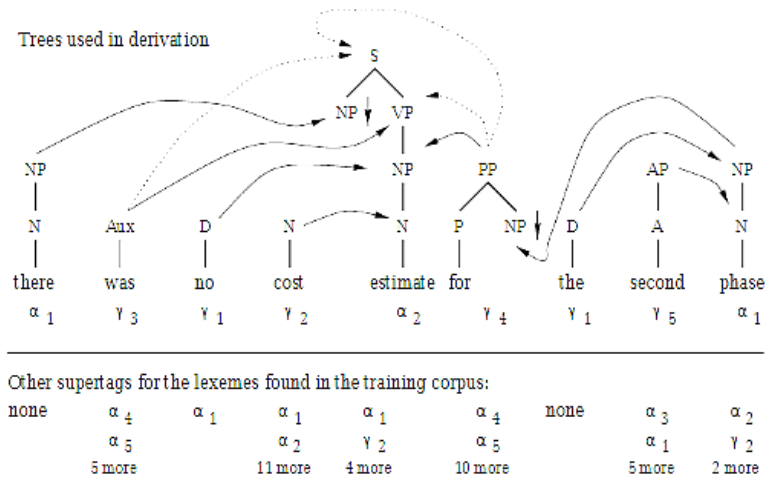


Рисунок 1 – HALogen [5]

Граматична модель у цій реалізації представлена у вигляді структури, що називається "випадковий ліс" (random forest). За допомогою стохастичного алгоритму оцінювання може бути вибраний найбільш підходящий варіант. У даному випадку цей підхід використовує базу у формі n -грам, тоді як сучасні підходи виконують великі експерименти з сучасними та інноваційними моделями для досягнення кращих результатів[6]. Існують різні види n -грам.

Уніграми (1-грами) – це найпростіші n-грами, які представляють окремі слова. Вони не містять контексту та розглядаються ізольовано. Наприклад, у реченні "Сьогодні гарний день", уніграмами будуть "Сьогодні", "гарний", "день".

Біграми (2-грами) – це n-грами, які складаються з двох слів. Вони дозволяють враховувати контекст, але тільки в обмеженому обсязі. Наприклад, для того ж речення, біграмами будуть "Сьогодні гарний", "гарний день".

Триграми (3-грами) – це n-грами, які мають три слова в послідовності. Вони враховують більший контекст, ніж біграми. Наприклад, для того ж речення, триграмами будуть "Сьогодні гарний день".

Чотириграми (4-грами) – це n-грами з чотирма словами в послідовності.

Що стосується використання n-грамів, вони використовуються для створення статистичних моделей мови, які визначають ймовірність входження певної послідовності слів у текст. Автоматичний переклад, використовуються для визначення найбільш ймовірних перекладів.

Розпізнавання мови в основному використовуються для визначення найімовірніших слів або фраз в аудіозаписах. Автокоректори та системи підказки. Використовують n-грами для визначення найбільш ймовірного продовження введеного тексту.

Важливо враховувати, що зі збільшенням значення n (кількість слів в n-грамі), зростає складність обробки та обсяг затребуваної статистики для навчання моделі. З іншого боку, більші значення n дозволяють враховувати більший контекст та покращувати якість результатів.

N-грами знаходять застосування у багатьох галузях, де важливо аналізувати текстову інформацію та розуміти її контекст. Використовуються для прогнозування ймовірностей появи певних слів чи фраз у тексті. Це важливо для завдань, таких як автоматичний переклад, розпізнавання мови, генерація тексту тощо. N-грами використовуються для визначення найбільш ймовірних перекладів для конкретних слів чи фраз. Використовують n-грами для визначення найбільш ймовірного продовження введеного тексту, що допомагає вказувати на можливі помилки або надавати рекомендації. N-грами використовуються для визначення найбільш ймовірних слів чи фраз в контексті генерування тексту. N-грами можуть бути використані для прогнозування подій чи трендів на основі аналізу текстових даних.

N-грами, хоч і є потужним інструментом для аналізу тексту та розуміння контексту, мають кілька недоліків. Для багатьох завдань, особливо в глибоких аналізах, n-грами обмежені в тому, що вони не можуть врахувати дуже великий контекст. Це особливо стає проблемою у випадках, коли значення слова залежить від довшого контексту. Велика кількість n-грам може бути рідкісними, тобто вони можуть взагалі не зустрічатися в тренувальних даних. Це ускладнює побудову надійних статистичних моделей. Для великих значень n (наприклад, 4-грами та вище), розмір словника та потрібна кількість обчислень для побудови моделі можуть бути вкрай великими. N-грами враховують тільки послідовність слів, але не

їхній фактичний порядок. Це може призводити до неправильних або незрозумілих висновків.

Інший приклад цього може бути підхід, що не вимагає складних обчислень для сортування та автоматичної генерації. Він використовує статичну інформацію для генерації відповіді у момент вибору та прийняття рішення. Цей метод часто використовується в системі PCRU, яка була вперше запропонована в 2007 році [7]. Робота цієї системи показана на рисунку 2. Вона може генерувати потенційне закінчення речення, яке має найбільшу ймовірність.

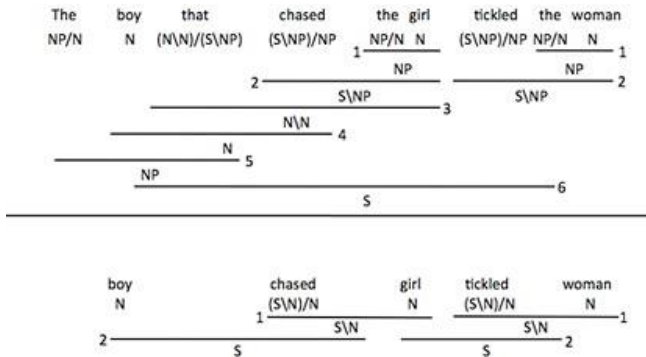


Рисунок 2 – Робота системи PCRU

Вагомим прикладом є фреймворк OpenCCG[8]. Цей інструмент є потужним засобом для аналізу великих повідомлень різних форматів та складності. Він використовує граматичний підхід [9] і базу початкових даних, побудовану на основі бібліотеки Penn Treebank (рисунок 3), яка широко використовується для статистичної оцінки мовних моделей.

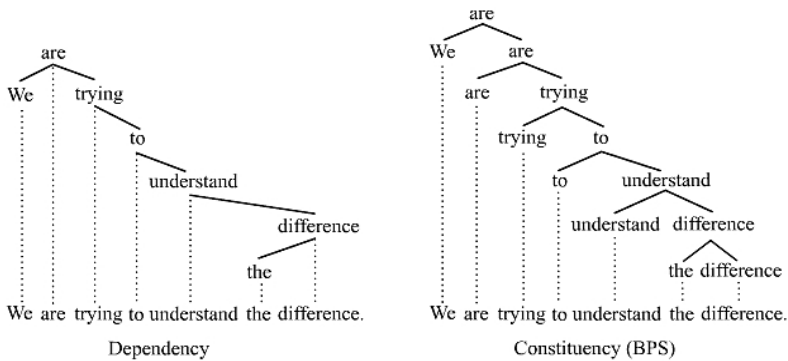


Рисунок 3 – Penn Treebank

Щоб розпочати роботи з цією системою автоматичної генерації текстових повідомлень потрібно підготувати корпус (див. рисунок 4), на якому ми будемо навчати нашу модель, а також визначити необхідну кількість слів у вихідному тексті. Генератор видасть "очищену" послідовність слів та всіх розділових знаків. Також доданий ще один генератор, який надає три токени поспіль. У цьому випадку токенами можуть бути слова або символи.

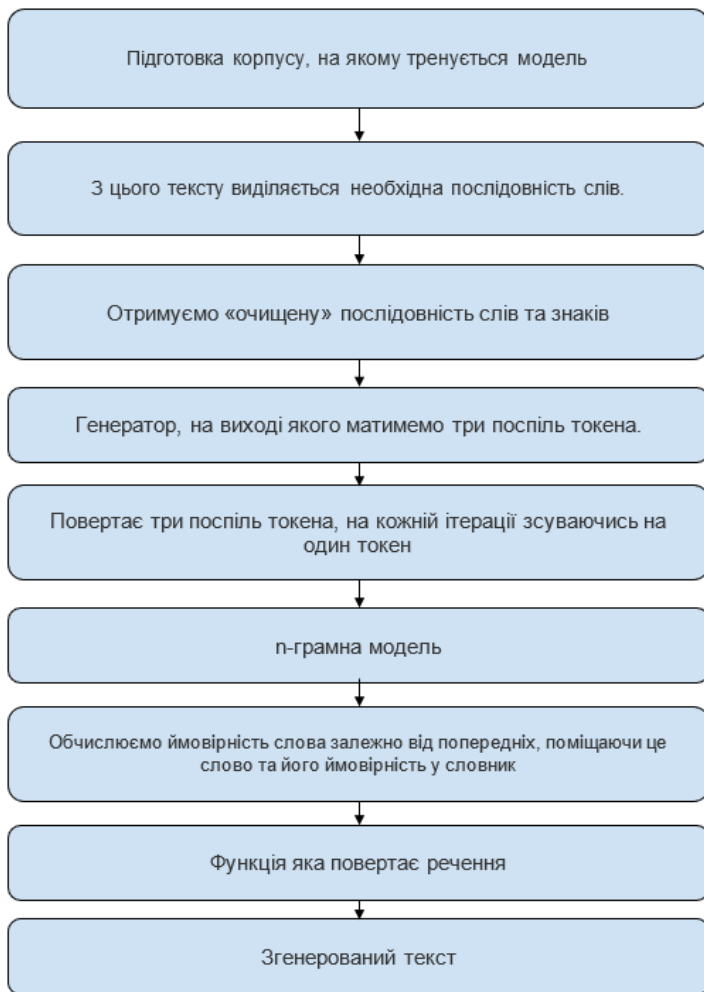


Рисунок 4 – Загальна схема роботи методу побудови текстів за допомогою n-грам



Наступним кроком є додавання функції, яка виводить кілька слів поспіль. Це полегшує вибір першого слова у фразі, що генерується. Узагалі, метод працює так: він повертає три токени поспіль, кожен наступний зрушується на один рівень після кожної ітерації.

Для початку ініціалізуємо генератори. Потім обчислюємо n-грами та визначаємо ймовірність кожного слова в залежності від попередніх. Далі, це слово та його ймовірність додаються у словник. Важливо зауважити, що цей метод може не бути найбільш оптимальним, оскільки він може вимагати значних ресурсів пам'яті. Проте для невеликих корпусів він є досить ефективним.

Цей метод ґрунтується на поступовому виборі найбільш ймовірних слів та розділових знаків до того моменту, коли виявляємо початок наступної фрази.

Основною метою є інтеграція всіх компонентів та етапів в одній системі машинного навчання. Це може призвести до створення оптимізованих та зручних систем, які не потребують попередньої обробки вхідних даних або редагування та форматування тексту.

Тому були ретельно проаналізовані ключові приклади розробки інформаційних систем, які використовують лексичні n-грами для автоматичної генерації текстових повідомлень з визначеною семантичною спрямованістю. Результати цієї роботи свідчать про значущий прогрес у сфері автоматизованої генерації контенту та його аналізу.

### Перелік посилань

1. Text Message Automation. URL: <https://www.slicktext.com/text-message-automation.php>
2. Google Assistant. URL: <https://www.techrepublic.com/article/google-assistant-the-smart-persons-guide/>
3. Natural language generation. URL: <https://research.aimultiple.com/nlg/>
4. A design framework for novice researchers. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6318722/>.
5. Model for Generation. URL: [https://www.researchgate.net/publication/2473335\\_Exploiting\\_a\\_Probabilistic\\_Hierarchical\\_Model\\_for\\_Generation](https://www.researchgate.net/publication/2473335_Exploiting_a_Probabilistic_Hierarchical_Model_for_Generation);
6. OpenCCG. URL: <http://openccg.sourceforge.net/>;
7. Combinatory categorial grammar. URL: [https://en.wikipedia.org/wiki/Combinatory\\_categorial\\_grammar](https://en.wikipedia.org/wiki/Combinatory_categorial_grammar);
8. Chart Generation grammar. URL: <https://www.inf.ed.ac.uk/teaching/courses/nlg/readings/KayACL96.pdf>;
9. Grammar-Based Approach to Microplanning. URL: <https://www.aclweb.org/anthology/J17-1001.pdf>

УДК 004.9

Козельський О.В.

*Хмельницький національний університет*

## **МЕТОДИ ТА ЗАСОБИ СТВОРЕННЯ МУЛЬТИКОМП'ЮТЕРНИХ СИСТЕМ З ПОДВІЙНОЮ АВТЕНТИФІКАЦІЄЮ ПОТОКІВ ДАНИХ В КОРПОРАТИВНИХ МЕРЕЖАХ**

*Розглянуто проблеми створення ефективних методів та засобів мультимедійних систем з подвійною автентифікацією потоків даних корпоративних мережах. В роботі пропонується метод комбінованої автентифікації на основі біометрії та блокчейну з використанням технології .NET, а саме за допомогою кроссплатформеної технології .NET Core.*

*The problems of creating effective methods and tools of multi-computer systems with dual authentication of corporate networks are considered. The work proposes a combination authentication method based on biometry and blockchain using .NET technology, namely using the .Net Core crosspaying technology.*

В епоху глобалізації та інтенсивного розвитку інформаційних технологій корпоративні мережі стають основою діяльності багатьох підприємств і організацій. У такому середовищі гарантія безпеки і цілісності передачі даних має вирішальне значення. Особливо актуальним є запитання створення ефективних методів та засобів для створення мультимедійних систем, які можуть забезпечити подвійну автентифікацію потоків даних.

Традиційно автентифікація користувача в мережі здійснюється за допомогою логіна та паролю, але такий підхід не завжди забезпечує необхідний рівень безпеки. Атаки з використанням злову паролів, фішингові атаки та інші загрози стають все більш розповсюдженими, що вимагає розробки нових методів захисту[1].

Методи подвійної автентифікації, що базуються на комбінації двох різних факторів автентифікації, таких як щось, що знає користувач (пароль), та щось, що він має (електронний ключ або смартфон), стають стандартом в індустрії безпеки. Однак, незважаючи на додатковий рівень захисту, який вони пропонують, вони не вільні від вразливостей та обмежень.

Зважаючи це, розробка методів та засобів створення мультимедійних систем з подвійною автентифікацією потоків даних в корпоративних мережах є не

лише актуальною, але й необхідною задачею для гарантування безпеки даних та сервісів у сучасному цифровому світі.

Однією з ключових вимог до сучасних систем безпеки є не тільки захист від несанкціонованого доступу, а й забезпечення автентичності користувачів та даних. У цьому контексті, Метод комбінованої автентифікації на основі біометрії та блокчейну претендує бути одним з найбільш перспективних підходів[2].

Біометрична автентифікація, заснована на унікальних фізичних або поведінкових особливостях особи, таких як відбитки пальців, розпізнавання обличчя або голосу, дозволяє значно підвищити рівень безпеки в порівнянні з традиційними методами, що використовують паролі або пін-коди. Але, як і будь-яка інша система, біометрична автентифікація може мати свої слабкі місця, зокрема щодо захисту самої біометричної інформації[3].

Використання технології блокчейн для зберігання та обробки біометричних даних може забезпечити їх незмінність, прозорість та безпеку. Це стає можливим завдяки децентралізованій структурі блокчейну, де кожний новий блок інформації підтверджується мережею учасників і, однією з ключових особливостей, є незмінність минулих записів. Отже, поєднання біометрії та блокчейну дозволяє створити систему автентифікації, яка з одного боку максимально індивідуалізує доступ до системи, базуючись на унікальних особливостях користувача, і з іншого - гарантує захист, надійність та прозорість цієї інформації за допомогою технології блокчейн (рисунок 1).

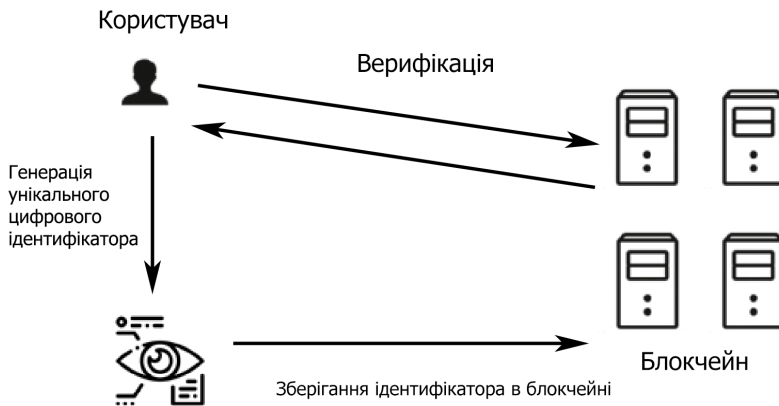


Рисунок 1 – Схема генерації біометричного ідентифікатора і верифікації по ньому в блокчейні

Особливу увагу треба звернути на конфіденційність біометричних даних в блокчейні [4]. Блокчейн є прозорим і відкритим, а біометричні дані по суті є паролем, тому дуже важливо хешувати дані. А також обрати найбільш ефективні біометричні дані, наприклад розпізнавання інформації, яка не змінюється зі старістю, по ДНК(дезоксирибонуклеїнова кислота), або ж за райдужною оболонкою ока, що є більш економічно вигіднішим варіантом.

Розглянемо реалізацію комбінованої автентифікації на основі біометрії та блокчейну в рамках платформи .NET Core, яка передбачає використання кількох компонентів та технологій. Зображено основні кроки та компоненти, які можуть бути використані для такої реалізації:

– Біометричний модуль: Використовуючи зовнішні бібліотеки або API (наприклад, Windows Hello для Windows або інші сторонні бібліотеки для різних платформ), розробник може інтегрувати функції біометричної автентифікації в своє застосування .NET Core[5].

– Блокчейн модуль: Є кілька бібліотек та платформ для роботи з блокчейном на .NET Core, наприклад, Nethereum для Ethereum. Цей модуль буде відповідальний за створення та взаємодію з блокчейном, включаючи додавання нових блоків і перевірку існуючих.

– Зберігання даних: Вибір засобів зберігання біометричних даних є критично важливим. З огляду на конфіденційність біометричних даних, може бути розглянута модель зберігання "hash" від біометричних даних у блокчейні, що дозволить перевіряти автентичність без необхідності зберігання самих біометричних даних.

– Автентифікація: Процес автентифікації починається з отримання біометричних даних від користувача, перетворення їх у "hash" і перевірки цього "hash" у блокчейні. Якщо відповідний запис знаходиться в блокчейні, автентифікація вважається успішною.

– Безпека: Додаткові механізми безпеки, такі як шифрування даних, можуть бути втілені за допомогою вбудованих засобів .NET Core, таких як ASP.NET Core Identity для захисту ідентичності користувача.

– Інтерфейс та користувацький досвід: З урахуванням особливостей біометричної автентифікації, інтерфейс застосування має бути інтуїтивно зрозумілим та простим для користувача.

– Масштабування та продуктивність: З урахуванням можливого великого обсягу біометричних даних та транзакцій в блокчейні, реалізація має бути оптимізована для високої продуктивності та масштабування(Асинхронне програмування async/await, пулінг пам'яті "System Buffers").

Застосування розробленого методу збільшує ефективність захисту автентифікації потоків даних в корпоративних мережах, при цьому гарантуючи їх конфіденційність.

Для підтвердження результатів роботи планується провести експерименти, де буде застовано реалізований описаний метод автентифікації даних з метою підтвердження його ефективності.

### **Перелік посилань**

1. Jessica Berrios; Elias Mosher; Sankofa Benzo; Cinthya Grajeda; Ibrahim Baggili. Factorizing 2FA: Forensic analysis of two-factor authentication applications / Journal of Information Security and Applications, Volume 45, July 2023, Page 301569
2. Abigail Akosua Addobea; Qianmu Li; Isaac Amankona Obiri Jr.; Jun Hou. Secure multi-factor access control mechanism for pairing blockchains / Journal of Information Security and Applications, volume 74, May 2023, 103477
3. Riseul Ryu, Soonja Yeom, David Herbert, Julian Dermoudy. The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction / ICT Express, April 2023
4. Mahdi Ghafourian, Bilgesu Sumer, Ruben Vera-Rodriguez, Julian Fierrez, Ruben Tolosana, Aythami Morales, and Els Kindt. Combining Blockchain and Biometrics: A Survey on Technical Aspects and a First Legal Analysis: Current status, challenges and future direction / arXiv - CS - Cryptography and Security, Feb 2023
5. Abigail Akosua Addobea; Qianmu Li; Isaac Amankona Obiri Jr.; Jun Hou. Memory analysis of .NET and .Net Core applications / Journal of Information Security and Applications, volume 42, July 2022, 301404

УДК 004.4

Козенко О.В., Мазурець О.В., Молчанова М.О., Собко О.В.

*Хмельницький національний університет*

## **ВИКОРИСТАННЯ МЕТРИК КОСИНУСНОЇ СХОЖОСТІ ТА ІНДЕКСУ ЖАККАРА ДЛЯ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ СЕМАНТИЧНОЇ ПОДІБНОСТІ ТЕКСТОВИХ ДОКУМЕНТІВ**

*Робота присвячена дослідженню та застосуванню метрик косинусної схожості та індексу Жаккара у контексті рекомендації текстових документів відповідно до запитань користувачів. Згідно до проведеного аналізу, обрано використання зазначених метрик у контексті порівняння векторів, що представляють текстові документи. Отримані результати аналізу можуть бути використані для подальшого вдосконалення систем рекомендацій та інформаційного пошуку, зокрема в областях, де ключовим є семантичне порівняння текстової інформації.*

*The work is devoted to the study and application of cosine similarity metrics and the Jaccard index in the context of recommending text documents according to user queries. According to the conducted analysis, it was chosen to use the specified metrics in the context of comparing vectors representing text documents. The results of the analysis can be used for further improvement of recommendation systems and information retrieval, in particular in areas where semantic comparison of textual information is key.*

Наразі існує багато методів пошуку релевантних документів за запитом користувача. Один з найпоширеніших методів – це використання метрик подібності. Метрики подібності використовуються для вимірювання подібності між запитом та документом. Чим більша подібність між запитом та документом, тим більш релевантний документ [1].

Нижче наведено деякі поширені метрики подібності [1]:

– TF-IDF – це метрика, яка враховує частоту виникнення слів у документі та частоту виникнення слів у наборі документів.

– Косинусна схожість (Cosine similarity) – це метрика, яка враховує кут між векторами запиту та документа.

– Індекс Жаккара (Jaccard similarity) – це метрика, яка враховує кількість спільних слів у запиті та документі.

Метрики косинусної схожості та індексу Жаккара пропонується використовувати у рамках методу рекомендації текстових документів за запитаннями користувачів на базі служби психологічної підтримки призначений для пошуку релевантних рекомендацій з бази текстових порад за текстовим запитом користувача та вхідними даними має датасет із набором очищених лематизованих асоціативних запитів, векторизований корпус та користувацький запит, що

перетворює їх у вихідні дані у вигляді текстової рекомендації релевантної до запиту.

Основна ідея косинусної схожості полягає в тому, що якщо два вектори спрямовані в одному напрямку (кут між ними дорівнює 0 градусів), то їхні вектори мають найвищу косинусну схожість та вважаються дуже схожими. Навпаки, якщо кут між векторами дорівнює 90 градусів, то косинусна схожість дорівнює 0, що вказує на максимальну різницю між ними [2].

Для обчислення косинусної схожості між двома векторами тексту (наприклад, словниковими представленнями документів), використовується наступна формула:

$$\text{Cosine Similarity } (A, B) = (A \cdot B) / (||A|| * ||B||),$$

де:  $A$  та  $B$  – вектори тексту або документів.  $A \cdot B$  - скалярний добуток векторів  $A$  і  $B$ .  $||A||$  та  $||B||$  – норми (довжини) векторів  $A$  і  $B$ .

Значення косинусної схожості зазвичай лежать в діапазоні від -1 (повна протилежність) до 1 (повна ідентичність), де 0 означає відсутність схожості.

Цей метод широко використовується в пошукових системах, рекомендаційних системах, аналізі тексту та класифікації документів для визначення ступеня схожості між текстами та відбору найбільш релевантних результатів. У роботі буде застосований як одна із метрик подібності запиту користувача до наявних шаблонів запитів з метою отримання релевантної відповіді.

Індекс Жаккара (Jaccard index), також відомий як Жаккардова схожість чи коефіцієнт Жаккара, є метрикою схожості, яка використовується для порівняння множин елементів. Ця метрика визначає ступінь схожості двох множин шляхом вимірювання кількості спільних елементів в обох множинах відносно загальної кількості унікальних елементів [3].

Індекс Жаккара обчислюється за наступною формулою:

$$J(A, B) = |A \cap B| / |A \cup B|,$$

де:  $J(A, B)$  – індекс Жаккара між множинами  $A$  і  $B$ .  $|A \cap B|$  – кількість спільних елементів між множинами  $A$  і  $B$ .  $|A \cup B|$  – кількість унікальних елементів у множинах  $A$  і  $B$  разом.

Значення Індексу Жаккара можуть лежати в діапазоні від 0 до 1, де 0 означає відсутність спільних елементів, а 1 означає повну ідентичність множин. Значення, близькі до 1, вказують на високу схожість множин, тоді як значення, близькі до 0, свідчать про низьку схожість.

Індекс Жаккара широко використовується в різних галузях, включаючи аналіз тексту, рекомендаційні системи, пошукові системи та біологічні дослідження. В роботі буде використовуватися для визначення схожості між ключовими словами користувацького запиту та наявних рекомендацій.

### Перелік посилань

1. Cosine Similarity. URL: <https://www.geeksforgeeks.org/cosine-similarity/>
2. Cosine Similarity. URL: <https://www.learndatasci.com/glossary/cosine-similarity/>
3. Jaccard Similarity Made Simple: A Beginner's Guide to Data Comparison. URL: <https://medium.com/@mayurdhvajsinhjadeja/jaccard-similarity-34e2c15fb524>

УДК 620.98:004.9+004.89

Комін А.С., Бойко О.В.

Сумський державний університет

## **АРХІТЕКТУРНЕ РІШЕННЯ ДЛЯ ПІДСИСТЕМИ ПІДТРИМКИ УПРАВЛІННЯ ГІБРИДНОЮ ЕНЕРГОСИСТЕМОЮ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ НА МОБІЛЬНИХ ПРИСТРОЯХ**

*Розглянуто п'ятирівневу крайово-хмарну архітектуру у межах задачі проектування систем управління гібридними енергосистемами з підвищеним рівнем забезпечення приватності даних користувачів. Запропонована діаграма потоку даних архітектурного рішення для вирішення задачі управління гібридною енергосистемою з використанням моделей машинного навчання на мобільних пристроях.*

*A five-layer edge-cloud architecture was considered in terms of the task of designing a hybrid energy management system with an increased level of user data privacy. An architectural solution dataflow diagram is proposed as a resolution to the problem of a household hybrid energy network management using machine learning models on mobile devices.*

Глобалізація та розвиток технологій з кожним роком призводять до росту рівня споживання електроенергії. Відповідно до [1] домогосподарства, транспорт та промисловість є основними споживачами електроенергії, де частка домогосподарств сягає 40%. Використання систем генерації енергії на основі відновлюваних джерел у домогосподарствах дозволить не тільки зменшити використання вичерпних ресурсів, але й зменшить рівень викиду парникових газів від класичних засобів генерації. Нажаль процес переходу до використання відновлюваних джерел енергії не є швидким, тому широко розповсюдженим варіантом переходу до 100% чистої енергетики є використання гібридних енергосистем, тобто тих, що об'єднують різні джерела генерації енергії в одну систему.

Системи підтримки управління гібридними енергосистемами (СПУГЕ) мають відповідати багатьом вимогам, таким як високий рівень масштабованості, надійності, сумісності, стійкості, безпеки та конфіденційності даних, низький рівень затримки [2]. Правильний вибір архітектури системи є одним з ключових етапів її проектування, що впливає як на вибір компонентів, так і на подальшу вартість підтримки.

Метою даної роботи є огляд можливих архітектурних рішень для проектування СПУГЕ та реалізація прототипу із забезпеченням високого рівня приватності даних користувачів.



Дослідники пропонують різні архітектурні рішення для систем на базі пристроїв Інтернету речей, основна задача яких - збір, передача та обробка даних. З урахуванням цих задач була створена трирівнева архітектура, що включає рівень сприйняття, мережевий рівень та рівень застосунків [2]. З точки зору проектування таких складних систем, як СПУГЕ, запропонована трирівнева архітектура не дозволяє повністю описати архітектуру системи. Як відповідь на цю проблему була запропонована п'ятирівнева крайово-хмарна архітектура [3], що додає ще два рівні – проміжний та бізнес рівні (рисунок 1).

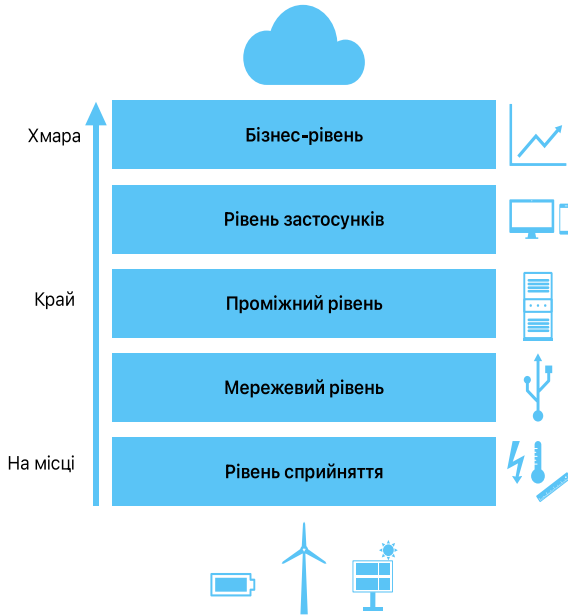


Рисунок 1 – П'ятирівнева крайово-хмарна архітектура

Наявність проміжного рівня в архітектурі дозволяє використовувати крайові обчислення - такі, що дозволяють обробляти та зберігати дані ближче до їх джерела. Бізнес-рівень необхідний для забезпечення підтримки прийняття глобальних рішень щодо моделей функціонування системи в цілому, як з економічної так і з технічної точки зору. Більш детальний опис рівнів архітектури наведено нижче в таблиці 1.

Питання приватності інформації у СПУГЕ є дуже важливим, адже, дані про споживання електроенергії домогосподарством можуть розкрити інформацію про кількість постійно проживаючих осіб, їхні звички та періоди відсутності у приміщенні. Регламенти та закони, такі як GDPR [4] чи закон України про захист

персональних даних [5], ставлять вимоги та обмеження до способу зберігання та обробки персональних даних, їх порушення може призвести до значних штрафів. Користувачі з кожним роком стають більш вибагливими щодо правил поводження з їх особистими даними. Їх побоювання породжують додатковий критерій - «довіра до системи». Надійний захист, збір, обробка та зберігання тільки необхідної інформації є важливими умовами для задоволення цієї вимоги. Це може сприяти успішному впровадженню системи [6].

Таблиця 1 – Опис п'ятирівневої крайово-хмарної архітектури

<b>Рівень</b>	<b>Опис</b>
Рівень сприйняття	Забезпечує збір інформації із розумних датчиків, лічильників та інших пристроїв, що підключені до засобів генерації, транспортування та споживання електроенергії для подальшої передачі на наступні рівні.
Мережевий рівень	Забезпечує передачу інформації між іншими рівнями. Реалізація має відповідати вимогам захищеності, пропускну здатності, затримки, швидкості передачі інформації між конкретними рівнями і може використовувати різні технології в рамках однієї системи.
Проміжний рівень	Відповідає за попередню обробку та фільтрацію інформації. Може зберігати дані користувачів без передачі у хмару для їх більшої приватності. Дозволяє розвантажати як обчислювальні потужності, так і мережеву пропуску здатність для наступних рівнів. Надає можливість для прийняття рішень щодо режимів функціонування локальних енергетичних мереж.
Рівень застосунків	Реалізує програмні інтерфейси, мікросервіси, застосунки для споживачів та постачальників електроенергії в гібридній мережі для забезпечення її енергоефективності – контролю генерації та споживання, балансування мережі, прогнозуванням регламентних робіт, вибору оптимального режиму роботи обладнання, тощо.
Бізнес-рівень	Надає інструменти для аналізу роботи системи на глобальному рівні, пошуку закономірностей, вибору бізнес-моделі, аналізу індексу повернення інвестицій (ROI), тощо.

Таким чином, нами пропонується підхід при якому приватність даних щодо історичного споживання енергії забезпечується їх зберіганням та обробкою на стороні користувача, тобто крайовими обчисленнями на його домашньому хабі, персональному мобільному телефоні та у персональному захищеному хмарному сховищі. Користувач у будь-який момент може керувати цими даними і при

необхідності їх видаляти. Дані для навчання моделей у хмарних сервісах фільтруються, передаються у захищеному вигляді та не зберігаються після використання.

Схема потоку даних для підсистеми прогнозування споживання електроенергії домогосподарства (рис. 2) описує взаємодію її компонентів, таких як домашній хаб, мобільний додаток-клієнт на базі платформи iOS, сховище даних CloudKit, сервіси тренування та оцінки моделей прогнозування споживання електроенергії, а також сховище моделей. Розглянемо дані компоненти з точки зору п'ятирівневої краю-хмарної архітектури.

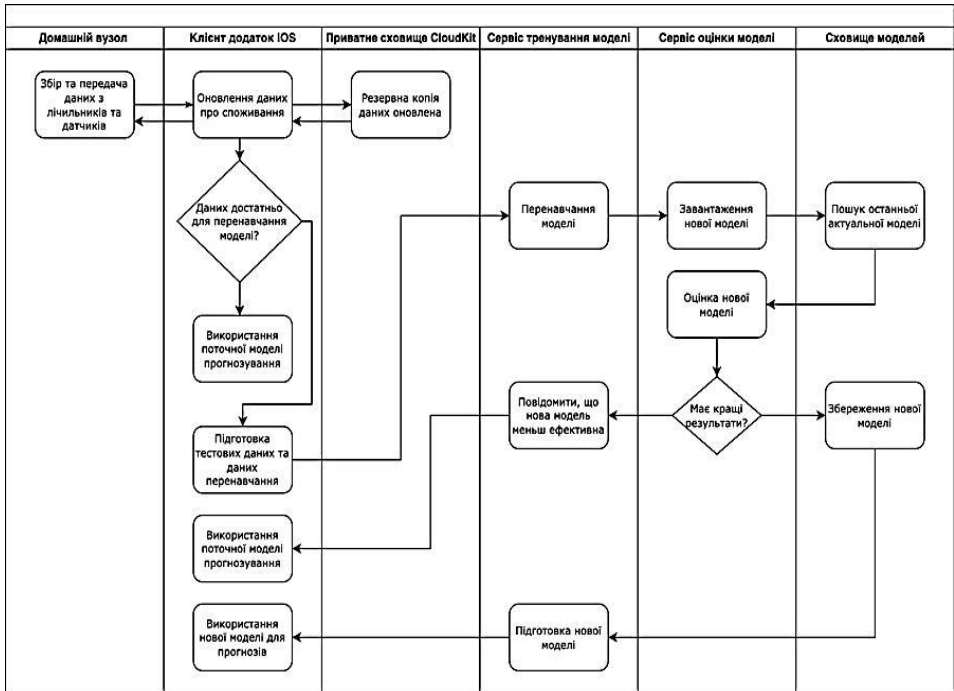


Рисунок 2 – Діаграма потоку даних

Домашній хаб відіграє роль збору даних лічильників та їх підготовки до подальшої обробки – це рівень сприйняття та проміжний рівень. Мобільний додаток зчитує дані з хабу, архівує їх у сховище та надає прогнози щодо рівня споживання електроенергії, що допомагають користувачеві приймати рішення стосовно вибору режиму роботи системи. Також додаток готує дані для перенавчання та тестування моделей прогнозування, таким чином його можна віднести до рівня застосунків та проміжного рівня. Приватне сховище CloudKit відноситься до проміжного рівня та акумулює дані про споживання електроенергії у приватній хмарі, при чому навіть

адміністратор хмари не має доступу до перегляду цих даних, ними керує особисто користувач, використовуючи обліковий запис iCloud. Сервіс тренування моделей навчає нову версію моделі на основі даних з додатку та не зберігає отримані дані користувача, а лише використовує їх для тренування і видаляє після використання. Сервіс оцінки моделі порівнює попередню версію моделі з новою на основі нових даних з додатку, не зберігаючи дані користувача після завершення сесії. Сховище моделей зберігає історію ефективних моделей для подальшого порівняння з новими моделями. Всі три сервіси є хмарними мікросервісами і частиною проміжного рівня системи.

В даній роботі проаналізовано вибір архітектури для розробки СПУГЕ та запропонована схема потоку даних для реалізації підсистеми прогнозування споживання електроенергії домогосподарством. Схема дозволяє забезпечити високий рівень приватності та безпеки зберігання даних користувача і надає можливість виконувати адаптацію моделі прогнозування споживання електроенергії на основі актуальних даних, робити прогнози щодо рівня споживання електроенергії за допомогою крайових обчислень на мобільному пристрої. У перспективі ця схема може бути втілена у вигляді прототипу для подальшої її інтеграції з іншими підсистемами СПУГЕ.

### **Перелік посилань**

1. Directive (EU) 2023/1791 of the European Parliament and of the Council of 13 September 2023 on energy efficiency and amending Regulation (EU) 2023/955 (recast) URL: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL\\_2023\\_231\\_R\\_0001&qid=1695186598766](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2023_231_R_0001&qid=1695186598766) (дата звернення: 26.10.2023).
2. Talebkhah M., Comprehensive Review on Development of Smart Cities Using Industry 4.0 Technologies. IEEE Access. 2023, Vol. 11, P. 91981-92030.
3. Lombardi M., Pascale F., Santaniello D., Internet of Things: A General Overview between Architectures, Protocols and Applications. 2021, Information, Vol 12, №2, P. 87
4. Art. 83 GDPR General conditions for imposing administrative fines URL: <https://gdpr.eu/article-83-conditions-for-imposing-administrative-fines/> (дата звернення: 26.10.2023)
5. Закон України про захист персональних даних: Указ президента України від 01.06.2010 р. №2297-VI. Відомості Верховної Ради України. 2010, №34, С.481
6. Fotia L., Delicato F., Fortino G., Trust in Edge-based Internet of Things Architectures: State of the Art and Research Challenges. ACM Comput Surv. 2023, Vol. 55, №9, С. 1-34.

УДК 004.4

Кузьмін А.А.

*Хмельницький національний університет*

## **КОНЦЕПЦІЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ АВТОМАТИЗОВАНОЇ ГЕНЕРАЦІЇ ЦИФРОВОГО КОНТЕНТУ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ**

*Розглянуто результати статистичних досліджень щодо актуальності та частоти застосування генеративних мовних моделей для різних галузей людського життя. Запропоновано концепцію інформаційної системи для автоматизованої генерації цифрового контенту на основі ШІ.*

*The results of statistical studies on the relevance and frequency of application of generative language models for various areas of human life are considered. The concept of an information system for the automated generation of digital content based on AI is proposed.*

З появою генеративних моделей на основі штучного інтелекту (ШІ), їх використання стало помітним практично у всіх галузях людської діяльності. За статистичними даними компанії Statista, у 2022 році 25% компаній у світі використовували ШІ для генерування тексту. До 2025 року очікується зростання використання великих мовних моделей до 40%. Найпоширенішим способом використання ШІ для генерування тексту є створення контенту для соціальних медіа. Інші популярні способи використання ШІ для генерування тексту включають створення маркетингових матеріалів, написання статей і переклад мов. 15% компаній у світі використовували ШІ для генерування зображень. Очікується зростання цього числа до 30% у 2025 році. Найпоширенішим способом використання ШІ для генерування зображень є створення контенту для соціальних медіа. Інші популярні способи використання ШІ для генерування зображень включають створення маркетингових матеріалів, створення ілюстрацій і створення 3D-моделей. Згідно з дослідженням Statista[1], у 2022 році 10% компаній у світі використовували штучний інтелект (ШІ) для генерування відео. Це число очікується зрости до 20% у 2025 році. Найпоширенішим способом використання ШІ для генерування відео є створення контенту для соціальних медіа. Інші популярні способи використання ШІ для генерування відео включають створення маркетингових матеріалів, створення навчальних відео і створення 3D-відео. За даними опитування, проведеного Gartner з 31 березня до 4 квітня 2023 року[2] (рисунок 1), компанії, які відповіли, що вони використовують генеративний ШІ,

окрім ChatGPT (n=119), назвали аналіз даних і прогнозування (56%), а також маркетинг і рекламу (53%) як найпопулярніші сфери використання. Близько третини стверджують, що вони використовують ШІ для операцій і логістики (34%), досліджень і розробок (32%) або виявлення шахрайства та кібербезпеки (30%). Розробка продукту 22%. Людські ресурси 9%. Фінансові операції 5%. Інше (розробка та тестування програмного забезпечення) 2%. Респонденти, які кажуть, що їхні організації використовують або планують використовувати генеративний ШІ цього року (n = 174) очікують, що це матиме найбільший вплив на ефективність бізнес-процесів (62%) і клієнтський досвід (51%).

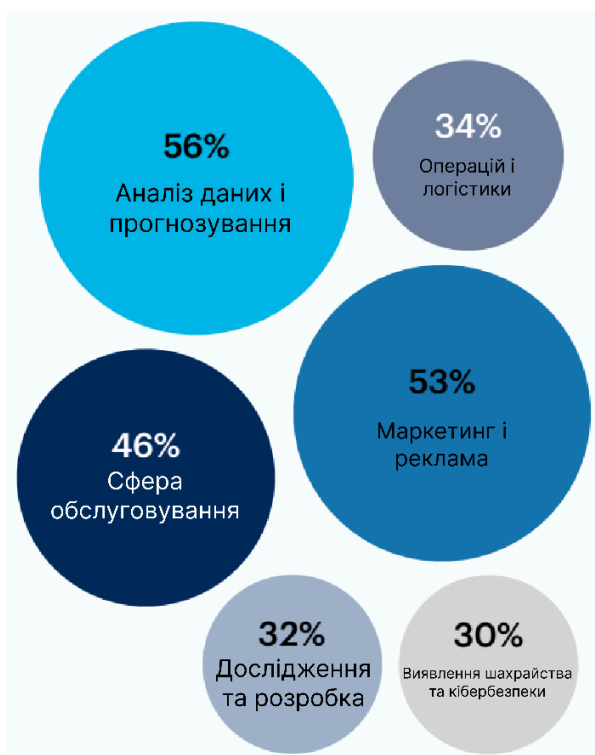


Рисунок 1 – Результати опитування компаній щодо використання генеративного ШІ у своїй діяльності [2]

На питання «Як ви очікуєте, у яких конкретних сферах генеративний ШІ матиме найбільший вплив у вашій організації цього року? Виберіть до 3» найчастішою відповіддю було підвищення ефективності ведення бізнесу (62%).

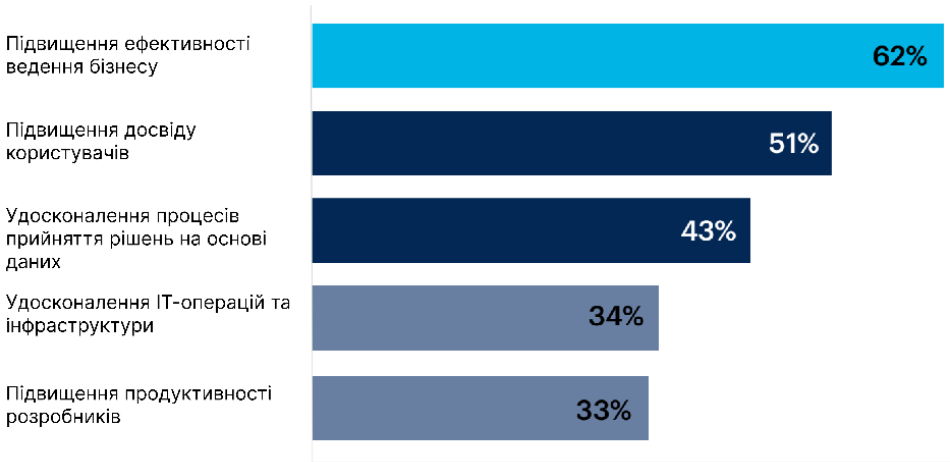


Рисунок 2 – Сфери застосування генеративного ШІ за результатами [1]

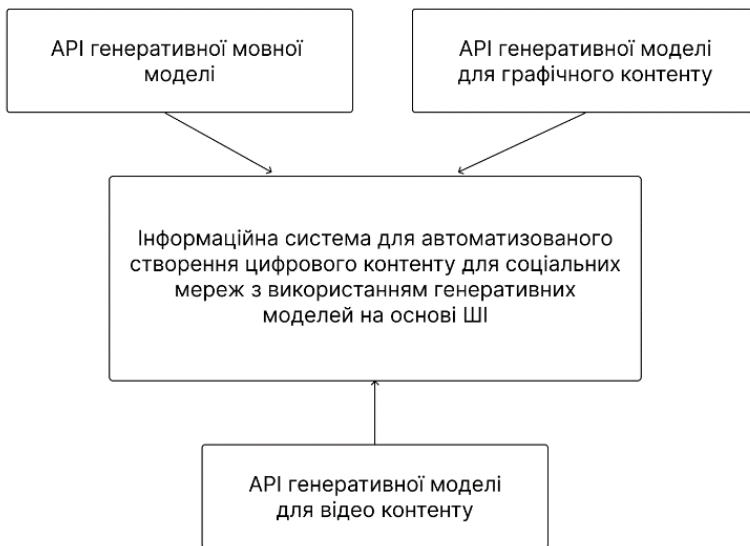


Рисунок 3 – Структурна схема інформаційної системи для автоматизованого створення цифрового контенту на основі ШІ

Оскільки вказані вище факти доводять, що генеративні мовні моделі лише набирають обертів у їхньому застосуванні для різних сфер діяльності людини та

підтверджують актуальність дослідження у напрямку створення інформаційної системи для автоматизованого генерування цифрового контенту. Структурна схема запропонованої інформаційної системи наведена на рисунку 3.

Наразі дослідження знаходиться на етапі побудови концепції архітектури цієї системи та на етапі збору інформації, адже, як можна побачити з рисунку 3, для інтеграції в систему, нам потрібні АПІ підсистем, тобто генеративних мовних моделей для автоматизованого створення тексту, зображень та відеоконтенту. Для цього потрібно провести дослідження і дізнатися, чи наявні ці АПІ у відкритому доступі, чи є вони платними чи безкоштовними, і які умови розробники ставлять для їх отримання.

Подальші зусилля будуть спрямовані на аналіз наведених вище проблем, отримання АПІ великих мовних моделей для генерування тексту, зображень та відео, та подальшу їх інтеграцію у практичну реалізацію.

### **Перелік посилань**

1. Statista (2023). Використання ШІ для генерування відео зростає. URL: <https://www.statista.com/>
2. Gartner Peer Community. Generative AI and ChatGPT: Adoption and Use. URL: <https://emtemp.gcom.cloud/ngw/globalassets/en/information-technology/images/infographics/gpc-omi-generative-ai-and-chatgpt-adoption-and-use.pdf> (Доступ 27.09.2023)
3. Uzun L. ChatGPT and academic integrity concerns: Detecting artificial intelligence generated content. *Language Education and Technology*. 2023. Т. 3. №. 1.



УДК 004.4

Кучменко К.Ю., Праворська Н.І.

*Хмельницький національний університет*

## **ІГРОВИЙ ЗАСТОСУНОК У ЖАНРІ «ПЛАТФОРМЕР» З ІНТЕРФЕЙСОМ УПРАВЛІННЯ НА ОСНОВІ ГОЛОСОВОЇ ВЗАЄМОДІЇ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ UNITY**

*Розглянуто прикладні аспекти розробки ігрового застосунку у жанрі «Платформер» з інтерфейсом управління на основі голосової взаємодії з використанням технологій Unity. При проектуванні було запропоновано унікальний інтерфейс управління, де гравець може використовувати різні звуки, такі як крики, сміх та інші можливі звуки, для керування персонажем. Це відкриває безліч можливостей для творчого геймплею, де гравець може вибирати, які звуки використовувати, щоб пройти рівні. В ході розробки проводився аналіз існуючих програмних додатків на ринку та обрано стратегію власної розробки.*

*The applied aspects of the development of a game application in the "Platformer" genre with a control interface based on voice interaction using Unity technologies were considered. During the design, a unique control interface was proposed, where the player can use various sounds, such as screams, laughter and other possible sounds, to control character. This opens up a lot of possibilities for creative gameplay, where the player can choose which sounds to use to pass the levels. During the development, an analysis of existing software applications on the market was carried out and a strategy was chosen for its own development.*

Геймінгова індустрія постійно розвивається, і важко не помітити безперервну появу різних технологій і, звісно ж, ігор, які використовують ці інновації. При розробці вказаного програмного застосунку було обрано одну конкретну технологію, а саме голосове управління, для дослідження та її реалізації.

Мета роботи полягає в розгляді та аналізі інноваційного підходу до розробки ігрового застосунку у жанрі "Платформер" з інтерфейсом управління на основі голосової взаємодії використовуючи технології Unity. Головною метою є розуміння та визначення потенціалу голосового управління для покращення інтерактивності та ігрового досвіду гравців у такому ігровому жанрі.

Крім того, було проведено аналіз ринку відео-ігор, які використовують подібну технологію – голосове керування і відносяться до платформерів. На основі проведених досліджень виявилось, що таких ігор є не так багато, але вони відзначаються високою популярністю серед гравців. У більшості випадків такі ігри надають можливість насолоджуватися позитивними емоціями, і вони особливо

цікаві для гри з друзями, родиною або колегами. Кумедний образ гравця, створений завдяки голосовому керуванню, додає до гри екстра дозу розваги та дозволяє гравцям якісно провести час разом. Перелік популярних ігор які використовують подібну технологію (таблиця 1).

Таблиця 1 – перелік популярних ігор які використовують технологію голосового керування

Назва гри	Короткий опис
One Hand Clapping	Ця 2D платформа, яка може викликати подразнення горла, вимагає від гравців вокально взаємодіяти — незалежно від того, чи вони співають, гудуть, кричать чи кричать — в мікрофон, щоб рухатися та стрибати на рівнях. Гра також містить ритмічні елементи, які вимагають від гравців аплодувати або навіть бітбоксити, щоб перемогти тишу та виходити наверх.
Scream Go Hero	Гра "Scream Go Hero" схожа на "Stick Hero", але замість того, щоб будувати паличкові мости для переходу на наступну платформу, користувач керує стрибками свого героя, кричачи. Висота та відстань стрибків залежать від гучності крику гравця. Невеликі стрибки вимагають тихих буркотінь, тоді як далекі пройдені відстані потребують тривалої ноти, яка могла б заслужити вам "Греммі".

Основною особливістю цієї гри є голосове керування, де ви генеруєте різноманітні звуки, і ваш персонаж реагує на ваші команди. Головною метою гравця є досягнення порталу, розташованого на протилежному кінці карти. Серед інших унікальних особливостей гри варто виділити розмаїтість перешкод та механізмів, з якими гравцеві необхідно взаємодіяти для просування крізь рівні. Також в грі існує система зірок, дозволяючи гравцю пройти рівень зі збором усіх трьох зірок, які можуть бути досить важко доступні або приховані на рівнях. Крім цього, гра пропонує можливість кастомізації персонажа, яку гравець може отримувати після проходження рівнів і прикрашати свого персонажа. Однією з цікавих особливостей є секретні рівні, які гравець може розблокувати, розв'язуючи головоломки та шукаючи секрети в грі.

Діаграма життєвого циклу гри - це інструмент, який показує всі етапи від створення гри до її завершення. Давайте перейдемо до розгляду цієї діаграми, щоб краще зрозуміти, як розробляється гра від ідеї до готового продукту (Рисунок 1)

Для створення гри був обраний двигун Unity, який підтримує об'єктно-орієнтовану мову програмування C#. Це обрано з метою створення високоякісної гри. Unity обрано також через його зручність для розробки кросплатформених ігор і мобільних додатків.



Рисунок 1 – Життєвий цикл гри

Для процесу розробки проекту була обрана гнучка методологія Agile Scrum для ефективної та ітеративної розробки продукту. (Рисунок 2)

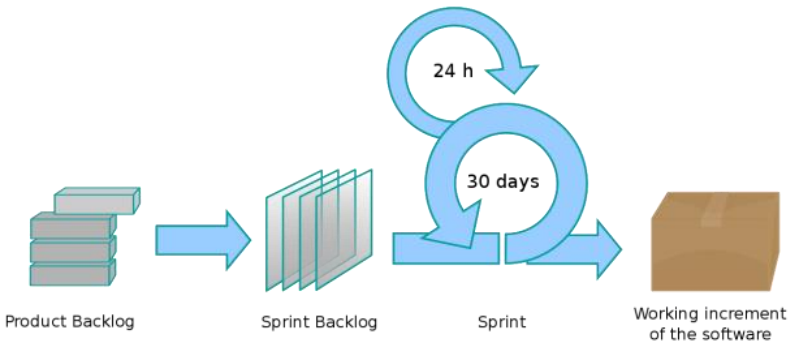


Рисунок 2 – Демонстрація того, як працює методологія

Для створення гри було прийнято рішення обрати стиль, в якому гра буде виглядати, і обраним стилем став піксель-арт. Піксель-арт – це графічний стиль, який використовує пікселі як основний графічний елемент. (Рисунок 3) У цьому

стилі графіка створюється шляхом розміщення та кольоризації пікселів на растрі, що надає грі характерну ретро-естетику.



Рисунок 3 – Приклад піксель-арт графіки

У підсумку, можна підкреслити важливість використання голосового керування в ігровій індустрії. Технології, що дозволяють гравцям взаємодіяти з грою за допомогою голосу, створюють унікальні можливості для створення незабутнього ігрового досвіду. Голосове керування додає елемент емоцій та взаємодії, який зробить гру більш цікавою та веселою для гравців. На сьогоднішній день ігри, які використовують голосове керування, набувають популярності та пропонують нові способи розваги. Розглянуті ігрові застосунки дозволяють гравцям відчувати власну важливість у створенні музики і контролі героїв, що робить геймплей незабутнім та унікальним. Голосове керування – це один із напрямків, який сприяє розширенню можливостей в ігровій сфері та приносить гравцям більше задоволення від гри.

### Перелік посилань

1. Гра «Scream Go Hero». URL:  
<https://play.google.com/store/search?q=scream+go+hero&c=apps&hl=en&gl=US>
2. Гра «One Hand Clapping». URL:  
[https://store.steampowered.com/app/893720/One\\_Hand\\_Clapping/](https://store.steampowered.com/app/893720/One_Hand_Clapping/)
3. Діаграма Agile Scrum. URL:  
[https://uk.m.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Scrum\\_process.svg](https://uk.m.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Scrum_process.svg)

УДК 004.5

Лаптев М.П., Лисий А.М., Сергєєв Є.В., Віжевський П.В.

*Хмельницький національний університет*

## **МЕТОД КРИПТОГРАФІЧНОГО ЗАХИСТУ ПРОТОКОЛІВ В ЗАСОБАХ КОМУНІКАЦІЇ ІНТЕРНЕТУ РЕЧЕЙ**

*Розроблено метод, що здійснює криптографічний захист і досягає найнижчої наскрізної затримки серед аналогів. Це робить його придатним для пристроїв нижчого класу. Як крок до повністю постквантового блокчейну пропонується протокол Proof of Work (PoW), який мінімізує переваги квантового майнера. Новий протокол базується на проблемі найкоротшого вектора у евклідовій нормі та забезпечує швидкий алгоритм перевірки. Щоб зменшити перешкоду передачі сертифікатів і перевірки для низького рівня пристроїв, представлено криптосистеми на основі ідентифікації та без сертифікатів, створені за допомогою спеціальних алгоритмів генерації ключів.*

*A method has been developed that provides cryptographic protection and achieves the lowest end-to-end latency among peers. This makes it suitable for lower end devices. As a step towards a full post-quantum blockchain, a Proof of Work (PoW) protocol is proposed, which minimizes the benefits of a quantum miner. The new protocol is based on the shortest vector problem in the Euclidean norm and provides a fast verification algorithm. To reduce the barrier of certificate transmission and verification for lower-level devices, identity-based and certificate-less cryptosystems created using special key generation algorithms are introduced.*

Інтернет речей (IoT) – це гетерогенна система, що складається з великої кількості підключених датчиків, розумних пристроїв, трансиверів, мікрокомп'ютерів тощо. Такі системи часто спираються на спілкування в режимі реального часу, щоб забезпечити заплановану функціональність. Вони можуть бути піддані спрямованій з боку зловмисника атаці, яка може бути направлена на автентифікацію, цілісність та/або конфіденційність даних, що передаються/зберігаються. Наявний широкий спектр криптографічних схем, призначених для ефективного пом'якшення/попередження на такі напади.

Ці криптографічні схеми можна в основному розділити на системи з симетричними або відкритими ключами. Проте схеми на основі симетричних ключів пропонують [1, 2] високоефективні та безпечні рішення, але вони можуть бути не ідеальними для впровадження в деяких налаштуваннях IoT через спільний ключ обчислення та розповсюдження. Для схем на основі симетричних ключів потрібен протокол узгодження ключів. Потрібно обчислити спільний секретний ключ перед ініціюванням безпечного зв'язку. Хоча це може бути здійсненним попередньо завантаживши ці спільні ключі на всі пристрої в деяких програмах, але це може бути досить складно для систем, у яких рухомі датчики/пристрої потребують зв'язку з безліччю нових пристроїв у режимі реального часу Зберігання спільного доступу до ключів для великих мереж IoT з тисячами або навіть мільйонами пристроїв створює теж проблеми. Зберігання попередньо обчислених

спільних ключів може бути неможливими на пристроях нижчого класу через їх обмежене сховище. Відсутність публічної перевірки та неспростовності в схемах автентифікації. Хоча існує багато понять на основі симетричних ключів для забезпечення автентифікації, вони не можуть забезпечити неспростування.

Системи IoT часто покладаються на пристрої низького рівня для надсилання вимірювань іншим сторонам, і залежно від налаштувань несанкціонована зміна та/або порушення конфіденційності цих заходів може мати катастрофічні наслідки. Тому, забезпечення ефективної автентифікації, цілісності та конфіденційності в цих параметрах є життєво важливим. Хоча звичайні криптографічні засоби можуть бути використані для задоволення цих вимог безпеки, незважаючи на їх дизайн, вони часто занадто дорогі з обчислювальної точки зору для пристроїв низького класу. Ситуація ще більше посилюється, коли береться до уваги захист від квантових комп'ютерів.

Розроблено серію нових ефективних звичайних і постквантових криптографічних схем, щоб відповідати суворим вимогам таких систем IoT. У рядку пропозицій ефективних схем автентифікації пропонується дві схеми підпису. Перша схема підпису заснована на звичайних криптографічних проблемах і використовує кодування повідомлень із сімействами без покриття та особливі властивості функцій для досягнення значного приросту продуктивності порівняно з аналогами. Друга схема заснована на постквантових примітивах і досягається шляхом розширення одноразових підписів до (поліноміально обмежених) багаторазових підписів, використовуючи адитивні гомоморфні властивості узагальнених компактних функцій.

Схема досягає найнижчої наскрізної затримки серед аналогів, що робить її придатною для пристроїв нижчого класу. Як крок до повністю постквантового блокчейну пропонується протокол Proof of Work (PoW), який мінімізує переваги квантового майнера. Новий протокол базується на проблемі найкоротшого вектора Ерміта (Hermite-SVP) у евклідовій нормі та забезпечує швидкий алгоритм перевірки. Щоб зменшити перешкоду передачі сертифікатів і перевірки для низького рівня пристроїв, представляємо криптосистему на основі ідентифікації та без сертифікатів, створені за допомогою спеціальних алгоритмів генерації ключів, які використовують властивість адитивної гомоморфності експонент, щоб дозволити користувачам включати свої приватні ключі в ключ, наданий довіреною третьою стороною, не підробляючи його. Нові схеми досягають кращої ефективності обчислень і порівнянної ефективності зв'язку порівняно з аналогами на основі ідентифікації та без сертифікатів.

### Перелік посилань

1. Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, and Greg Zaverucha. Post-quantum zero-knowledge and signatures from symmetric-key primitives. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS '17, pages 1825–1842, New York, NY, USA, 2017. ACM.

2. Léo Ducas. Shortest Vector from Lattice Sieving: a Few Dimensions for Free (talk). <https://eurocrypt.iacr.org/2018/Slides/Monday/TrackB/01-01.pdf>, April 2018.

УДК 004.4

Левандовський А.О., Муляр І.В.

Хмельницький національний університет

## МЕТОД АНАЛІЗУ ТРАФІКУ З МЕТОЮ ВИЯВЛЕННЯ АТАК НА КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

*У даній роботі було розглянуто метод аналізу трафіку як ефективний інструмент виявлення атак на інформаційні системи. Досліджено різні аспекти цього методу. Пропонований метод аналізу трафіку спрямований на виявлення аномалій та підозрілих патернів. Робота спрямована на висвітлення сучасних тенденцій у сфері аналізу трафіку для виявлення атак.*

*In this work, the method of traffic analysis was considered as an effective tool for detecting attacks on information systems. Various aspects of this method have been studied. The proposed method of traffic analysis is aimed at detecting anomalies and suspicious patterns. The work is aimed at highlighting modern trends in the field of traffic analysis to detect attacks..*

У сучасному інформаційному суспільстві, де комп'ютеризація та мережеві технології стають неодмінною частиною ділового та особистого середовища, питання забезпечення безпеки інформації набувають все більш актуального характеру.

Інформаційні системи стають об'єктом спроб несанкціонованого доступу, втручання та руйнування з боку зловмисників, що може призвести до серйозних наслідків для організацій, користувачів та суспільства в цілому.

Комплексні системи захисту інформації (КСЗІ) - це сукупність технологій, процедур, методів та інструментів, які призначені для захисту конфіденційності, цілісності та доступності інформації в інформаційних системах. Ці системи використовуються для запобігання несанкціонованому доступу до даних, їхнього розголошення чи втрати, а також для забезпечення функціонування інформаційних ресурсів в нормальному режимі навіть в умовах атак або катастроф [1].

Ці системи можуть включати в себе різноманітні компоненти, такі як файрволи, антивіруси, системи виявлення вторгнень, шифрування даних, аутентифікаційні методи, фізичні заходи безпеки та багато іншого. Вони використовуються в різних сферах, які обробляють конфіденційну інформацію

Ці системи важливі для захисту інформації в сучасному світі, де інформація відіграє ключову роль у багатьох аспектах суспільства та бізнесу.

Забезпечення безпеки інформації є завданням важливим як для державних структур, так і для підприємств і інших організацій.

Інтеграція технічних та організаційних заходів грає ключову роль у забезпеченні спільної роботи різних компонентів для досягнення оптимального рівня захисту. Комплексні системи захисту інформації продовжують розвиватися, адаптуючись до зростаючих технологічних викликів та різноманітних кіберзагроз, забезпечуючи високий рівень захисту для конфіденційної інформації та інфраструктури в інформаційному середовищі.

Організаційні та управлінські компоненти включають політики безпеки, тренування персоналу, процедури відновлення після інциденту та моніторинг безпеки.

Аналіз трафіку в комплексних системах захисту інформації є динамічним процесом, який вимагає поєднання технологій та людського експертного втручання для ефективного виявлення та відвернення кіберзагроз

Головна ідея - це стежити за тим, як дані пересуваються, шукати щось, що може бути нестандартним або небезпечним, і вчасно реагувати, щоб запобігти можливим проблемам у безпеці інформації.

Метою цієї роботи є вивчення, аналіз та розробка методу аналізу трафіку з метою виявлення атак на комплексні системи захисту інформації, а також розкриття ефективності таких методів у забезпеченні кібербезпеки та виявленні потенційно небезпечних аномалій у мережевому трафіку

Враховуючи постійний розвиток кіберзагроз та їхню вдосконаленість, аналіз трафіку виявляється ефективним інструментом у недопущенні серйозних наслідків для конфіденційності, цілісності та доступності інформації.

Метою використання методу аналізу трафіку є створення надійних та ефективних систем захисту, які здатні протистояти різноманітним загрозам у сучасному цифровому середовищі.

Подальший розвиток цього методу передбачає вдосконалення та адаптацію до змінюючогося характеру кіберзагроз, щоб забезпечити високий рівень безпеки інформації в умовах постійного технологічного розвитку.

Метод аналізу трафіку з метою виявлення атак на комплексні системи захисту інформації включає в себе кілька етапів та підходів.

- Моніторинг мережевого трафіку для виявлення несподіваного або підозрілого трафіку, який може вказувати на атаки або несанкціонований доступ;
- використання алгоритмів виявлення аномалій для ідентифікації незвичайних патернів у трафіку, що можуть вказувати на потенційні атаки або порушення;
- використання спеціалізованих систем виявлення вторгнень для виявлення атак, які відбуваються на основі аналізу мережевого трафіку та виявлення вразливостей у системах;



- використання бази даних з підписами відомих атак для порівняння з моніторинговим трафіком з метою виявлення відповідних атак;
- аналіз потоку даних з точки зору шаблонів атак та нормального трафіку для виявлення відхилень від очікуваного поведінки;
- аналіз журналів подій для виявлення незвичайної або підозрілої активності, яка може вказувати на потенційні атаки або вторгнення.

Отже цей метод використовуються для забезпечення максимального рівня захисту інформації та виявлення потенційних загроз для комп'ютерних систем і мереж. Цей метод допомагає підвищити рівень безпеки комплексних систем захисту інформації, виявлюючи атаки рано і запобігаючи їх негативним наслідкам. метод аналізу трафіку дозволяє ефективно виявляти аномалії у мережевому середовищі, вказуючи на можливі атаки або інші загрози інформаційній безпеці.

Важливим аспектом є не лише реакція на вже відомі атаки, але й передбачення та запобігання новим загрозам. Такий підхід дозволяє комплексним системам захисту інформації підтримувати високий рівень безпеки в непередбачуваному кіберпросторі.

Також рекомендується постійне вдосконалення методів аналізу трафіку, враховуючи змінюючийся характер кіберзагроз, та впровадження нових технологій для ефективного виявлення та запобігання атакам для забезпечення ефективного протидії невизначеним і постійно зростаючим кіберзагрозам у сучасному інформаційному середовищі..

Такий підхід допоможе забезпечити безпеку інформаційних систем в умовах постійно зростаючого рівня загроз та комплексності кібератак. метод аналізу трафіку є важливою ланкою у системах кібербезпеки, забезпечуючи необхідний рівень захисту для комплексних систем.

### **Перелік посилань**

1. Комплексні системи захисту інформації Навчальний посібник. / Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін // 2018
2. Технології захисту інформації Навчальний посібник. / А. В. Жилін, О. М. Шаповал, О. А. Успенський // 2020

УДК 004.9

Лигун О.О.

Хмельницький національний університет

## МЕТОДИ ТА ЗАСОБИ ВИЯВЛЕННЯ ЗЛОВМИСНИХ ДРОПЕРІВ В КОМП'ЮТЕРНИХ СИСТЕМАХ

*Розглянуто та проаналізовано вже існуючі методи та засоби виявлення зловмисних дроперів в комп'ютерних системах. В роботі пропонується розробити методи та засоби виявлення зловмисних дроперів в комп'ютерних системах та для покращення ефективності їх виявлення, розглянут нові методи та засоби, зокрема ті, які базуються на поведінкових сигнатурах. Поведінкові сигнатури дозволяють визначити аномалії в поведінці програми, які можуть вказувати на зловмисну діяльність. Важливим аспектом є розвиток архітектур засобів виявлення, в які впроваджуються ці методи. Змішування різних методів та архітектур може покращити результативність виявлення зловмисних дроперів в комп'ютерних системах.*

*Considered and analyzed already existing methods and means of detecting malicious droppers in computer systems have been. The paper proposes to develop methods and means of detecting malicious droppers in computer systems and to improve the efficiency of their detection, new methods and means will be considered, in particular, those based on behavioral signatures. Behavioral signatures allow you to identify anomalies in program behavior that may indicate malicious activity. An important aspect is the development of detection architectures into which these methods are implemented. Mixing different methods and architectures can improve the performance of detecting malicious droppers in computer systems.*

Однією з найпоширеніших та нещадних методів введення зловмисне програмне забезпечення (ЗПЗ) в комп'ютерні системи є використання зловмисних дроперів. Зловмисні дропери (зловмисні програми для поширення шкідливого коду) є серйозною загрозою для безпеки комп'ютерних систем, призначені для того, щоб завантажити та встановити на комп'ютері жертви інші зловмисні програми, такі як троянці, віруси або шпигунське програмне забезпечення. Ця техніка є дуже ефективною, оскільки дозволяє зловмисникам обходити багато відомих методів виявлення антивірусного програмного забезпечення та залишати мінімальний слід на комп'ютері жертви. Тому розробка методів та засобів виявлення зловмисних дроперів є актуальною проблемою в області кібербезпеки.

Відомі методи виявлення зловмисних дроперів базуються на різних підходах і техніках, які домагаються ідентифікувати шкідливий програмний код або дії зловмисників на комп'ютерних системах. Ось деякі з цих методів та їх недоліки:

1. Антивірусне програмне забезпечення (AV): Антивірусні програми використовують базу даних сигнатур для виявлення відомих шкідливих дроперів.

Вони також можуть застосовувати аналіз поведінки для виявлення невідомих загроз. Основним недоліком є те що антивіруси не завжди можуть виявити нові атаки, оскільки вони ґрунтуються на сигнатурах. Зловмисники можуть застосовувати техніки поліморфізму для уникнення виявлення.

2. Системи виявлення вторгнень (IDS): IDS моніторять мережевий трафік та системні журнали для виявлення підозрілих дій та атак. Основним недоліком є те що вони можуть сприймати нормальну активність як підозрілу, породжуючи багато ложних позитивів. IDS не завжди ефективні в виявленні атак всередині захищеної мережі.

3. Аналіз поведінки програм: Спостереження за діями програм на системі і виявлення незвичайних або підозрілих дій. Проблемою є те що деякі програми з підозрілою поведінкою можуть бути не правильно класифіковано як загрози. Іноді зловмисники можуть знаходити способи обхід цього виду виявлення.

4. Аналіз сигнатур: Використання бази даних сигнатур для порівняння файлів та процесів на системі з відомими шкідливими дроперами. Цей метод ефективний лише для відомих загроз. Він не допомагає виявляти нові атаки або варіації вже існуючих.

5. Віртуальне середовище: Використовується віртуальне середовище для запуску сумнівних програм та спостереження їх дій без впливу на основну систему. Але зловмисники можуть розпізнати віртуальне середовище та приховати свої шкідливі дії.

Кожен метод має свої переваги і недоліки, і найбільш ефективним підходом може бути комбінація декількох методів та засобів виявлення. Також важливо пам'ятати, що загрози постійно еволюціонують, тому системи безпеки повинні регулярно оновлюватися та адаптуватися до нових видів атак.

Традиційні методи виявлення, такі як аналіз сигнатур (підписів), виявлення аномалій та схожості, можуть бути неефективними у виявленні цих дроперів, оскільки вони можуть легко змінювати свою сигнатуру та вести себе "нормально" для уникнення виявлення. Але можна створити систему, в якій будуть враховані недоліки цих систем, що розширить можливості з використання методів.

Метою роботи є покращення ефективності виявлення зловмисних дроперів в комп'ютерних системах.

Для підтвердження результатів роботи розробляється методика оцінки ефективності запропонованих рішень, яка застосовується до розробленої системи та методу виявлення зловмисних дроперів в комп'ютерних системах.

УДК 004.4

Мазур К.Р., Пасічник О.А., Скрипник Т.К.

*Хмельницький національний університет*

## **МЕТОД ВИЯВЛЕННЯ БОЄПРИПАСІВ, ЩО НЕ РОЗІРВАЛИСЬ, ЗА ЗОБРАЖЕННЯМ З ТЕПЛОВІЗОРА ЗАСОБАМИ ГЛИБОКОГО НАВЧАННЯ**

*Розглянуто метод виявлення боєприпасів що не розірвалися за зображенням з тепловізора засобами глибокого навчання, що забезпечує пошук нерозірваних боєприпасів на необхідній території. Запропонований метод забезпечує точний і швидкий пошук боєприпасів що не розірвалися за зображенням з тепловізора.*

*The method of detecting unexploded ordnance based on the image from a thermal imager by deep learning means, which ensures the search for unexploded ordnance in the required territory, is considered. The proposed method provides an accurate and fast search for unexploded ordnance based on the image from the thermal imager.*

Боєприпаси – це військові сили, військова техніка, вибухові речовини, ракети, стрілецька зброя та інші матеріальні засоби, призначені для використання в бойових діях. Вони використовуються як частина військової стратегії і тактики для досягнення військових цілей. Це включає вогневу підтримку, оборону і наступ. Використання боєприпасів ґрунтується на національній військовій доктрині, тактиці і стратегії. Вони використовуються для досягнення різних цілей, таких як знищення ворожої техніки, перешкодження пересуванню сил противника, захист власних військ та об'єктів, нейтралізація ворожих загроз. Дотримання міжнародних законів і конвенцій, таких як Женевські конвенції та Конвенція про заборону мін, має важливе значення для мінімізації жертв серед цивільного населення та захисту гуманітарних наслідків конфлікту. Однак загальна статистика показує, що лише невеликий відсоток правил і норм дотримується під час війни або конфлікту, що збільшує ймовірність жертв як серед військовослужбовців, так і серед цивільного населення [1-5].

Розмінування – це процес виявлення та нейтралізації нерозірваних вибухівок (НВВ) та вибухонебезпечних об'єктів (ВНО) на території, де є загроза для безпеки людей і майна. Це надзвичайно важлива галузь діяльності, оскільки нерозірвані вибухівки можуть залишатися в ґрунті, будівлях, на водному дні, в лісі, на полігоні, на аеродромі, на військових полігонах та інших місцях[4]. Розмінування виконується спеціалізованими командами, які мають відповідні навички, обладнання та знання для виявлення та безпечної знищення НВВ та ВНО.

Основні аспекти розмінування включають:

1. Виявлення: Команди розмінування використовують різні технічні засоби, включаючи металошукачі, гідролокацію, рентгеновські пристрої та інші для пошуку потенційно небезпечних об'єктів.

2. Ідентифікація: Після виявлення можливої НВВ чи ВНО важливо правильно ідентифікувати їх тип, стан та потенційну небезпеку.

3. Нейтралізація: Якщо виявлена вибухова речовина вважається небезпечною, то вона повинна бути безпечно нейтралізована. Це може включати вибухову детонацію на безпечній відстані, контрольоване підпалювання або інші методи.

4. Порятунком і рятування: У разі вибухів та аварій з НВВ команди розмінування можуть бути запрошені для порятунку і допомоги постраждалим.

5. Попередження: Розмінування також включає в себе навчання та консультування громадськості та організацій з питань уникнення НВВ та ВНО та прояву обережності.

Команди розмінування часто співпрацюють з військовими, правоохоронними органами, гуманітарними організаціями та іншими службами, щоб забезпечити безпеку та видалити загрозу від нерозірваних вибухів. Розмінування є необхідною складовою гуманітарних операцій та заходів зі врятування у зонах конфліктів і катастроф.

Тепловізійні камери і аналіз теплових зображень пропонують багато переваг і вигод при пошуку НВВ і мін [3]:

1. Ефективні вночі і в умовах поганої видимості: тепловізійні камери можуть виявляти теплове випромінювання, що корисно, коли звичайна видимість обмежена, наприклад, вночі або в умовах поганої видимості;

2. Теплові аномалії Виявлення: НВВ і міни можуть випромінювати теплове випромінювання, особливо під впливом сонця або при фізичному контакті. Тепловізійні камери можуть допомогти виявити ці теплові аномалії і визначити потенційно небезпечні ділянки.

3. Швидкість і мобільність: тепловізійні камери є портативними і можуть використовуватися швидко. Це дозволяє швидко обстежувати великі території і своєчасно виявляти боєприпаси, що не розірвалися.

4. Безконтактний аналіз: аналіз теплових зображень дозволяє безконтактно виявляти боєприпаси, що не розірвалися, зменшуючи ризик для саперних бригад і уникаючи потенційно небезпечних ситуацій.

5. Точність і висока чутливість: сучасні тепловізійні Тепловізійні камери мають високу роздільну здатність і високу чутливість до різниці температур. Це дозволяє їм точно виявляти НВВ навіть у складних умовах.

6. Можливість інтеграції з ГІС: тепловізійні камери можна легко інтегрувати з географічними інформаційними системами (ГІС), що дозволяє точно визначити місцезнаходження і координати виявлених НВВ.

7. Підвищена безпека і ефективність розмінування: тепловізійні камери Виявлення і локалізація НВВ за допомогою тепловізійних камер дозволяє командам

розмінування уникати небезпечних зон і зосередитися на точному розмінуванні. Завдяки цим перевагам тепловізійні камери є ефективним інструментом для виявлення НВБ і мін, а також сприяють підвищенню безпеки в зоні ураження.

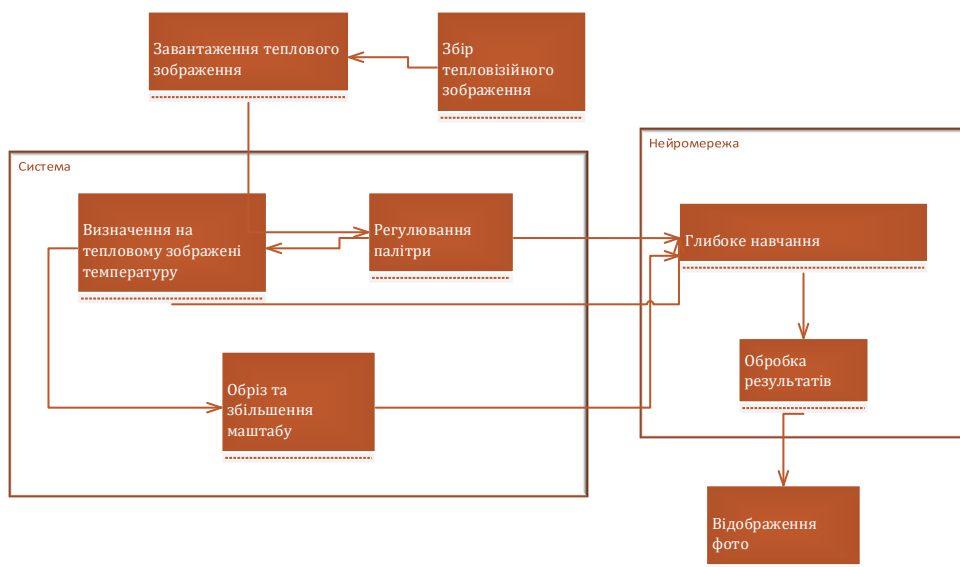


Рисунок 1 – Принцип роботи програми і методу

Програма виявлення НВБ за допомогою теплових зображень на основі глибокого навчання працює наступним чином:

1. Збір теплових зображень Першим кроком є збір теплових зображень, наприклад, з ділянки, де можуть бути знайдені НВБ. Тепловізійні камери вимірюють теплове випромінювання об'єкта і перетворюють його на теплову карту. Такі зображення можуть ідентифікувати боєприпаси, що не розірвалися, за характерним тепловим сигналом.

2. Попередня обробка: зображення можна попередньо обробити, наприклад, видалити шум, підвищити контрастність і підготувати до подальшої обробки за допомогою глибоких нейронних мереж.

3. Глибоке навчання: для аналізу теплових зображень використовуються глибокі нейронні мережі, зазвичай згорткові нейронні мережі (CNN). Мережі навчаються розпізнавати патерни, характерні для боєприпасів, що не вибухнули. Для навчання використовується набір даних, що містить тепловізійні зображення з позначенням місцезнаходження НВБ.

4. Тестування і виявлення: навчені моделі можна використовувати для аналізу нових тепловізійних зображень. Модель шукає закономірності, подібні до

тих, що були вивчені під час навчання, і визначає можливі місця розташування НВБ на зображенні.

5. Оповіщення і дії: Якщо модель виявляє на зображенні можливий НВБ, оператор може вжити відповідних заходів для забезпечення безпеки. Це може включати евакуацію місцевості, проведення розвідки, визначення типу снаряда і вжиття заходів для його знищення або нейтралізації.

6. Відображення результатів: Результати аналізу можуть відображатися на відповідному екрані або інтерфейсі, щоб оператори і користувачі могли приймати швидкі і обгрунтовані рішення.

Принцип роботи методу і програми схематично показаний на рисунку 1.

Ця програма використовує глибоке навчання для автоматичного виявлення боєприпасів, що не вибухнули, на тепловізійних зображеннях, допомагаючи таким чином підвищити безпеку в польових умовах і в зонах, де можуть бути присутніми небезпечні матеріали.

### **Перелік посилань**

1. Боєприпаси. URL: <https://ips.ligazakon.net/document/TM022582>
2. Що варто знати про розмінування та мінну безпеку в Україні. URL: <https://ukrainer.net/minna-bezpeka/>
3. Складність мінування територій України зростає з кожним днем. URL: <https://www.ukrinform.ua/rubric-ato/3752365-skladnist-minuvanna-ukrainskih-teritorij-sodna-zrostaе-mvs.html>
4. Про протимінну діяльність в Україні та гуманітарне розмінування Донбасу. URL: <https://ips.ligazakon.net/document/JH7081CA>
5. Про протимінну діяльність в Україні. URL: [https://ips.ligazakon.net/document/view/T182642?\\_ga=2.121279624.1853336528.1697650787-712735037.1697531357#\\_gl=1\\*1vn19j2\\*\\_gcl\\_au\\*MzI5MjgzNjQxLjE2OTc1MzEzNTc](https://ips.ligazakon.net/document/view/T182642?_ga=2.121279624.1853336528.1697650787-712735037.1697531357#_gl=1*1vn19j2*_gcl_au*MzI5MjgzNjQxLjE2OTc1MzEzNTc)

УДК 004.056.5

Малицький Т.Б., Чешун О.В., Чешун В.М.

*Хмельницький національний університет*

## **МАТЕМАТИЧНА ІНТЕРПРЕТАЦІЯ КОНЦЕПЦІЇ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ КОРПОРАТИВНОЇ МЕРЕЖІ ІЗ ЗАСТОСУВАННЯМ ІМОВІРНІСНИХ КРИТЕРІЇВ ДОВІРИ**

*Розглянуто концептуальні положення методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу із застосуванням імовірнісних критеріїв довіри, наведено базові положення методу та загальний опис математичної моделі, представлено концепцію реалізації методу в термінах запропонованої математичної моделі.*

*The conceptual provisions of the method of protecting information resources of the corporate network from unauthorized access based on probabilistic assessments of trust criteria are considered, the basic provisions of the method and a general description of the mathematical model are given, and the concept of method implementing in terms of the proposed mathematical model is presented.*

В умовах все більшого поширення та інтелектуалізації цифрових технологій та зростання кіберзагроз безпека корпоративних мереж стає важливою складовою сучасного бізнесу. Досягнення ефективної безпеки корпоративних мереж вимагає комплексного підходу, враховуючи технологічні інновації та ретельний аналіз потенційних загроз [1]. Технологічні інновації охоплюють сукупність організаційних та програмно-апаратних безпекових заходів [2,3]: міжмережеві екрани, антивірусне програмне забезпечення, шифрування даних; аутентифікація та авторизація; навчання персоналу; регулярні оновлення та патчі; резервне копіювання та відновлення даних, моніторинг та аналіз активності мережі.

Одним із ключових заходів інформаційної безпеки корпоративних мереж є моніторинг та аналіз активності мережі та блокування шкідливих дій з її ресурсами [4]. Постійний моніторинг мережі і виявлення загроз допомагають вчасно реагувати на кібератаки та аномальну активність, запобігаючи можливим інцидентам. Проблема бокування шкідливих дій полягає не безпосередньо в операції блокування, а у прогнозуванні зловмисності дій, тобто, в оцінці «довіри» до ініціатора цих дій. Довіра в інформаційній безпеці є ключовим аспектом для забезпечення захисту конфіденційної інформації та інфраструктури [5]. Щоб оцінити рівень довіри в інформаційній безпеці потрібні критерії визначення, наскільки ефективно застосовуються заходи безпеки та враховуються ризики.

Проведені дослідження свідчать на користь використання в якості критерію



довіри суб'єктів взаємодії в інформаційному просторі корпоративної мережі імовірнісного показника, що формується на основі накопичуваної статистики попередньої діяльності кожного суб'єкта із урахуванням зафіксованих випадків шкідливої активності відносно загального показника активності.

Концепція методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу із застосуванням імовірнісних оцінок критеріїв довіри базується на положеннях:

- метод розробляється для підвищення ефективності захисту інформаційних ресурсів мережі від несанкціонованого доступу;

- метод базується на виявленні аномальної поведінки користувачів інформаційних ресурсів корпоративної мережі і обмеженні прав доступу до зазначених ресурсів при виявленні порушень користувачем вимог політики безпеки роботи в мережі;

- реагування на порушення користувачем вимог політики безпеки роботи в корпоративній мережі з прийняттям рішення щодо обмеження доступу до її інформаційних ресурсів здійснюється системою захисту інформації автоматично в реальному масштабі часу;

- реалізація методу захисту інформаційних ресурсів корпоративної мережі в реальному масштабі часу системою захисту без втручання людини зумовлює потребу у використанні чітко визначеного математичного базису та правил роботи методу на основі цього базису, що є основою для алгоритмічної і подальшої технічної (програмної) реалізації методу;

- математичною основою методу є визначена ймовірнісна статистична математична модель управління доступом на основі концепції (критеріїв) довіри;

- базовим критерієм для динамічного управління розподілом прав доступу є імовірнісний критерій довіри, що розраховується і постійно динамічно корегується з урахуванням активності користувача в мережі;

- імовірнісний критерій довіри до користувача є основним при визначенні і зміні прав користувача на доступ до інформаційних ресурсів корпоративної мережі та при автоматичному блокуванні доступу користувача до зазначених ресурсів тощо.

Розроблена в термінах математичної моделі структурно-логічна схема реалізації концепції методу представлена на рисунку 1.

Методики, прийоми та засоби, які використовуються для збору статистичних даних щодо поведінки користувачів, їх аналізу і обробки, алгоритми виконання конкретних завдань у рамках методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу із застосуванням імовірнісних оцінок критеріїв довіри засновані на ймовірнісній статистичній математичній моделі управління доступом на основі концепції (критеріїв) довіри.

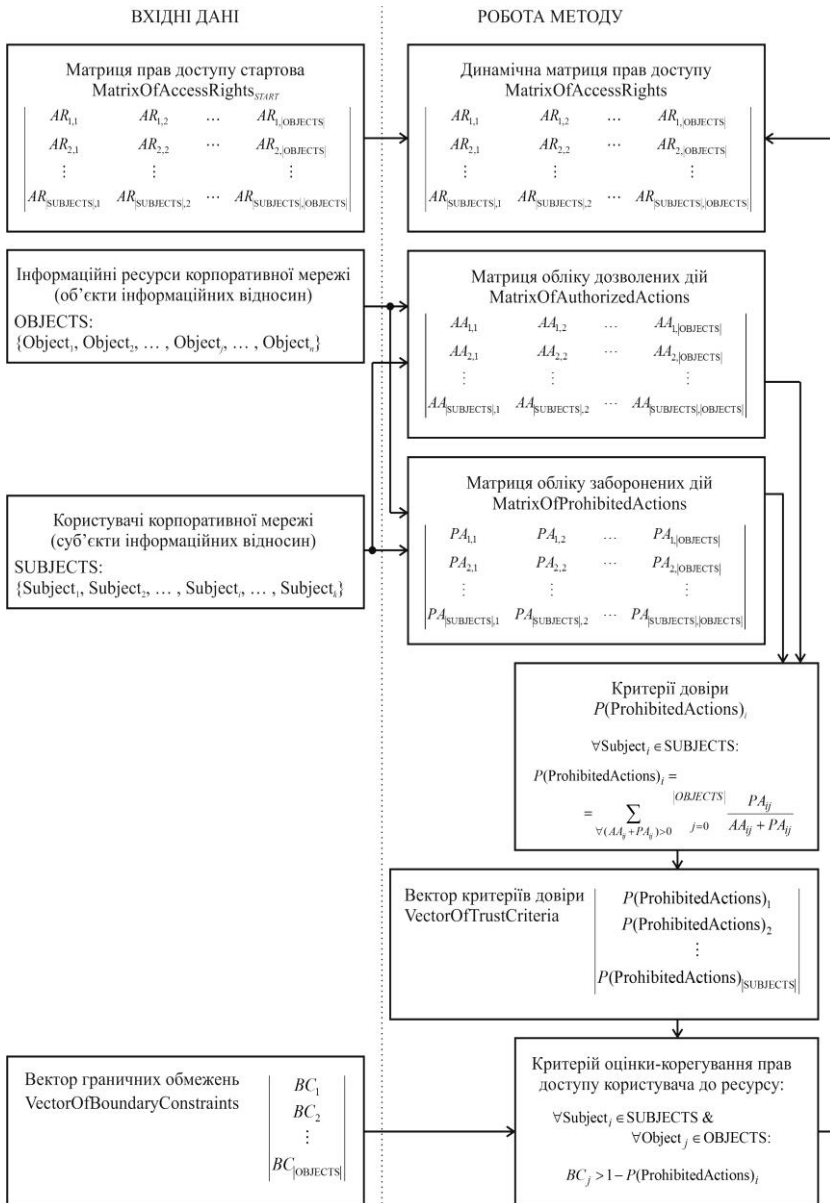


Рисунок 1 – Структурно-логічна схема реалізації концепції методу в термінах математичної моделі

Метод базується на аналізі характеру дій (активностей) користувачів інформаційних ресурсів, що в математичній моделі розглядається як взаємодія зазначених суб'єктів і об'єктів інформаційних відносин, відображених в моделі множинами SUBJECTS і OBJECTS відповідно.

Базовим елементом визначення прав доступу користувачів  $Subject_i \in SUBJECTS$  до інформаційних ресурсів  $Object_j \in OBJECTS$  корпоративної мережі є бінарна матриця прав доступу *MatrixOfAccessRights*.

Базовим критерієм для динамічного управління розподілом прав доступу є імовірнісний критерій довіри  $P(\text{ProhibitedActions})_i$ , що розраховується і постійно динамічно корегується з урахуванням активності користувача  $Subject_i \in SUBJECTS$  в мережі, яка зводиться до статистики дій користувача корпоративної мережі.

Накопичувані статистичні дані щодо дій суб'єктів  $Subject_i \in SUBJECTS$  інформаційних відносин над об'єктами  $Object_j \in OBJECTS$  корпоративної мережі формуються з розподілом даних щодо дій користувачів на коректні і некоректні з точки зору дотримання вимог політики безпеки роботи в мережі та узагальнюються в моделі у формі матриць санкціонованих дій *MatrixOfAuthorizedActions* і заборонених дій *MatrixOfProhibitedActions*.

Імовірнісний критерій довіри розраховується на основі накопичуваних статистичних даних щодо дій суб'єктів інформаційних відносин над об'єктами (інформаційними ресурсами) корпоративної мережі (даних матриці санкціонованих дій *MatrixOfAuthorizedActions* і матриці заборонених дій *MatrixOfProhibitedActions*) і узагальнюється для всіх користувачів  $Subject_i \in SUBJECTS$  інформаційних ресурсів корпоративної мережі в формі вектора критеріїв довіри *VectorOfTrustCriteria*.

Вектор критеріїв довіри *VectorOfTrustCriteria* до користувачів  $Subject_i \in SUBJECTS$  інформаційних ресурсів корпоративної мережі, який, фактично, є відображенням статистичної імовірності несакціонованих дій користувача  $Subject_i \in SUBJECTS$  в полі OBJECTS інформаційних ресурсів корпоративної мережі, передбачається до використання як основний критерій довіри методу захисту інформаційних ресурсів корпоративної мережі і як інструмент динамічного управління правами доступу користувачів до ресурсів корпоративної мережі.

Для реалізації динамічного управління правами доступу користувачів  $Subject_i \in SUBJECTS$  до ресурсів  $Object_j \in OBJECTS$  корпоративної мережі використовуються рівні обмеження довірчого допуску до кожного інформаційного ресурсу  $Object_j \in OBJECTS$ , систематизовані у вигляді вектора граничних обмежень *VectorOfBoundaryConstraints* довірчого допуску до ресурсів мережі.

Якщо відображуванa вектором критеріїв довіри *VectorOfTrustCriteria* статистика дій певного користувача  $Subject_i \in SUBJECTS$  в полі OBJECTS інформаційних ресурсів корпоративної мережі призводить до падіння рівня його довіри нижче за обмеження довірчого допуску до певного інформаційного ресурсу  $Object_j \in OBJECTS$  корпоративної мережі, то доступ відповідного користувача до цього ресурсу блокується.

Блокування доступу користувача  $Subject_i \in SUBJECTS$  до інформаційного ресурсу  $Object_j \in OBJECTS$  передбачає зміну статусу зазначеного в матриці прав доступу  $MatrixOfAccessRights$  рівня прав доступу користувача – зміну значення елемента  $AR_{ij} \in MatrixOfAccessRights$  на нульове. Умова  $AR_{ij}=0$ , відповідно, блокує доступ користувача  $Subject_i \in SUBJECTS$  до інформаційного ресурсу  $Object_j \in OBJECTS$ .

### Перелік посилань

1. Карпович І.М., Гладка О.М., Наконечна Ю.А. Аналіз ризиків безпеки інформаційної системи ІТ-підприємства. *Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки*. 2020. Том 31 (70) № 5. С. 69-74.
2. Чинчик Д., Коробейнікова Т., Захарченко С. Методи та засоби комплексного захисту корпоративної мережі. *InterConf*, 2021, №84. С. 433-450.
3. Гапак О.М., Балого С.І. Захист інформації в комп'ютерних системах: підручник. Ужгород: Державний вищий навчальний заклад «Ужгородський НУ», 2021. 184 с.
4. Храпкін О.М. Захист інформаційно-комунікаційної мережі установи від несанкціонованого доступу. *Системи озброєння і військова техніка*. 2020. № 3(63). С.45-53.
5. Pienta D., Tams S., Bennet Thatcher J. Can Trust be Trusted in Cybersecurity? *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020. P. 4264-4273.

УДК 005.21:005.8:004.8

Мандрик А.І., Лисенко С.М.

*Хмельницький національний університет*

## **МЕТОД ОПТИМІЗАЦІЇ ПЛАНУВАННЯ ПРОЄКТІВ ТА ФОРМУВАННЯ КОМАНД З ВИКОРИСТАННЯМ ГЕНЕТИЧНОГО АЛГОРИТМУ**

*Розроблено метод оптимізації планування проєктів та формування команд з використанням генетичного алгоритму. Метод включає в себе розробку генетичного алгоритму та послідовність етапів, таких як ініціалізація популяції, мутація, кросовер, задля вибору оптимального розподілу розробників на проєкті.*

*The methodological and practical aspects of creating a method for optimizing project planning and team formation using a genetic algorithm has been developed. The method involves the development of a genetic algorithm and a sequence of steps, such as population initialization, mutation, and crossover, to select the optimal distribution of developers on a project.*

**Вступ.** В епоху швидкого розвитку та вдосконалення технологій, проблема невдалих програмних проєктів стає все більш актуальною та вимагає термінового аналізу. Згідно з звітом CHAOS, опублікованим Standish Group у 2020 році, лише 16% програмних проєктів виконуються успішно, дотримуючись запланованих термінів, бюджетів та стандартів якості [1]. Враховуючи ці обставини, невідкладним стає пошук шляхів оптимізації методів управління проєктами, зокрема, в аспектах планування та формування команд. Важливість правильного технічного оснащення команди, а також раціональність планування та бюджетування проєкту, не можна недооцінювати, адже вони можуть визначати, чи стане проєкт успішним, чи призведе до збитків [2-4].

**Метод оптимізації планування проєктів та формування команд з використанням генетичного алгоритму.** Метою є розробка методу, яка використовує генетичні алгоритми для оптимізації планування проєктів та кадрового планування. Він має на меті забезпечити точне моделювання математичної природи планування проєктів та формування команд за її допомогою [5-7]. Особлива увага приділяється визначенню відносних переваг різних можливих рішень відповідно до важливих якостей, що стосуються проблем планування та формування команд.

В рамках цієї роботи, методи генетичних алгоритмів дозволяють визначити оптимальні стратегії для відбору, кросинговеру та мутації, забезпечуючи максимізацію пристосованості протягом наступних поколінь [8, 9]. Основні області застосування цього методу включають кадрове забезпечення команд та планування розкладу проєкту. Так, інформація про обмеження щодо навичок і послідовність

виконання завдань моделюються для забезпечення ефективного призначення завдань працівникам на основі їхніх навичок та досвіду.

Генетичний алгоритм, використовує гібридне кодування [10], яке дозволяє ефективно оптимізувати виконання завдань та призначення працівників. Час виконання завдань представлений додатковим, ненульовим цілим числом, що вказує, коли задача починається. Також, використовується двійкове кодування для визначення, чи був працівник задіяний у виконанні завдань (рисунок 1).

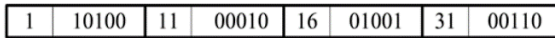


Рисунок 1 – Двійкове представлення генетичного алгоритму

Алгоритм був запущений 30 разів для кожного тестового проекту. В результаті, були отримані різні ступені збіжності. У першому експерименті близько 60% реалізацій виявились найкращими рішеннями, а в третьому експерименті – лише 5% збіжність була досягнута. Це підкреслює важливість стохастичності початкового вибору популяції та генетичних операцій у впливі на збіжність алгоритму [2].

Таблиця 1. Рівень досвіду співробітників для тестових проектів

	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10
S1	0	0.2	0	0	0	0	0	0	0	0.6
S2	0	0	0.8	0	0.6	0.6	0	0.6	0.2	0.4
S3	0.4	0.4	0	0.4	0	0.4	0.4	0.6	0.4	0
S4	0.8	0	0	0.8	0	0.8	0.8	0.8	0	0
S5	0	0	0	0.6	0	0	0	0	0	0.6

Основними факторами, які впливають на результати, є варіабельність часу виконання та стохастичність вибору (Рисунок 2).

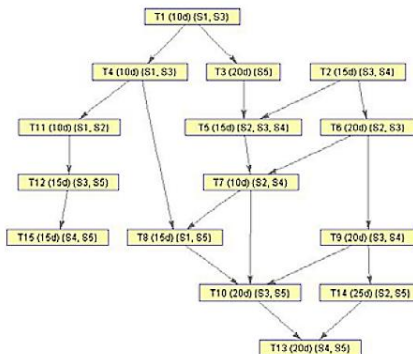


Рисунок 2 – Граф пріоритетів завдань для тестових проектів

Даний генетичний алгоритм використовує гібридне кодування, де час виконання завдань виражається через додатні цілі числа, а участь працівників – через двійкове кодування.

### Експерименти

У цій роботі було використано метод на основі генетичного алгоритму, реалізований за допомогою бібліотеки DEAP та мови програмування Python [11].

Початковий експеримент полягав у виконанні шести різних завдань, кожне з яких вимагало певних навичок. Було вирішено об'єднати ці завдання з командою, що складалася з шести членів, кожен з яких мав унікальну комбінацію навичок. Щоб забезпечити всебічне дослідження простору рішень, генетичний алгоритм був налаштований на ітерації протягом 40 поколінь, кожне з яких містило популяцію з 50 потенційних командних утворень. З ймовірностями кросингверу та мутації, зафіксованими на рівні 0,7 та 0,2 відповідно, алгоритм мав широкі можливості як комбінувати успішні рішення, так і вводити випадкові варіації.

У міру розгортання ітерацій алгоритм демонстрував чітку траєкторію вдосконалення. До кульмінації 40-го покоління він визначив оптимальний склад команди, який отримав оцінку придатності 6.0. Цей показник свідчив про ідеальну узгодженість, коли навички кожного члена команди резонували з вимогами поставленого перед ним завдання. Наприклад, оптимальне рішення отримала учасниця команди, наділена дизайнерськими навичками, Аліса, яка отримала завдання "Дизайн UI/UX", що було влучно позначено як "Дизайн UI/UX", результат роботи програми у консолі показано на рисунку 1.

```
me $
  gen    nevals
  0      50
  1      31
  2      42
  ... [intermediate generations and evaluations]
  39     36
  40     29

Best individual: ['Alice', 'Bob', 'Charlie', 'Dana', 'Emily', 'Frank']
me $ Fitness: 6.0
```

Рисунок 3 – Результат роботи алгоритму

### Висновки

Розроблений метод з використанням генетичного алгоритму оптимізації дозволяє ефективно розв'язувати проблеми планування програмних проєктів та

формування команд. Проблеми виникли при визначенні пріоритетності призначення досвідчених працівників, що мали вплив на загальну тривалість проекту. Вдосконалення, такі як застосування багатоцільової оптимізації та ітераційні уточнення, можуть виявитися корисними у розв'язанні цих викликів.

### **Перелік посилань**

1. Standish Group CHAOS Report. Standish Group International. URL: <https://hennyportman.files.wordpress.com/2021/01/project-success-qrc-standish-group-chaos-report-2020.pdf> (дата звернення: 20/09/2023).
2. José G. M. Esgario, Iago E. da Silva, and Renato A. Krohling. Application of Genetic Algorithms to the Multiple Team Formation Problem. Arxiv, 2019.
3. Leksakul K., and Phetsawat S. Nurse scheduling using genetic algorithm Math. Probl. Eng. 2019 0–17 pp.
4. Alharbi A., Alqahtani K. A. Genetic Algorithm Solution for the Doctor Scheduling Problem The Tenth International Conference on Advanced Engineering Computing and Applications in Sciences. 2022. 91 p.
5. Kristiadi D., and Hartanto R. Genetic Algorithm for lecturing schedule optimization. 2019. 13–83 pp.
6. Parera S., Sukmana H. T., Wardhani L. K. Application of genetic algorithm for class scheduling. 2019. 3–7pp.
7. Mardiyono A. Intelligent System for Course Scheduling in Higher Educations Int. J. Inf. Technol. Bus. Manag. 2022. 29–34 pp.
8. Eletrotécnica E. Dynamic Scheduling for Maintenance Tasks Allocation supported by Genetic Algorithms. 2018. pp.
9. Kaleeswaran A., Ramasamy V., Vivekanandan P. Dynamic Scheduling Of Data Using Genetic Algorithm In Cloud Computing Int. J. Adv. Eng. 2018.
10. Swarm-based hybrid optimization algorithms: an exhaustive analysis and its applications to electricity load and price forecasting. URL: <https://link.springer.com/article/10.1007/s00500-023-07928-0> (дата звернення: 20.10.2023)
11. DEAP is a novel evolutionary computation framework for rapid prototyping and testing of ideas. URL: <https://deap.readthedocs.io/en/master/> (дата звернення: 10.08.2023)



УДК 004.4

Манзюк Е.А.

Хмельницький національний університет

## ЗАСТОСУВАННЯ РОЗПАРАЛЕЛЮВАННЯ ДЛЯ КРИПТОГРАФІЇ З ВИКОРИСТАННЯМ ГУБЧАСТОЇ СТРУКТУРИ

У запропонованій роботі розглядається новий підхід до розв'язання проблем у криптографії, який базується на паралельному використанні губчастої криптографії. Використовуючи режими на основі перестановок, автори пропонують симетричний криптографічний примітив, що дозволяє використовувати різні рівні паралелізму та перестановки. Запропонований підхід ґрунтується на використанні бітової криптографічної перестановки чи сім'ї перестановок з різною кількістю раундів. Шифр включає шар отримання маски, шар стиснення і шар розширення, кожен з яких використовує паралельні перестановки. Такий підхід спрямований на простоту та ефективність, подібну до конструкції губок, і відрізняється можливістю обчислення для інкрементних вхідних даних. Він є універсальним і може бути реалізований з використанням різних криптографічних перестановок. Зазначається, що запропонований підхід може бути легко реалізований на різних платформах, що робить його ефективним і гнучким для застосування в сучасних системах криптографії.

*This work introduces a novel solution to cryptographic challenges through the application of parallel sponge cryptography. Utilizing permutation-based modes for all key operations in symmetric cryptography, the proposed approach accommodates various levels of parallelism and permutations of length shorter than the boundary  $2s$ . Similar to sponge constructions, this method relies on a composite primitive and associated modes. The primitive functions as a pseudorandom generator, accepting a key and a string or sequence of strings as input, and producing output bits of arbitrary length. To an adversary ignorant of the key, these output bits present themselves as independent and uniformly distributed random bits. This primitive serves as a fundamental component suitable for authenticity verification, stream ciphers, and other cryptographic applications. Simple modes can transform it into an authenticated encryption scheme and a variable-length block cipher.*

В сфері симетричної криптографії переважають блокові шифри. За винятком деяких спеціалізованих потокових шифрів, стандарти застосовували шифрування, автентифікацію переважно використовуючи блочні шифри [1, 3]. Досить часто для хешування використовувалися режими, побудовані на основі блочних шифрів.

Останнім часом у розробку блокових шифрів було внесено значні інновації, що включають у себе визначення нових режимів. При більш детальному аналізі цих режимів можна виявити тенденцію до уникнення використання обернених відображень блочних шифрів.

Варто зауважити, що підтримка оберненого відображення накладає обмеження на обробку вхідних даних ключа та вхідного блоку інформації. Ключ обробляється у режимі генерації ключів, а дані обробляються у потоці даних, при цьому не відбувається дифузії від потоків даних до потоку генерації ключів. Це обмеження суттєво ускладнює можливість ефективної дифузії, як це вказано граничними значеннями для обох розмірів блоків. Таким чином, використання блочного шифру в режимі, що уникає використання його оберненої проєкції, вважається не оптимальним з обчислювальної точки зору. Прикладами функцій на основі блочних шифрів, що уникають використання обернених відображень, є шифрування в режимі шифрування СМЕ або перевірка автентичності на основі блочного шифру.

На відміну від блокових шифрів, криптографічні перестановки не розрізняють між ключем і введеними даними, і, отже, не піддаються зазначеному обмеженню. Їх використання набуло популярності, зокрема під час конкурсу SHA-3, оскільки кілька кандидатів базувались на цьому типі примітивів [2]. На сьогодні криптографія, заснована на конструкціях типу "губка" (sponge) стала повноцінною альтернативою блочному шифру.

Проте губка та дуплексні конструкції є послідовними за своєю природою. Основна частина обчислень включає повторні обчислення перестановок, і для кожного обчислення потрібен результат попереднього. Сучасні високопродуктивні процесори настільки потужні, що обчислення  $n$  перестановок одночасно відбувається швидше, ніж їх послідовне обчислення. З метою отримання оптимальної продуктивності для хешування можна використовувати деревовидне хешування. Подібні методи можна застосовувати для окремих випадків автентифікації або шифрування. Однак для дуплексного шифрування з автентифікацією необхідно заздалегідь знати обсяг доступного паралелізму.

В залежності від методів використання та можливостей потенційного супротивника для досягнення стійкості на рівні  $s$  біт, кількість раундів (перестановок) повинна знаходитися в діапазоні між  $s$  та  $2s$ . Таким чином, для досягнення стійкості на рівні 128 біт, кількість раундів при ширині перестановки 128-256 біт повинна бути меншою за ширину перестановки. Це призводить до обмеження базової перестановки до певної мінімальної ширини, і для відносно невеликих блоків ефективність не є оптимальною.

Для вирішення цих проблем пропонується паралельний варіант губчастої криптографії. Використовуються режими на основі перестановок для всіх операцій з ключами у симетричній криптографії, які можуть використовувати будь-який рівень паралелізму і перестановки, що можуть бути менші за граничну довжину  $2s$ . Подібно до губок, цей підхід заснований на складеному примітиві та режимах, що працюють з ним. Цей примітив є псевдовипадковою функцією, яка приймає на вхід ключ та рядок або послідовність рядків і генерує вихідні біти довільної довжини. Для противника, який не знає ключа, ці вихідні біти виглядають як незалежні рівномірно розподілені випадкові біти. Цей підхід є базовим примітивом, який можна легко використовувати в якості перевірки автентичності, потокового шифру

тощо. За допомогою деяких простих режимів його можна трансформувати в схему шифрування з автентифікацією і в блоковий шифр, який підтримує змінну довжину блоку.

Підхід ґрунтується на використанні  $b$ -бітової криптографічної перестановки або сім'ї перестановок з різною кількістю раундів. Розроблений шифр приймає на вхід ключ і послідовність рядків даних довільної довжини, генеруючи при цьому вихідні дані довільної довжини. Він складається з шару отримання маски, шару стиснення і шару розширення, кожен з яких передбачає паралельне використання перестановки.

Шар стиснення застосовує одну з перестановок до вхідних блоків, при цьому кожен блок маскується ковзною  $b$ -бітовою вхідною маскою, і їхні виходи побітно додаються до  $b$ -бітового блоку. Щодо шару розширення, накопичувач піддається перестановці, а потім використовується як рухомий стан для генерації виходу. Кожен вихідний блок є результатом додавання вихідної маски та виходу перестановки, яка застосовується до поточного стану.

Конструкція спрямована на простоту та ефективність і має спільні риси з конструкцією губки. Подібно до губок, вона не використовує зворотню перестановку. Ще однією спільною особливістю з губками є здатність до обчислення для інкрементних вхідних даних. Якщо у губках це реалізується дуплексною конструкцією, то в даному підході це досягається тим, що вхідний блок залежать лише від його значень та позицій на вході.

Даний підхід можна розглядати як розпаралелений варіант губки для криптографічних систем. Зокрема, виклики перестановок можна виконувати паралельно, щойно згенерованої вхідної маски. Цей підхід легко реалізується на різних платформах, включаючи і сучасні процесори з одноінструкційними блоками з множинними даними. Крім того, він може бути ефективним, оскільки кількість раундів у перестановках може бути значно меншою, ніж у режимах на основі губки, завдяки тому, що противник ніколи не має доступу до як входу, так і виходу виклику перестановок.

З огляду на його властивості введення-виведення, цей підхід є універсальним. Його можна реалізувати з використанням будь-якої криптографічної перестановки.

### Перелік посилань

1. Abdullah A. M. Advanced encryption standard (AES) algorithm to encrypt and decrypt data. Cryptography and Network Security. 2017. Vol. 16, No. 1. Pp. 11.
2. Gupta D. N., Kumar R. Sponge based lightweight cryptographic hash functions for IoT applications: 2021 International Conference on Intelligent Technologies (CONIT), IEEE, 2021. Pp.1–5.
3. Hidayat T., Mahardiko R. A Systematic literature review method on aes algorithm for data sharing encryption on cloud computing. International Journal of Artificial Intelligence Research. 2020. Vol. 4, No. 1. Pp. 49–57.

УДК 004.4

Мантур В.А.

*Хмельницький національний університет*

## **ВИКОРИСТАННЯ КОДУВАННЯ ЗОБРАЖЕНЬ У ФОРМАТІ BASE64 ДЛЯ ВЕБЗАСТОСУНКІВ З ВИКОРИСТАННЯМ РЕЛЯЦІЙНИХ БАЗ ДАНИХ**

*У даному дослідженні представлена методологія розробки програмного забезпечення, яке передбачає функції збереження та передачі зображень, з використанням кодування Base64. Робота орієнтована на спільне використання клієнт-серверної архітектури та реляційних баз даних. Описаний метод, може бути корисний при взаємодії застосунків з великою кількістю зображень, які потребують регулярного резервного копіювання.*

*This study presents a methodology for developing software that provides image storage and transfer functions using Base64 encoding. The work is focused on the joint use of client-server architecture and relational databases. The described method can be useful when interacting with applications with a large number of images that require regular backups.*

На сьогоднішній день, використання веб-застосунків стало повсякденним процесом. З розвитком технологій та потреб користувачів, виникла необхідність постійної передачі даних через веб-мережу, що особливо стосується застосунків з клієнт-серверною архітектурою. Один з найважливіших видів інформації, якою активно обмінюються різні пристрої – це зображення.

Більшість сайтів потребують використання зображень, як для покращення візуальної складової застосунку, так і для практичного застосування, де як приклад можна навести інтернет-магазини. Власники таких застосунків потребують створення зручних та безпечних сховищ даних, які, при по требі, можливо швидко переміщувати на інші сервери, або для яких потрібно регулярно створювати резервні копії. Але, при класичному використанні нереляційних баз даних для зберігання зображень [1], може втратитись загальна структурованість інформаційних сховищ, через що виникає потреба в інших рішеннях. У даній статті ми розглянемо підхід до збереження та передачі зображень між клієнтом та сервером, з використанням форматом кодування Base64, який можна використовувати у реляційних базах даних.

Метою роботи є розробка методології для використання кодування зображень у форматі Base64 для збереження та передачі зображень у веб-застосунках побудованих з використанням клієнт-серверної архітектури, які використовують реляційні бази даних, а також аналіз її використання.

При розробці програмних продуктів, потрібно враховувати, яким чином буде спроектована файлова система додатку, особливо, якщо при взаємодії з клієнтом беруть участь сторонні файли, як наприклад зображення. При використанні стандартного методу зберігання таких файлів у нереляційних базах даних, може виникнути проблема з переміщенням та резервним копіюванням інформації. Таким чином, щоб уникнути додаткової реалізації виконання таких процесів, існує можливість спроектувати реляційну базу даних, яка зможе розміщувати в собі і файли.

Один з найкращих способів розміщення даних зображення у базі даних – це зберегти його дані у форматі масиву байтів. Але може виникнути проблема, при якій збільшиться навантаження на сервер, через потребу постійного конвертування інформації з різних форматів, які залежать від задач та способу передачі інформації до клієнта. Таким чином, для вирішення даної проблеми, можна використовувати на, стандартний для веб-застосунків, формат кодування Base64, який перетворює масив байтів на рядковий формат, при цьому не змінить розмір та якість зображення [3].

Зручність використання і збереження у форматі Base64 полягає у тому, що він може використовуватися для передачі даних між клієнтом та сервером, що позбавляє потреби у додатковому перетворенні даних на стороні серверу. Тому, дана методологія буде корисна в випадках, де на стороні серверу не мусить відбуватись додаткових маніпуляцій з зображеннями, окрім їх зберігання та передачі між різними модулями.

Якщо веб-застосунок використовує мову розмітки HTML, тоді зникає потреба у додатковій обробці переданих зображень і на стороні клієнта. Це спричинено тим, що браузері здатні автоматично відображати зображення, якщо замість посилання на файл, розмістити дані закодовані у форматі Base64.

Іншою позитивною стороною даного підходу є те, що при використанні формату Base64, може бути спрощена передача великої кількості зображень від клієнта до серверу. Якщо користувач завантажить власні зображення на клієнтську частину, надається можливість реалізувати алгоритми, які конвертують файли до масиву рядків у форматі Base64, саме на стороні клієнта. Але потрібно враховувати, що при передачі рядків на сервер, в будь-якому випадку потрібно перевіряти правильність переданого формату, що може бути виконано за один цикл проходження по рядку, перевіривши лише використання доступних символів та кратність розміру рядка числу 6.

Єдина проблема, яка може виникнути під час використання даної методології полягає у тому, що передача зображень може відбуватись під час передачі відображення сторінки користувача на клієнтську частину. В такому випадку, час очікування результатів може бути довгим, особливо при взаємодії з великою кількістю файлів. Для вирішення цієї проблеми, варто реалізовувати алгоритми на стороні сервера, які здатні передавати зображення до клієнта поступово, після того, як відображення повністю буде передано користувачу. Даний

алгоритм можна реалізувати різними способами, в залежності від інструментів, які використовуються при розробці застосунку. Один з варіантів реалізації описаного процесу, можна побачити на рисунку нижче (рисунок 1)



Рисунок 1 – Блок-схема поступової відправки зображень

Інший варіант для підвищення продуктивності при передачі зображень у форматі Base64 – це використання декількох паралельних серверів. При даному підході, один сервер буде формувати та відправляти лише сформоване відображення для користувача, яке буде містити запит до іншого сервера, який буде формувати список зображень та відправляти їх користувачеві. В даному випадку, швидкість відображення сторінки, буде подібною до випадку, коли використовується нереляційна база даних.

В узагальненому вигляді, описана методологія може допомогти створити єдине реляційне сховище даних, яке дозволить спростити взаємодію з інформацією, а також дозволить зменшити навантаження на сервер при передачі даних у додатках з клієнт-серверною архітектурою. Проаналізувавши запропоновану методологію, можна дійти висновку, що її використання може бути корисним саме в описаних випадках.

### Перелік посилань

1. Andreas, M. (2019). Essential Scrum: SQL & NoSQL Databases: Models, Languages, Consistency Options and Architectures for Big Data Management.
2. Fehily, C. (2019). SQL (Database Programming).
3. Rakesh, R. (2018). Base64 Encoding: Hacking series.Gerardus, B. (2016). Preemptive multithreading The Ultimate Step-By-Step Guide.

УДК 004.4

Медведєва К.С., Антипенко В.П.

Сумський державний університет

## WEB-ОРІЄНТОВАНА СИСТЕМА АВТОМАТИЗАЦІЇ ПРОЦЕСУ АНАЛІЗУ ЯКОСТІ ПРОГРАМНОГО ПРОДУКТУ

*У даній роботі розглянуто рішення для автоматизації процесу аналізу якості програмного продукту (ПП). Пропонується використовувати документ Bug review. Це забезпечить підвищення якості виконання процесів розробки програмного продукту та його тестування під час реалізації проєкту в рамках ІТ-компанії. Запропонована web-орієнтована система дозволяє виявити області, де необхідні зміни та, відповідно, удосконалення, у процесах розробки та тестування програмного продукту, якщо показники виходять за межі норма лізованих значень.*

*This work presents a solution for automation the process of analyzing the quality of a software product (SP). It is suggested to use the Bug review document. This will ensure an increase in the quality of software product development and testing during project implementation within the IT company. The proposed web-oriented system allows to identify areas where changes and, accordingly, improvements are needed in the processes of software product development and testing, if the indicators go beyond the normalized values.*

У зв'язку зі стрімким розповсюдженням інформаційних технологій (ІТ) майже у всі сфери життя суспільства, сьогодні значно виросла як кількість, так і різноманіття проєктів, виконуваних сучасними ІТ-компаніями. Також варто відмітити швидкий розвиток web-технологій, мов програмування, інструментів для автоматизації здійснення певних етапів життєвого циклу розробки програмних продуктів (ЖЦРПП) тощо. Тому, на основі вищевказаного, можна зазначити, що зараз нагальною є проблема удосконалення процесів реалізації ІТ-проєктів для забезпечення вищої якості їх виконання. І оскільки процес тестування (Quality Assurance – QA) розроблюваного програмного продукту, включаючи процес аналізу якості останнього, є обов'язковим видом діяльності в ЖЦРПП, він не є винятком і однозначно підлягає поліпшенню.

Дане питання є актуальним сьогодні. Автоматизація процесу аналізу якості програмного продукту стає досить важливою, оскільки це дозволяє певним учасникам команди проєкту, а саме розробникам та тестувальникам, більш ефективно виявляти та виправляти дефекти ПП за рахунок автоматизованого збору та аналізу даних і забезпечення постійного контролю якості розроблюваного програмного продукту.

Сучасні методи оцінки якості програмного забезпечення ґрунтуються на встановлених міжнародних і національних стандартах [1]. У сфері автоматизації аналізу якості ПП існують дослідження, які фокусуються на застосуванні технологій машинного навчання та штучного інтелекту [2]. Їх використання сприяє вдосконаленню процесів тестування та оцінки коду. Незважаючи на те, що статичний аналіз коду [3] застосовується для виявлення деяких видів вразливостей і помилок, він має обмеження в контексті симуляції реальних умов експлуатації ПП. Розвиток web-технологій сприяє створенню більш гнучких і доступних інструментів для забезпечення безперервного моніторингу якості програмного продукту в реальному часі.

Метою роботи є розробка web-орієнтованої системи автоматизації процесу аналізу якості програмного продукту для підвищення ефективності роботи розробників і тестувальників під час виконання проєктів у рамках ІТ-компанії. Вона генерує результати на основі дослідження документа Bug review. Це необхідно для ідентифікації слабких місць у процесі розробки і подальшого їх удосконалення наряду з відповідними процесами тестування. У свою чергу це також дозволить ефективно управляти дефектами ПП.

Таблиця 1 – Метрики для аналізу документа Bug review

Назва метрики	Пояснення значень результатів метрики
Defect density	Щільність дефектів за конкретним програмним продуктом. Якщо показник $>0,3$ необхідно внести зміни в процеси команди розробки.
Time bugs solving by Priority	Час на виправлення дефекту відносно його пріоритету. Відображається за допомогою тренду змін.
Bugs Environment	Місце знаходження дефектів відносно середовища розробки. Якщо більшість дефектів було виявлено на dev/stage середовищі – команда QA працює правильно, якщо більшість дефектів знайдено на production середовищі – необхідні зміни в QA процесах.
Bug Discovery Source	Аналіз ким були знайдені дефекти. Якщо більшість дефектів було знайдено QA та розробниками це свідчить про налагодженість та надійність процесів в команді розробки, якщо дефект був знайдений користувачем – необхідно поліпшити методи тестування та розробки.

Далі розглянемо суть документа Bug review. Це інструмент для структурованого аналізу дефектів. Останні збираються під час тестування та розробки програмного продукту. Документ Bug review містить основні



характеристики кожного дефекту: його ID та назву, номер спринту, хто знайшов дефект, оточення, функціонал, скільки разів відтворювався дефект, його причина, статус, пріоритет, серйозність, дата створення, дата зміни, час на виправлення дефекту. Це дозволяє ретельно дослідити якість розробки та тестування програмного продукту.

Для ефективного аналізу документа Bug review використовуються різні метрики тестування. Їх опис надано в таблиці 1.

Використання web-орієнтованої системи для аналізу якості програмного продукту має численні переваги. Перш за все, її застосування дозволяє здійснювати дослідження дефектів ПП в режимі реального часу, забезпечуючи доступ до даних з будь-якого місця і в будь-який час. Крім того, дана web-орієнтована система дає можливість візуалізації результатів аналізу документа Bug review у зручному форматі, що сприяє кращому розумінню проблеми та прийняттю відповідних рішень.

Автоматизація процесу аналізу якості програмного продукту є важливим завданням у ході підтримки етапів ЖЦРПП. Використання запропонованої web-орієнтованої системи, яка базується на аналізі документа Bug review, дозволяє підвищити якість розробки та тестування програмного продукту. У свою чергу це веде до удосконалення всього процесу реалізації сучасних ІТ-проектів у цілому. Впровадження метрик тестування дозволяє ефективно виявляти та управляти дефектами. Це впливає на підвищення якості ПП та процесів розробки. Такі підходи допомагають забезпечити надійність і конкурентоспроможність програмного продукту в умовах постійних змін і вимог ринку та користувачів.

### **Перелік посилань**

1. Незамай Б. Прогнозування якості програмного забезпечення. In 2022 International Conference on Innovative Solutions in Software Engineering (ICISSE), 2022. С. 86.
2. Tran H. M., Le S. T., Nguyen S. V., & Ho P. T. An analysis of software bug reports using machine learning techniques. SN Computer Science, 1, 2020. P. 1-11.
3. Смелик Я. М. Аналіз якості програмного забезпечення за допомогою програмних метрик. Магістерська дис.:121 Інженерія програмного забезпечення, Київ, 2022. 114 С.

УДК 004.5

Мельник В.М., Сорочинський О.Ю., Глухенький О.А., Семенюк Б.В.

*Хмельницький національний університет*

## **МЕТОД СТВОРЕННЯ БЕЗПЕЧНОЇ КІБЕРФІЗИЧНОЇ СИСТЕМИ ДЛЯ АВТОМАТИЗАЦІЇ ПРИМІЩЕНЬ ПІДПРИЄМСТВ З ВИКОРИСТАННЯМ ОПЕРАЦІЙНИХ СИСТЕМ НА ОСНОВІ МІКРОЯДРА**

*Розроблено метод створення безпечної кіберфізичної системи для автоматизації приміщень підприємств з використанням операційних систем на основі мікроядра. Реалізовано на системному рівні забезпечення надійних обчислень на основі пристроїв і контролерів. Використовуються такі основні функції безпеки, як надійний модульний дизайн, невеликий код привілеїв і можливість формальної перевірки архітектури мікроядра,*

*Розроблено концепцію операційної системи з підвищеним рівнем безпеки з вбудованим обов'язковим контролем доступу і комунікаційну основу на основі проксі для контролерів автоматизації приміщень. Це рішення забезпечує комунікацію та ізоляцію між критичними та некритичними програмами в потенційно складному кіберсередовищі.*

*A method of creating a safe cyber-physical system for the automation of enterprise premises using microkernel-based operating systems has been developed. It is implemented at the system level to ensure reliable calculations based on devices and controllers. Core security features such as robust modular design, small privilege code, and the ability to formally verify the microkernel architecture are used.*

*A security-enhanced operating system concept with built-in mandatory access control and a proxy-based communication framework for room automation controllers has been developed. This solution provides communication and isolation between critical and non-critical applications in this complex cyber environment.*

Системи автоматизації приміщень підприємств – це великомасштабні розподілені системи керування, які мають на меті покращення автономного контролю та індивідуального керування середовищем приміщень. А типова така система контролює всі аспекти роботи будівлі від освітлення, опалення, вентиляції та кондиціонування повітря до протипожежної безпеки, контролю доступу, відео та багато іншого. Операції в ній безпосередньо впливають на споживання енергії будівельними об'єктами. Тому, актуальним є завдання з розробки нової кіберіфікованої системи для приміщень підприємств, щоб покращити комфорт, зменшити енергоспоживання та експлуатаційні витрати.

Традиційно такі системи [1-5] складаються з кількох автономних підсистем для конкретної програми. Кожна підсистема забезпечує лише одну послугу,

наприклад контроль температури, вентиляцію тощо. Пристрої в кожній підсистемі підключені через мережі автоматизації будівель, які раніше були відділені від ІТ-систем у середовищі. Логіка управління здійснюється через центральне управління сервером, які називаються системами управління приміщень, які з'єднуються з програмованими логічними контролерами у схемі головний-підлеглий. Різні підсистеми об'єднані в різні контрольні домени (наприклад, домен безпеки, домен безпеки) і керуються окремо.

Зі швидким комерційним розширенням кіберфізичних систем або загальновідомих технологій Інтернету речей у промисловості, розробники та дослідники прагнули охопити концепцію «розумних будинків», яка використовує різні датчики для кращого розуміння контексту життя, надає приводи з підтримкою IP для керування навколишнім середовищем і з'єднує існуючу систему керування з тим, щоб краще реагувати на індивідуальні потреби. Будинки зазнають трансформації краще обслуговувати клієнтів і мешканців за допомогою передової автоматизації та мереж.

Система автоматизації приміщень підприємств – це складна розподілена система керування, яка широко використовується в комерційних, житлових і промислових приміщеннях для моніторингу та керування механічним/електричним обладнанням. Завдяки зростанню промислових і технологічних досягнень, компоненти управління стають все більш взаємопов'язаними. Разом із потенційними перевагами інтеграція також створює нові вектори атак, що значно підвищує ризики безпеки та безпеки в системі керування. Історично склалося так, що система не має дизайну безпеки та покладається на фізичну ізоляцію та «безпеку через невідомість». Ці методи неприйнятні з технологіями «розумного будинку». Галузь потребує переоцінки безпеки та безпеки поточної автоматизації приміщень, систему та розробку комплексного рішення для забезпечення цілісності, надійності та конфіденційності як на рівні системи, так і на рівні мережі.

Реалізовано на системному рівні забезпечення надійних обчислень на основі пристроїв і контролерів. Використовуються такі основні функції безпеки, як надійний модульний дизайн, невеликий код привілеїв і можливість формальної перевірки архітектури мікроядра,

Розроблено концепцію операційної системи з підвищеним рівнем безпеки з вбудованим обов'язковим контролем доступу і комунікаційну основу на основі проксі для контролерів автоматизації приміщень. Це рішення забезпечує комунікацію та ізоляцію між критичними та некритичними програмами в потенційно складному кіберсередовищі.

### Перелік посилань

1. Friedrich Praus, Wolfgang Kastner, and Peter Palensky. Software Security Requirements in Building Automation. Sicherheit 2016, 2016.
2. Ronghui Gu, Zhong Shao, Hao Chen, Xiongnan (Newman) Wu, Jieung Kim, Vilhelm Sjöberg, and David Costanzo. Certikos: An extensible architecture for building certified concurrent os kernels. In OSDI, volume 16, pages 653–669, 2016.
3. Adam Lackorzynski and Alexander Warg. Timing aware hardware virtualization on the l4remicrokernel system. In 2016 IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), page 67, 2016.
4. Jornt van der Wiel, Konstantin Zykov, Vicente Diaz, and Yury Namestnikov. Hajime, the Mysterious Evolving Botnet, Apr 2017.5. Fukang Liu, Christoph Dobraunig, Florian Mendel, Takanori Isobe, Gaoli Wang, and Zhenfu Cao. Efficient Collision Attack Frameworks for RIPEMD-160. In Alexandra Boldyreva and Daniele Micciancio, editors, Advances in Cryptology – CRYPTO 2019, pages 117–149, Cham, 2019. Springer International Publishing.
5. Xiaolong Wang, Masaaki Mizuno, Mitch Neilsen, Xinming Ou, S. Raj Rajagopalan, Richard Habeeb, Siddharth Amaravadi, John Hatcliff, and Srivatsan Varadarajan. Enhanced Security of Building Automation Systems Through Microkernel-Based Controller Platforms. Proceedings of the Second Workshop on Communication, Computing, and Networking in Cyber Physical Systems (CCNCPS 2017), Jun 2017.

УДК 004.4

Миронюк К.Г.

*Київський національний університет імені Тараса Шевченка*

## **ЗАДАЧА ТРАНСПОРТУВАННЯ РЕСУРСІВ СПОЖИВАЧАМ**

*Представлено процес розробки програмного рішення для задачі транспортування ресурсів та його модифікації. Основною метою цього дослідження є вирішення практичних проблем логістики та оптимізації ресурсообміну між джерелами та споживачами. Розроблена програма містить різні алгоритми та методи пошуку рішення, візуалізацію результатів, кроків та проміжних таблиць.*

*The process of developing a software solution for the resource transportation problem and its modifications is presented. The main goal of this research is to address practical logistics and resource exchange optimization challenges between sources and consumers. The developed program includes various algorithms and solution search methods, visualization of results, steps, and intermediate tables.*

Задача транспортування ресурсів споживачам є важливою через свою широку поширеність в різних галузях, складність розв'язання, великий вплив на ефективність та потенціал для використання сучасних технологій. Дослідження цієї задачі має стратегічне значення для оптимізації логістичних процесів та підвищення конкурентоспроможності підприємств.

За останні роки транспортну задачу все частіше використовують для навчання нейронних мереж [2]. Також алгоритми розв'язання цієї задачі знайшли застосування у зіставленні зображень, сейсмології, економічному моделюванні.

Метою роботи є аналіз підходів в теорії транспортування та розробка застосунку для розрахунку оптимального плану перевезень ресурсів від постачальників до споживачів різними методами.

Для пошуку опорних планів реалізовані методи [1]:

1. Метод північно-західного кута.
2. Метод найменшої вартості.
3. Методи мінімуму в рядку і мінімуму стовпці.
4. Метод подвійної переваги.
5. Метод апроксимації Фогеля.

Для обчислення оптимальних планів в програмному засобі реалізовані наступні методи:

- Розподільний метод [4].
- Метод потенціалів.
- Симплекс-метод [1].

- Генетичний алгоритм [5].
- Пошук максимального потоку мінімальної вартості [3].

Формально математична модель [1] описується наступним чином: потрібно визначити план транспортування  $X = \{x_{ij}\}, i = \underline{1}, \underline{m}, j = \underline{1}, \underline{n}$ , який задовольняє наступні умови:

$$\left\{ \begin{array}{l} \sum_{j=1}^n x_{ij} = a_i, i = \underline{1}, \underline{m} \\ \sum_{i=1}^m x_{ij} = b_j, j = \underline{1}, \underline{n} \\ x_{ij} \geq 0, \forall i, j \end{array} \right.$$

Транспортна задача з неправильним балансом приводиться до збалансованого вигляду. Перетворення виконується шляхом введення фіктивного постачальника/споживача.

Якщо в таблиці розв'язку менше ніж  $m+n-1$  зайнятих клітин, то він називається виродженням. Щоб побороти виродженість потрібно додати нескінченно мале значення  $\epsilon$  в незайняту клітку, так щоб вона не створювала із зайнятими клітками циклу.

Щоб зменшити значну кількість кроків, необхідних для отримання оптимального рішення, доцільно перейти до опорного плану, що є близьким до оптимального. Одною з проблем на даному етапі є те, що неможливо просто передбачити чи транспортна задача матиме вироджене рішення.

Часто має місце наступна ситуація: постачальник транспортує ресурси не напряму споживачу, а через деякого посередника. Такий посередник називається проміжним пунктом. В його ролі може виступати, наприклад, склад із ресурсами. У цій модифікації наявні  $p$  проміжних пунктів  $E_k, k = \underline{1}, \underline{p}$  і додаткові потреби в ресурсі  $e_k$ .

Математична модель:

$$\left\{ \begin{array}{l} \sum_{k=1}^p x_{ki} = a_i, i = \underline{1}, \underline{m} \\ \sum_{k=1}^p y_{kj} = b_j, j = \underline{1}, \underline{n} \\ \sum_{i=1}^m x_{ki} - \sum_{j=1}^n y_{kj} = e_k, k = \underline{1}, \underline{p} \\ x_{ki} \geq 0, \forall i, k \\ y_{kj} \geq 0, \forall k, j \end{array} \right.$$

$$L(X) = \sum_{i=1}^m \sum_{k=1}^p c_{ki}^{(1)} x_{ki} + \sum_{k=1}^p \sum_{j=1}^n c_{kj}^{(2)} y_{kj} \rightarrow \min$$

У модифікації транспортної задачі з проміжними пунктами та заборонаю перевезень існують сценарії, коли певні маршрути перевезень заборонені або недопустимі, і тому не можуть бути включені в оптимальний план перевезень.

Багатоіндексні транспортні задачі враховують неоднорідність типів ресурсів, які треба розподілити. Також може братись до уваги неоднорідність засобів транспорту чи якісь інші змінні. Дана модифікація транспортної задачі вирішується за допомогою узагальнення методу потенціалів. Також задачу можна розділити на підзадачі і вирішити симплекс-методом.

Існують варіації транспортних задач, у яких цільова функція має бути максимізована, а не мінімізована. Така модифікація доцільна коли потрібно

отримати максимальний прибуток від поставок ресурсу. Ці задачі можна вирішити, перетворивши задачу максимізації в задачу мінімізації.

Для перевірки оптимальності розв'язку використовують означений цикл. Якщо в циклі позначити кутові клітки з непарними номерами знаком «плюс», а клітки з парними номерами знаком «мінус», то цей цикл називається означеним. Для нього характерне поняття перерозподілу – збільшення величини змінних у клітках, позначених знаком «плюс», і зменшення величини у клітках, позначених знаком «мінус», на задану величину.

У методі потенціалів для оптимального розв'язку існують потенціали постачальників  $u_i, i=1, m$  і потенціали споживачів  $v_j, j=1, n$ . Згадані потенціали задовольняють наступні умови:

$$u_i + v_j \leq c_{ij}, x_{ij} = 0$$

$$u_i + v_j = c_{ij}, x_{ij} > 0$$

Транспортну задачу можна представити і вирішити як задачу теорії графів [3]. Розглядається двочастковий граф, у якому пункти постачальників перебувають у верхній частці, а пункти споживання у нижній. Пункти постачальників та споживачів попарно з'єднуються ребрами нескінченної пропускної спроможності та вартості.

Панель з користувацьким інтерфейсом застосунку містить вкладки «Вхідні дані» (рисунко 1), «Балансування задачі», «Опорний розв'язок», «Оптимальний розв'язок» (рисунко 2), «Результат».

Вхідні дані		Балансування задачі		Опорний розв'язок		Оптимальний розв'язок		Результат	
Кількість поставників:	4	Оновити	Кількість споживачів:	5	Оновити	Постачальник 1	Споживач 1	5	
#1	Постачальник 1	24	#1	Споживач 1	21	Постачальник 1	Споживач 2	8	
#2	Постачальник 2	20	#2	Споживач 2	12	Постачальник 1	Споживач 3	9	
#3	Постачальник 3	35	#3	Споживач 3	3	Постачальник 1	Споживач 4	2	
#4	Постачальник 4	18	#4	Споживач 4	7	Постачальник 1	Споживач 5	3	
			#5	Споживач 5	38	Постачальник 2	Споживач 1	6	
						Постачальник 2	Споживач 2	9	
						Постачальник 2	Споживач 3	10	
						Постачальник 2	Споживач 4	2	
problem.json	Завантажити		Метод північно-західного кута		Розподільний метод		Min	Знайти розв'язок	

Рисунок 1 – Вхідні дані

Вхідні дані	Балансування задачі		Опорний розв'язок	Оптимальний розв'язок	Результат		
Попередній крок		8 / 14			Наступний крок		
	Споживач 1	Споживач 2	Споживач 3	Споживач 4	Споживач 5	Залишок	
Постачальник 1	-	-	-	-	24	-	24
	5	8	9	2	3	0	
Постачальник 2	-	-	-	7	-	13	20
	6	9	10	2	5	0	
Постачальник 3	21	11	3	-	-	-	35
	3	9	4	7	5	0	
Постачальник 4	-	1	-	-	14	3	18
	15	2	9	4	4	0	
	21	12	3	7	38	16	

Рисунок 2 – Оптимальний розв'язок

Отже, дослідження та розвиток методів розв'язання задачі транспортування ресурсів споживачам залишається актуальним завданням і має великий потенціал для покращення логістичних процесів та ефективного розподілу ресурсів. Інновації в цій галузі можуть сприяти підвищенню продуктивності та зменшенню витрат в бізнесі та інших сферах економіки.

#### Перелік посилань:

1. Introduction To Operations Research. Frederick S. Hillier, Gerald J. Lieberman, 1995.
2. Computational Optimal Transport. Gabriel Peyré, Marco Cuturi. 2018.
3. L. R. Ford Jr., D. R. Fulkerson. Flows in Networks. 1962.
4. Stepping Stone | Transportation Problem [Електронний ресурс] – <https://www.educationlessons.co.in/notes/stepping-stone>
5. Genetic Algorithm [Електронний ресурс] – [https://en.wikipedia.org/wiki/Genetic\\_algorithm](https://en.wikipedia.org/wiki/Genetic_algorithm)



УДК 004.4

Міроник М.В., Праворська Н.І.

*Хмельницький національний університет*

## **ІГРОВИЙ ЗАСТОСУНОК В ЖАНРІ «ROGUE-LITE» З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ UNITY**

*Розглянуто аспекти розробки ігрового застосунку в жанрі «Rogue-lite» з використанням технології «Unity». Запропонована розробка захопливого геймплею, який базується на випадковому генеруванні рівнів та послідовному покращенні персонажа, при цьому зберігаючи елементи ризику і випадковості, які характеризують цей жанр. В процесі розробки було оглянуто недоліки та переваги популярних відео-ігор та з'ясовано їх позитивні та негативні сторони. На основі цього було розроблено вимоги до розроблюваного додатку. Визначено основні модулі, які допоможуть при подальшій роботі над застосунком.*

*Aspects of developing a game application in the "Rogue-lite" genre using the "Unity" technology are considered. It is proposed to develop an exciting gameplay that is based on the random generation of levels and the consistent improvement of the character, while maintaining the elements of risk and randomness that characterize this genre. In the development process, the disadvantages and advantages of popular video games were reviewed and their positive and negative aspects were clarified. Based on this, the requirements for the developed application were developed. The main modules that will help in further work on the application are defined.*

З початком глобалізації та розвитком мережі інтернет науковцями по всьому світу було зафіксовано розвиток таких суспільних проблем як депресія, невпевненість у собі, а також загальна невдоволеність своїм життям.

Як правило такі проблеми вирішуються за допомогою лікарів або з використанням медикаментів. На жаль такі методи, як правило, лише тимчасово призупиняють дії таких психічних захворювань.

Саме тому, деякі науковці та ентузіасти вирішили перевірити чи здатні відео-ігри допомогти в боротьбі з даними хворобами, що було підтверджено не одноразово незважаючи на загальне ставлення до відео-ігор, як до чогось шкідливого.

Запропонована прикладна програма допоможе відволіктись від хвилювань в зовнішньому світі, а також дати собі змогу розслабитись.

В ході розробки програмного застосунку було проведено аналіз ринку ігрових додатків, для виділення позитивних елементів які потрібно реалізувати в майбутньому ігровому застосунку.

Було виділено двох найпопулярніших конкурентів, як з ринку персональних комп'ютерів, так і з ринку смартфонів аби поєднати найкращі аспекти з двох ігор.

Таблиця 1 – Аналіз конкурентів

Конкурент	Опис
«Enter the Gungeon»	Відео-гра жанру «Rogue-lite» з особливістю «Bullet hell». Даний ігровий застосунок виділяється приємною та атмосферною графікою, важкими, але захоплюючими ворогами та простим, але зрозумілим сюжетом.
«Remixed Dungeon: Pixel Dungeon»	Мобільний ігровий застосунок, який виділяється простою піксельною графікою, покроковими ходами та складністю. Гравцю потрібно досліджувати безкінечно генеровані підземні лабіринти відбиваючись від ворогів та слідкуючим за станом свого героя.

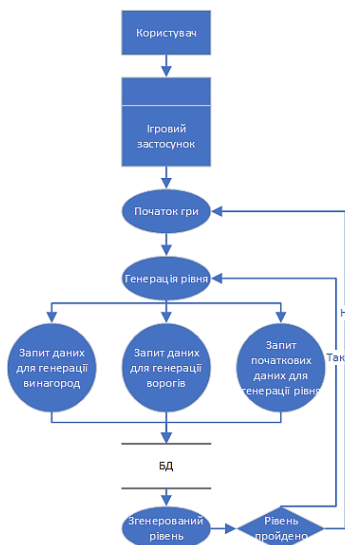


Рисунок 1 – Діаграма потоків даних

#### Переваги «Enter the Gungeon»:

- 1) стиль графіки – приємний та унікальний стиль ворогів та всесвіту, робить гру впізнаваною та легкою для запам'ятовування;
- 2) сюжет – простий, але зрозумілий, де гравцю позначають його мету та ціль, після чого відпускають досліджувати світ гри;
- 3) бойова система – динамічна та проста для розуміння, але складна в освоєнні;
- 4) елемент випадковості – результативність проходження підземелля, в більшості випадків залежить від того, чи віднайде сильну зброю гравець в скринях які генеруються на рівні;

5) захоплюючі боси та вороги – боси та вороги, примушують гравця обдумувати свої наступні дії наперед, що певним чином може нагадувати партію в шахи, адже кожна дія може стати фатальною.

Переваги «Remixed Dungeon: Pixel Dungeon»:

1) простота – на відміну від попереднього ігрового застосунку, дана відео-гра проста, як зі сторони графічного оформлення, так і ігрових механік;

2) «вбивач часу» – даний застосунок доступний, як на смартфонах так і на персональних комп'ютерах, що дозволяє гравцеві грати майже в будь-який час, незважаючи де він знаходиться;

3) доступність – ігровий застосунок повністю безкоштовний та займає мало місця на електронних пристроях;

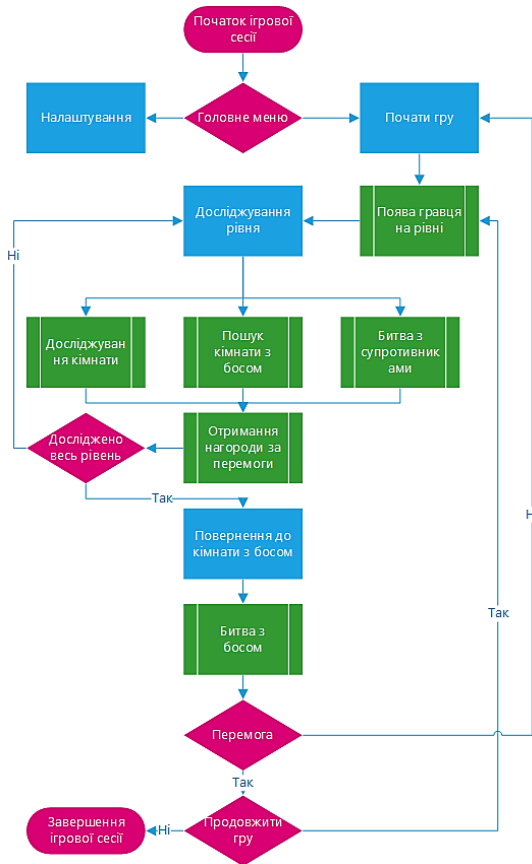


Рисунок 2 – Взаємодія користувача з ігровим застосунком

Мета запропонованого для розробки проекту полягає в розробці захопливого ігрового застосунку в жанрі «Rogue-lite» з використанням технології «Unity». При розробці важливо було створити захопливий світ, де гравці матимуть можливість безкінечно досліджувати випадково генеровані рівні, стикатися з низкою викликів і небезпек, які стануть їхнім шляхом, що в майбутньому допоможе гравцям розслабитись та дати своєму мозку відпочити.

На рисунку 1 представлена діаграма потоків даних, яка допоможе провести візуалізацію процесів обробки даних. На ній показано, звідки надходять дані, які види діяльності обробляють дані, і як використовуються вихідні результати діяльністю або зовнішнім суб'єктом.

Взаємодія користувача з ігровим застосунком показана на рисунку 2. Ця блок-схема стане основою для подальшої розробки програмного застосунку, написанню коду і тестування.

Розробка буде проводитись на базі технології ігрового рушія «Unity», при підтримці мови програмування C# та використанні життєвого циклу ітераційної та інкрементної розробки, що дозволяє розробнику створити ігровий застосунок найвищої якості та надати гравцям незабутню подорож у цьому захоплюючому ігровому жанрі.

Отже, запропонований ігровий застосунок покликаний стати не лише розважливим дозвіллям для гравців, але й підтримкою для тих, хто шукає втіху та відволікання від сучасних життєвих труднощів. Дана відео-гра розвиватиме навички прийняття рішень, допомагатиме виробити стратегічне мислення та навички співпраці в режимі спільної гри.

Завдяки ретельному аналізу конкурентів, було враховано найкращі аспекти відомих ігор і поєднано їх у розроблюваному застосунку. Відповідно, дана прикладна програма пропонує баланс між простотою та складністю, доступністю та викликами, що робить її привабливою для гравців різних рівнів. Будучи способом втекти від проблем реальності, цей ігровий застосунок збагачує дозвілля та надає можливість зануритися в захоплюючий світ пригод.

### Перелік посилань

1. HOW VIDEO GAMES CAN TEACH YOUR BRAIN TO FIGHT DEPRESSION. URL: <https://paintedbrain.org/blog/how-video-games-can-teach-your-brain-to-fight-depression#:~:text=Top%20Benefits%20Of%20Playing%20Video,help%20you%20in%20real%20life>.
2. Are There Mental Health Benefits of Video Games?. URL: <https://www.webmd.com/mental-health/mental-health-benefits-of-video-games>
3. Computer and Video Games in Mental Health. URL: [https://www.researchgate.net/publication/370396965\\_Computer\\_and\\_Video\\_Games\\_in\\_Mental\\_Health#:~:text=Traditionally%2C%20the%20research%20has%20focused,wide%20range%20of%20cognitive%20skills](https://www.researchgate.net/publication/370396965_Computer_and_Video_Games_in_Mental_Health#:~:text=Traditionally%2C%20the%20research%20has%20focused,wide%20range%20of%20cognitive%20skills).

УДК 004.4

Морський О.О., Лукманов Т.К., Манзюк Е.А.

Хмельницький національний університет

## **ВИЯВЛЕННЯ ЗАБРУДНЕНЬ НАВКОЛИШНЬОГО СЕРЕДОВИЩА МЕТОДАМИ ШТУЧНОГО ІНТЕЛЕКТУ З ВИКОРИСТАННЯМ СУПУТНИКОВИХ ЗОБРАЖЕНЬ**

*Розроблено та реалізовано систему виявлення забруднень навколишнього середовища за допомогою методів штучного інтелекту, які базуються на аналізі супутникових зображень та виявленні негативних впливів на довкілля. Було сформовано множину ознак і параметрів, які використовуються як вхідні дані для методів штучного інтелекту. В рамках дослідження використовувалися як методи з наявністю даних еталону, так і методи без нього для виявлення забруднень на поверхні Землі. Результати дослідження підтвердили високу ефективність запропонованих методів у виявленні та моніторингу забруднень навколишнього середовища за допомогою супутникових зображень.*

*The system of environmental pollution using artificial intelligence methods, which are based on the analysis of satellite images and negative effects on the environment, has been identified, developed and implemented. A set of features and parameters were formed, which are used as input data for artificial intelligence methods. As part of the study, both methods with the availability of training data and methods without it were used to detect pollution on the Earth's surface. The results of the study confirmed the high efficiency of the proposed methods of detection and monitoring of environmental pollution using satellite images.*

У сучасному суспільстві проблема незаконного захоронення відходів наростає, приносячи серйозні наслідки як для навколишнього природного середовища, так і для економіки [1, 2]. Ця актуальна проблема вимагає термінового розв'язання, а одним з ефективних методів її подолання є застосування глибокого навчання, зокрема з використанням згорткових нейронних мереж (CNN) [3].

Основною метою даного дослідження є аналіз можливостей використання сучасних методів глибокого навчання, в поєднанні з супутниковими знімками, для точної ідентифікації нелегальних сміттєзвалищ. Ця мета включає два ключових аспекти: перше - розпізнавання на супутникових знімках зображень звалищ і відсутність таких звалищ, а друге - класифікацію різних видів сміття на супутникових знімках, де виявлено наявність сміттєзвалищ.

CNN-моделі виявляються корисними у процесі класифікації незаконно захоронених відходів на основі аналізу супутникових знімків. Сам процес навчання передбачає тренування цих моделей на анотованих супутникових зображеннях, включаючи ті, що містять відзначені звалища, а також зображення, де ці звалища відсутні. Цей підхід надає змогу нейронним мережам надійно розпізнавати та класифікувати незаконно захоронені матеріали з високою точністю.

Слід зазначити, що цей підхід виявляється перспективним у контексті боротьби із проблемою незаконного захоронення відходів, сприяючи водночас переходу до циркулярної економіки, де ресурси використовуються більш обережно

та раціонально. Успішність такої моделі залежить від розміру набору даних і тривалості процесу навчання, але за належної настройки параметрів вона може досягти хорошої точності у класифікації, що зміцнює перспективи вирішення даної глобальної проблеми.

Отже, слід відзначити, що розроблена модель глибокого навчання на основі згорткових нейронних мереж є перспективним інструментом у розв'язанні проблеми незаконного захоронення відходів і сприяє створенню більш сталого та екологічно чистого суспільства.

Слід враховувати, що ефективність такої моделі значно впливає на розмір наявного набору даних та тривалість процесу її навчання. З належними налаштуваннями параметрів моделі та використанням об'ємного та різноманітного набору даних, можна досягти належної точності у класифікації. Це, у свою чергу, сприяє більш ефективному вирішенню проблеми незаконного захоронення відходів та сприяє переходу до більш сталої та циркулярної споживчої парадигми.

Для покращення точності класифікації, було проведено навчання кількох моделей на відносно невеликому наборі даних, який включав два зовсім різних класи відходів. На жаль, цей набір даних був значно обмеженим як за обсягом доступних зображень, так і за рівнем докладних анотацій.

Моделі були навчені розрізняти два різних класи відходів на основі цього датасету. Застосовуючи методи розширення даних для компенсації цього обмеження, було досягнуто результат з точністю класифікації на рівні 72%.

В ході дослідження використовували обмежений обсяг даних, і це, безумовно, є одним з ключових обмежень. Проте, важливо підкреслити, що розвиток глибоких нейронних мереж CNN в поєднанні з високороздільними супутниковими зображеннями має потенціал стати важливим напрямком у вирішенні проблеми незаконного захоронення відходів. Звісно, для досягнення цієї мети необхідно подолати ряд обмежень та постійно вдосконалювати методологію та підходи.

Отже, майбутні можливості у цьому напрямку передбачають розширення доступу до великих обсягів даних і докладних зображень з високою роздільною здатністю, що дозволить поліпшити точність та надійність моделей глибокого навчання. Додавання нових підходів і методів до обсягу досліджень може відкрити нові можливості у боротьбі з проблемою незаконного захоронення відходів та позитивно вплинути на сталість та раціональне використання ресурсів.

### Перелік посилань

1. D'Amato A., Mazzanti M., Nicolli F., Zoli M. Illegal waste disposal: Enforcement actions and decentralized environmental policy. *Socio-Economic Planning Sciences*. 2018. Vol. 64. Pp. 56–65. URL: <https://doi.org/10.1016/j.seps.2017.12.006>.
2. Shittu O. S., Williams I. D., Shaw P. J. Global E-waste management: Can WEEE make a difference? A review of e-waste trends, legislation, contemporary issues and future challenges. *Waste Management*. 2021. Vol. 120. Pp. 549–563. URL: <https://doi.org/10.1016/j.wasman.2020.10.016>.
3. Song F., Zhang Y., Zhang J. Optimization of CNN-based Garbage Classification Model: *Proceedings of the 4th International Conference on Computer Science and Application Engineering*, New York, NY, USA, Association for Computing Machinery, 2020. Pp.1–5. URL: <https://doi.org/10.1145/3424978.3425089>.

УДК 004.8

Муляр Е.Р., Багрій Р.О., Пасічник О.А., Манзюк Е.А.

*Хмельницький національний університет*

## **МЕТОД ВИЯВЛЕННЯ ОЗНАК НАСИЛЬСТВА У ВІДЕОМАТЕРІАЛАХ НЕЙРОМЕРЕЖЕВИМИ ЗАСОБАМИ**

*Проблема виявлення насильства у відеопотоці є актуальною в сучасному світі, де зростає кількість відеоматеріалів з насильницькими сценами. Виявлення та реагування на такі сцени мають велике значення для забезпечення безпеки громадських просторів та захисту прав людини. Запропоновано метод виявлення ознак насильства у відеоматеріалах нейромережевими засобами. Метод відкриває шлях до розв'язання завдань виявлення ознак насильства на відеоматеріалах у реальному часі, а також фільтрації контенту на потокових мультимедійних платформах.*

*The problem of detecting violence in a video stream is relevant in the modern world, where the number of videos with violent scenes is growing. Detecting and responding to such scenes is important for ensuring the safety of public spaces and protecting human rights. The paper proposes a method for detecting signs of violence in video materials using neural network tools. The method opens the way to solving the problems of detecting signs of violence in real-time video materials, as well as filtering content on streaming multimedia platforms.*

### **Вступ**

Сьогодні для протидії такій суспільній проблемі як насильство розпочали активно використовувати системи відеоспостережень. Такі країни, як Китай та Південна Корея, є лідерами у встановленні камер відеоспостереження, і результати використання цих систем є вражаючими. У Китаї рівень насильства у громадських місцях знизився на 60%, а в Південній Кореї - на приблизно 50% [1]. Однак, ці системи мають деякі недоліки. Основною проблемою є людський фактор, зокрема неуважність та недбалість операторів-спостерігачів. Зазвичай оператор може ефективно контролювати лише обмежену кількість камер відеоспостереження. Однак, коли кількість камер перевищує їх межі, оператори можуть допускати помилки або пропускати випадки насильства. Для вирішення цієї проблеми сьогодні активно використовуються передові інформаційні технології, зокрема штучні нейронні мережі. Завдяки цим технологіям, системи відеоспостереження можуть автоматично аналізувати великий обсяг відеоданих і виявляти потенційні випадки насильства. Штучний інтелект допомагає зменшити навантаження на операторів і забезпечує більш точне та ефективне виявлення подій [2].

### Аналіз існуючих публікацій

Для реалізації інтелектуального відеоспостереження сьогодні активно використовують підходи модифікації та поєднання різних методів та архітектур нейромереж [3].

Прикладом такого підходу є модель нейронних мереж BiConvLSTM (Bidirectional Convolutional LSTM). Ця модель поєднує в собі два потужних компоненти: двосторонню згорткову мережу (BiConv) та рекурентну нейронну мережу LSTM (Long Short-Term Memory). BiConvLSTM використовується для аналізу послідовних даних, таких як зображення або відео, з метою виявлення шаблонів та залежностей у цих даних [4].

Іншим прикладом використання нейронних мереж для задачі виявлення насильства у відеопотоці є 3D CNN (3D Convolutional Neural Network). Дана модель являється згортковою нейронною мережею, що використовується для обробки тривимірних даних, таких як відео, медичні зображення або тривимірні моделі [5].

Приклад використання моделі BiConvLSTM наведено у роботі [6], де розглянуто підхід до виявлення насильства у відео за допомогою методу «просторово-часовий кодер». «Просторово-часовий кодер» представляє собою метод який побудований на основі декількох архітектур: BiConvLSTM, VGG13 [7] для кодування кожного відеокадру як набір карт функцій. Ці карти функцій потім передаються до BiConvLSTM для подальшого кодування у часовому напрямку відео. Виконується поелементна максимізація кодувань для створення представлення відео, яке передається класифікатору для виявлення насильства. Щодо результатів роботи даного підходу, то для набору даних «Hockey fights» точність склала 96.54%, для набору даних «Violent flows» - 92.18%.

У роботі [8] запропоновано метод до виявлення насильства у відео за допомогою 3D-CNN. 3D-CNN спочатку обробляє кожний кадр відео, використовуючи набори фільтрів для виявлення важливих ознак, таких як рух, форма та колір. Потім 3D-CNN обробляє послідовність кадрів, використовуючи 3D-фільтри. Класифікація здійснюється шляхом застосування логістичної регресії до вихідного тензора 3D-CNN. На рахунок результатів роботи даного методу, то для набору даних «Hockey fights» точність склала 98.3%, для набору даних «Violent flows» - 97.17%.

В наведених публікаціях не розглянуто підходи до взаємодії запропонованих методів з відеоматеріалами у реальному часі, тому виникають питання в ефективності даних підходів при роботі з відеопотоком даних в реальному часі.

**Метою роботи** є розробка методу для виявлення ознак насильства у відеоматеріалах нейромережевими засобами. Метод повинен працювати як зі статичним відеоматеріалом (відеоролик) так і з динамічним (відеопотік в реальному часі).



## Метод виявлення ознак насильства у відеоматеріалах неймережевими засобами

Робота запропонованого методу полягає в отриманні ознак насильства з кадрів вхідного відео за допомогою згорткової нейронної мережі і визначення ступеню насильства у відсотковому відношенні у відеопотоці за допомогою SVM (методу опорних векторів). На рисунку 1 представлено архітектуру даного методу.

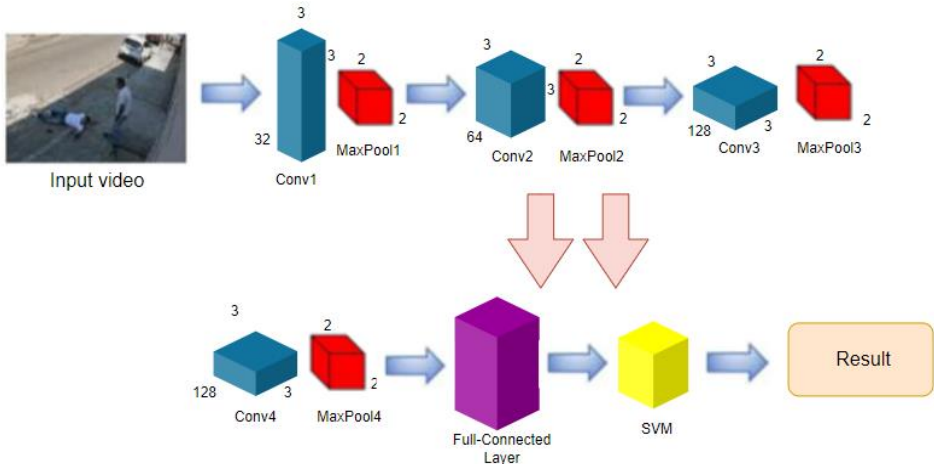


Рисунок 1 – Архітектура запропонованого методу

### Етап 1 – Отримання кадрів із вхідного відеоматеріалу

Необхідно розбити вхідний відеоматеріал на послідовність кадрів та перетворити кожен кадр у карту зображень.

### Етап 2 – Операція згортки

На даному етап необхідно виконати операцію згортки на вхідне зображення для того, щоб отримати карту ознак. Для виконання даної операції використовуються фільтри (матриця параметрів). Для даної нейронної мережі було обрано 4 рівня фільтрів по 32, 64, 128, 128 фільтрів на кожному рівні відповідно. Формування карти ознак можна здійснити за допомогою наступної математичної формули:

$$M(i, j) = (K * X)(i, j) = \sum_m \sum_n K(m, n) X(i - m, j - n), \quad (1)$$

де  $M$  – елемент карти ознак з координатами  $i$  та  $j$ ,  $X$  – вхідне зображення,  $K$  – детектор ознак,  $(m, n)$  – розмірності детектора ознак.

### Етап 3 – Операція максимального об'єднання

Максимальне об'єднання являється операцією, яка об'єднує елементи в межах фільтра на карті ознак і вибирає найбільший елемент. Тобто, після проходження через шар максимального об'єднання, отримується нова карта ознак, яка містить найбільш помітні ознаки з попередньої карти ознак. Виконати дану операцію можна за допомогою наступної формули:

$$p(i, j) = \max_{i,j}(x(i - m, j - n)), \quad (2)$$

де  $p(i, j)$  – значення елемента поточного рівня з координатами  $i$  та  $j$ ,  $x$  – вхідні дані з попередніх рівнів,  $(m, n)$  – розмірність рецептивного поля.

### Етап 4 – Повнозв'язний рівень

Повнозв'язний рівень представляє собою модель багаторівневого перцептрона, де всі нейрони з наступного шару з'єднані з нейронами попереднього шару. Цей рівень використовуються на передостанньому етапі роботи мережі для підготовки результатів на виході мережі. На даному рівні виконується обчислення скалярного добутку даних та параметрів з додаванням зсуву.

### Етап 5 – Класифікація отриманих ознак за допомогою SVM

Метод опорних векторів (SVM) використовується для знаходження параметрів гіперплощини у великому чи нескінченному вимірному просторі, яка може служити для класифікації. Головна ідея полягає в тому, щоб знайти гіперплощину, яка має найбільшу відстань до найближчих навчальних точок будь-якого класу. На виході класифікатор SVM видає оцінку, яка представляє ймовірність того, що вхідні дані належать до певного класу (насилницького або не насилницького).

Для того, щоб запропонований метод міг працювати з відеоматеріалом в реальному часі під час процесу навчання нейронної мережі використовувався метод fine-tuning. Суть даного методу полягає в тому, що нейромережу спочатку навчають на наборі даних готових відео, а потім поступово додають до набору даних відеопотоки у реальному часі. Це допомагає нейромережі навчитися розпізнавати насильство в умовах шуму, швидкої зміни та різноманітності.

### Аналіз ефективності створеного методу

Для того, щоб оцінити ефективність роботи запропонованого методу, проведено декілька експериментів щодо двох наборів даних для виявлення насильства: «Hockey fights» [9], «Livestream» [10]. Оцінка ефективності методу базується на визначенні загальної точності для кожного набору даних.

Загальна точність для набору даних «Hockey fights» склала 98.5%, представлено на рисунку 2.

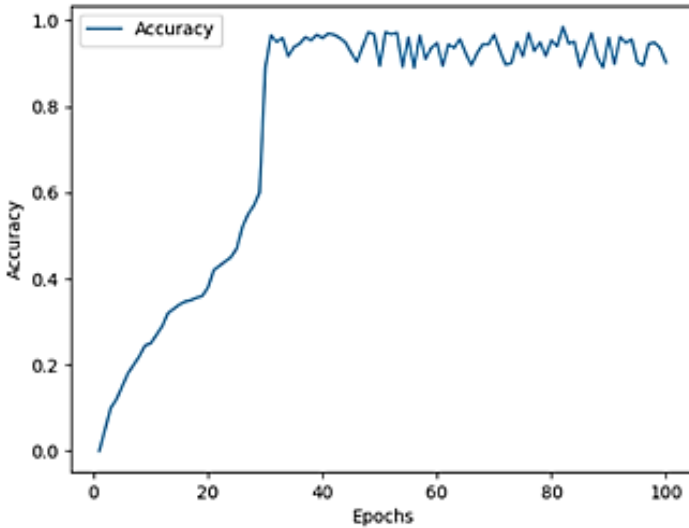


Рисунок 2 – Загальна точність набору даних «Hockey fights»

Загальна точність для набору даних «Livestream» склала 87.4%, представлено на рисунку 3.

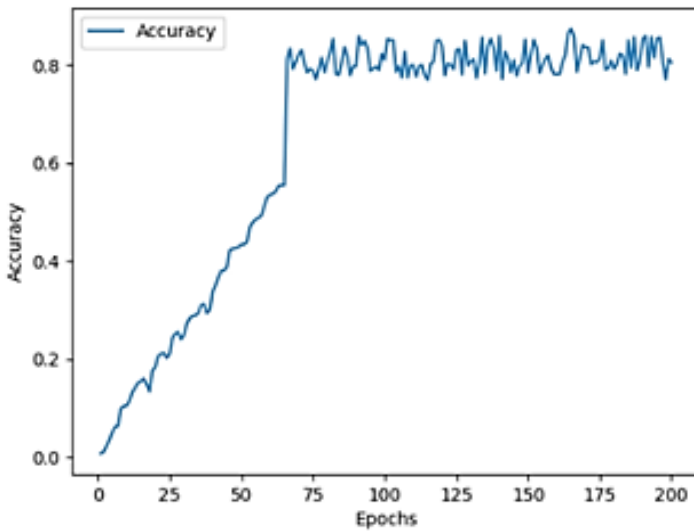


Рисунок 3 – Загальна точність набору даних «Livestream»

## Висновки

Отже, запропонований метод для виявлення ознак насильства у відеоматеріалах неймережевими засобами дозволяє визначити ступінь насильницького характеру у відсотковому відношенні, відповідно на статичних відеоматеріалах так і на динамічних (відеопотік). Подальші дослідження спрямовані на пришвидшення роботи та покращення точності запропонованого методу для набору даних, які пов'язані з насильницькими діями у реальному часі.

## Перелік посилань

1. Violence a global public health problem URL: <https://www.scielo.br/j/csc/a/3hrn64cpBqBFb9mNfP4KGXr/?lang=en>
2. Використання технологій штучного інтелекту протидії злочинності URL: [https://ivpz.kh.ua/wp-content/uploads/2020/12/Матеріали-семінару\\_Використання-техн-штучного-інтел\\_5.11.2020.pdf](https://ivpz.kh.ua/wp-content/uploads/2020/12/Матеріали-семінару_Використання-техн-штучного-інтел_5.11.2020.pdf)
3. A CNN-RNN Combined Structure for Real-World Violence Detection in Surveillance Cameras URL: <https://www.mdpi.com/2076-3417/12/3/1021>
4. NABNet: A Nested Attention-guided BiConvLSTM network URL: <https://www.sciencedirect.com/science/article/abs/pii/S1746809422007017>
5. 3D Convolutional Neural Network — A Guide for Engineers URL: <https://www.neuralconcept.com/post/3d-convolutional-neural-network-a-guide-for-engineers>
6. Convolutional LSTM for the Detection of Violence in Videos URL: [https://openaccess.thecvf.com/content\\_ECCVW\\_2018/papers/11130/Hanson\\_Bidirectional\\_Convolutional\\_LSTM\\_for\\_the\\_Detection\\_of\\_Violence\\_in\\_Videos\\_ECCVW\\_2018\\_paper.pdf](https://openaccess.thecvf.com/content_ECCVW_2018/papers/11130/Hanson_Bidirectional_Convolutional_LSTM_for_the_Detection_of_Violence_in_Videos_ECCVW_2018_paper.pdf)
7. Simonyan, K., Zisserman, A.: Very deep convolutional networks for large-scale image recognition. In International Conference on Learning Representations (2015) URL: <http://arxiv.org/abs/1409.1556>
8. Efficient Violence Detection Using 3D Convolutional Neural Networks URL: [https://www.researchgate.net/profile/Tanfeng-Sun/publication/337537845\\_Efficient\\_Violence\\_Detection\\_Using\\_3D\\_Convolutional\\_Neural\\_Networks/links/5f75e252a6fdcc00864ccb95/Efficient-Violence-Detection-Using-3D-Convolutional-Neural-Networks.pdf](https://www.researchgate.net/profile/Tanfeng-Sun/publication/337537845_Efficient_Violence_Detection_Using_3D_Convolutional_Neural_Networks/links/5f75e252a6fdcc00864ccb95/Efficient-Violence-Detection-Using-3D-Convolutional-Neural-Networks.pdf)
9. Hockey Fight Detection Dataset URL: <https://paperswithcode.com/dataset/hockey-fight-detection-dataset>
10. Livestream URL: <https://www.twitch.tv/directory/category/just-chatting>

УДК 004.896

Наймитенко С.І., Подорожняк А.О.

*Національний Технічний Університет  
“Харківський політехнічний інститут”*

## **РОЗРОБКА ТА ДОСЛІДЖЕННЯ СЕРВІСУ ДЛЯ РОЗУМНОГО ПРОТЕЗУ**

*Розглянуто прикладні аспекти розробки та дослідження бюджетного та простого у виробництві протезу верхніх кінцівок, а саме руки та передпліччя. Наведено результати аналізу функціонування розумного протезу що управляється мікропроцесором. Запропоновано тип протезу що буде розроблятися, виконано підбір компонентів відповідно до поставленої задачі. Наведено результати тестування розробленого сервісу на основі цифрової та аналогової версії.*

*The applied aspects of the development and research of a budget and easy-to-produce prosthesis of the upper limbs, namely the hand and forearm, are considered. The results of the analysis of the functioning of a smart prosthesis controlled by a microprocessor are given. The type of prosthesis to be developed is proposed, the components are selected in accordance with the task. The results of testing the developed service based on the digital and analog versions are given.*

На даний час велика частина наших захисників що боронять територіальну цілісність України зазнали тяжких травм які також можуть бути пов'язані з втратою кінцівок, а саме рук. На жаль багато хто не може дозволити собі своєчасно професійне протезування яке коштує тисячі доларів. До того ж на саме протезування є великі черги і людина може чекати навіть роки доки отримає свій протез, а за такий час можливо втратити навіть теоретичну можливість використання травмованою людиною біонічного протезу через часткову атрофію залишків нервових закінчень [1, 2]. Саме тому було остаточно вирішено питання із темою дослідження.

Метою роботи є розробка бюджетного та швидкого у виготовленні протеза який може покрити хоча б мінімальні потреби людини у повсякденному житті як, наприклад тримання столових приборів під час приймання їжі, відкриття дверей чи тримання неважких предметів.

Для початку розберемося з начинкою самого протезу. Нам потрібно п'ять сервоприводів котрі будуть відповідати за кожний палець нашого протезу. Сигналом для наших приводів будуть імпульси котрі будуть зчитуватись датчиками під час скорочення залишків м'язів передпліччя [3]. Для контролю над цим всім буде використовуватися мікроконтролер Arduino або інший більш бюджетний

контролер. Джерелом живлення для цього всього буде літій-іонний акумулятор, який можна буде заряджати за допомогою звичайної micro usb зарядки (рисунок 1).

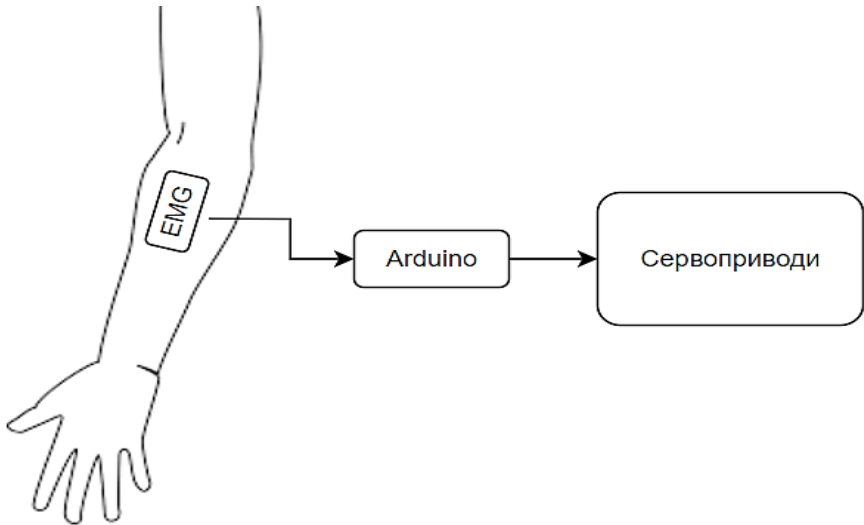


Рисунок 1 – Пояснення роботи сервісу

Для відтворення самої кінцівки ми створюємо її модель. Беремо міцний пластик та на його основі за допомогою 3D принтера друкуємо кінцівку із заготовленої моделі. В самому створеному протезу ми фіксуємо всі внутрішні елементи. Фіксуємо виріб на передпліччі. Протез готовий до використання.

Робота алгоритму створеної мікроконтролерної системи запропонованого розумного протезу виглядає наступним чином. Після запуску та ініціалізації необхідних змінних програмне забезпечення зчитує сигнал з пінів електроміографічного (ЕМГ)-датчика. Потім цей сигнал проходить через етапи дискретизації та додаткової фільтрації завад зчитування міосигнала з використанням спеціального цифрового фільтру Баттерворта 4-го порядку.

Після цього програма мікроконтролера визначає максимальний сигнал для подальшого використання при визначенні, чи виконувати рух (стиснення/розслаблення) . Рух відбувається за умов, коли користувач напружує м'язи на 2/3 від максимального значення. Окрім цього, використовуються булеві змінні для більш чіткої роботи виробу.

Узагальнена блок схема алгоритму роботи програми мікроконтролера наведена на рисунку 2.

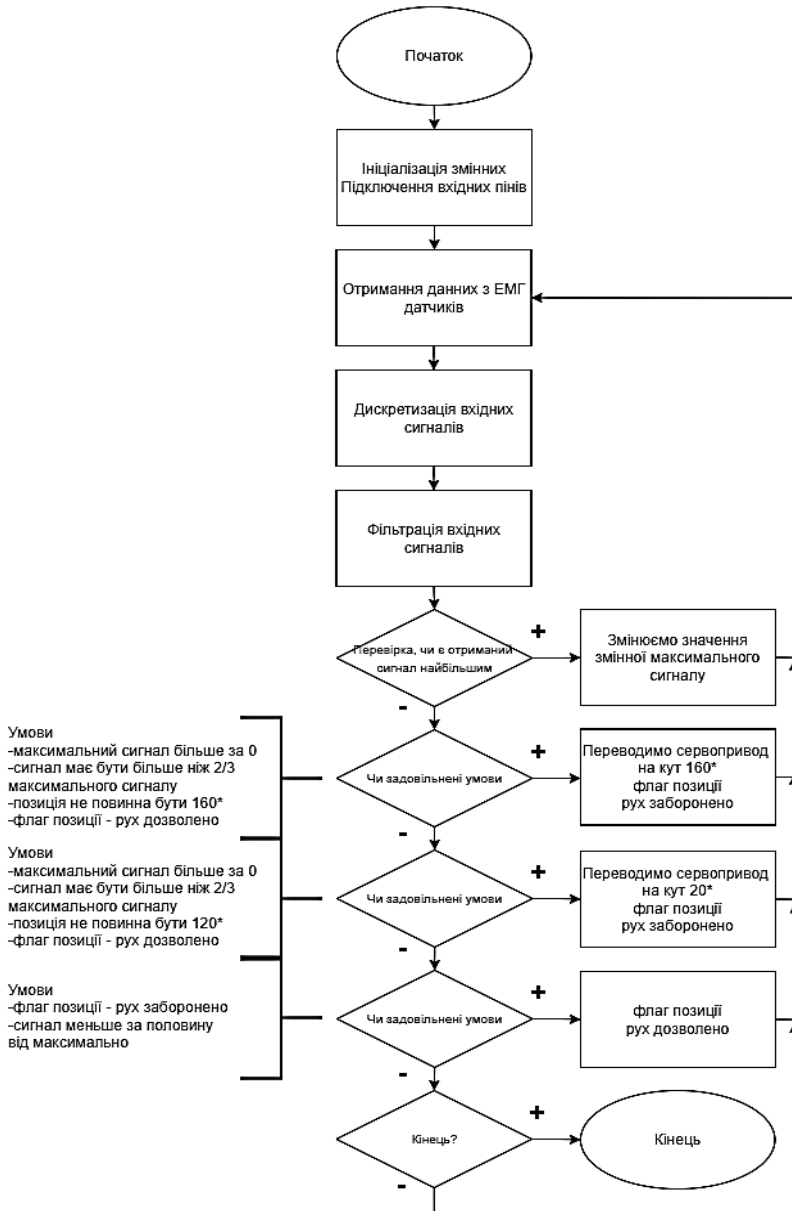


Рисунок 2 – Узагальнена блок схема алгоритму роботи програми мікроконтролера

В подальшому можна збільшити протез до ліктьового та плечового суглоба. Тим самим збільшити його функціональність. Використовувати більш складну систему із сервоприводів котрі не лише збільшать масу, що може витримати протез, але й нададуть додаткову можливість керувати кистю. Виготовлення корпусу протеза з більш стійкого матеріалу. Застосування при управлінні протезом нейромережєвих алгоритмів [4]. Але всі доопрацювання не повинні відходити від початкової ідеї – бюджетність, швидкість та доступність у виготовленні.

### Перелік посилань

1. Протези рук. Всеукраїнський центр реабілітації та протезування «Здоров'я». URL: <https://health-ukraine.com.ua/protez-ruki/>
2. Протези: як технології допомагають людям відновлювати втрачені кінцівки. URL: <https://www.youtube.com/watch?v=FISs-RHx5r0>
3. Наймитенко С. І., Подорожняк А. О. Апаратно-програмний сервіс для розумного протезу. Інформаційні технології: наука, техніка, освіта, здоров'я: Тези доповідей XXXI міжнародної науково-практичної конференції MicroCAD-2023, 17-19 травня 2023 р. Харків: НТУ “ХПІ”, 2023. С. 1125.
4. Parzhin Y., Kosenko V., Podorozhniak A., Malyeyeva O., Timofeyev V. Detector neural network vs connectionist ANNs. Neurocomputing. 2020, Vol. 414, pp. 191-203. URL: <https://doi.org/10.1016/j.neucom.2020.07.025>.



УДК 004.8

Нечепорук О.А., Ващенко С.М., Івашова Н.В.

*Хмельницький національний університет*

## **РЕКОМЕНДАЦІЙНІ СИСТЕМИ КОНТЕНТУ РІЗНОГО ТИПУ**

*Розглянуто моделі рекомендацій контенту в сучасних інформаційних та розважальних сервісах. Наведено порівняльний аналіз методів фільтрації контенту з визначенням оптимального для подальшого використання в універсальній рекомендаційній системі, що може бути використана будь-яким сервісом незалежно від типу контенту.*

*Models of recommendation content in modern information and entertainment services are considered. A comparative analysis of content filtering methods is presented with the determination of the optimal one for further use in a universal recommender system that can be used by any service regardless of the type of content.*

Сучасні інформаційні чи розважальні сервіси використовують різноманітні моделі та системи формування рекомендацій контенту для максимізації тривалості сесії користування ресурсом, що в свою чергу має позитивний вплив на монетизацію шляхом розміщення реклами чи системи платних підписок. Враховуючи специфіку застосування певних рекомендаційних моделей, в тому числі обмеження, обумовлені типом контенту – існує потреба в розробці універсальної моделі, здатної задовільнити потреби будь-яких інформаційних сервісів, незалежно від змісту даних, що рекомендуються.

Під час дослідження методів рекомендацій контенту було проаналізовано сучасні інформаційні сервіси та розважальні платформи з різним типом контенту, а саме: Netflix, YouTube, Facebook, Instagram, Spotify, Reddit. Опрацьовані дослідження присвячені порівнянню методів персоналізації контенту та їх вдосконаленню, а також праці, що стосуються створенню універсальної моделі рекомендацій на базі глибоких мереж Gated Recurrent Units (GRU) та з використанням класичного item-based алгоритму колаборативної фільтрації з властивою для нього проблемою «холодного старту».

Метою дослідження є аналіз методів рекомендацій контенту в сучасних інформаційних та розважальних сервісах, враховуючи різноманітність типів даних елементів, що рекомендуються для подальшого використання в сторонніх сервісах, незалежно від представленого в них типу контенту.

Завдяки рекомендаційним системам підвищується зручність користування сервісом для його користувачів, що покращує конкурентоспроможність ресурсу. Зважаючи на це, існує велика кількість рекомендаційних систем, створених для конкретних задач, проте їх можна класифікувати за базовими методами фільтрації (рисунком 1). [1]

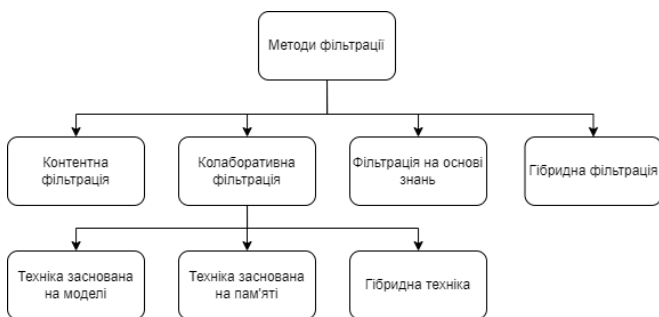


Рисунок 1 – Класифікація методів фільтрації контенту

Під час дослідження проаналізовано властивості та області застосування контентної фільтрації, колаборативних фільтрацій за техніками (заснованими на моделі, пам'яті та гібридна), фільтрацію на основі знань, а також гібридні методи в різних їх аспектах; розглянуто переваги та недоліки кожного з методів. Результати дослідження наведені у таблиці 1.

Таблиця 1 – Порівняльна таблиця методів фільтрації контенту

Метод	Переваги	Недоліки
Контентна фільтрація [2]	Точність рекомендацій за рахунок аналізу метаданих контенту.	Залежність між типом контенту та його метаданими; Вузконаправленість; Проблеми масштабування.
Колаборативна фільтрація [3]	Використовуються явні оцінки користувачів, більш персоналізовані рекомендації на основі власних і чужих вподобань.	Проблема «холодного старту»; [4] Проблема розрідженості даних через недостатню кількість явних оцінок; Проблема «сірих овець».
Фільтрація на основі знань [5]	Вирішує проблему різноманіття та дозволяє диверсифікувати рекомендації.	Вузконаправленість; Потребує часу для створення правил/кейсів які залежні від предметної області сервісу; Вимагає глибоких знань у предметній області.
Гібридні фільтрації [6]	Використання декількох методів в одній системі; Використання переваг та подолання недоліків певних методів фільтрації; Гнучкість для сервісів з різноманітним контентом.	Складність реалізації та налаштування

Очевидно, що використання декількох методів фільтрації в рамках однієї рекомендаційної системи дозволяє застосовувати всі можливі відомості як щодо

одиниць контенту, так і всієї системи сервісу, тому й існують розбіжності у класифікацій варіантів використання гібридних рекомендаційних систем.

Разом із широкою варіативністю використання гібридних методів зростає складність у реалізації, а саме: розробка математичної моделі, врахування всіх необхідних параметрів та факторів при реалізації, масштабність розробленої системи. Враховуючи широкі можливості використання різних підходів та системних даних можна розробити власну рекомендаційну систему, що буде позбавлена основних відомих недоліків окремих методів фільтрації контенту, одночасно застосовувавши їх переваги, а також маючи дані щодо типу та властивостей одиниць контенту – гнучко використати розроблену модель не обмежуючись лише знаннями про контент чи про взаємодію між користувачами та елементами систем.

Отже, для подальшої розробки універсальної рекомендаційної системи, що може бути використана будь-яким сервісом незалежно від типу контенту що рекомендується та зваживши переваги та недоліки обрано гібридну модель рекомендації контенту, що поєднує колаборативну фільтрацію на основі моделі та контентну фільтрацію. Планується реалізація системи у вигляді API для розробників веб-сервісів, а також інтерфейсу адміністрування з можливістю гнучкого налаштування параметрів моделі для покращення оцінок точності рекомендацій об'єктів із врахуванням їх властивостей та моделі взаємодії користувачів з контентом.

### Перелік посилань

1. Raghuvanshi S. K. Recommendation Systems: Techniques, Challenges, Application, and Evaluation / S. K. Raghuvanshi, R. K. Pateriya // *Soft Computing for Problem Solving*. – 2017. – Vol. 2. – Pp. 151-164. – Mode of access: [https://doi.org/10.1007/978-981-13-1595-4\\_12](https://doi.org/10.1007/978-981-13-1595-4_12).
2. Парфененко Ю. Рекомендаційна інформаційна система для пошуку відеоматеріалів / Ю. Парфененко, А. Ковтун, А. Вербицька // *Вісник КрНУ імені Михайла Остроградського*. – 2019. – Vol. 5 (118). – С. 97-102. – Режим доступу: <https://doi.org/10.30929/1995-0519.2019.5.97-102>.
3. Nilashi A. A recommender system based on collaborative filtering using ontology and dimensionality reduction techniques / A. Nilashi, O. Ibrahim, K. Bagherifard // *Expert Systems with Applications*. – February, 2018. – Vol. 92. – Pp. 507-520. – Mode of access: <https://doi.org/10.1016/j.eswa.2017.09.058>.
4. Kwan C. A Comparison Study Between Content-Based and Popularity-Based Filtering via Implementing a Book Recommendation System / C. Kwan, M. Q. Koh, M. B. Jasser // *INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING & TECHNOLOGY*. – December, 2020. – Vol. 11 (12). – Pp. 1121-1135. – Mode of access: [https://www.researchgate.net/publication/348190964\\_A\\_Comparison\\_Study\\_Between\\_Content-Based\\_and\\_Popularity-Based\\_Filtering\\_via\\_Implementing\\_a\\_Book\\_Recommendation\\_System](https://www.researchgate.net/publication/348190964_A_Comparison_Study_Between_Content-Based_and_Popularity-Based_Filtering_via_Implementing_a_Book_Recommendation_System).
5. Ameen A. Knowledge based Recommendation System in Semantic Web – A Survey / A. Ameen // *International Journal of Computer Applications* (0975 – 8887). – March, 2019. – Vol. 182 (43). – Pp. 20-25. – Mode of access: <https://doi.org/10.5120/ijca2019918538>.
6. Al Mani I. A. M. Collaborative filtering recommendation system: Comparison study / Inas Amjed Mohammed Al Mani. – May, 2018. – Pp. 1-86. – Mode of access: <https://hdl.handle.net/20.500.12939/1724>.

УДК 004.41:633

Ничік С.О., Мельников О.Ю.

Донбаська державна машинобудівна академія

## СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ОПТИМІЗАЦІЇ РОЗПОДІЛУ ПОСІВНИХ ПЛОЩ АГРАРНОГО ПІДПРИЄМСТВА

*Розглянуто проблему застосування математичного моделювання та інформаційних технологій для отримання переваг у веденні агробізнесу. Сформульовано задачу розробки системи підтримки прийняття рішень для оптимізації розподілу посівних площ аграрного підприємства. Наведено математичну та інформаційну моделі проєктованої системи та приклади розрахунків.*

*The problem of applying mathematical modeling and information technologies to obtain advantages in agribusiness is considered. The task of developing a decision-making support system to optimize the distribution of acreage of an agricultural enterprise is formulated. Mathematical and information models of the designed system and examples of calculations are presented.*

Для отримання переваг у веденні агробізнесу потрібно застосувати математичне моделювання та інформаційні технології. У низці робіт розглядаються основні моделі, що можуть бути застосовані для процесів аграрного виробництва [1], виконуються розрахунки коефіцієнта ймовірності врожайності культури [2], проводиться оптимізація виробничої структури галузі рослинництва підприємства шляхом економіко-математичного моделювання [3].

Було поставлено задачу розробки системи підтримки прийняття рішень для оптимізації розподілу посівних площ аграрного підприємства.

Створена математична модель розрахунку оптимального розподілу посівних площ. Головна проблема рослинництва – раціональний розподіл посівних площ виходячи з номенклатури культур, що вирощуються, середньої врожайності з гектара та ціни реалізації. Загальна площа сільськогосподарського підприємства  $S$  може бути записана так:

$$S = S_1 + S_2 + S_3, \quad (1)$$

де  $S_1$  – площа, що вже використовується під посіви,  $S_2$  – площа, яка ще не використовується для посівів,  $S_3$  – площа, що використовується для господарських потреб.

Для переведення якоїсь частини площі  $S_2$  у категорію  $S_1$  необхідно витратити певну суму, що виражається функцією:

$$C_{21} = F_{21}(x), \quad (2)$$

де  $x$  – це 1 га площі, що передається.

Прийmemo такі позначення:

- $x_i$  – площа, яку займає  $i$ -а культура, гектар;
- $x_{0i}$  – площа, яку займала  $i$ -а культура до цього часу, гектар;
- $u_i$  – ціна реалізації одного центнера  $i$ -ї культури, гривень;
- $y_i$  – врожайність  $i$ -ї культури, центнер / га;
- $m_i$  – матеріально-грошові витрати на 1 га посівів  $i$ -ї культури, гривень;
- $t_i$  – трудові витрати на 1 гектар посівів  $i$ -ї культури;
- $cm_i$  – вартість однієї людино-години, гривень;
- $n$  – кількість оброблюваних культур.

Тоді прибуток від продукції рослинництва можна записати у вигляді формули:

$$Z = \sum_{i=1}^n (u_i y_i - m_i - m_i c m_i) x_i - F_{21} \left( \sum_{i=1}^n x_i - S_1 \right). \quad (3)$$

Другим елементом формули (3) є додаткові витрати на освоєння цілинних та інших земель несільськогосподарського призначення, які можна використовувати за призначенням.

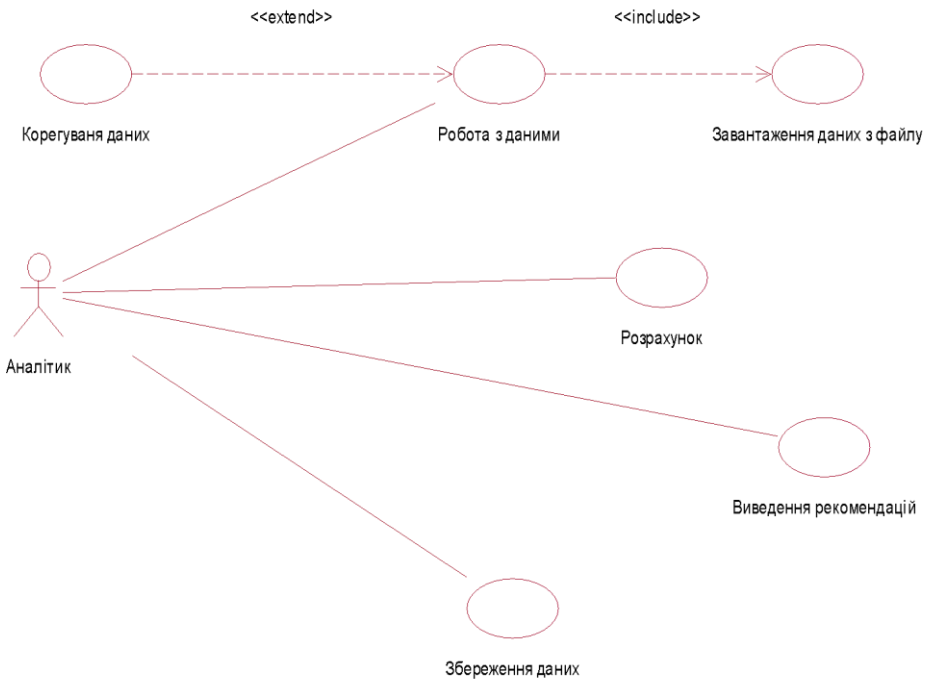


Рисунок 1 – Діаграма варіантів використання

Обмеження моделі:

- по посівній площі, що використовується;
- матеріально-грошові;
- трудові;
- рекомендація про недоцільність різкої (понад 10%) зміни посівних площ під ту саму культуру;
- невід'ємність аргументів.

Можливості проєктованої системи показано на рисунку 1, її структуру – на рисунку 2, послідовність дій – на рисунку 3 [4].

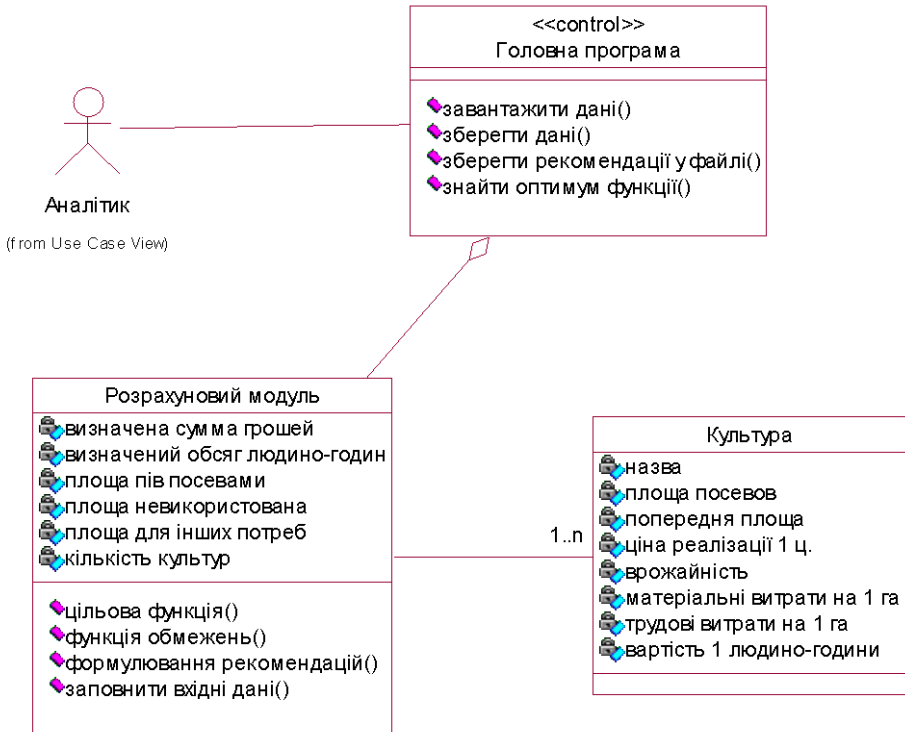


Рисунок 2 – Діаграма класів

На рисунку 4 та рисунку 5 наведено приклади роботи створеного додатка.

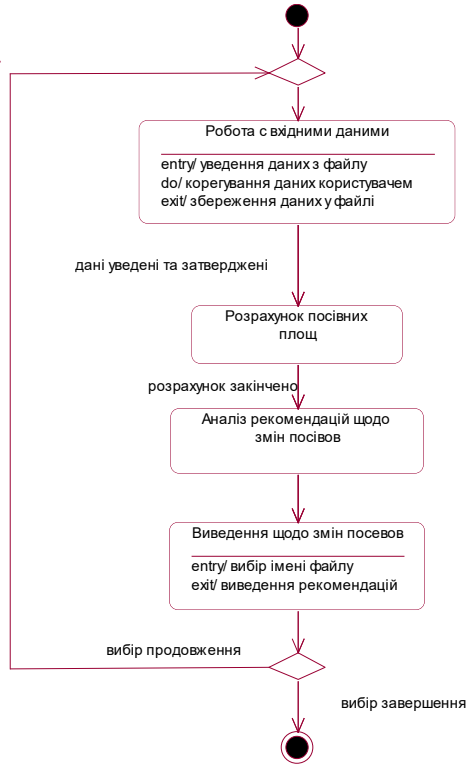


Рисунок 3 – Діаграма станів

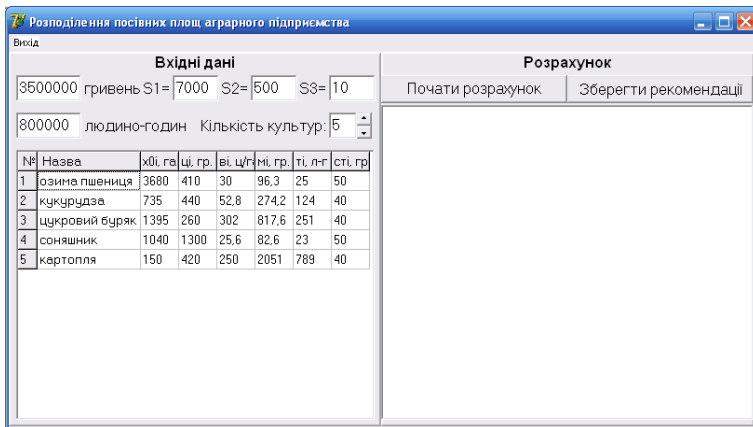


Рисунок 4 – Уведені дані

**Розподілення посівних площ аграрного підприємства**

Вихід

**Вхідні дані**

3500000 гривень S1= 7000 S2= 500 S3= 10

800000 людино-годин Кількість культур: 5

№	Назва	x0, га	цi, гр.	вi, ц/г	мi, гр.	тi, л-г	стi, гр.
1	озима пшениця	3680	410	30	96.3	25	50
2	кукурудза	735	440	52.8	274.2	124	40
3	цукровий буряк	1395	260	302	817.6	251	40
4	соняшник	1040	1300	25.6	82.6	23	50
5	картопля	150	420	250	2051	789	40

**Розрахунок**

Почати розрахунок Зберегти рекомендації

СИСТЕМА РЕКОМЕНДУЄ змінити площі посівів:

- озима пшениця: 3932.9 га замість 3680 га (зміна 252.9 га)
- кукурудза: 805.6 га замість 735 га (зміна 70.6 га)
- цукровий буряк: 1500.9 га замість 1395 га (зміна 105.9 га)
- соняшник: 1110.6 га замість 1040 га (зміна 70.6 га)
- картопля: 150 га замість 150 га (зміна 0 га)

Збільшення прибутку становитиме 12968828.91 гривень (204933521.91 замість 191964693)

Площа під посіви: 7500 га замість 7000 га (зміна 500 га)

Доцільно освоїти 500 га нової площі, для цього необхідно витратити 499999.89 гривень

Рисунок 5 – Розрахунок оптимальних показників

### Перелік посилань

- Самарська Д.О., Домаскіна М. А. Застосування економіко-математичного моделювання для визначення раціональної галузевої структури аграрних підприємств // Глобальні та національні проблеми економіки. №7, 2015. – С. 472–477. URI: <http://global-national.in.ua/archive/7-2015/102.pdf>
- Білоног А. І., Бромот Д. І., Гнатієнко Г. М., Снитюк В. Є. Задача та нейромережна модель оптимізації структури посівних площ фермерського господарства // Енергетика і автоматика. – 2022. – №1. – С. 23–36. – URI: <https://doi.org/10.31548/energiya2022.01.23>
- Горобець Н. М., Дьяченко Н. К. Економіко-математичні підходи до оптимізації виробничої програми аграрних підприємств // Інвестиції: практика та досвід. – 2019. – № 13. С. 30–34. – URI: <https://doi.org/10.32702/2306-6814.2019.13.30>
- Мельников О. Ю. Об'єктно-орієнтований аналіз і проєктування інформаційних систем: посібник для студентів спеціальностей «Системний аналіз» та «Інформаційні системи та технології» / О. Ю. Мельников. – Вид. 3-є, перероб. та доп. – Краматорськ : ДДМА, 2020. – 208 с.



УДК 004.4

Новак Я.В., Мазурець О.В.

*Хмельницький національний університет  
Лицей №1 Імені Володимира Красицького, м. Хмельницький*

## **ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ МЕТОДУ АВТОМАТИЗОВАНОЇ ІДЕНТИФІКАЦІЇ ОСОБИ ЗА ВІДБИТКАМИ ПАЛЬЦІВ**

*Розглянуто підхід до автоматизованого вирішення задач лінійного програмування та розглянуто прикладні аспекти відповідного програмного застосунку. Забезпечено можливість розв'язувати різні типи завдань лінійного програмування, обробку великого обсягу вхідних даних, підтримку різноманітних типів задач лінійного програмування, відтворення для знаходження результату.*

*The approach to automated solution of linear programming problems is considered and the applied aspects of corresponding software application are considered. The ability to solve various types of linear programming tasks, processing of large volume of input data, support for various types of linear programming tasks, reproduction to find the result is provided.*

У сучасному світі, де технології швидко розвиваються, індивідуальна ідентифікація особи є надзвичайно важливою задачею в багатьох сферах життя, включаючи безпеку, транспорт, фінанси та державні послуги. Традиційні методи ідентифікації, такі як паролі та ідентифікаційні картки, втрачають свою ефективність і надійність перед сучасними технологіями.

Одним з перспективних напрямків у сфері ідентифікації особи є використання фотозображень відбитків пальці [1]. Відбитки пальців мають унікальну структуру, яка визначається долинами, горбками та перехрестями, і вони є практично незмінними протягом життя. Це робить їх ідеальними для ідентифікації особи.

Однак, ручна обробка та аналіз великого обсягу фотозображень відбитків пальців є складною та часоємною задачею для людей. Тут на допомогу приходять згорткові нейронні мережі, які є потужними інструментами для автоматизованого аналізу зображень. Одним з головних пріоритетів є використання цього методу в сфері безпеки. Біометрична ідентифікація на основі відбитків пальців забезпечує надійний рівень аутентифікації особи, що дозволяє уникнути випадків підробки або несанкціонованого доступу. Застосування цього методу у сфері безпеки може включати контроль доступу до об'єктів, розблокування електронних пристроїв або ідентифікацію осіб на публічних заходах [2].

Схема функціонування досліджуваного методу ідентифікації особи за відбитком пальців наступна. Спершу фотозображення відбитків пальців та перелік

імен людей повинні бути збережені у форматі, який підтримує робота з зображеннями, наприклад, у форматі JPG або PNG. Це дозволить зручно працювати з цими файлами в подальших етапах. Файли повинні бути пов'язані з відбитками пальців та людьми, які їх належать. Наприклад, ім'я файлу може відповідати імені людини, до якої належить відбиток пальця.

На наступному етапі потрібно отримати різні фотозображення відбитків пальців з різними видами дефектів, наприклад, подряпини, рубці або забруднення. Це дозволить перевірити алгоритм ідентифікації на різних варіантах відбитків пальця з дефектами. Після одержання файлів з дефектами, потрібно виконати необхідні попередні операції, такі як обробка зображень, зменшення розміру, нормалізація тощо, для забезпечення належної якості та однорідності даних.

У випадку, якщо виникають помилки під час обробки або ідентифікації відбитків пальця, слід передбачити обробку цих помилок і виведення відповідного повідомлення про помилку. Це допоможе операторам або користувачам зрозуміти причину невдачі та вжити відповідних заходів для виправлення ситуації.

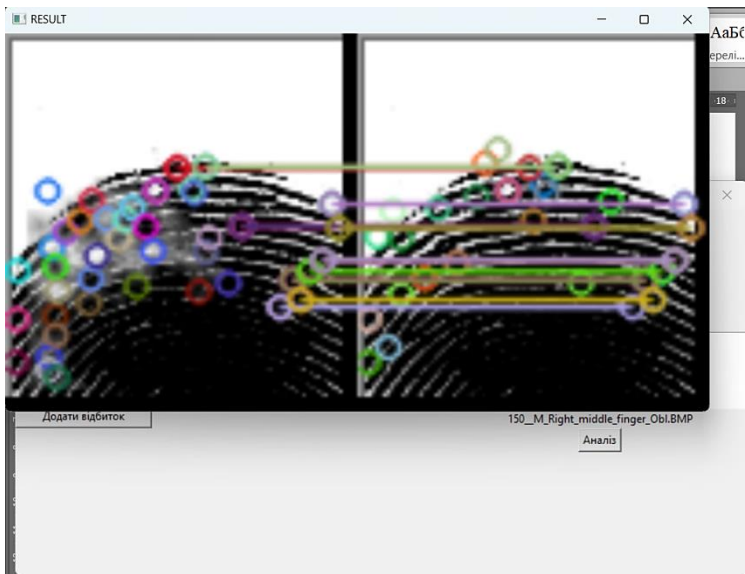


Рисунок 1 – Відображення результату автоматизованої ідентифікації особи за відбитками пальців

Після процесу ідентифікації відбитків пальця (рис. 1) вихідні дані можуть включати: інформацію про носія відбитка, таку як ім'я людини, якій належить відбиток пальця; фотозображення з характеристиками зовнішньої різниці між образами, це можуть бути зображення, які показують різні дефекти або відмінності між оригінальним відбитком пальця і зразками з дефектами; значення сумісності

або подібності, яке вказує на ступінь відповідності між відбитками пальця, це можуть бути числові значення або відсоткові показники, що відображають ступінь схожості чи різниці між відбитками.

Для реалізації конкретної дії програмного застосунку використовувався датасет «SOCOFing Fingerprint Database» доступний на платформі Kaggle та використовується для проведення досліджень у галузі розпізнавання та верифікації відбитків пальців. Він містить зображення реальних та альтерованих відбитків пальців. Реальні відбитки є автентичними, тоді як альтеровані відбитки були змінені шляхом додавання шуму, роздражнення або зміни розміру. Кожне зображення в датасеті має унікальне ім'я файлу та класифікаційний тег, які використовуються для визначення типу та якості відбитку пальця. Деякі зображення також мають розмітку (анотації), що надає додаткову інформацію про відбиток пальця. Цей датасет надає дослідникам можливість використовувати його для розробки та тестування алгоритмів розпізнавання відбитків пальців та оцінки їхньої ефективності.

В рамках даного дослідження розглядалися два методи початкової генерації ваг синапсів для автоматизованої ідентифікації особи за фотозображенням відбитків пальців. Перший метод базується на нормальному розподілі, де ваги генеруються за нормальним законом. Другий метод використовує гармонійний розподіл для генерації ваг [3].

Дослідження проводилося на основі набору даних, що включав реальні та альтеровані відбитки пальців. Застосовувалися згорткові нейронні мережі, а ваги синапсів в обох методах генерувалися безпосередньо перед навчанням моделі. Нормальний розподіл використовувався для незалежної генерації ваг кожного синапсу, тоді як гармонійний розподіл забезпечував більшу концентрацію значень ближче до середнього.

Після генерації ваг відбувався процес навчання, під час якого ваги синапсів оновлювалися з метою досягнення оптимальної точності ідентифікації. Для оцінки ефективності кожного методу проводилося порівняння результатів на тестовому наборі даних. З метою визначення найкращого методу використовувалася метрика точності ідентифікації.

На основі аналізу результатів дослідження було встановлено, який з методів генерації ваг синапсів є більш ефективним для задачі автоматизованої ідентифікації особи за фотозображенням відбитків пальців. А також згідно дослідженню результатів та обрахування їхньої залежності відсотку точності, то зображується наступна діаграма (рисунок 2), але так як зображень 1000, то використовуються лише 10 для схематичного відображення.

Кожен з образів відбитку пальців вміщує в собі схожість з іншими образами та певну подібність до оригінальних зображень, тому будь-який результат не може дорівнювати 0%. І так як образи для аналізу обираються саме з дефектами, то максимальний відсоток подібності не може досягати вище 70%. Тому використовуючи ідентифікацію особи за зображенням відбитків пальця слід

зазначити, що кожен з фотозображень підлягає порівнянню і при виведенні результату можуть враховуватися похибки у точності значень.

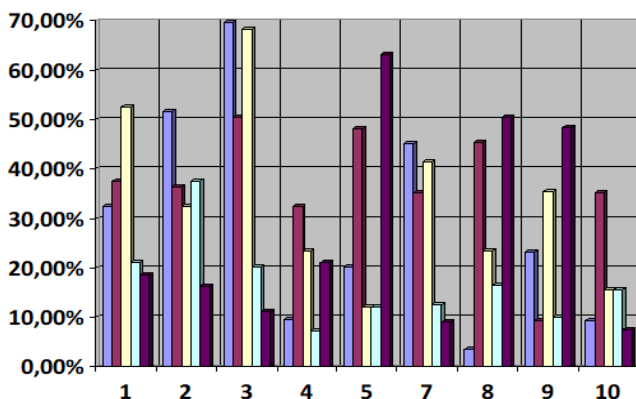


Рисунок 2 – Діаграма залежності відсотку точності результату

В результаті даного дослідження було встановлено, що метод генерації ваг синапсів на основі гармонійного розподілу виявився більш ефективним для автоматизованої ідентифікації особи за фотозображенням відбитків пальців. Використання гармонійного розподілу забезпечило більшу концентрацію значень ваг ближче до середнього, що сприяло досягненню кращої точності ідентифікації в порівнянні з методом на основі нормального розподілу. Отримані результати можуть бути корисними для подальшого розвитку та вдосконалення систем ідентифікації осіб за відбитками пальців.

Загалом, розглянутий метод автоматизованої ідентифікації особи за фотозображенням відбитків пальців з використанням згорткових нейронних мереж може мати застосування в безпеці, медицині, фінансах та інших галузях сприяє підвищенню рівня безпеки, зручності та ефективності у багатьох процесах. З ростом технологічного розвитку, методи ідентифікації на основі відбитків пальців продовжують здобувати популярність та стають необхідними інструментами в сучасному світі.

### Перелік посилань

1. Portal. Біометрична ідентифікація URL: <https://dl.acm.org/doi/fullHtml/10.1145/328236.328110>
2. APA PsycNet. Розвиток ідентифікації. URL: <https://psycnet.apa.org/record/2009-06337-008>
3. ScinceDirect. Зв'язні нейромережі. URL: <https://www.sciencedirect.com/science/article/abs/pii/S0959440X2300012X>

УДК 004.9

Новацький О.В., Сороколіт В.О., Яшина О.М.

*Хмельницький національний університет*

## **МЕТОД ПІДТРИМКИ ЯКОСТІ ПРОГРАМНОГО КОДУ НА ОСНОВІ АВТОМАТИЧНОГО ТЕСТУВАННЯ**

*Розглянуто задачу підтримки якості програмного коду на основі автоматичного тестування, що дозволяють здійснювати правильне оформлення програмного коду згідно правил та стандартів. Здійснено аналіз доцільності підтримки коду програмного забезпечення в сучасних реаліях роботи розробника.*

*The task of maintaining the quality of the software code based on automatic testing, which allows for the correct design of the software code according to rules and standards, is considered. An analysis of the expediency of software code support in the modern realities of the developer's work was carried out.*

Тестування є найстарішим і найсучаснішим типом підтримки якості програмного забезпечення. Загалом, тестування є важливим процесом у багатьох галузях техніки: будь то новий телевізор, програмне забезпечення системи автомобіля тощо, тестування може допомогти інженерам виявити дефекти та переконатися в тому, що продукт міцний та надійний в різних умовах використання.

Тестування програмного забезпечення має ту ж мету, що й тестування, яке застосовується в інших галузях техніки, а саме виявлення дефектів або недоліків товару. Тестування можна умовно розділити на дві категорії: ручне тестування та автоматизоване тестування. У ручному тестуванні виконуються тестові випадки вручну людиною без будь-якої підтримки інструментів чи сценаріїв, тобто тестувальник вручну перевіряє виріб на виявлення дефектів і складає звіт після цього; в автоматизованому тестуванні, тестові випадки виконуються за допомогою інструментів, сценаріїв і програмного забезпечення.

Для виконання тестових операцій вручну потрібен тестувальник програмного забезпечення: це дуже важливо, оскільки незалежно від того, наскільки воно покращується, автоматизація не може замінити людську інтуїцію, умовиводи та індуктивне міркування. Наприклад, людина може змінити курс посеред тестового запуску, щоб перевірити щось, чого не було розглянуто раніше. Крім того, автоматизоване тестування не може перевірити деякі аспекти коду, наприклад зручність для користувача або взаємодію з клієнтом. З іншого боку, є й такі великі недоліки: деякі типи тестування (наприклад, тестування навантаження та продуктивності) не можуть бути виконані вручну, і, що найголовніше, ручне тестування займає багато часу. Ось чому компанії покладаються (здебільшого) на автоматизовані тести. У цій практиці тестувальники розробляють тестові сценарії для автоматичної перевірки продукту. Іншими словами, вони не тестують «вручну» програмні продукти, але покладаються на попередньо розроблені тести, які

виконуватимуться автоматично. Враховуючи це, виконання тестів і підрахунок їх успішності автоматизоване тестування є швидшим і надійнішим, ніж ручне тестування.

Особливістю автоматичного тестування програмного забезпечення є те, що як продукт, так і тести зроблені з того самого «матеріалу» і розроблені таким же чином: продукт під тестування - це код (називається робочим кодом), і він перевіряється за допомогою іншого коду (називається тестовим кодом). Як можна собі уявити, тестування програмного забезпечення передбачає тестування різних аспектів робочого коду: у нас є нефункціональне тестування (спрямоване на тестування нефункціональних аспектів програмного забезпечення систем, таких як продуктивність, зручність використання, надійність, безпека), а також функціональне тестування перевіряє, чи кожна функція програми працює відповідно до специфікації вимог. Функціональні тести - це переважна більшість тестів, написаних розробниками. У цій галузі тестування можна знайти модульне тестування (тести, які перевіряють один блок програмного забезпечення), інтеграційне тестування (тести, які інтегруються у різні підрозділи та їх взаємодія), системне тестування, регресійне тестування тощо. Існують буквально сотні різних типів тестування, кожен окремо з них вимірює різні аспекти виробничого коду.

Подібно до інженерії в інших дисциплінах, використовується тестування програмних систем, щоб виявити помилки на ранніх етапах циклу розробки (наприклад, до того, як код буде створено, здійснюється відправлення клієнтам). Без належного тестування програмного забезпечення помилки можуть дійти до клієнтів, що може бути дорогим для виправлення або навіть небезпечним для життя та здоров'я.

Отже, автоматичне тестування стало важливим процесом для покращення якості програмного забезпечення системи. Автоматизовані тести можуть допомогти переконатися, що виробничий код є надійним у багатьох умовах використання та що код відповідає вимогам продуктивності та безпеки.

### Перелік посилань

1. Коцовський В.М. Супровід програмних систем: Методичний посібник для студентів спеціальності «Інженерія програмного забезпечення» / В. М. Коцовський. – Ужгород: Видавництво УжНУ «Говерла», 2016. – 52 с.
2. Robert Brautigam. Why I Never Null-Check Parameters. URL - <https://dzone.com/articles/why-i-never-null-check-parameters>, 2018.
3. Benjamin Floyd, Tyler Santander, and Westley Weimer. 2017. Decoding the Representation of Code in the Brain: An fMRI Study of Code Review and Expertise. In Proceedings of the International Conference on Software Engineering (ICSE). 175– 186.
4. Загальносистемні принципи та етапи створення програм. Життєвий цикл програмного виробу. [Електронний ресурс] – URL: <http://lib.mdpu.org.ua/e-book/vstup/L7.htm>.
5. Simon Butler, Michel Wermelinger, Yijun Yu, and Helen Sharp. 2009. Relating Identifier Naming Flaws and Code Quality: An Empirical Study. In Proceedings of the Working Conference on Reverse Engineering (WCRE). 31–35.
6. ISO/IEC 9126-1:2001. Software engineering – Software product quality – Part 1: Quality model.

УДК 004.4

Овчарук О.М., Мазурець О.В.

*Хмельницький національний університет*

## **ПРОГНОЗУВАННЯ ЗНАЧЕНЬ ПАРАМЕТРІВ ЗА ЇХ ЧАСОВИМИ РЯДАМИ РЕКУРЕНТНОЮ ТЕМПОРАЛЬНОЮ НЕЙРОННОЮ МЕРЕЖЕЮ**

*Описано особливості використання засобів для прогнозування значень параметрів за їх часовими рядами у вигляді рекурентної темпоральної нейронної мережі із згортковим шаром. Це дозволило за вхідними даними у вигляді вибірки залежних від часу значень визначеного параметру протягом досліджуваного періоду одержувати вихідні дані у вигляді вибірки із прогнозованими значеннями параметру для подальшого прогнозування рівня епідеміологічної небезпеки засобами нейромережевого моделювання.*

*Features of the use of tools for forecasting parameter values based on their time series in the form of a recurrent temporal neural network with a convolutional layer are described. This made it possible, based on the input data in the form of a sample of time-dependent values of the specified parameter during the studied period, to receive output data in the form of a sample with predicted parameter values for further forecasting the level of epidemiological danger by means of neural network modeling.*

Використання підходів машинного навчання, а саме штучних нейронних мереж є одним із способів прогнозування швидкості поширення інфекційних захворювань [1]. Методологія штучних нейронних мереж добре відома і підходить для вирішення завдань, де проведення аналітичного дослідження є доволі складним. [2]. На сьогоднішній день розроблено велику кількість варіацій штучних нейронних мереж, які можуть відрізнятися за своєю архітектурою, кількістю нейронів, кількістю прихованих шарів, функціями активації нейронів та підходами до навчання. Формального підходу до вибору характеристик штучних нейронних мереж не існує, в переважній більшості використовуються наступні типи нейронних мереж або їхні комбінації чи модифікації: нейронні мережі прямого розповсюдження; рекурентні нейронні мережі; згорткові нейронні мережі.

Рекурентні нейронні мережі активно використовуються в глибокому навчанні та при розробці моделей, що імітують активність нейронів у людському мозку. RNN особливо ефективні у випадках коли для прогнозування результату потрібно враховувати послідовність попередніх подій, наприклад: прогнозування наступного слова в тексті та прогнозування часових рядів. Особливістю даних НМ є використання циклів зворотного зв'язку, що застосовуються для обробки послідовності даних на основі яких формується остаточний результат. Цей ефект в RNN часто називають пам'яттю. При прийнятті рішень даною НМ мережею

враховуються як поточні вхідні дані та дані які подавалися на її входи на попередніх ітераціях [3].

Також важливою особливістю RNN є те що в них необов'язково один вхід має відповідати одному виходу нейронної мережі. В RNN можливі наступні залежності між кількістю входів та кількістю виходів (рисунку 1):

- один до одного;
- один до багатьох;
- багато до одного;
- багато до багатьох [4].

До переваг RNN можна віднести здатність запам'ятовувати кожен частину інформації у часі. Також до переваг даної НМ мережі можна віднести можливість обробки вхідних даних різної розмірності. До недоліків RNN можна віднести достатньо довгий час навчання та неможливість врахування майбутніх вхідних даних.

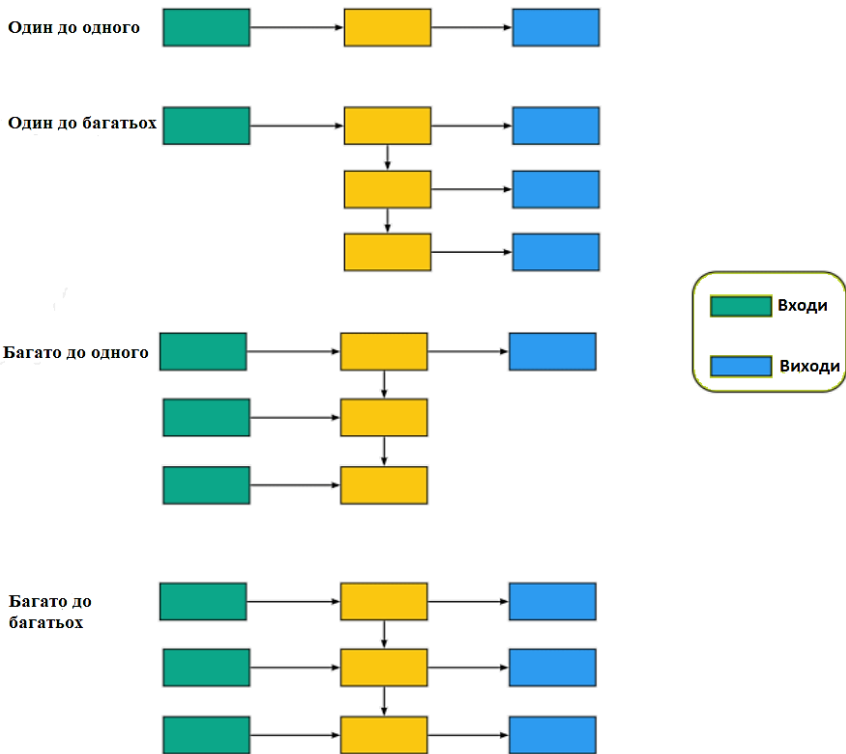


Рисунок 1 – Схема залежності між кількістю входів та кількістю виходів в RNN [4]



Згорткові нейронні мережі є типом моделі глибокого навчання та застосовуються для даних що мають сітчасту структуру, наприклад зображень. CNN зазвичай складається з трьох типів шарів: шару згортки, шару активації та повнозв'язного шару.

Згортковий шар є основним блоком в CNN, і саме в ньому відбувається більша частина обчислень. Одним з елементів даного шару є детектор. Детектор представляє матрицю значень, в основному розмірності 3 на 3. Значення якими заповнена дана матриця називаються фільтром. Детектор застосовується до частини зображення та проводить обчислення скалярного добутку між вхідними пікселями та фільтром. Після закінчення обрахунків проводить зміщення детектора на іншу частину зображення після чого обрахунки повторюють. У результаті повного проходження детектору по зображенню відбувається формування карти [5].

Повнозв'язний шар є шаром у якого всі вихідні нейрони пов'язані з усіма вхідними нейронами. Основним завданням повнозв'язкового шару є моделювання складної нелінійної функції, що найчастіше використовується для класифікації. Ця опція оптимізується в процесі навчання мережі, що дозволяє покращувати якість розпізнавання. Шари, що йдуть до повнозв'язкового, є засобами попередньої обробки зображення, тобто вони використовуються для виділення різних ознак, які потім подаються на входи повнозв'язкового шару.

Отже, для автоматизованого прогнозування рівня епідеміологічної небезпеки засобами нейромережевого моделювання варто скористатись рекурентною темпоральною нейронною мережею із згортковим шаром для формування додаткових вхідних даних у вигляді додаткової вибірки із прогнозованими значеннями параметрів для підвищення точності визначення рівня епідеміологічної небезпеки. Відповідно, за вхідними даними вибірок актуальних параметрів протягом досліджуваного періоду слід одержувати вихідні дані у вигляді результуючого експертного висновку, який містить прогнозовані варіанти рівня епідеміологічної небезпеки й оцінки кожного із них.

Темпоральні згорткові мережі є розширенням класичних згорткових нейронних мереж однак до них додаються певні властивості рекурентних нейромереж. Темпоральні згорткові мережі складаються з причинно-наслідкових одновимірних згорткових шарів з однаковою довжиною вхідних та вихідних шарів. TCN заснована на двох принципах: не може бути витоку з майбутнього в минуле, і мережа прогнозує вихідні дані тієї ж довжини, що і вхідні дані. Для виконання першого пункту TCN використовує каузальні згортки, в яких вихідні дані в момент часу  $T$  згорнуті для всіх попередніх елементів числового рядку включаючи  $T$  у вхідному шарі.

Щоб досягти другого пункту, TCN використовує архітектуру одновимірної повністю згорткової нейронної мережі, де кожен прихований шар має ту ж довжину, що і вхідний шар, для виконання цієї умови додається нульове доповнення довжини до кожного шару (рисунок 2).

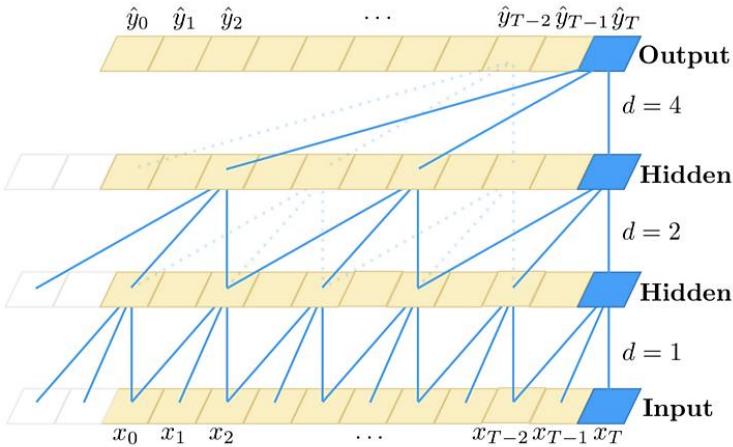


Рисунок 2 – Архітектура одновимірної TCN

На рисунку 2 також зображено архітектурні елементи TCN, включаючи розширену причинну згортку з коефіцієнтами розширення  $d = 1, 2$  і  $4$  і розміром фільтра 3. Рецептивне поле здатне охоплювати всі значення вхідної послідовності. Стандарт вибірки вибирається відповідно до значення параметру  $d$ , де перший рівень  $d$  дорівнює 1, що означає, що вибрано на даному шарі вибрано кожне число. Вибір більшого розміру фільтра або збільшення коефіцієнта розширення призведе до збільшення кількості шарів мережі.

Щоб TCN не була просто складною моделлю лінійної регресії, необхідно додати функції активації після згорткових шарів, це дозволить додати нелінійність до моделі. Зазвичай використовуються функції активації ReLU, що додаються до залишкових блоків після згорткових шарів (рисунок 3).

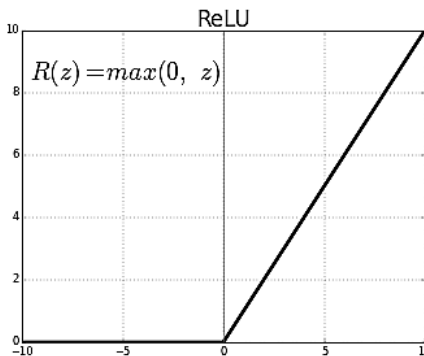


Рисунок 3 – Графік функції активації ReLU для TCN

Щоб нормалізувати введення вхідних даних прихованих шарів застосовується нормалізація ваги до кожного згорткового шару. Після функції активації застосовується шар Dropout, що дозволяє виключити з процесу навчання деякі нейрони TCN. Якщо в моделі відсутній шар Dropout то перша частина навчальних вибірок непропорційно сильно впливає на навчання нейромережі (рисунок 4).

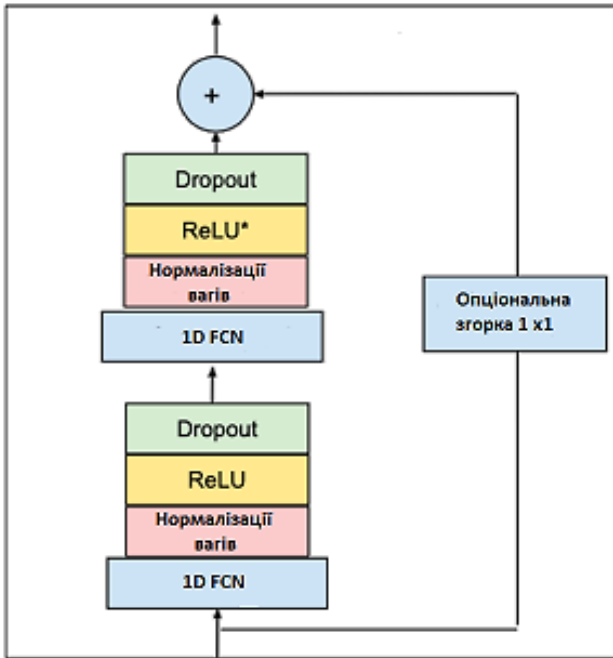


Рисунок 4 – Схема залишкових блоків

До переваг TCN можна віднести можливість виконувати згортання паралельно, також присутня можливість налаштувати розміри рецептивного поля за допомогою кількості шарів, коефіцієнтів розширення та розмірів фільтрів, що дозволяє контролювати розмір пам'яті моделі для різних вимог предметної області.

Таким чином, було використано засоби для прогнозування значень параметрів за їх часовими рядами у вигляді рекурентної темпоральної нейронної мережі із згортковим шаром. Це дозволило вдосконалити метод прогнозування значень параметрів за їх часовими рядами [1] рекурентною темпоральною нейронною мережею із згортковим шаром, а саме за вхідними даними у вигляді вибірки залежних від часу значень визначеного параметру протягом

досліджуваного періоду одержувати вихідні дані у вигляді вибірки із прогнозованими значеннями параметру для подальшого прогнозування рівня епідеміологічної небезпеки засобами нейромережевого моделювання.

### Перелік посилань

1. Овчарук О.М., Мазурець О.В., Собко О.В., Молчанова М.О., Кліменко В.І. Інформаційна технологія прогнозування рівня епідеміологічної небезпеки з використанням нейромережевого моделювання. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2023. №4 (323). С. 224-230.
2. Bai Y., Jin Z. Prediction of SARS epidemic by BP neural networks with online prediction strategy // Chaos, Solitons and Fractals. — 2005. — Vol. 26, № 2. —P. 559–569.
3. A Guide to Recurrent Neural Networks: Understanding RNN and LSTM Networks. URL: <https://builtin.com/data-science/recurrent-neural-networks-and-lstm>
4. Recurrent neural networks. URL: <https://www.techtarget.com/searchenterpriseai/definition/recurrent-neural-networks>
5. Convolutional Neural Networks URL: <https://www.ibm.com/cloud/learn/convolutional-neural-networks>

УДК 004.054

Олійник П.О.

Хмельницький національний університет

## УДОСКОНАЛЕНИЙ МЕТОД РОБОТИ З МЕТРИКАМИ ПОКРИТТЯ КОДУ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОГО ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

*Розглянуто програмну систему, яка має на меті повністю автоматизувати процес розрахунку метрик покриття коду, що забезпечує ефективне оцінювання результатів тестування програмних продуктів. Був виконаний опис архітектури розробленої програмної системи. Представлена програмна система має на меті спростити завдання розробників, тестувальників та керуючого проектами персоналу, забезпечуючи підвищену ефективність та автоматизацію процесу оцінювання покриття коду та тестування.*

*The software system is considered, which aims at a fully automated process of calculating the code coverage metric, which provides an effective evaluation of the results of testing software products. The description of the developed software system' architecture was completed. The presented software system aims to simplify the tasks of developers, testers and staff project managers, ensuring high efficiency and automation of evaluating code coverage and testing processes.*

У наш час стрімкої популярності розробки програмного забезпечення гостро постає питання у якості та ефективності проведення тестування програмного коду. Задля отримання детальних результатів стосовно правильності тестування використовуються метрики покриття коду, а саме їх процентні співвідношення, що показують ступінь покриття програмного коду тестами. Метрики покриття коду включають велику кількість метрик, серед яких виділяють метрику покриття рядків коду, метрику покриття функцій, метрику покриття класів [1]. Метою даного дослідження є вирішення наступних конкретних завдань:

1. Розробка програмної, яка автоматизовано збирає та аналізує дані щодо метрик покриття коду та результатів тестування в програмному забезпеченні.
2. Зниження витрат часу та ресурсів, які витрачаються на ручну перевірку покриття коду та виконання тестів, завдяки автоматизованій системі розрахунку метрик покриття коду.
3. Забезпечення підтримки DevOps та CI/CD, що допоможе автоматизувати та прискорити процес розробки та впровадження програмного забезпечення.

Задля реалізації програмної системи, що допоможе ефективно проводити розрахунок метрик покриття коду, було використано ряд технологій, серед яких можна виділити дві найбільш вагомих, а саме GitHub Actions та платформу AWS разом із її функціональними сервісами.

GitHub Actions є платформою безперервної інтеграції та безперервної доставки, що дозволяє автоматизувати розробку програмного забезпечення, його тестування та розгортання. GitHub містить багато різноманітних компонентів та може бути гнучко налаштованим в залежності від потреб розробників [2].

AWS є хмарною платформою, яка надає понад 200 повнофункціональних послуг із центрів обробки даних, розташованих по всьому світу, і є найповнішою у світі хмарною платформою [3]. У розробці програмної системи будуть використовуватись такі сервіси як Amazon S3 Bucket що виконує роль сховища файлів, Amazon ECS призначений для оркестрації Docker контейнерів, Amazon ECR який виконує роль реєстру Docker імеджів та Amazon EventBridge який дозволяє створювати події та запускати відповідні операції у відповідь на події що відбуваються.

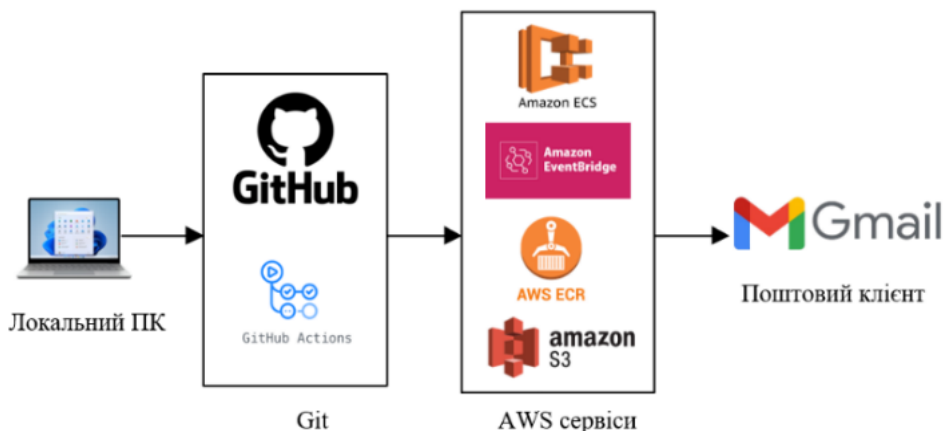


Рисунок 1 – Основних компоненти програмної системи

У відповідь на відправку змін розробником у віддалений GitHub репозиторій, GitHub Actions будуть здійснювати відсилання файлів репозиторію до сервісу Amazon S3 Bucket. У відповідь на подію додавання файлів у Amazon S3 Bucket буде відбуватись запуск контейнеру в сервісі Amazon ECS який буде відправляти електронний лист на вказану пошту одержувача. Лист буде містити

інформацію про автора Git коміту та результати розрахунку метрик покриття коду. Дана програмна система повинна автоматизувати процес розрахунку метрик покриття коду, що позитивно відобразиться на якості програмних продуктів. Загальний вигляд програмної системи та її основних компонентів можна представити у вигляді графічної схеми (рисунок 1).

Отже, була розглянута структура та поданий короткий опис запропонованої програмної системи, що допоможе розробникам, тестувальникам та іншим відповідальним особам у покращенні процесів тестування програмного забезпечення, сприятиме створенню високоякісних продуктів та дозволить підтримувати високий темп розробки у сучасній індустрії програмного забезпечення.

### **Перелік посилань**

1. Code Coverage Metrics 2023: Guide & Explanation [Електронний ресурс] – Режим доступу до ресурсу: <https://blog.gitnux.com/code-coverage-metrics/> .
2. What is GitHub Actions? Automated CI/CD for GitHub [Електронний ресурс] – Режим доступу до ресурсу: <https://www.infoworld.com/article/3698188/what-is-github-actions-automated-cicd-for-github.html> .
3. What is AWS: An Ultimate Guide to Amazon Web Services [Електронний ресурс] – Режим доступу до ресурсу: <https://www.simplilearn.com/tutorials/aws-tutorial/what-is-aws> .

УДК 004.4

Онікієнко С.С., Глухов В.Ю., Манзюк Е.А.

*Хмельницький національний університет*

## **ДЕТЕКТУВАННЯ ОБ'ЄКТІВ НА ЗОБРАЖЕННЯХ З НЕВЕЛИКОЮ РОЗДІЛЬНОЮ ЗДАТНІСТЮ**

*Створена та реалізована система для автоматичного виявлення об'єктів з невеликою роздільною здатністю на зображеннях шляхом застосування методів штучного інтелекту. Дані для аналізу були отримані з низки зображень, які мали обмежену якість і роздільну здатність. В рамках дослідження використовувалися як методи, які вимагали наявності зразків об'єктів, так і методи без них для виявлення цих об'єктів на низькороздільних зображеннях. Результати дослідження свідчать про високу ефективність запропонованих методів у виявленні об'єктів з невеликою роздільною здатністю на зображеннях.*

*A system for automatic detection of objects with low resolution on images has been developed and implemented using artificial intelligence methods. Data for analysis were obtained from a set of images with limited quality and resolution. The research encompassed methods that required the presence of object samples as well as methods that did not, for the detection of these objects on low-resolution images. The research results confirm the high effectiveness of the proposed methods in detecting objects with low resolution on images.*

Здатність виявлення та точне визначення місця розташування об'єктів на зображеннях, отриманих з супутників або безпілотних апаратів, має широкий потенціал застосування у різних галузях, включаючи екологічний моніторинг, контроль лісових ресурсів, забезпечення національної безпеки та управління дорожнім рухом. Однак існуючі дослідження свідчать про обмежену ефективність виявлення, особливо у випадках, коли зображення мають низьку роздільну здатність і схильні до шуму, особливо в контексті малих об'єктів [2, 3]. Ця проблема залишається актуальною навіть для високороздільних зображень, де ефективність виявлення невеликих об'єктів падає в порівнянні з їх більшими аналогами.

Сучасні детектори виявили високу точність при використанні стандартних наборів даних, які містять зображення, де об'єкти помітні та великі, такі, як CIFAR. Проте такі набори даних не відображають специфічні вимоги роботи з супутниковими знімками та потреби виявлення менших об'єктів. Розробка ефективних методів для подолання цих викликів стає актуальним завданням для



поліпшення систем виявлення об'єктів в реальних умовах дистанційного спостереження.

У межах цього дослідження виникає завдання виявлення невеликих об'єктів на супутникових знімках із низькою роздільною здатністю. Ця проблема є складною через обмежену якість таких зображень. У цьому контексті розглядається метод, що передбачає створення зображень високої роздільної здатності на основі вихідних низькороздільних супутникових знімків і одночасне виявлення об'єктів на зображеннях високої роздільної здатності. Цей метод ґрунтується на використанні глибокої генеративної змагальної мережі [1], яка має потенціал у поліпшенні якості зображень.

В покращених зображеннях відсутня важлива інформація, яка стосується деталей та контурів об'єктів. Ця відсутність інформації негативно впливає на результати виявлення невеликих об'єктів на відновлених та зашумлених зображеннях із низькою роздільною здатністю.

З метою подолання цієї проблеми було розроблено новий підхід, який передбачає використання генеративної змагальної мережі для покращення контурів об'єктів та створення високої роздільної здатності для покращення якості супутникових зображень. У цьому контексті застосовуються різноманітні мережі для виявлення об'єктів в режимі співпраці, де втрачаються, що виникають під час виявлення об'єктів, передаються генеративної змагальної мережі з генерацією об'єктів із покращеними контурами з метою підвищення ефективності процесу виявлення.

Цей підхід сприяє покращенню можливостей виявлення об'єктів на супутникових знімках низької роздільної здатності після застосування заходів для відновлення інформації та підвищення загальної якості зображень.

В рамках цього підходу впроваджена інтегрована архітектура, яка включає у себе покращену генеративну змагальну мережу, мережу для покращення граничних контурів та мережу для виявлення об'єктів. Для реалізації генеративної змагальної мережі були використані блоки з залишковим з'єднанням, тоді як для детекторної мережі застосована швидка згортова мережа, що базується на регіонах, і одноступінчастий мультибоксовий детектор. Розширені експерименти, проведені на наборі даних для супутникових знімків, підтвердили переваги цього методу в порівнянні з використанням окремих нейронних мереж.

Збільшена роздільна здатність зображень позитивно впливає на завдання виявлення об'єктів на супутникових знімках. У дослідженнях використано набори даних від супутників і проводили одночасне поліпшення зображень та виявлення об'єктів, використовуючи глибоку згортову нейронну мережу та одноступінчастий мультибоксовий детектор.

Запропоновано використання глибокого генератора, побудованого на основі згорткової нейронної мережі, для перетворення низькороздільних зображень у високороздільні. Також використано багатозадачну мережу як дискримінатор і для локалізації та класифікації об'єктів. Дослідження проводяться на стандартних зображеннях, які вимагають пари зображень - низькороздільних і високороздільних.

Крім того, використовуємо метод одночасного використання високороздільності та виявлення об'єктів на супутникових знімках. Архітектура мережі розроблена на основі циклічно узгодженої глибокої змагальної мережі.

У ході розв'язання завдання виявлення об'єктів, було створено метод та відповідні системи для маркування, навчання та виявлення об'єктів на великих супутникових знімках, що охоплюють значні території. Цей метод спрощує завдання виявлення невеликих об'єктів на супутникових знімках, роблячи можливим оптимізацію процесу навчання сучасних моделей виявлення об'єктів та точне визначення їх розташування на зображеннях.

### **Перелік посилань**

1. Durgadevi M. Generative adversarial network (gan): a general review on different variants of gan and applications: 2021 6th International Conference on Communication and Electronics Systems (ICCES), IEEE, 2021. Pp.1–8.i
2. Wang Z.-Z., Xie K., Zhang X.-Y., Chen H.-Q., Wen C., He J.-B. Small-object detection based on yolo and dense block via image super-resolution. IEEE Access. 2021. Vol. 9. Pp. 56416–56429.
3. Wu X., Hong D., Chanussot J. UIU-Net: U-Net in U-Net for infrared small object detection. IEEE Transactions on Image Processing. 2022. Vol. 32. Pp. 364–376.

УДК 004.4

Охота В.В., Міхалевський В.Ц., Скрипник Т.К.

*Хмельницький національний університет*

## **МЕТОД ЗДІЙСНЕННЯ РІЧКОВОЇ ПЕРЕПРАВИ ТРАНСПОРТНИХ ЗАСОБІВ ЗА МУРАШИНИМ АЛГОРИТМОМ**

*Розглянуто метод здійснення річкової переправи транспортних засобів за основи мурашиного алгоритму. Суть методу полягає в оптимізації процесу перетину великих водних перешкод. Шляхом використання цього алгоритму, ресурси та транспортні засоби розподіляються оптимально для максимально ефективного подолання річкових бар'єрів. Описано також інтерфейс, що надає можливість користувачам відслідковувати поточний стан процесу річкової переправи.*

*The method of carrying out the river crossing of vehicles based on the ant algorithm is considered. The essence of the method is to optimize the process of crossing large water obstacles. By using this algorithm, resources and vehicles are allocated optimally to overcome river barriers as efficiently as possible. An interface that enables users to monitor the current state of the river crossing process is also described.*

Метод здійснення річкової переправи транспортних засобів на основі мурашиного алгоритму передбачає оптимізацію перетину великих водних перешкод.

Мурашині алгоритми базуються на імітації поведінки мурах при пошуку їжі та побудові маршрутів до місць її знаходження. Це включає в себе використання феромонів - хімічних речовин, які мурахи залишають за собою. Феромони служать яскравими точками для інших мурах і вказують, який маршрут є більш оптимальним.

Вивчення поведінки мурашиних колоній важливе для комп'ютерних наук, оскільки це надає уявлення про роз'єднану організацію, що дуже корисно для вирішення складних задач оптимізації. Мурашині алгоритми стали джерелом натхнення для розробки оптимізаційних методів у сферах, де необхідно знаходити найкращі рішення в умовах обмежень та невизначеності.

Використовуючи такий алгоритм, ресурси та транспортні засоби розподіляються оптимально для максимально ефективного подолання річкових бар'єрів. Також описується інтерфейс, що дозволяє користувачам відстежувати поточний стан процесу річкової переправи.

Виконання дій в кілька етапів здійснюється за допомогою ітерацій одночасно кількома мурахами. Під час однієї ітерації кожна мураха проходить маршрут через всі вершини незалежно від інших. Для мурахи, яка перебуває у вершині *i*, перехід до вершини *j* залежить від трьох компонент: пам'яті мурахи,

видимості та віртуального сліду феромону. Пам'ять мурахи - це список вершин, які мураха вже відвідала і не повинна повторно відвідувати. Наявність цього списку гарантує, що мураха не відвідає ту саму вершину двічі. З рухом мурахи цей список зростає і обнуляється на початку кожної ітерації.  $J_i, k$  - це список вершин, які мураха  $k$ , яка перебуває у вершині  $i$ , ще не відвідала. Ясно, що  $J_i, k$  є доповненням до пам'яті мурахи.

Видимість – це величина обернена до відстані:  $\eta_{ij} = 1/D_{ij}$ , де  $D_{ij}$  — відстань між вершинами  $i$  та  $j$ . Видимість базується тільки на локальній інформації і являє собою «евристичну бажаність» вибору вершини  $j$ , під час перебування у вершині  $i$ . Чим ближче вершини  $i$  та  $j$ , тим більше бажання відвідати їх.

Віртуальний слід феромону на шляху між вершинами  $i$  та  $j$  є прагматичним бажанням мурахи відвідати місто  $j$  з міста  $i$ , підтверджене досвідом. На відміну від видимості, ця величина змінюється після кожної ітерації алгоритму. Кількість віртуального феромону на шляху з міста  $i$  в місто  $j$  на ітерації  $t$  позначається як  $\tau_{ij}(t)$ .

Основні сутності предметної області для задачі, що розглядається, наведені в Таблиці 1.

Таблиця 1 – Головні сутності алгоритму

Сутність	Опис
Річка	Природний бар'єр, через який потрібно переправити.
Береги	Два береги річки, між якими знаходяться транспортні засоби.
Транспорт	Засоби, які потрібно перевести через річку.
Мурахи	Віртуальні мурахи, які використовуються в алгоритмі для пошуку шляху.
Переправа	Процес переправи транспортних засобів через річку, включаючи вибір шляху та використання мурашиного алгоритму.

Запропонований метод здійснення річкової переправи транспортних засобів за мурашиним алгоритмом розробляє оптимальний підхід до подолання водних перешкод в умовах невизначеності. Цей метод спрямований на ефективне використання доступних ресурсів та забезпечення надійної переправи.

Система програмного забезпечення для задачі річкової переправи транспортних засобів включає наступні компоненти:

1) Компонент для управління даними: Цей компонент відповідає за зберігання та обробку даних, пов'язаних з річкою, транспортними засобами та іншими факторами. Ці дані можуть включати в себе інформацію про річку (ширина, глибина, швидкість течії), транспортні засоби (габарити, швидкість, вантажопідйомність), погодні умови (рівень води, вітер) та дані про переправи (час відправлення, час прибуття).

2) Компонент для планування маршрутів: Цей компонент відповідає за планування маршрутів переправи транспортних засобів. При плануванні маршрутів необхідно враховувати обмеження транспортних засобів (габарити, швидкість,

вантажопідйомність), погодні умови (рівень води, вітер) та динаміку навколишнього середовища, таку як зміна рівня води.

3) Компонент для відстеження переправ: Цей компонент відповідає за відстеження переправ транспортних засобів і забезпечення їх безпеки. При відстеженні переправ необхідно враховувати положення транспортних засобів, їх швидкість та стан навколишнього середовища.

4) Компонент для взаємодії з користувачами: Цей компонент відповідає за взаємодію з користувачами, включаючи операторів переправ і клієнтів. При взаємодії з користувачами важливо забезпечити зручність використання, безпеку та надійність.

Ці компоненти можуть бути реалізовані на різних мовах програмування та технологіях. Для реалізації системи програмного забезпечення для задачі річкової переправи транспортних засобів можна використовувати такі технології: **Java** (мова програмування, яка дозволяє розробляти різноманітні типи програмного забезпечення, включаючи веб-додатки та десктопні додатки); **Spring** (фреймворк для Java, який спрощує розробку різних типів додатків); **Spring Data** (модуль фреймворка Spring для роботи з даними, що допомагає спростити доступ до інформації); **Lombok** (бібліотека для спрощення кодування на Java, що полегшує розробку); **MySQL** (система керування базами даних для зберігання даних про річку, транспортні засоби та переправи); **Spring Web** (модуль фреймворка Spring для розробки веб-додатків); **Docker** (технологія, що дозволяє створювати контейнери для програмного забезпечення та спрощує розгортання додатків).

Майбутні дослідження будуть спрямовані на тестування та оптимізацію методу, а також на його інтеграцію з реальними системами для задач річкової переправи.

### Перелік посилань

1. Rukundo, O., Cao, H. Advances on image interpolation based on ant colony algorithm URL: <https://springerplus.springeropen.com/articles/10.1186/s40064-016-2040-9>.
2. Оптимізація колонії мурах. URL: <https://www.sciencedirect.com/topics/engineering/ant-colony-optimization>
3. Вступ до оптимізації колонії Ant (ACO) URL: <https://towardsdatascience.com/the-inspiration-of-an-ant-colony-optimization-f377568ea03f>
4. Алгоритми мурах для дискретної оптимізації URL: [https://people.idsia.ch/~luca/ij\\_23-alife99.pdf](https://people.idsia.ch/~luca/ij_23-alife99.pdf)

УДК 004.4

Павлова О.О., Рудик І.В.

*Хмельницький національний університет*

## **ПОСТ-ОБРОБКА СИГНАЛІВ ТРИВОГИ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ ЗА ДОПОМОГОЮ НЕЙРОМЕРЕЖІ YOLOV8**

*Розглянуто проблему похибок розпізнавання об'єктів на зображеннях з камер зовнішнього спостереження. Запропоновано рішення пост-обробки сигналів тривоги систем відеоспостереження за допомогою нейромережі YOLOv8.*

*The problem of object recognition errors in images from outdoor surveillance cameras is considered. A solution for post-processing alarm signals of video surveillance systems using the YOLOv8 neural network is proposed.*

Наразі застосування камер зовнішнього спостереження для забезпечення безпеки на території певних об'єктів, підприємств та організацій є досить поширеною практикою. Проте, якщо територія огляду є великою, людина фізично не може безперервно стежити за усіма моніторами. Для цього використовують штучну нейронну мережу для автоматизованого розпізнавання об'єктів на відео з камери.

Проте, таке розпізнавання не завжди дає точний результат. Розглянемо таку ситуацію на прикладі фірми, яка спеціалізується на наданні комплексних послуг з відеоспостереження. Щодня їхні оператори отримують сигнали про порушення з декількох десятків камер. Середньодобова кількість сигналів становить майже 3000 (Більше 86 тис. за жовтень 2023 року). Слід зазначити, що переважна кількість камер знаходяться зовні, і зазнають значного впливу різних чинників, що спричиняють фальшиві спрацювання. Ці чинники можна об'єднати в 3 категорії : опади (дощ, сніг), вітер (розхитує об'єкти в полі зору камери, або саму камеру), світлові впливи (мерехтіння світла на території або за її межами, світло фар авто – в нічний час, відблиски від сонця, або просто тінь від хмари – в денний). Всі згадані чинники, а частіше – їх комбінації – мають значний вплив на фальшиві спрацювання камер. Так, за згаданий місяць кількість фальшивих спрацювань сягнула 44 тис, тобто понад 51% від усіх сигналів тривоги. На рисунку 1 (а, б, в) представлено зображення з камер з помилками розпізнавання об'єктів. Зважаючи на те, що кожен сигнал тривоги має бути перевірений людиною – фальшиві сигнали тривоги спричиняють значні збитки компанії, змушуючи утримувати на роботі збільшену кількість операторів.

Щодо рішень, які вже були запропоновані для вирішення цієї проблеми – це збільшення кількості камер, введення в експлуатацію новітніх систем аналізу потокового відео. Проте наразі це не дало дієвого результату.

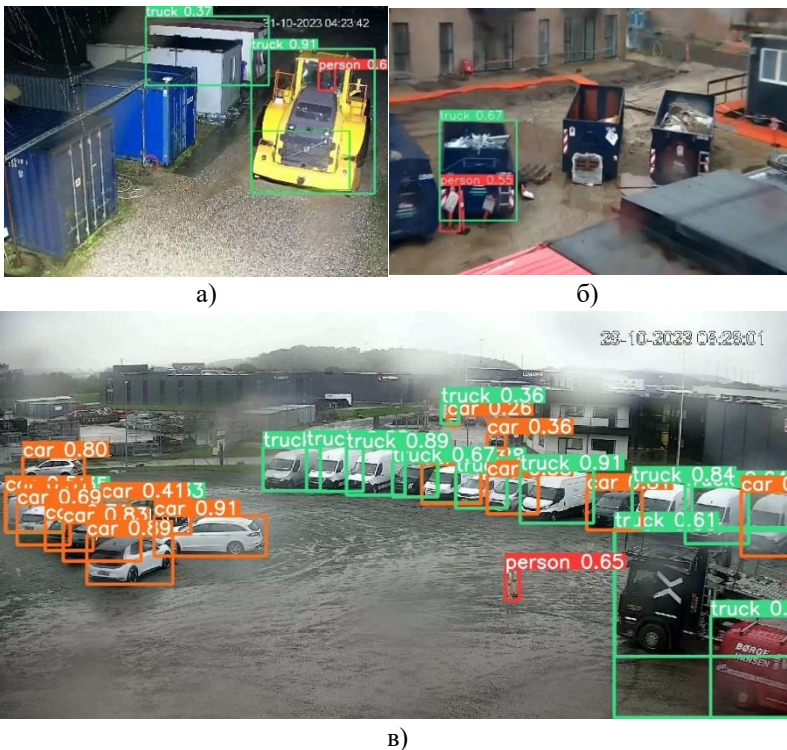


Рисунок 1 – Помилки розпізнавання об'єктів на зображеннях з камер зовнішнього спостереження

Як можна побачити з рисунку 1, у більшості випадків неймережа помилково розпізнає наявність людини на зображенні, приймаючи тонкий вертикальний об'єкт за особу.

Тому було прийнято рішення застосувати найновішу версію нейронної мережі YOLOv8 [1,2] для того, щоб навчити неймережу на реальних зображеннях з камер зовнішнього спостереження з метою підвищення точності розпізнавання об'єктів у полі зору камер.

Таким чином, алгоритм дій буде наступним:

1. Зібрати реальні датасети з камер зовнішнього спостереження для навчання неймережі на реальних об'єктах, які знаходяться в полі зору даних

камер (об'єкти, які найчастіше є на підприємстві – автомобіль, бульдозер, вантажівка, вантажний контейнер тощо);

2. Зібрати реальні датасети з камер зовнішнього спостереження для навчання нейромережі на предмет «людина – не людина», а саме зображення, де дійсно присутні особи та де нейромережа помилково розпізнала певні предмети як людину (рисунок 1 а, б, в);

3. Провести навчання нейромережі та експерименти щодо успішності чи неуспішності навчання та чи є підвищення якості розпізнавання після перенавчання нейромережі, у порівнянні із початковими результатами.

Для навчання було обрано нейромережу YOLOv8[1, 2]. На це будуть спрямовані зусилля авторів у подальших дослідженнях на тему пост-обробки сигналів тривоги систем відеоспостереження.

### **Перелік посилань**

1. Ultralytics YOLOv8 Docs URL: <https://docs.ultralytics.com/> (Доступ 2.10.2023)
2. Ultralytics on GitHub.com URL: <https://github.com/ultralytics/ultralytics/blob/main/docs/models/yolov8.md> (Доступ 2.10.2023)
3. Radiuk, P., Pavlova, O., El Bouhissi, H., Avsiyevych, V., Kovalenko, V. Convolutional Neural Network for Parking Slots Detection. CEUR Workshop Proceedings 2022, 3156, pp. 284–293



УДК 004.4

Побережна А.Ю.

*Хмельницький національний університет*

## **КІБЕРФІЗИЧНА СИСТЕМА МОНІТОРИНГУ СТАНУ РОСЛИН В РЕЖИМІ РЕАЛЬНОГО ЧАСУ**

*Розглянуто прикладні аспекти розробки кіберфізичної системи, що дозволяє здійснювати моніторинг стану рослин в режимі реального часу. Запропонована кіберфізична система надає точні параметри умов в, яких знаходиться рослина для їх покращення.*

*The applied aspects of the development of a cyber-physical system, which allows monitoring the condition of plants in real time, are considered. The proposed cyberphysical system provides accurate parameters of the conditions in which the plant is located for their improvement.*

Рослини відіграють важливу роль у житті кожної людини. Завдяки проведеним дослідженням було встановлено вплив на психологічний стан суспільства, а саме зниження стресу, поліпшення настрою, підвищення продуктивності та покращення концентрації уваги [1]. Фізичне здоров'я також покращується, знижується артеріальний тиск та головна біль. Всі ці позитивні наслідки на самопочуття особи, що взаємодіє з рослинністю спричинені тим, що вона перебуває в здоровому стані. Але ситуація кардинально змінюється коли потреби рослини ігноруються. Наслідком цього є погіршення здоров'я не тільки рослини, а і людини, що знаходиться поруч з нею. Хвора рослинність може бути джерелом патогенних мікроорганізмів і грибків, які впливають на самопочуття шляхом аерозольної інфекції. Деякі види домашніх квітів виділяють токсичні речовини, які є вкрай небезпечними. Описані наслідки поганого догляду за рослинами показують важливість вчасного передбачення їх потреб.

Практичним завданням є спостереження за станом рослини у зручному форматі, в режимі реального часу.

На сьогоднішній день існують прилади, що здатні здійснювати спостереження за рослинами. Наприклад відома китайська компанія Xiaomi, відома своїм широким асортиментом побутової техніки, випустила пристрій Xiaomi Mi Flora. Прилад вимірює температуру, вологість ґрунту та кількість поживних речовин. Додаток Mi Home забезпечує обробку та перегляд вимірних даних. Xiaomi Mi Flora використовує технологію Bluetooth та має невеликий розмір.

Незважаючи на всі переваги Xiaomi Mi Flora він має ряд недоліків. У приладі відсутні повідомлення про зниження рівня вологості. Функціонал обмежується в залежності від місцезнаходження. Також потрібно перевіряти сумісність пристрою з смартфоном на якому встановлюється програмне

забезпечення.. При відсутності достатньої вологи прилад не здатен здійснити надання води рослині. Пристрій некоректно працює у горщиках з великим субстратом, наприклад як в орхідеї [2].

Існують також аналоги Xiaomi Mi Flora, а саме Parrot Flower Power та FYTA Beam. Вони мають подібний функціонал і недоліки Xiaomi Mi Flora.

Враховуючи всі описані критерії Xiaomi Mi Flora і його аналогів вони не вирішують проблеми правильного моніторингу стану рослин.

Кіберфізична система моніторингу стану рослин в режимі реального часу вирішує поставлені завдання. Завдяки даному пристрою користувач має можливість дізнатися про вологість ґрунту (в якому перебуває рослина), вологість повітря, температуру повітря. Прилад чітко вимірює показник вологості субстрату різного розміру [3]. Місцезнаходження для користування не важливе, пристрій працює у будь-якому регіоні. Також кіберфізична система моніторингу стану рослин оснащена розумним горщиком, що надає рослині при потребі необхідну кількість води для встановлення оптимальної вологості ґрунту. Весь функціонал проводиться через додаток у смартфоні або комп'ютері.

Метою роботи є розробка кіберфізичної системи, що дозволяє здійснювати моніторинг стану рослин в режимі реального часу.

Розробка кіберфізичної системи моніторингу стану рослин в режимі реального часу складається з таких етапів: проєктування апаратної частини, налаштування програмного забезпечення, розробка апаратної частини, інтеграція всіх складових системи.

Проєктування апаратної частини розпочинається з вибору її компонентів (таблиця 1).

Таблиця 1 – Компоненти апаратної частини

Назва	Призначення
Wi-Fi модуль NodeMCU на основі ESP8266	Надсилання та отримання даних
Ємнісний датчик вологості ґрунту	Визначення вологості ґрунту
Сенсорний модуль DHT11	Визначення температури та вологості
Драйвер двигунів L293D	Керування наданням води
Водяний насос 5В	Надання води
Шланг довжиною 1 метр та діаметром 1 сантиметр	Переливання води
Батареї на 9В	Джерело електричної енергії
Контактні піни	З'єднання між платами
Діоди 1N4007	Перетворення змінного струму в постійний
Загальна друкована плата	Підтримка та з'єднання всіх компонентів
Провід	Проведення електричного струму

Далі розробляється принципова схема кіберфізичної системи моніторингу стану рослин в режимі реального часу (рисунок 1).

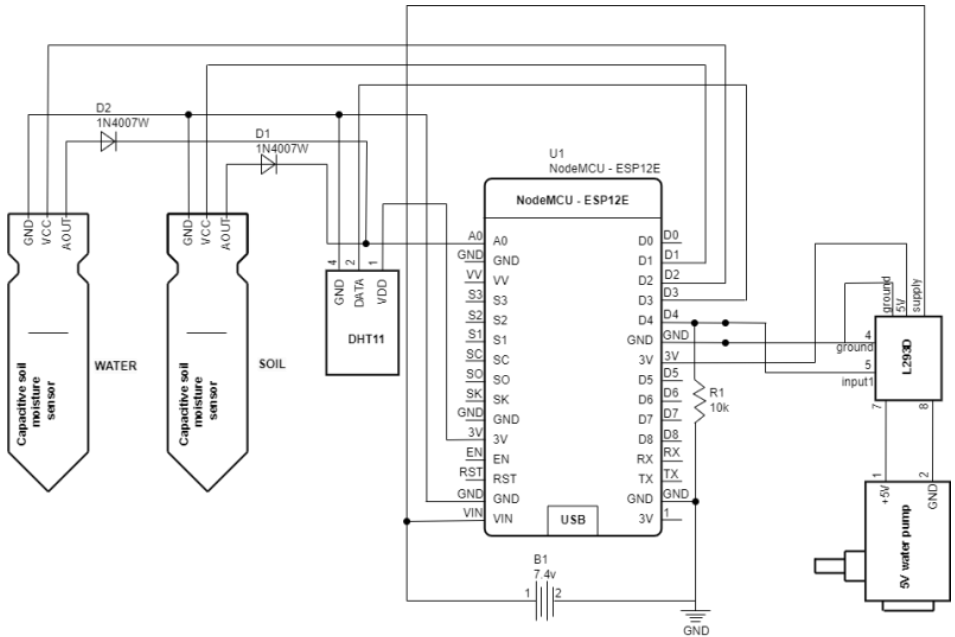


Рисунок 1 – Принципова схема кіберфізичної системи моніторингу стану рослин в режимі реального часу

NodeMCU зчитує значення датчиків вологі та модуля DHT, а потім надсилає ці значення на сервер Blynk через Wi-Fi з'єднання. Крім того, він керує насосом відповідно до вологості ґрунту або за допомогою команд програми. Позитивні клеми датчиків вологі під'єднуються до цифрових контактів 1 і 2, тому є можливість вмикати та вимикати кожен датчик. Тобто, якщо D1 ввімкнено, це означає, що датчик 1 ввімкнено. Діоди підключаються до виходів кожного датчика, а інша сторона діода під'єднується до аналогового штифта. Спочатку обертається D1 і одночасно зчитується аналогове значення. Отже, отримується аналогове значення 1 датчика. Далі вимикається D1 і вмикається D2 для отримання аналогового значення 2 датчика. Датчик DHT11 підключається до цифрового контакту 3, а драйвер двигуна L293D до D4. Резистор 10кОм використовується для витягування штифту двигуна. Модуль драйвера двигуна L293D має три контакти живлення на 5В. Контакт живлення L293D під'єднується до позитивної сторони батареї та до контакту 3,3В NodeMCU.

Налаштування програмного забезпечення відбувається в додатку Blynk. У ньому потрібно додати параметри, які зчитуються апаратною складовою. Це

температура, вологість ґрунту та вологість повітря. Для подання води мотором додається кнопка запуску.

Розробка апаратної частини здійснюється на основі принципової схеми (рисунок 2).

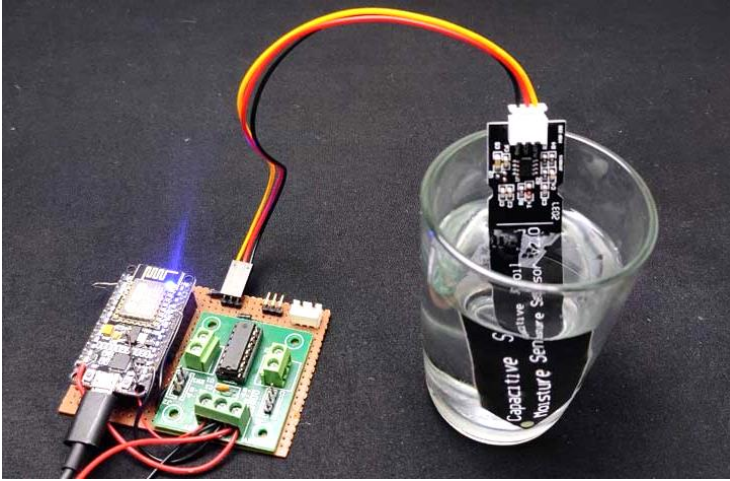


Рисунок 2 – Апаратна частина кіберфізичної системи моніторингу стану рослин в режимі реального часу



Рисунок 3 – Кіберфізична система моніторингу стану рослин в режимі реального часу

На останньому кроці розробки відбувається інтеграція апаратної та програмної частини через Wi-Fi. У результаті отримується кіберфізичної системи моніторингу стану рослин в режимі реального часу (рисунок 3).

Отже, запропонована кіберфізична система моніторингу стану рослин в режимі реального часу надає можливість отримати достовірні дані про вологість ґрунту, вологість повітря, температуру повітря, а також має функцію поливу. Подальші дослідження спрямовані на додавання нового функціоналу (система подання поживних речовин у ґрунт).

### Перелік посилань

1. Rudnyk-Ivashchenko O. I., Tsandur M. M., Schwartau V. V. Features of the impact of low temperatures on *Actinidia arguta*. *Fiziologia rastenij i genetika*. 2022. Т. 54, № 5. С. 450–459.
2. Xiaomi Mi Flora. URL: <https://www.danielmartingonzalez.com/en/caring-your-plants-with-mi-flora-and-home-assistant/>
3. Barrett S. F., Pack D. J. *Microcontrollers Fundamentals for Engineers and Scientists. Synthesis Lectures on Digital Circuits and Systems*. 2022. Т. 1, № 1. С. 1–124.

УДК 004.4

Присяжнюк О.О.

*Хмельницький національний університет*

## **ДОСЛІДЖЕННЯ ТА ПРОЕКТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ**

*Штучний інтелект – це сукупність раціональних, логічних і формалізованих інструментів правила, розроблені та закодовані людьми, які організують процеси та діяльність наслідування раціональних/інтелектуальних структур та створюють та відтворювати цілеспрямовані практики, а також механізми побудови подальшого кодування та прийняття рішень.*

*Artificial Intelligence is an ensemble of rational, logical, and formalized instrumental rules developed and coded by human beings that organize the processes and activities to emulate rational/intellectual structures and fabricate and reproduce goal-oriented practices as well as the mechanisms for constructing further coding and decision making.*

Штучний інтелект з'являється у свідомості людей як комбінація трьох тверджень - явища, проблеми і фрази (або концепції).

Як явище повсякденного життя, штучний інтелект не може бути розкритий іншим способом, крім як у формі матеріалізованих (відчутних) продуктів/пристроїв. Таким чином, ці пристрої мають подвійне призначення — технічне і соціальне. З одного боку, штучний інтелект постає як технологічний пристрій, призначений для вирішення завдання, яке неможливе для людини. З іншого боку, штучний інтелект існує не тільки в технічному середовищі. Технології, спочатку орієнтовані на інструментальні завдання, стають середовищем існування і учасниками людських взаємодій. Цю тенденцію називаємо “штучною соціальністю”[1].

Як дослідницька проблема, штучний інтелект: (1) піднімає філософські (світоглядні) питання; (2) по-новому характеризує соціальну реальність; проливає нове світло на специфіку і потенціал соціальної реальності; закликає переглянути панівні уявлення про соціальну реальність; (3) проявляється по-різному в різних науках. Для природничих та інженерних наук проблеми штучного інтелекту пов'язані з вирішенням технічних та інструментальних завдань. Для соціології та інших суспільних наук питання про штучний інтелект, по суті, є маргінальним, побічним питанням. У філософії, як і в гуманітарних науках в цілому, штучний інтелект обговорюється у зв'язку зі світоглядними проблемами, які по-різному вирішувалися в різні історичні епохи і в різних інтелектуальних традиціях.

Як словосполучення (концепція) в науковій літературі, штучний інтелект ще не визначений але має загальноприйняте значення.

Однак вчені повинні прийти до згоди у визначенні ШІ, щоб перейти до раціонального мислення про впровадження ШІ в реальність людського життя і суспільного розвитку.

### **Перелік посилань**

1. Rezaev A. V. (2021) Twelve thoughts on Artificial Intelligence and Artificial Sociality.
2. Pigge E., Tzudnowski I. Kuenstliche Intelligenz: Continental staerkt weltweites Experten-Netzwerk bis 2021.
3. Як створюється штучний інтелект. URL: <https://lemon.school/blog/yak-stvoryuyetsya-shtuchnyj-intelekt>
4. Штучний інтелект та artificial intelligence ACT. URL: <https://cedem.org.ua/analytics/artificial-intelligence-act/>
5. Історія розвитку «Штучного інтелекту в ІК». URL: <https://web.archive.org/web/20131203002125/http://www.iprinet.kiev.ua/gf/sergl.htm>

УДК 004.056.5

Рижий Я.О., Мельник М.М., Чешун О.В., Орленко В.С.

*Хмельницький національний університет*

## **КЛАСИФІКАЦІЯ АТРИБУТИВ ОСОБИ І ФОРМУВАННЯ ЦИФРОВОГО ПІДПISУ НА ЇХ ОСНОВІ**

*Здійснено ідентифікацію та класифікацію атрибутів для реалізації технології атрибутивного цифрового підпису в системах електронного документообігу, запропоновано спосіб формалізованого представлення різних класів атрибутів в математичній моделі та презентовано схему синтезу сигнатури підпису на основі формалізованого представлення особових атрибутів підписанта. Технологія синтезу підпису базується на принципах гнучкості, адаптивності та мультиатрибутності ЕЦП.*

*The identification and classification of attributes for the implementation of the technology of attributive digital signature in electronic document circulation systems is carried out, a method of formalized representation of various classes of attributes in a mathematical model is proposed, and a scheme of signature synthesis based on a formalized representation of the signatory's personal attributes is presented. The signature synthesis technology is based on the principles of flexibility, adaptability and multi-attribute EDS.*

Невід'ємною складовою сучасних технологій автоматизованого документообігу є електронні цифрові підписи (ЕЦП). ЕЦП забезпечує безпеку і юридичну дійсність віртуальних документів, ефективність їх обробки, ідентифікує автора документа, гарантує цілісність вмісту та має в електронному середовищі юридичний статус традиційного підпису на паперовому носії.

Згідно Закону України [1], «електронний підпис – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис».

Традиційна технологія формування ЕЦП базується на застосуванні асиметричної криптографії з використанням пари ключів (приватного і публічного) та алгоритмів обчислення хеш-функцій електронного документа[2]. Такий підхід забезпечує високий рівень безпеки та можливість перевірки цілісності документа, що робить криптографічний ЕЦП важливим інструментом для забезпечення конфіденційності та автентифікації в електронному документообігу.

В той же час, криптографічний ЕЦП має в певних аспектах використання ряд недоліків, до яких відносять знеособлення підписанта, вузькоспеціалізоване



застосування та звернення за послугами сертифікованих довірених сервісів при кожному підписанні документів[3].

Альтернативним напрямком технологій ЕЦП, який на сьогодні набуває популярності через відсутність вади знеособлення підписанта, гнучкість процедур і способів формування підпису та має перспективи нетрадиційного для ЕЦП застосування, є формування сигнатури підпису на основі особових атрибутів підписанта[3-5].

При вирішенні завдання технології синтезу ЕЦП на основі атрибутів підписанта виникає потреба вибору та класифікації атрибутів для включення до сигнатури підпису, формалізації вхідних даних технології та визначення принципів синтезу сигнатури на основі формалізованого представлення особових атрибутів, чому і присвячена дана робота.

Проведений аналіз дозволив виділити три типових категорії атрибутів особи:

- ідентифікаційні атрибути;
- неідентифікаційні атрибути;
- контекстуальні атрибути.

Як ідентифікаційні атрибути розглядаємо такі, які однозначно дозволяють ідентифікувати особу без додаткових уточнень.

До ідентифікаційних атрибутів відносяться: відбиток пальця; малюнок сітківки ока; ПІБ; підпис особи (рукописний); ідентифікаційний код; серія-номер паспорта; серія-номер диплома; офіційний псевдонім (псевдонім, який однозначно пов'язаний з особою); ідентифікатор (номер або серія-номер) посвідчення з місця роботи; номер водійського посвідчення; номер телефона (за умови індивідуального користування); особистий ідентифікатор електронної пошти (e-mail) або соціальних мереж тощо.

Як неідентифікаційні атрибути визначено такі дані особи, які в певному аспекті ідентифікують особу, але не дозволяють однозначно її ідентифікувати без додаткових уточнень, оскільки можуть належати певному колу осіб або мають масове розповсюдження.

До неідентифікаційних атрибутів можна віднести: ім'я; по батькові; розповсюджене прізвище; освіту; факс; місце роботи; посада; неідентифікуючий особу псевдонім (широко розповсюджений або такий, що відомий тільки довірений особі або обмеженому колу довірених осіб); дата народження; вік; дата видачі паспорта (будь-якого іншого документа тощо); орган, що видав паспорт (будь-який інший документ тощо); номер телефона загального користування та інші.

Якщо ідентифікаційні атрибути служать для точної ідентифікації особи, то неідентифікаційні атрибути надають контекст і додаткову інформацію без прямої

ідентифікації.

З наведених прикладів слідує, що неідентифікуючими атрибутами можуть бути як широко розповсюджені дані особи, так і нікому не відомі дані про особу.

Особливістю неідентифікуючих атрибутів є можливість отримання на їх основі у певних ситуаціях ідентифікаційного атрибута або ідентифікаційного набору атрибутів. Розповсюджені прізвище, ім'я та по батькові при об'єднанні утворюють ідентифікаційний атрибут ПІБ. Освіта, посада, місце роботи підписанта тощо можуть ідентифікувати його особу, якщо при аналізі визначиться відсутність конкурентів за відповідним атрибутом в колі здійснення ідентифікаційного аналізу. Така можливість повинна враховуватись в технології використання цифрового підпису в системах електронного документообігу, що є предметом подальших досліджень.

Як контекстуальні атрибути підпису будемо розглядати такі характеристики або ж параметри, які визначаються або можуть змінюватися залежно від конкретного контексту чи поточних обставин. В контексті ідентифікації особи ці атрибути надають додаткову інформацію про користувача, яка може бути корисною для точнішої та надійнішої ідентифікації підписанта в певному середовищі чи ситуації.

До контекстуальних атрибутів можна віднести: часові параметри накладання ЕЦП (дата, час, день тижня, місяць тощо); геолокаційні параметри накладання ЕЦП (геолокаційні координати, адреса або складові адреси, установа або офіс з можливістю уточнення їх місцезнаходження тощо); змінювані біометричні параметри фізичного стану особи (пульс, температура тощо); зовнішні умови оточуючого середовища; тип пристрою, задіяний для накладання ЕЦП; дані автентифікації під час входу в систему; права та повноваження підписанта; роль підписанта у певному конкретному контексті тощо.

У контексті електронного цифрового підпису саме комбінація різних типів атрибутів спрямована на створення безпечних та адресно-орієнтованих підписів. Зрозуміло, що не всі перелічені атрибути при реалізації технології доцільно включати до ЕЦП одночасно і загалом не всі вони є зручними для використання в технології та доцільними відповідно кожному окремо взятому застосуванню.

При визначенні базових принципів технології будемо акцентувати увагу на забезпеченні гнучкості, адаптивності та мультиатрибутності ЕЦП. Зазначені принципи передбачають надання підписанту можливості формувати цифровий підпис з довільної кількості атрибутів та визначати їх склад за власним побажанням або у відповідності до потреб.

Для гнучкості процедур автоматизованого вибору атрибутів і забезпечення математичного підґрунтя адаптивності мультиатрибутного формування ЕЦП

формується множини відповідних атрибутів. В якості ідентифікаторів множин атрибутів використано аббревіатури англomовного перекладу назв множин:

- $IA$  – ідентифікаційні атрибути (Identifying Attributes);
- $NIA$  – неідентифікаційні атрибути (Non-Identifying Attributes);
- $CA$  – контекстуальні атрибути (Contextual Attributes).

Таким чином ми отримуємо три множини атрибутів:

$$IA: \{IA_1, IA_2, \dots, IA_b, \dots, IA_k\}, \quad (1)$$

$$NIA: \{NIA_1, NIA_2, \dots, NIA_j, \dots, NIA_m\}, \quad (2)$$

$$CA: \{CA_1, CA_2, \dots, CA_b, \dots, CA_n\}, \quad (3)$$

де  $IA$  – множина ідентифікаційних атрибутів  $IA_i \in IA$  особи-підписанта;  $NIA$  – множина неідентифікаційних атрибутів  $NIA_j \in NIA$  особи-підписанта;  $CA$  – множина контекстуальних атрибутів  $CA_l \in CA$  особи-підписанта або самого підпису.

Схематично процедура формування цифрового підпису в примітивах математичної моделі технології представлена на рисунку 1.

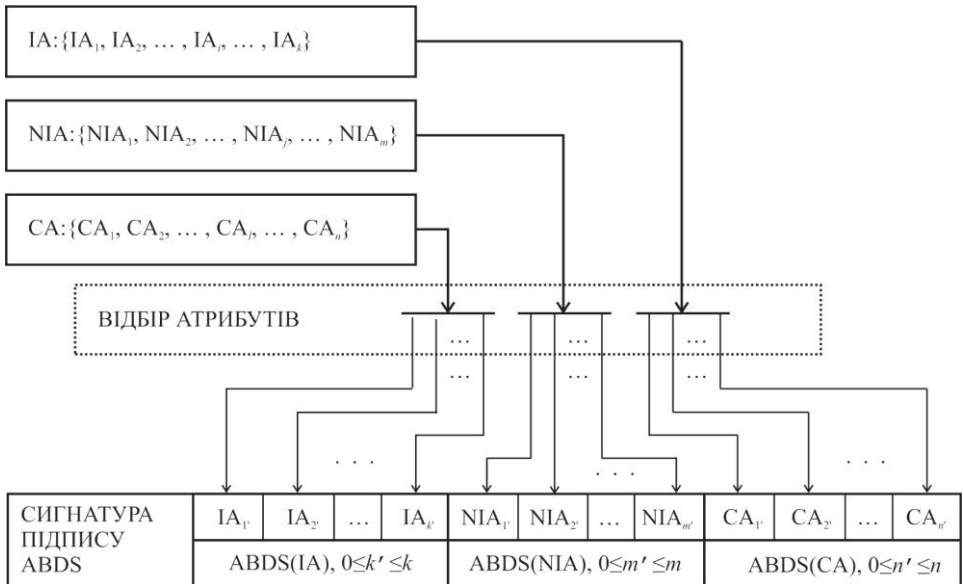


Рисунок 1 – Схема утворення сигнатури цифрового підпису з атрибутів

Кожне значення атрибуту  $IA_i \in IA$ ,  $NIA_j \in NIA$  і  $CA_l \in CA$  є двійковим представленням відповідного атрибуту, тому далі будемо ідентифікувати елементи

множин як двійкові коди або двійкові вектори атрибутів. Формування цифрового підпису в примітивах математичної моделі технології зводиться до вибору елементів множин  $IA_i \in IA$ ,  $NIA_j \in NIA$  і  $CA_l \in CA$ , які відповідають потребам-побажанням підписанта, та поєднання їх у єдину двійкову послідовність – вектор (сигнатуру) цифрового підпису на основі атрибутів ABDS (Attribute-Based Digital Signature).

Сигнатура ABDS цифрового підпису, синтезована на основі двійкових векторів атрибутів, разом з хеш-сигнатурою відкритого тексту, може піддаватися криптографічному шифруванню (закриттю) і додаватися до відкритого тексту за класичними технологіями накладання ЕЦП. В той же час, можливе використання сигнатури цифрового підпису на основі атрибутів ABDS і у відкритому вигляді, без закриття шифруванням, що визначається цілями та потребами підписанта. Ці дві передбачувані перспективи роблять можливим використання технології цифрового підпису в системах електронного документообігу більш широкими, а саму технології гнучкішою і більш універсальною.

### Перелік посилань

1. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 01.12.2022р. URL:<https://zakon.rada.gov.ua/laws/show/2155-19/ed20231231#Text> (дата звернення: 09.11.2023).
2. Метьолкін А.О., Кардашук В.С. Дослідження методів підвищення криптографічної стійкості. Вісник східноукраїнського національного університету імені Володимира Даля. 2018. № 6 (247). С. 90-95.
3. Ke Gu, Keming Wang, Lulu Yang. Traceable attribute-based signature. Journal of Information Security and Applications. Volume 49. 2019. Article ID 102400.
4. Victor Sucasas, Georgios Mantas, Maria Papaioannou, Jonathan Rodriguez. Attribute-Based Pseudonymity for Privacy-Preserving Authentication in Cloud Services. IEEE Transactions on Cloud Computing. 2023. Vol.11, №.1. pp.168-184.
5. Qianqian Su, Rui Zhang, Rui Xue, You Sun, Sheng Gao. Distributed Attribute-Based Signature With Attribute Dynamic Update for Smart Grid. IEEE Transactions on Industrial Informatics, 2023. Vol.19, №.9. pp. 9424-9435.

УДК 004.4

Ровінчук Д.Ю.

*Хмельницький національний університет*

## **МЕТОД ТА ПРОГРАМНІ ЗАСОБИ ВИЯВЛЕННЯ МЕТАМОРФНИХ КОМП'ЮТЕРНИХ ВІРУСІВ**

*Розглянуто важливий аспект кібербезпеки, а саме виявлення та аналіз метаморфних вірусів, надається інформація про різні методи та підходи до цього завдання, що забезпечує ефективність боротьби з таким видом шкідливого програмного забезпечення. Запропоновано метод розпізнання та передбачення для боротьби з такими вірусами.*

*An important aspect of cyber security, namely the detection and analysis of metamorphic viruses, is considered, and information is provided on the various methods and approaches to this task that ensure the effectiveness of combating this type of malware. A recognition and prediction method is proposed to combat such viruses.*

Ще більш досконалою технікою є метаморфічний код, у якому вірус повністю переписує себе під час кожного виконання. Метаморфізм - це техніка, яка мутує динамічний двійковий код задля обходу виявлення. Вона змінює опкоди при кожному запуску інфікованої програми і не використовує жодного шифрування чи дешифрування. Зловмисне програмне забезпечення ніколи не зберігає однакову послідовність опкодів в пам'яті. Ця техніка також називається динамічною обфускацією коду. Існують два види метаморфного зловмисного програмного забезпечення: "Зловмисне програмне забезпечення закритого світу", який не залежить від зовнішньої комунікації і може генерувати новий мутований код, використовуючи або двійковий трансформатор, або метамову, і "Зловмисне програмне забезпечення відкритого світу", яка може взаємодіяти з іншими сайтами в Інтернеті та оновлювати себе новими функціями.

Метою даної роботи є детальний аналіз та розгляд різноманітних методів, технологій та програмних засобів, призначених для ефективного виявлення та протидії метаморфним вірусам у комп'ютерних системах. Додатково, буде розглянуто приклади практичного використання цих методів у реальних сценаріях, щоб продемонструвати їхню ефективність та застосовність в сучасному антивірусному забезпеченні.

Метод лінійного дискримінантного аналізу (LDA) часто використовується у багатьох областях, таких як машинне навчання та шаблони розпізнавання для виділення ознак, які зберігають клас роздільності. LDA базується на концепції пошуку для лінійної комбінації предикторів, яка найкраще розділяє два або більше класів.

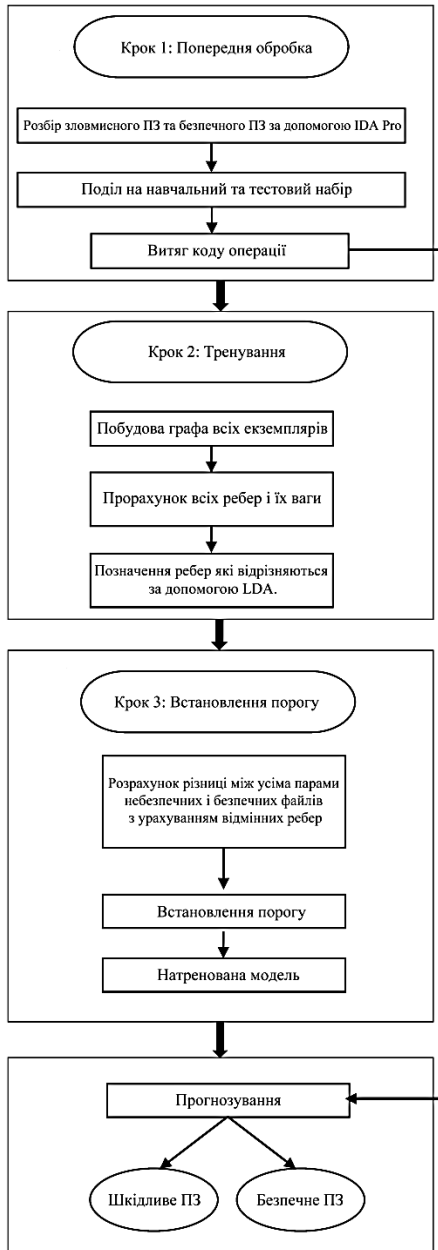


Рисунок 1 – Блок-схема запропонованого методу

За допомогою LDA вибираються функції на основі співвідношення сумарної внутрішньокласової мінливості і міжкласової відмінності. Внутрішньокласова матриця розсіювання  $S_w$  обчислюється наступним чином:

$$S_w = \sum_{i=1}^c P_k S_i \quad (1)$$

де  $c$  – кількість класів (у нашому випадку це буде 2, оскільки існує два класи, тобто шкідливе програмне забезпечення і доброякісне програмне забезпечення),  $P_k$  – ймовірність для класу  $k$ ,  $S_i$  - відхилення від функції.

На рисунку 1 наведено узагальнену методологію, запропоновану в цій роботі. Основною метою тут є покращення методу визначення схожості графів опкодів (OGS) за допомогою LDA. Щодо техніки OGS, необхідно створити графи на основі опкодів і порівнювати їх для визначення, чи належить вхідний файл до метаморфної родини чи ні.

На першому етапі нам потрібно підготувати наш набір даних. Наш метод базується на статичному аналізі, тому необхідно видобути послідовності опкодів з файлів. Для видобутку опкодів, кожен файл повинен бути перетворений на машинні інструкції. Для цього ми використовували IDA Pro. Операнди в машинних інструкціях не відіграють важливої ролі, тому ми їх виключаємо. Потім набір даних розділяється на навчальний та валідаційний набори. У цьому дослідженні використовується метод перехресної перевірки  $k$ -кратності.

Як вже зазначалося, в методології OGS всі ребра та вузли відіграють важливу роль у результаті аналізу. У метаморфних шкідливих програмах часто використовується техніка обфускації, яка включає в себе вставку "мертвого" коду. Такий "мертвий" код також враховується у графах та ребрах, і це може призвести до неправильних сигналів у методології OGS. Згідно з дослідженням, OGS не здатний відізнати високо обфускованих метаморфних черв'яків від безпечних програм. Тому основною метою цього етапу є вилучення "мертвого" коду та зайвих ребер з графів.

Запропонований підхід для виявлення метаморфних комп'ютерних вірусів, який базується на графі коду операцій, забезпечує високу ефективність у виявленні шкідливого програмного забезпечення. Майбутні дослідження спрямовані на практичне використання цих методів у реальних сценаріях, з метою продемонструвати їхню ефективність і придатність для сучасних антивірусних рішень.

### Перелік посилань

1. Spafford, E. H., Heaphy, K. A., and Ferbrache, D. J. 1989. A computer virus primer
2. R. Mirzazadeh. 2015. Metamorphic Malware Detection Using Linear Discriminant Analysis and Graph Similarity.
3. A.K. Jha, A. Vaish, 2022. A Novel Framework for Metamorphic Malware Detection.
4. J. Aucocck, Computer Viruses and Malware. Springer Science+Business Media, LLC, 2006

УДК 004.4

Родін О.О., Яшина О.М.

*Хмельницький національний університет*

## **МЕТОД СПЕКТРАЛЬНИХ ХАРАКТЕРИСТИК ЗВУКОВОГО СИГНАЛУ ДЛЯ ВИЗНАЧЕННЯ РІВНЯ ПСИХОЛОГІЧНОГО СТАНУ ЛЮДИНИ ЗА ДОПОМОГОЮ ГЛИБИННОГО НАВЧАННЯ**

*Розглянуто використання методу спектральних характеристик звукового сигналу для оцінки психологічного стану особи. Запропонований підхід дозволяє покращувати точність оцінки психологічного стану не лише на основі збільшення об'ємів даних, а й за рахунок динамічного визначення найбільш релевантних наборів використовуваних характеристик.*

*The use of spectral characteristics of a sound signal to assess a person's psychological state is considered. The proposed approach makes it possible to improve the accuracy of the assessment of the psychological state not only based on increasing data volumes but also due to the dynamic determination of the most relevant sets of used characteristics.*

Депресія – це серйозний психічний розлад, який впливає на ментальне, емоційне і фізичне здоров'я людини. Ця проблема вимагає уваги та лікування, оскільки має серйозні наслідки для індивідуального та суспільного здоров'я. Раннє виявлення депресії є дуже важливим аспектом в сучасному світі, оскільки дає змогу почати лікування на ранніх стадіях на відміну від пізніх і клінічних стадій депресії. Звернення до лікаря зазвичай відбувається лише при наявності симптомів, які характеризують помірну або тяжку депресію. Саме тому важливо мати змогу проводити раннє детектування ознак депресії в людей шляхом простого зручного ненав'язливого способу, як от наприклад, мобільний застосунок.

Детектування депресії на основі звукового сигналу має безліч переваг, бо на відміну від інших способів, звуковий сигнал найпростіше отримати і обробити (в порівнянні з, наприклад, відео-сигналом, сигналами з МРТ чи енцефалограми головного мозку та ін.) [1]. На даний момент методи визначення психологічного стану людини на основі обробки голосових даних можна розділити на 2 групи [2]:

- статична обробка голосових маркерів звукового сигналу (метод lookup);
- динамічна обробка потоку голосового сигналу з використання нейронних мереж.

*Статистична обробка* потребує менших потужностей і часу обробки але має досить низький рівень точності визначення психологічного стану людини, в той



час як динамічна обробка з використанням нейронних мереж має вищу точність але і потребує більше часу та виконавчих потужностей.

*Динамічна обробка* звукового сигналу з використанням нейронних мереж будується на основі визначенні і виокремленні характеристик звукового сигналу. Основними типами характеристик звукового сигналу є [3]:

- акустичні характеристики;
- просодичні характеристики;
- спектральні характеристики.

*Акустичні характеристики* (висота, сила, довгота, тон, шум, тембр) є досить суб'єктивними і не можуть бути уніфікованими для отримання результату.

*Просодичні характеристики* (мелодика, відносна сила вимови слів та їхніх частин, співвідношення відрізків мовлення по довготі, загальний темп мовлення, паузи, загальне темброве забарвлення тощо) а особливо варіативність значень цих характеристик частково корелюють з психо-емоційним станом людини.

*Спектральні характеристики* (Intensity, LPCC, Formant, ZCR та ін.) є найбільш сприйнятливими для оцінки психоемоційного стану людини.

Відповідно до останніх досліджень, найбільш доцільним є використання наборів характеристик для отримання результату [3]. На відміну від використання певної спектральної характеристики звукового сигналу, використання групи характеристик дає вищу точність отриманого результату. В порівнянні з використанням всіх можливих спектральних характеристик мови, використання набору характеристик є значно швидшим та потребує менше потужностей, а також все ще є точнішим (спектральні характеристики які мають слабку кореляцію з психо-емоційним станом та додають інформаційного шуму, виключаються з вибірки). Здебільшого, при використанні груп спектральних характеристик використовуються групи з 3ох характеристик, та відбувається дискримінація ефективності цих характеристик на основі гендерної приналежності суб'єктів. Приклад точності визначення психологічного стану людини з використання груп акустичних характеристик наведена в таблиці 1 для чоловіків та в таблиці 2 для жінок.

Як видно з даних, наведених в таблицях 1 та 2, точність визначення психоемоційного стану з використанням груп спектральних характеристик для жінок є вищою ніж для чоловіків. А також, набори найбільш ефективних спектральних характеристик, відрізняються для різних гендерів. Також, приведена точність визначення психоемоційного стану не є достатньою для попередньої оцінки психоемоційного стану особи.

Окрім дискримінації точності результатів поза гендером особи, існують відмінності в точності результатів з використанням груп спектральних характеристик сигналу на основі вікової групи а також расової приналежності [4].

Також, на точність результату впливає рівень володіння мовою особи, яка піддається оцінці психоемоційного стану.

Таблиця 1 – Класифікаційний показник поєднання трьох класів ознак для чоловіків

Група ознак			
Ознака 1	Ознака 2	Ознака 3	Точність
Intensity	LPCC	Formant	62.4%
Intensity	Jitter	ZCR	62.1%
LPCC	Jitter	Formant	62.1%
Intensity	Jitter	LPCC	61.8%

Таблиця 2 – Класифікаційний показник поєднання трьох класів ознак для жінок

Група ознак			
Ознака 1	Ознака 2	Ознака 3	Точність
TEO	Mel logarithmic power	LPCC	67.3%
Mel logarithmic power	TEO	ZCR	67.0%
Mel logarithmic power	TEO	Formant	66.9%
jitter	Intensity	Mel logarithmic power	66.8%

Беручи до уваги особливості наведені вище, пропонується розробити комбінований метод, що використовуватиме глибокі мережі, множиною вхідних даних для яких буде точність отриманих результатів для різних наборів спектральних характеристик, гендерного розподілу, расової приналежності та вікової групи. Результатом роботи глибокої мережі буде отримання комбінації з наступних складових:

- група спектральних характеристик звукового сигналу;
- гендерна приналежність;
- расова приналежність;
- вікова група.

Перевагою даного методу є отримання наборів складових характеристик для подальшого використання, що призводитиме до збільшення точності отриманого результату зі збільшенням оброблених даних.

Недоліком методу є необхідність отримання досить великого набору даних, рівномірно розподіленого між віковими групами, етнічною складовою, гендерною приналежністю та групами спектральних характеристик звукового сигналу.

Отже, запропонований метод являється методом для отримання метайнформації щодо найбільш ефективних наборів складових характеристик, значення яких далі використовуватимуться для оцінки психо-емоційного стану. Також, зі збільшенням кількості вхідних даних, запропонований метод прогнозуватиме набори складових характеристик, які дозволяють отримати результат визначення психо-емоційного стану особи з найбільшою точністю.

Подальші дослідження спрямовані на реалізацію запропонованого методу, підтвердження очікуваних результатів емпіричним шляхом, оцінку точності методу та перевірку працездатності методу в поточних реаліях.

#### **Перелік посилань**

1. Faming Yin, Jing Du, Xinzhou Xu, Li Zhao: Depression Detection in Speech Using Transformer and Parallel Convolutional Neural Networks. URL: <https://www.mdpi.com/2079-9292/12/2/328> (2023).
2. Hongbo Wang, Yu Liu, Xiaoxiao Zhen, Xuyan Tu: Depression Speech Recognition With a Three-Dimensional Convolutional Network. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8514878/> (2021).
3. Han Tian, Zhang Zhu, Xu Jing: Deep learning for Depression Recognition from Speech. URL: <https://link.springer.com/article/10.1007/s11036-022-02086-3> (2023)
4. Taylor W. Hargrove, Carolyn T. Halpern, Lauren Gaydosh, Jon M. Hussey, Eric A. Whitsel, Nancy Dole, Robert A. Hummer, Kathleen Mullan Harris: Race/Ethnicity, Gender, and Trajectories of Depressive Symptoms across Early- and Mid-Life among the Add Health Cohort. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7338256/> (2020).

УДК 004

Савчук А.В.

*Київський національний університет імені Тараса Шевченка*

## **РОЗРОБКА БІБЛІОТЕКИ ДЛЯ ПОБУДОВИ ТА ОБЧИСЛЕНЬ ЕЛЕКТРИЧНИХ КІЛ**

*Описано процес створення програмної бібліотеки, що призначена для проектування, моделювання та аналізу електричних кіл. Розроблена бібліотека містить серію алгоритмів для точних розрахунків таких параметрів кіл, як напруга, струм і потужність, і може застосовуватися у сфері освіти та наукових досліджень.*

*Described is the process of creating a software library for designing, simulating, and analyzing electrical circuits. The developed library incorporates a suite of algorithms for accurate calculations of circuit parameters like voltage, current, and power, making it suitable for use in educational and research settings.*

Зі зростанням потреби в точних та ефективних методах аналізу електричних кіл у виробництві та освіті, виникає необхідність у розробці бібліотек, які дозволять швидко та легко обчислювати необхідні параметри.

Метою роботи є створення бібліотеки, що дозволяє ефективно виконувати обчислення для електричних кіл і може бути інтегрована з іншими програмними інструментами.

Для обчислення параметрів кіл використано метод контурних струмів (Mesh Current Analysis) та метод вузлових потенціалів (Nodal Analysis), які є стандартними для цієї галузі та забезпечують високу точність результатів [1].

Метод контурних струмів ґрунтується на розрахунку гіпотетичних струмів у незалежних контурах схеми, що дозволяє знаходити реальні струми у гілках кола. Метод вузлових потенціалів використовує систему лінійних рівнянь для визначення потенціалів вузлів відносно загальної землі, що також дозволяє обчислити струми в кожній гілці кіл.

Бібліотека надає функціональні можливості для:

- Моделювання лінійних та нелінійних елементів кіл;
- Врахування частотних характеристик компонентів;
- Аналізу перехідних процесів та стійкості систем;
- Визначення режимів роботи та оптимізації параметрів.

Результати обчислень можуть бути використані для:

- Прогнозування поведінки кіл при зміні параметрів;
- Оптимізації елементів схем для досягнення бажаних характеристик;
- Навчальних цілей, для ілюстрації базових та складних концепцій електротехніки;
- Дослідження ефектів, властивих певним типам електричних кіл.

Крім того, бібліотека обладнана інтерфейсом для інтеграції з популярними САД-системами та підтримує модульну архітектуру для легкого розширення функціоналу в майбутньому [2]. Такий підхід дозволяє інженерам та науковцям швидко адаптувати бібліотеку під конкретні завдання та сприяє впровадженню новітніх наукових розробок у практичну діяльність.

### **Перелік посилань**

1. Smith, J. "Advanced Circuit Analysis and Simulation". IEEE Press, 2021.
2. Green, M., and Brown, L. "Integration of Simulation Software with CAD Tools". Journal of Electrical Engineering, vol. 67, no. 3, 2022, pp. 153-160.

УДК 004.052.32

Сверба А.А.

*Хмельницький національний університет*

## **УДОСКОНАЛЕННЯ МЕТОДУ РОБОТИ З МЕТРИКОЮ СЕРЕДЬНОГО ЧАСУ МІЖ ВІДМОВАМИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОГО ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ**

*Розглянуто основні аспекти метрики середнього часу між відмовами, що застосовується на етапі тестування програмного забезпечення. Представлено підходи до удосконалення методу роботи з даною метрикою з використанням різних додаткових компонентів та аспектів сфери інженерії програмного забезпечення. Запропоновані способи удосконалення мають на меті покращити результати розрахунку показника метрики, дати можливість швидкого реагування на зміни параметрів надійності та забезпечити ефективніше оцінювання результатів тестування в цілому.*

*The main aspects of the mean time between failures metric, which is used at the stage of software testing, are considered. Approaches to improving the method of working with this metric using various additional components and aspects of software engineering are presented. The proposed methods of improvement are aimed at improving the results of the calculation of the metric indicator, enabling a quick response to changes in reliability parameters, and ensuring a more efficient evaluation of test results in general.*

Інформаційний прогрес суспільства виступає рушійною силою для розробки різноманітного програмного забезпечення, яке використовується у всіх сферах нашого життя. Життєвий цикл ПЗ поділений на певну кількість етапів, кожен з яких є однаково важливими для загального функціонування програми. Одним з них є тестування. Тестування програмного забезпечення є етапом розробки, що забезпечує виправлення помилок, виявлення вразливостей ПЗ і забезпечення відповідності програми вимогам користувачів [1].

Процес безпосереднього тестування відбувається за допомогою різних засобів та додаткових компонентів, які сприяють збільшенню якості отриманих результатів тестування. Одним з таких компонентів виступають метрики тестування. Метрики – це вимірювані параметри та показники, які використовуються для оцінки процесу та результатів тестування програмного забезпечення [2]. Вони надають об'єктивну інформацію про якість програми, ефективність тестування та його прогрес, що допомагає розробникам та тестувальникам приймати обґрунтовані рішення та вдосконалювати процес розробки.

Важливою метрикою етапу тестування програмного забезпечення є метрика середнього часу між відмовами (MTBF), яка використовується для оцінки надійності ПЗ та вимірювання часу його безпомилкової роботи [2]. Існують різні варіанти вимірювання даної метрики, кожен з яких описує власний підхід до перевірки стабільності роботи програми. Проте наявні способи розрахунку використовують більш традиційний підхід знаходження результатів метрики, що може призвести до зниження ефективності тестування програмного забезпечення. Саме тому існує потреба удосконалення методу роботи з метрикою MTBF для покращення надійності роботи ПЗ.

Доступні на сьогодні публікації та дослідження даної тематики описують певні способи, що можуть покращити процес роботи з метрикою MTBF. Серед наявних покращень вказані такі: використання різних статистичних методів для точнішого прогнозу надійності роботи програмного забезпечення, застосування методів машинного навчання для якіснішого знаходження та представлення результатів процесу оцінки надійності [3], застосування різних архітектурних моделей програмних систем для деталізації процесу взаємодії різних компонентів системи та їх вплив на надійність загальної роботи ПЗ [4], використання емпіричних даних про відмови в роботі програми та їх послідовний моніторинг для встановлення певних закономірностей у разі зупинки роботи ПЗ [5]. Аналіз останніх публікацій та досліджень є дуже важливим, оскільки основні їх моменти будуть слугувати для досягнення мети дослідження.

Основною метою даного дослідження є опис та представлення способів удосконалення методу роботи з метрикою середнього часу між відмовами, висвітлення їх ключових аспектів та напрямків для подальшого прогресу.

Враховуючи основне завдання роботи, можна сформулювати декілька нових підходів до роботи з метрикою середнього часу між відмовами. Одним з перших способів удосконалення є розвиток нових моделей та алгоритмів для розрахунку показника середнього часу між відмовами. Прогрес в дослідженні нових структур може внести суттєвий вклад у покращення методу MTBF та оцінки надійності програмного забезпечення. Основні напрямки розвитку можуть включати: розробку моделей та алгоритмів, які базуються на складних взаємозв'язках між компонентами програмного забезпечення; покращене моделювання, основні принципи якого разом із оцінкою MTBF повинні бути використані ще на ранніх етапах розробки програмного забезпечення; використання штучного інтелекту для якіснішого прогнозування показника MTBF на основі вже відомих даних про роботу програмної системи.

Наступним загальним способом удосконалення методу роботи з метрикою MTBF є інтеграція з іншими метриками. Поєднання різних метрик допомагає сформулювати більш докладне уявлення про стабільність системи і виявити можливі проблеми, які могли бути пропущені у випадку використання лише метрики MTBF. Різні метрики ґрунтуються на різних показниках і призначені для надання оцінки в конкретних ситуаціях. У спільному використанні з MTBF вони можуть стати

надійним інструментом для оцінки надійності та загальної продуктивності програми. Серед метрик, які можуть бути використані в комбінації з метрикою середнього часу між відмовами, існують такі: MTTF (метрика середнього часу до першої відмови), SER (метрика, яка дозволяє визначити кількість помилок, виявлених у програмному забезпеченні протягом певного періоду час), TTF (метрика, що визначає час до відмови окремого компонента або модуля системи), MTTR (метрика середнього часу відновлення ПЗ після відмови), динамічні метрики для покращення вимірювання різних показників (Code Coverage, Fault Detection Rate, Failure Rate).

Ще одним способом для удосконаленої роботи з метрикою MTBF може бути впровадження автоматизації розрахунку показника метрики. Введення такого заходу може значно спростити розрахунки, вдосконалити метрику середнього часу між відмовами програмного забезпечення і підвищити його ступінь надійності. В межах даного напрямку покращення важливим може бути використання спеціалізованих програмних інструментів для швидкого та точного розрахунку показника MTBF на основі емпіричних даних про ПЗ, а також впровадження інтеграції з системами моніторингу та журналювання для автоматичного збору інформації про помилки у роботі ПЗ та інші необхідні параметри.

Останнім способом удосконалення методу роботи з метрикою середнього часу між відмовами може виступати розробка методів та інструментів для моніторингу MTBF в реальному часі. У поєднанні з попереднім методом дана процедура представляє собою абсолютно новий підхід до збору інформації про всю роботу програмної системи. Така інформація надходить автоматично в режимі реального часу, що дозволяє реагувати на будь-які зміни та постійно відстежувати показник MTBF. Також швидкий збір інформації сприяє негайному проведенню її аналізу для прийняття різних рішень, що пов'язані з роботою програмного забезпечення.

Отже, інтеграція запропонованих у статті підходів до вдосконалення методики використання метрики MTBF сприятиме підвищенню точності оцінки результатів тестування програмного забезпечення та забезпечить створення більш надійних програмних систем. Подальші дослідження можуть бути спрямовані на практичне впровадження та перевірку ефективності запропонованих підходів.

### **Перелік посилань:**

1. В.Е. Льюїс, Тестування програмного забезпечення та постійне покращення якості (3-є видання), 2016.
2. Ф. Норман, Метрики програмного забезпечення: суворий і практичний підхід (3-тє видання), 2014.
3. Є. Лініг, Х. Брюммер, «Аналіз надійності», Основи проектування електронних систем, 2017.
4. А. Біроліні, Розробка надійності: теорія та практика, Берлін 2013.
5. С. Кумар, С. Ратор, Прогноз програмних збоїв: дорожня карта, 2017.



УДК 004.7

Свистун С.О., Мельниченко О.В., Скрипник Т.К.

*Хмельницький національний університет*

## **ПРОЄКТУВАННЯ РОБОЧОЇ МІСІЇ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В ТРИВИМІРНОМУ ПРОСТОРІ**

*У статті розглядається процес проектування робочої місії безпілотних літальних апаратів (БПЛА) в тривимірному координатному просторі. Описуються ключові етапи планування місії, від визначення координат до тестування системи. Висвітлюється потреба у розробці нового методу побудови маршрутів для БПЛА, який би дозволяв автоматично коригувати траєкторію польоту та забезпечував самонавчання системи. Особливо розглядаються три можливі траєкторії польоту в конкретному робочому середовищі, а саме: пріоритетна, допустима та небажана. Аналізуються час та ефективність кожної з траєкторій, на підставі чого робиться висновок про перевагу пріоритетної траєкторії. Автори підкреслюють, що вибір оптимального маршруту сприяє підвищенню ефективності моніторингу та збору даних.*

*The article examines the process of designing the working mission of unmanned aerial vehicles (UAVs) in a three-dimensional coordinate space. It describes the key stages of mission planning, from determining coordinates to testing the system. The need for developing a new method of constructing routes for UAVs is highlighted, which would allow for automatic adjustment of the flight trajectory and facilitate the system's self-learning. Three possible flight trajectories in a specific working environment are separately considered: priority, permissible, and undesirable. The time and efficiency of each trajectory are analyzed, based on which a conclusion is made about the advantages of the priority trajectory. The authors emphasize that choosing the optimal route contributes to enhancing the efficiency of monitoring and data collection.*

**Постановка проблеми.** Ефективне здійснення робочого завдання вимагає попереднього його планування [1-3]. Окреслимо ключові етапи проектування робочої місії БПЛА у тривимірному просторі [4,5]: 1) встановлення стартових та кінцевих координат місії; 2) призначення технічних параметрів БПЛА; 3) розробка маршруту з урахуванням особливостей робочого середовища; 4) ініціація налаштувань технічного обладнання; 5) проведення перевірки та тестування.

Основною відмінністю функціонування робочої місії є формування та визначення шляху руху БПЛА у середовищі виконання завдання [6]. Завдання реалізується в умовах, що можуть змінюватись, з можливістю впливу зовнішніх факторів та подій на траєкторію руху БПЛА. Серед таких факторів можна виділити зміни погодних умов, пориви вітру, критичний стан батареї, появу несподіваних

перешкод і ін. [7,8]. Таким чином, важливим є розробка інноваційних методик побудови маршрутів для БПЛА у тривимірному просторі, які забезпечать можливість автоматичного корегування і відновлення координат руху після критичних збоїв та сприятимуть самонавчанню системи під час виконання завдань.

**Формалізація траєкторій польоту.** Аналіз типового середовища роботи в саду дозволив визначити три можливі траєкторії руху для групи БПЛА: (I) пріоритетну, (II) допустиму та (III) небажану. Їх графічне представлення демонструється на рисунку 1.

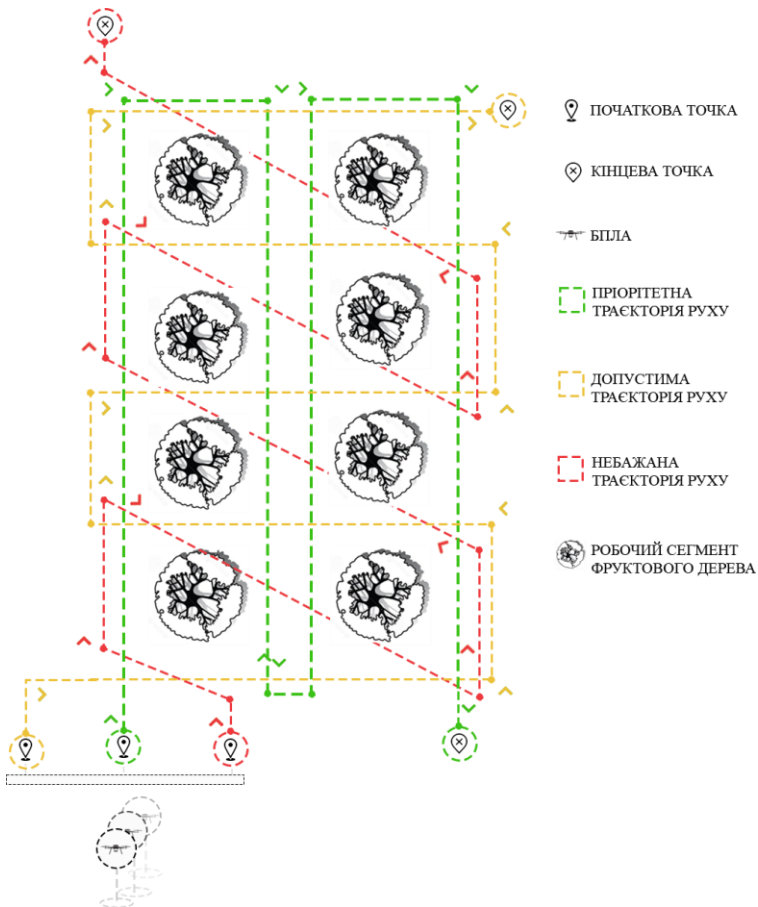


Рисунок 1 – Схема можливих траєкторій руху групи БПЛА у тривимірному координатному просторі

Розглянемо вибір саме пріоритетної траєкторії руху БПЛА з рисунку 1 проти решти варіантів за визначеним критерієм. Вибір траєкторії обльоту робочих сегментів фруктових дерев в експериментальному робочому середовищі обумовлений, насамперед, часом  $T$ , за який група БПЛА здійснює виконання робочої місії в робочому середовищі. Час на виконання робочої місії залежить від швидкості руху  $v$  кожного апаратного пристрою в групі БПЛА. Зазначимо, що  $v$  є постійною величиною для кожного БПЛА в групі за будь-якої траєкторії руху. Тоді, час що потрібен для обльоту робочого середовища, подамо через відношення відстані  $D$  і швидкості руху  $v$  за формулою:

$$T = \frac{D}{v}. \quad (1)$$

Далі задамо визначення згідно формули (1) для кожної з трьох визначених траєкторій.

Позначимо через  $d_1$  відстань між сусідніми робочими сегментами в ряді робочого середовища. Величина  $d_1$  є сталою величиною для всіх траєкторій і вказує на те, що відстань між робочими сегментами є однаковою. Позначимо через  $d_2$  відстань між рядами робочих сегментів у експериментальному робочому середовищі. Величина  $d_2$  є також сталою величиною і визначає однакоку відстань між рядами робочих сегментів. Нехай  $n$  – кількість робочих сегментів в одному ряду,  $m$  – кількість рядів у робочому середовищі, яку потрібно облетіти під час виконання програмної місії, а  $D^I$ ,  $D^{II}$  та  $D^{III}$  – відстані в метрах, які потрібно пролетіти групі БПЛА за траєкторіями руху (I), (II) та (III), відповідно.

Тоді, час обльоту у визначеній пріоритетній траєкторії (I) визначимо за наступною формулою:

$$T_1 = \frac{D^I}{v} = \frac{(n \times m \times d_1 + (m-1) \times d_1)}{v}. \quad (2)$$

Час обльоту у допустимій траєкторії руху (II) є таким:

$$T_2 = \frac{D^{II}}{v} = \frac{(n \times m \times (d_1 + d_2) - (m-1) \times d_2)}{v}. \quad (3)$$

I, нарешті, час обльоту у небажаній траєкторії руху (III) подамо так:

$$T_3 = \frac{D^{III}}{v} = \frac{\sqrt{d_1^2 + d_2^2} \times n \times m}{v}. \quad (4)$$

Параметри  $d_1$ ,  $d_2$ ,  $n$  та  $m$  використовуються у формулах (2-4) для обчислення відстані та часу для кожної можливої траєкторії руху групою БПЛА.

Значення цих параметрів є сталими для кожної траєкторії руху в процесі обльоту групою БПЛА. Для формального обґрунтування відмінності між траєкторіями за часом обльоту, обчислимо різницю між  $T_1$  та  $T_2$ , а також різницю між  $T_2$  та  $T_3$ . Різницю  $\Delta T_{1,2}$  між  $T_1$  та  $T_2$  визначимо так

$$\begin{aligned} \Delta T_{1,2} = T_1 - T_2 &= \frac{D^I}{v} - \frac{D^{II}}{v} = \frac{(n \times m \times d_1 + (m-1) \times d_2)}{v} = \\ &= \frac{(n \times m \times (d_1 + d_2) - (m-1) \times d_2)}{v} = \frac{(n \times m \times d_1 - n \times m \times d_2)}{v} \end{aligned} \quad (5)$$

Отже,  $\Delta T_{1,2} > 0$ , якщо  $n \times m \times d_1 > n \times m \times d_2$  тобто  $D^I > D^{II}$ . Іншими словами, обліт відбувається швидше, коли відстань між робочими сегментами в ряду більша, ніж за відстань між самими рядами.

Різницю  $\Delta T_{2,3}$  між  $T_2$  та  $T_3$  обчислимо так:

$$\begin{aligned} \Delta T_{2,3} = T_2 - T_3 &= \frac{D^{II}}{v} - \frac{D^{III}}{v} = \\ &= \frac{(n \times m \times (d_1 + d_2) - (m-1) \times d_2)}{v} - \frac{\sqrt{d_1^2 + d_2^2} \times n \times m}{v}. \end{aligned} \quad (6)$$

Отже,  $\Delta T_{2,3}$ , якщо  $(n \times m \times (d_1 + d_2) - (m-1) \times d_2) > \sqrt{d_1^2 + d_2^2} \times n \times m$   
 $(n \times m \times (d_1 + d_2) - (m-1) \times d_2) > \sqrt{(d_1^2 + d_2^2)} \times n \times m$ , тобто  
 $d_1 + d_2 > \sqrt{d_1^2 + d_2^2}$ , що є завжди істинним з огляду на геометричну інтерпретацію відстані.

З проведеного аналізу за формулами (5-6) маємо, що для будь-яких значень  $d_1$  та  $d_2$  різниці  $\Delta T_{1,2} > 0$  та  $\Delta T_{2,3} > 0$ , що означає  $T_1 < T_2$  та  $T_2 < T_3$ . Тому, для мінімізації часу обльоту  $T$ , траєкторія руху  $D^I$  є найкращим вибором для виконання робочих місій групою БПЛА.

### Висновок

Отже, з огляду на проведений аналіз часу, що необхідний для обльоту по різних траєкторіях руху БПЛА, встановлено, що “пріоритетна траєкторія руху”  $D^I$ , продемонстрована на рисунку 1, є найкращим варіантом для застосування в подальших дослідженнях. Математичні обрахунки підтверджують ефективність вибраної “пріоритетної траєкторії”, вказуючи на її здатність мінімізувати час обльоту у порівнянні з іншими траєкторіями, що висвітлює її значущість у створенні автоматизованих маршрутів для групи БПЛА. Водночас, ця траєкторія

забезпечує найшвидше оброблення даних у експериментальному робочому середовищі, підвищуючи тим самим продуктивність моніторингу та збору інформації.

### **Перелік посилань**

1. Melnychenko O., Savenko O. A self-organized automated system to control unmanned aerial vehicles for object detection. The 4th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS-2023) : CEUR-Workshop Proceedings. Vol. 3373. (Khmelnyskyi, Ukraine, 22–24 March 2023). Aachen : CEUR-WS.org, 2023. P. 589–600.
2. A comprehensive review on recent applications of unmanned aerial vehicle remote sensing with various sensors for high-throughput plant phenotyping / L. Feng et al. Computers and Electronics in Agriculture. 2021. Vol. 182. P. 106033.
3. Aggarwal S., Kumar N. Path planning techniques for unmanned aerial vehicles: A review, solutions, and challenges. Computer Communications. 2020. Vol. 149. P. 270–299.
4. Stott E., Williams R. D., Hoey T. B. Ground control point distribution for accurate kilometre-scale topographic mapping using an RTK-GNSS unmanned aerial vehicle and SfM photogrammetry. Drones. 2020. Vol. 4, No. 3. P. 55.
5. Amami M. Fast and reliable vision-based navigation for real time kinematic applications. International Journal for Research in Applied Science and Engineering Technology. 2022. Vol. 10, No. 2. P. 922–932.
6. Radiuk P., Pavlova O., Avsiyevych V., Kovalenko V. Convolutional neural network for parking slots detection. The 3rd International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS-2022) : CEUR-Workshop Proceedings. Vol. 3156. (Khmelnyskyi, Ukraine, 23-25 March 2022). CEUR-WS.org, Aachen, 2022. P. 284–293.

УДК 004.4

Слутяк Є.І., Радельчук Г.І., Балицький Б.І.

*Хмельницький національний університет*

## **УДОСКОНАЛЕННЯ ПЕРЕДАЧІ ДАНИХ У МЕРЕЖІ ІНТЕРНЕТ З ВИКОРИСТАННЯМ АЛГОРИТМУ ВЕРИФІКАЦІЇ ПОВІДОМЛЕНЬ**

*Проведено аналіз предметної області, досліджено наявні реалізації протоколів передачі даних та алгоритмів шифрування. Удосконалено передачу даних, що знизить ймовірність перехоплення даних користувачів під час їх передачі у мережі Інтернет. Запропонована удосконалена модель вирішує усі проблеми, виявлені під час дослідження.*

*An analysis of the subject area was carried out, existing implementations of data transfer protocols and encryption algorithms were investigated. Data transmission has been improved, which will reduce the probability of interception of user data during its transmission over the Internet. The proposed improved model solves all the problems identified during the research.*

Останні дослідження показують, що з кожним роком кількість користувачів мережі Інтернет зростає. Відповідно, разом з цим зростає трафік, який споживається цими користувачами у мережі. Так, відповідно до звіту Digital 2022 Global Statshot [1] близько 63% населення світу користуються мережею Інтернет станом на кінець 2022 року. Також, згідно зі зведеною статистикою приблизний щоденний обсяг інтернет-трафіку протягом останніх десяти років зріс з десятків ексабайт даних до сотень ексабайт даних.

Таке зростання популярності та поширеності мережі Інтернет призвів до значного зростання кіберзловмисників. Відповідно до звіту про роботу системи виявлення вразливостей та реагування на кіберінциденти [2] станом на кінець 2022 року кількість кіберзлочинів зросла у 2.8 разів. Згідно з даними Держспецзв'язку [3] близько 90% кібератак у 2022 році було здійснено хакерами з території Білорусії та Російської Федерації.

Саме тому проблема безпеки передачі даних є актуальною та потребує дослідження, аналізу та знаходження нових методологій та методів вирішення проблем безпеки передачі даних у мережі Інтернет.

Метою роботи є удосконалення методу передачі даних у мережі Інтернет з використанням алгоритму верифікації повідомлень.

Класичний метод передачі даних складається з двох частин, а саме:

- протокол передачі даних;
- алгоритм шифрування даних.

Загальна модель (рисунок 1), яка базується на класичному методі передачі даних, складається з двох частин: клієнта та сервера. Також класична модель передбачає односторонній зв'язок між складовими мережі.



Рисунок 1 – Класична модель передачі даних

Цей метод, з його розподілом та рівними відповідальності, має значну кількість недоліків. Зокрема, дана модель не дозволяє жодним чином проводити автентифікацію або верифікацію користувачів мережі. Тому такий підхід до передачі даних дозволяє зловмисникам перехоплювати (або навіть компрометувати) одного з користувачів та безперешкодно отримувати дані, які відправник чи кілька відправників надаватимуть отримувачу, не підозрюючи, що його було скомпрометовано та усі дані надходять зловмисникам.

Покращений метод передачі даних передбачає ще одну складову під час передачі даних – шар автентифікації та верифікації користувачів та даних (рисунок 2).



Рисунок 2 – Покращена модель передачі даних

Покращена модель містить стільки ж складових, скільки і класична, проте різницею між ними є те, що покращена модель передбачає двосторонній зв'язок під час передачі даних. Ця модель передбачає декілька кроків передачі даних.

Перший крок передачі даних (рисунок 3) передбачає автентифікацію відправника та перевірку наявності і стабільності з'єднання з отримувачем.

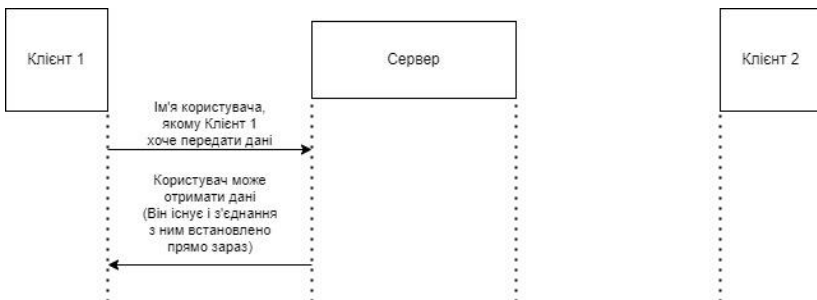


Рисунок 3 – Крок 1 передачі даних



Рисунок 4 – Крок 2 передачі даних

Таким чином, вирішується проблема «сліпої» передачі даних. Завдяки цьому етапу передачі даних сервер-посередник знатиме, що відправник має можливість надсилати дані, а також визначить, чи може отримувач безпечно отримати дані та чи не був отримувач скомпрометований.

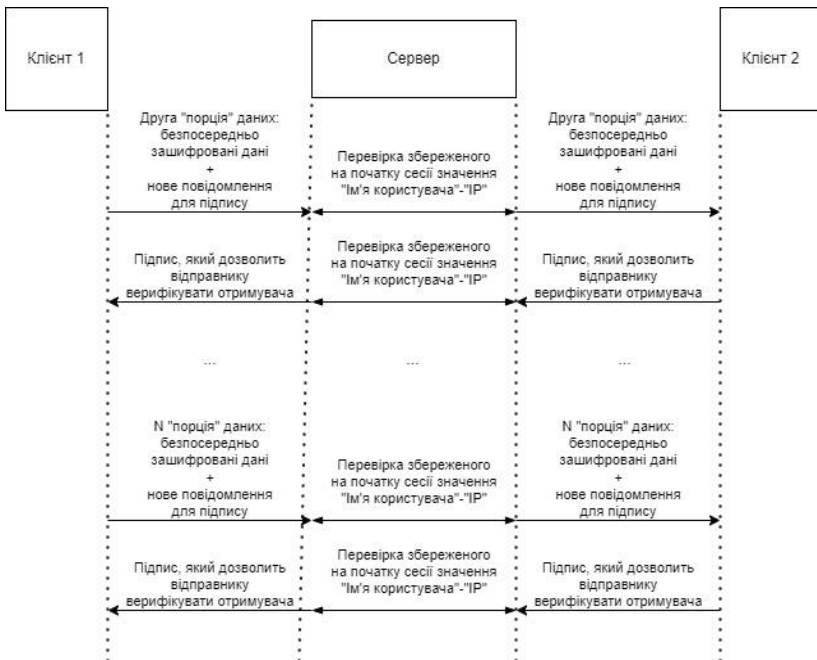


Рисунок 5 – Крок 3 передачі даних



Наступна модель передбачає, що дані передаватимуться отримувачу частинами. Під час виконання другого кроку передачі даних (рисунок 4) виконується передача першої частини даних. Під час передачі даних виконується реалізація алгоритму верифікації повідомлень. Отримувачу надсилається згенероване повідомлення, після чого він його підписує за допомогою власного ключа і повертає відправнику. Під час передачі даних сервер виконує важливу роль, проводячи автентифікацію обох учасників передачі даних.

Під час виконання третього кроку передачі даних (рисунок 5) відбувається повторна передача частин даних, включно з останньою частиною даних. Таким чином, це дає можливість не дати доступу зловмисникам до повного набору даних. Під час передачі кожної з частин повідомлень відбувається верифікація отримувача.

На завершальному етапі передачі даних відбувається відправка повідомлення отримувачу про завершення передачі даних (рисунок 6).



Рисунок 6 – Крок 4 передачі даних

Отже, удосконалений метод передачі даних через мережу Інтернет вирішує виявлені під час дослідження недоліки та суттєво підвищує захищеність процесу передачі інформації.

Подальші дослідження спрямовані на реалізацію розробленого методу удосконалення передачі даних протоколом TCP (Transmission Control Protocol) з використанням алгоритму шифрування Діффі-Хелмана.

### Перелік посилань

1. Digital 2022: October global statshot report. URL: <https://datareportal.com/reports/digital-2022-october-global-statshot> (дата звернення: 24.10.2023).
2. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, URL: <https://cip.gov.ua/services/cm/api/attachment/download?id=50943> (дата звернення: 27.10.2023).
3. У 2022 році кількість зареєстрованих кіберінцидентів виросла майже втричі – звіт. URL: <https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zareyestrovanih-kiberincidentiv-viroslo-maizhe-vtrichi-zvit> (дата звернення: 29.10.2023).

УДК 004.5

Смірнов О.П., Поплавський С.Ю., Ковальчук В.К., Лутюк Л.І.

*Хмельницький національний університет*

## **УДОСКОНАЛЕНИЙ МЕТОД ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ВІД ВРАЗЛИВОСТЕЙ В АПАРАТНОМУ ЗАБЕЗПЕЧЕННІ**

*Удосконалено метод криптографічного захисту від вразливостей в апаратному забезпеченні. Для запобігання крадіжці пропонується удосконалений метод і алгоритм відображення. Розроблений криптографічний алгоритм можна зламати за допомогою диференціальної атаки відкритого тексту із значно обмеженими ресурсами. Нарешті, щоб запобігти таким атакам, представляємо серію контрзаходів для всіх мережових шифрів із заміною та перестановкою, шляхом стимулювання нестатичної поведінки. Представляємо нову мережу взаємозв'язку мережі динамічної маршрутизації та модифіковані інваріантні елементи раунду на варіанти на основі раунду, які вимагають прийняття рішення зловмисником. Показано практичність і можливість виконання такої атаки на реальні фізичні реалізації.*

*The method of cryptographic protection against vulnerabilities in hardware has been improved. To prevent theft, an improved display method and algorithm is proposed. The developed cryptographic algorithm can be broken using a differential plaintext attack with significantly limited resources. Finally, to prevent such attacks, we present a series of countermeasures for all network substitution and permutation ciphers by encouraging non-static behavior. We present a new dynamic routing network interconnection network and modified round-invariant elements on round-based variants that require an attacker to make a decision. The practicality and possibility of performing such an attack on real physical implementations is shown.*

Протягом останніх десятиліть апаратне забезпечення все частіше піддається складним атакам [1-3]. Немає явної впевненості в тому, що виробники/постачальники не виробляють [4-6] підроблені проекти або що криптографічні алгоритми безпечні в програмному забезпеченні, також безпечні в апаратному забезпеченні. Новизна роботи полягає в наступному: вдосконалений метод захисту, який забезпечує підхід для перевірки права власності, демонстрація того, як зламати криптографічний алгоритм із значно обмеженими можливостями ресурсів і надати безліч апаратних засобів протидії таким атакам.

Схеми кодування стану впливають на синтез певним чином. Одне значення кодування стану має здатність повністю видалити синтезовану систему з діапазону допустимих накладних витрат. За допомогою коду стану тепер заглиблюються в проблему багатометричної оптимізації на багатьох напрямках. Аналізується розмір, довжина кодування, вільні значення кодування та підпис для вибору. Кожен з них

може негативно вплинути на результат не лише складності графа запиту, але й кодів стану, які застосовуються та вибираються вільно.

Щоб запобігти крадіжці, пропонується удосконалений метод і алгоритм відображення. В ньому застосовуємо гібридний генетичний алгоритм, який отримав назву для ефективного вирішення складної проблеми зіставлення підграфів. У результаті покращення складає максимум на 10-12%. Розроблений криптографічний алгоритм можна зламати за допомогою диференціальної атаки відкритого тексту із значно обмеженими ресурсами. Нарешті, щоб запобігти таким атакам, представляємо серію контрзаходів для всіх мережевих шифрів із заміною та перестановкою, шляхом стимулювання нестатичної поведінки. Представляємо нову мережу взаємозв'язку мережі динамічної маршрутизації та модифіковані інваріантні елементи раунду на варіанти на основі раунду, які вимагають прийняття рішення зловмисником. Показано практичність і можливість виконання такої атаки на реальні фізичні реалізації, які вирішують використовувати цю технологію архітектури в апаратному забезпеченні. Крім того, за допомогою мереж перестановок із «ключами» такій атаці можна або повністю запобігти, або призвести до додаткового часу та труднощів для зловмисника, щоб відновити секретний ключ. Крім того, представлена мережева техніка перестановки з «ключем» є загальною і спрямована лише на зміну самої функції перестановки. Він має незначний загальний вплив і багато архітектур шифру, що використовують структури SPN подібним чином, можуть використовувати представлену техніку, так і поєднувати її з додатковими методами захисту.

### Перелік посилань

1. Counterfeit integrated circuits: detection and avoidance. Springer, 2015.
2. U.S. Department of Defense Partners with GLOBALFOUNDRIES to Manufacture Secure Chips at Fab 8 in Upstate New York, Feb 2021.
3. N.A. Beresford, C.L. Barnett, S. Gashchak, A. Maksimenko, E. Guliaichenko, M.D. Wood, and M. Izquierdo. Radionuclide transfer to wildlife at a 'Reference site' in the Chernobyl Exclusion Zone and resultant radiation exposures. *Journal of Environmental Radioactivity*, 211:105661, January 2020.
4. Matthew Lewandowski and Srinivas Katkoori. Lightweight Countermeasure to Differential-Plaintext Attacks on Permutation Ciphers. In Augusto Casaca, Srinivas Katkoori, Sandip Ray, and Leon Strous, editors, *Internet of Things. A Confluence of Many Disciplines*, pages 159–176, Cham, 2020. Springer International Publishing.
5. Fukang Liu, Christoph Dobraunig, Florian Mendel, Takanori Isobe, Gaoli Wang, and Zhenfu Cao. Efficient Collision Attack Frameworks for RIPEMD-160. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019*, pages 117–149, Cham, 2019. Springer International Publishing.
6. Zachary J. McDowell and Matthew A. Vetter. It Takes a Village to Combat a Fake News Army: Wikipedia's Community and Policies for Information Literacy. *Social Media + Society*, 6(3):205630512093730, 2020.

УДК 004

Смолієнко Д.В., Петровський С.С.

*Хмельницький національний університет*

## **МЕТОД ПРОГНОЗУВАННЯ ЗАБРУДНЕННЯ ГРОМАДСЬКИХ ДОРІГ НА ОСНОВІ ПІДХОДУ ГЛИБОКОГО АКТИВНОГО НАВЧАННЯ**

*Запропоновано метод прогнозування рівня забруднення громадських доріг на основі підходу глибокого активного навчання з використанням зображень. Головна мета - поліпшити контроль та управління забрудненням доріг, забезпечуючи швидке та точне прогнозування рівня забруднення на основі вхідних зображень за допомогою методу, що використовує нейромережі глибокого навчання, зокрема згорткові нейромережі (CNN). Це дозволить вживатичасні заходи для зменшення забруднення на дорогах.*

*A method for predicting the level of pollution on public roads is proposed based on a deep active learning approach using images. The main goal is to improve the control and management of road pollution by providing fast and accurate forecasting of pollution levels based on input images using a method that utilizes deep learning neural networks, particularly Convolutional Neural Networks (CNN). This will enable timely measures to reduce road pollution.*

Забруднення доріг є серйозною проблемою в Україні, яка погіршує стан інфраструктури, повітря та здоров'я населення. Незважаючи на спроби вирішити цю проблему, рівень забруднення доріг продовжує зростати з кожним роком.

Глибоке активне навчання, що використовує згорткові нейронні мережі, може автоматизувати оцінку якості доріг в реальному часі. Аналіз зображень з камер спостереження дозволить збирати дані про рівень та типи забруднення. Ця інформація допоможе розробити комплексний підхід до моніторингу та покращення стану доріг в Україні.

Існуючі методи прогнозування забруднення доріг мають свої переваги і недоліки.

Згорткові нейронні мережі (CNN) ефективно розпізнають візуальні ознаки, автоматизують процес і масштабуються. Проте вони потребують багато даних, чутливі до шуму і складні в інтеграції.

Рекурентні нейронні мережі (RNN) моделюють послідовності і часову динаміку. Однак у них є проблеми із зникненням градієнта, довгостроковими залежностями і обчислювальною складністю.

Ансамблі моделей підвищують точність і стабільність за рахунок поєднання підходів. Проте вони складніші у навчанні, інтерпретації і потребують більше ресурсів.

Незважаючи на переваги, кожен метод має обмеження. Тому пропонується розглянути новий підхід, який дозволить подолати недоліки існуючих методів для ефективного та точного прогнозування забруднення доріг.

### Метод TFN

Розглянемо метод Temporal Fusion Network (TFN) для прогнозування забруднення доріг.

TFN поєднує переваги згорткових нейронних мереж та рекурентних нейронних мереж:

- Згорткові шари аналізують просторові особливості на зображеннях доріг.
- RNN-шар (LSTM) моделює часову динаміку змін забруднення.

Така архітектура дозволяє враховувати як візуальні, так і темпоральні закономірності.

Порівняно з іншими методами, TFN має такі переваги:

- Автоматичний підбір оптимальних параметрів моделі.
- Врахування динаміки змін рівня забруднення.
- Гнучкість та адаптивність до різних умов.
- Потенціал для підвищення точності прогнозування.

Загалом, TFN є перспективним підходом для прогнозування забруднення доріг на основі аналізу зображень з урахуванням часової динаміки.

Архітектура TFN (таблиця 1) складається з наступних основних компонентів:

1. Згорткові шари для аналізу просторових особливостей зображень:
  - Розмір ядра: 3x3 або 5x5
  - Кількість фільтрів: 16-32
  - Крок зсуву: 1 піксель
  - Активація: ReLU
2. RNN шар (LSTM) для моделювання часової динаміки:
  - Кількість LSTM одиниць: 32-64
  - Збереження коротко- та довгострокової пам'яті
3. Об'єднання особливостей згорткових і RNN шарів
4. Повнозв'язний шар для аналізу інтегрованих особливостей:
  - Кількість нейронів: 64-128
  - Активація: ReLU
5. Вихідний шар з 1 нейроном для прогнозування рівня забруднення:
  - Активація: лінійна або сигмоїдна

Загалом, TFN поєднує можливості CNN та RNN для аналізу просторових і часових закономірностей в даних про забруднення доріг. Кількість шарів і параметри можуть варіюватися в залежності від задачі.

Таблиця 1 – Архітектура TFN

	Шар	Опис
1.	Вхідний	Зображення дороги
2.	Згорткові	Виявлення просторових особливостей
3.	Пулінгові	Зменшення розмірності виходу згорткових шарів
4.	LSTM-рекурентний	Аналіз темпоральних залежностей та моделювання динаміки змін
5.	Повноз'язані	Остаточне прогнозування рівня забруднення доріг
6.	Вихідний	Прогнозована забрудненість доріг

### Навчання моделі

Навчання моделі за допомогою методу TFN включатиме мінімізацію функції втрати за допомогою оптимізаційного алгоритму, такого як стохастичний градієнтний спуск. Формула для оновлення параметрів моделі буде залежати від обраного алгоритму оптимізації.

Загальна формула оновлення параметрів моделі в процесі навчання може бути записана наступним чином:

$$\theta(t+1) = \theta(t) - \alpha * \nabla L,$$

де:  $\theta(t)$  – вектор параметрів моделі на кроці навчання  $t$ ,  $\alpha$  – швидкість навчання (learning rate),  $\nabla L$  – градієнт функції втрати  $L$  відносно параметрів моделі.

Конкретна формула для обчислення градієнту  $\nabla L$  залежить від використаної функції втрати та архітектури моделі. В даному випадку, згідно з гіпотетичним методом TFN, формула для обчислення градієнту буде включати зворотне поширення помилки (backpropagation) через згорткові та LSTM-рекурентні шари моделі.

За допомогою цієї формули, параметри моделі будуть оновлюватись на кожному кроці навчання, щоб мінімізувати значення функції втрати і покращити точність прогнозів моделі.

### Експериментальні результати

Експериментальне випробування методу було здійснено за допомогою мови програмування Python, що має багату екосистему бібліотек для потрібних завдань та зручний синтаксис.

Середовище розробки Google Colab стало найкращим вибором через інтерактивність роботи, широкий вибір вбудованих бібліотек Python та можливість використання обчислювальних ресурсів. Його інтерактивність проявляється у системі блокнотів для написання коду, що дозволяє виконувати код крок за кроком і бачити результати його дії. Google Colab підтримує багато популярних бібліотек та фреймворків для машинного навчання, такі як TensorFlow, PyTorch, Keras, що і застосовуються у експерименті. Також це середовище завжди готове до використання обчислювального ресурсу - Google Colab надає доступ до віртуальних машин з GPU та TPU, що дозволяє вам виконувати обчислення для навчання великих моделей швидше, ніж на звичайних CPU.

Обраний датасет з джерела Kaggle містить сотні різноманітних зображень із забрудненими та чистими дорогами, що і надає можливість робити подальші експерименти.

Експериментальні результати виявилися успішними, так як втрати при тренуванні моделі були низькими, а найвища акуратність лише при 10 ітераціях сягнула 96.43%, а час виконання сягнув лише 21 секунд.

Якщо ж збільшувати кількість ітерацій, втрати будуть зменшуватися, а акуратність відповідно збільшуватись, і вже при 20 ітераціях матимемо 100% акуратність і час виконання 47 секунд.

### **Висновки**

Результати дослідження показали, що TFN може забезпечувати точні прогнози рівня забруднення доріг, враховуючи просторові залежності в даних. Метод виявився ефективним у виявленні та аналізі просторових ознак на зображеннях доріг, а також у моделюванні та прогнозуванні темпоральних залежностей.

Використання автоматичного вибору оптимальних параметрів методу дозволяє досягти кращих результатів прогнозування та адаптуватися до різних умов та типів даних. Метод TFN відрізняється від інших готових методів завдяки поєднанню згорткових шарів та LSTM-рекурентного шару. Це дозволяє пришвидшити навчання машини та отримувати кращі результати.

Розроблений метод TFN є перспективним інструментом для прогнозування забруднення громадських доріг на основі аналізу зображень і моделювання динаміки змін. Подальші дослідження можуть включати оптимізацію архітектури TFN, вдосконалення функцій втрати та дослідження його ефективності на реальних даних.

### **Перелік посилань**

1. Екологічний паспорт області [Електронний ресурс] – Хмельницький, ХОВА, 2023 – Режим доступу: [https://www.adm-km.gov.ua/?page\\_id=7157](https://www.adm-km.gov.ua/?page_id=7157)
2. VPP: Visual Pollution Prediction Framework Based on a Deep Active Learning Approach Using Public Road Images [Електронний ресурс] – 2022 – <https://www.mdpi.com/2227-7390/11/1/186>
3. Згорткова нейронна мережа – просте пояснення CNN та її застосування [Електронний ресурс] – Україна, 2019 – Режим доступу: <https://evergreens.com.ua/ua/articles/cnn.html>
4. "Deep Learning Techniques for Natural Language Processing" [Електронний ресурс]. - Режим доступу: <https://www.sciencedirect.com/science/article/pii/S2666651721000127>
5. "Deep Learning Methods in Recommender Systems" [Електронний ресурс]. - Режим доступу: <https://www.sciencedirect.com/science/article/pii/S110866519300845>

УДК 004.4

Собко В.В.

*Хмельницький національний університет*

## **МЕТОД ПОЄДНАННЯ ТЕХНОЛОГІЙ REDUX-TOOLKIT ТА REDUX-SAGA ДЛЯ РОБОТИ З API ВЕБ-РЕСУРСІВ**

*Розглянуто метод поєднання технологій Redux-Toolkit та Redux-Saga для роботи з API веб-ресурсів для подальшого опрацювання даних з метою виводу їх на екран, збереження в локальне сховище пристрою, тощо. Запропонований метод є швидким, надійним, зрозумілим, дає змогу легко керувати запитами, моніторити їх стан, результат, наявність помилок та можливість їх обробляти.*

*The method of combining Redux-Toolkit and Redux-Saga technologies was considered for working with the API of web resources for further data processing with the aim of displaying them on the screen, saving them to the device's local storage, etc. The proposed method is fast, reliable, clear, allows you to easily manage requests, monitor their status, result, presence of errors, and the ability to process them.*

З розвитком нових технологій та постійним підвищенням рівня інформатизації суспільства, проблема ефективної обробки мережевих запитів в додатках стає дедалі актуальнішою. У цьому контексті поєднання технологій Redux-Toolkit та Redux-Saga для роботи з API веб-ресурсів виявляється надзвичайно актуальним і важливим підходом.

Метою дослідження даного методу є декілька чинників:

1. Оцінка Ефективності: дослідження може спрямовуватися на оцінку ефективності даного методу. Розробники можуть аналізувати час відгуку API, кількість запитів, споживану пам'ять і інші метрики для визначення, наскільки добре цей підхід впливає на продуктивність додатку.

2. Порівняння З Іншими Підходами: дослідження може проводитися з метою порівняння методу поєднання Redux-Toolkit і Redux-Saga з іншими підходами до управління станом та роботи з API, такими як Redux-Thunk, Apollo Client (GraphQL), або Fetch API. Це допоможе визначити переваги та недоліки кожного підходу.

3. Оптимізація Логіки Додатку: дослідження може відбуватися з метою оптимізації логіки додатку, зокрема роботи з API. Розробники можуть досліджувати, як краще організувати та структурувати запити до API, обробку помилок, кешування даних і інші аспекти логіки.

4. Покращення Досвіду Користувача: основною метою може бути покращення досвіду користувача. Дослідження може допомогти виявити шляхи покращення швидкодії та надійності додатку при взаємодії з API, що відобразиться на задоволенні користувачів.



5. Підготовка Розробників: дослідження може служити для підготовки розробників до використання цього методу в практиці. Відповідні тренінги, вебінари або навчальні матеріали можуть бути розроблені на основі дослідження, щоб забезпечити зростання компетентності в цій галузі.

6. Розробка Нових Рекомендацій: на основі дослідження можуть бути розроблені рекомендації або кращі практики щодо використання Redux-Toolkit і Redux-Saga для роботи з API, які можуть бути корисними для розробників у подальших проєктах.

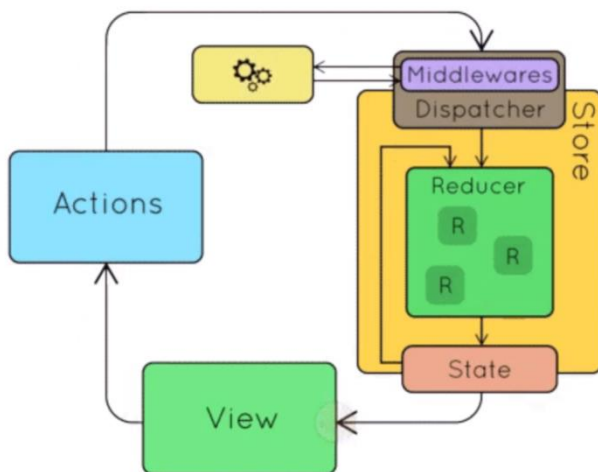


Рисунок 1 – Схема роботи досліджувального методу

Отже, запропонований метод для роботи з API веб-ресурсів забезпечує надійну архітектуру для клієнтських частин проєктів. Використання такого підходу суттєво зменшує кількість помилок при виконанні мережевих запитів, обробляє їх, дає можливість отримати всю інформацію про запит як в момент виконання, так і після завершення, а також легко опрацювати отримані дані. Подальші дослідження спрямовані на ще більшу автоматизацію процесу, що забезпечить можливість інтеграції даної програмної архітектури в справжні веб-додатки та системи, а також зробить легшим поріг входження для розробників, які з нею будуть працювати.

### Перелік посилань

1. Redux Fundamentals, Part 1: Redux Overview [Електронний ресурс] – Режим доступу до ресурсу: <https://redux.js.org/tutorials/fundamentals/part-1-overview/>.
2. Redux-Saga: Beginner Tutorial [Електронний ресурс] – Режим доступу до ресурсу: <https://redux-saga.js.org/docs/introduction/BeginnerTutorial/>.
3. Wieruch, Robin. Road to React: Your journey to master plain yet pragmatic React.js. – New York, 2020. – 226с.

УДК 004.4

Собкова Ю.В., Міхалевський В.Ц., Скрипник Т.К.

*Хмельницький національний університет*

## МЕТОД АВТОМАТИЗОВАНОГО ПІДБОРУ ТИМЧАСОВОГО ЖИТЛА ДЛЯ КАТЕГОРІЙ СПОЖИВАЧІВ ЗА ГЕНЕТИЧНИМ АЛГОРИТМОМ

*Розглянуто метод автоматизованого підбору тимчасового житла для категорій споживачів. Досліджено суть класифікації методів оптимізації на аналітичні та чисельні методи і показано, що схема генетичного алгоритму може бути виражена у вигляді схеми чисельного методу прямого пошуку. Наведено спосіб зведення заданої оптимізаційної задачі до такої, що може бути розв'язана генетичним алгоритмом, та окреслено клас задач, які можуть бути розв'язані подібним чином. Запропоновано деякі способи підвищення ефективності реалізації цієї процедури.*

*The method of automated selection of temporary housing for categories of consumers is considered. The essence of the classification of optimization methods into analytical and numerical methods is studied and it is shown that the scheme of the genetic algorithm can be expressed in the form of the scheme of the numerical method of direct search. A method of reducing a given optimization problem to one that can be solved by a genetic algorithm is presented, and a class of problems that can be solved in a similar way is outlined. Some methods of increasing the effectiveness of the implementation of this procedure are proposed.*

Розв'язується задача забезпечення автоматизованого пошуку житла для споживачів за критеріями. За основний метод вирішення завдання вибрано метод генетичного алгоритму (ГА).

Для ілюстрації принципів роботи генетичного алгоритму розглядається задача необмеженої оптимізації, в нашому випадку, задача максимізації:

$$\text{Maximize } f(x), x_i^l \leq x_i \leq x_i^u, i = 1, 2, \dots, N, \quad (1)$$

де,  $x_i^l$  та  $x_i^u$  - нижня та верхня межі, яких може набувати змінна  $x_i$ .

Для вирішення проблем з автоматизованим пошуком житла створили на мові Python програмне забезпечення системи пошуку житла для категорії споживачів на основі генетичного алгоритму. Першим кроком будується база даних з усіма користувачами, які мають бажання підібрати собі житло за деякими параметрами. Якщо користувач з таким логіном вже був зареєстрованим у базі даних, то про це повідомляється користувачу.

Наступний крок можливий лише для зареєстрованих осіб. Запускається вікно з полями вводу даних, які користувач повинен заповнити, зокрема, номер телефону, орієнтовну вартість оренди/купівлі житла, район міста чи відстань від міста та інше. Вікно для користувача зображено на Рисунку 1.

Автоматизований підбір житла для категорії споживачів

**Введіть, будь-ласка, комфортну для вас відстань(км) від дому до центра міста та ціну(грн) житла!**

Номер телефону:

Відстань:

Вартість:

Рисунок 1 – Початкове вікно для вводу даних

Після того як користувач введе номер телефону, відстань та вартість в поля для вводу, його дані будуть збережені в таблицю (Рисунок 2) та відкриється повідомлення про те, що користувача збережено (Рисунок 3):

	A	B	C	D
1	<b>Номер телефону користувача</b>	<b>Відстань</b>	<b>Вартість</b>	
2	380621459356	2	61000	
3	380982234562	1,2	30000	
4				
5				

Рисунок 2 – Збережені споживачі з параметрами житла

Автоматизований підбір житла для категорії споживачів

**Введіть, будь-ласка, комфортну для вас відстань(км) від дому до центра міста та ціну(грн) житла!**

Номер телефону:

Відстань:

Вартість:

Повідомлення


 Користувача успішно збережено

Рисунок 3 – Повідомлення про успішне збереження даних

Для прикладу візьмемо створену таблицю з переліком вулиць. В таблиці містяться лише дві критерії: вартість та відстань (Рисунок 4).

Опираючись на метод ГА, проводимо пошук оптимального за вказаними критеріями рішення, отримаємо в результаті рядок 6 із таблиці.

	A	B	C	D
1	Назва вулиці	Відстань від центра(км)	Вартість(грн)	
2	вулиця Європейська	2,10	9 000,00 ₴	
3	вулиця 4-а Нова	9,10	10 000,00 ₴	
4	вулиця 1-а Лугова	2,30	12 000,00 ₴	
5	вулиця Академіка Чеботарьова	9,00	12 000,00 ₴	
6	2-й провулок Ентузіастів	2,00	13 000,00 ₴	
7	вулиця Академіка Заболотного	6,30	13 000,00 ₴	
8	вулиця 2-а Комунарська 2-а	7,70	14 000,00 ₴	
9	вулиця Атерлея	8,10	14 000,00 ₴	
10	вулиця 2-а Лугів	8,00	15 000,00 ₴	
11	вулиця 2-а Нова	5,60	22 000,00 ₴	
12	1-й провулок Ентузіастів	1,00	23 000,00 ₴	

Рисунок 4 – Таблиця критеріїв

Отже, запропонований метод на основі генетичного алгоритму довів свою здатність і може бути застосований до автоматизованого підбору тимчасового житла для категорій споживачів.

### Перелік посилань

1. Beasley, D., Bull, D. R. and Martin, R. R., «An overview of genetic algorithms: Part 2, research topics», University Computing, Vol. 15, pp. 170–181. [citeseer.nj.nec.com/article/beasley93overview.html](http://citeseer.nj.nec.com/article/beasley93overview.html).
2. Chambers, L., Practical handbook of genetic algorithms: Applications, Vol. I, CRC Press, Boca Raton, Florida.
3. Charbonneau, P., «An introduction to genetic algorithms for numerical optimization». <http://www.hao.ucar.edu/public.research/si/pikaia/tutorial.html>.

УДК 004.9

Стецюк Ю.В.

*Хмельницький національний університет*

## **МЕТОДИ ОБРОБКИ ДАНИХ З ОБМЕЖЕНИМ ДОСТУПОМ В МУЛЬТИКОМП'ЮТЕРНИХ СИСТЕМАХ ІЗ ЗАСТОСУВАННЯМ ХМАРНИХ ТЕХНОЛОГІЙ ЇХ ЗБЕРІГАННЯ**

*Розглянуто проблеми обробки даних з обмеженим доступом в корпоративних мультікомп'ютерних системах при їх зберіганні в хмарних сховищах.*

*В роботі пропонується для підвищення ефективності пошукових операцій з гарантованим забезпеченням конфіденційності даних застосування методу з розбиттям масиву даних на блоки визначеної довжини співставлених із своїми множинами пошукових атрибутів з їх зберіганням в локальній базі корпоративної мережі (блокчейні).*

*The problems of data processing with limited access in corporate multi-computer systems when they are stored in cloud storage are considered.*

*In order to increase the efficiency of search operations with guaranteed data confidentiality, the work proposes to use the method of dividing the data array into blocks of a certain length, matched with their sets of search attributes, and storing them in the local database of the corporate network (blockchain).*

Хмарні технології все ширше застосовуються у всіх найважливіших сферах життя нашого інформаційного суспільства: науці, освіті, інженерній діяльності, охороні здоров'я та повсякденному житті. Їх головна особливість, яка зумовила таку високу популярність застосування, – надання великих обсягів обчислювальних ресурсів при досить низьких витратах.

Не залишилися осторонь і процеси функціонування інформаційних мультікомп'ютерних корпоративних систем в яких обробляються дані з обмеженим доступом. Перенесення корпоративних сховищ таких даних до хмарних, сулить різке зменшення фінансових витрат на підтримку їх функціонування та заходи забезпечення безпечного доступу до них. Ще одним фактором, що спонукає переходу до хмарних технологій зберігання і обробки даних є забезпечення оперативності доступу до них практично з будь якої точки нашої планети, а також можливість обміну ними [6].

Разом з тим перехід до нових технологій зберігання даних несе у собі потенційні загрози даним при їх зберіганні, пересиланні, перетворенні та відображенні, не зважаючи на те, що на сьогодні для подолання існуючих загроз, запропоновано ряд дієвих заходів.

На відміну від традиційного методу, що коли дані передаються між локальними вузлами через централізований сервер, що зменшує пропускну здатність та збільшує ймовірність порушення безпеки з наступною компрометацією інформації та можливою її втратою, пропонується схема збереження конфіденційності та безпечного обміну даними в корпоративній мережі за допомогою ієрархічного шифрування на основі атрибутів з обміном ключами [1]. При цьому використовується симетричне шифрування та обчислення коду автентифікації повідомлення на основі хешу із спільним секретним ключем для забезпечення безпеки передачі повідомлень між вузлами мережі зменшуючи навантаження на хмарний сервер.

Традиційні схеми забезпечення доступу до конфіденційних даних, зазвичай, використовують централізовану організацію контролю доступу. Однак вона є надто вразливою та непрозорою. Для вирішення проблеми пропонується застосування децентралізованої схеми контролю доступу на основі атрибутів для обміну даними на базі розподіленої мережі Hyperledger Fabric [2, 5]. Це дозволило зашифровані дані зберігати в розподіленій файлової системі, наприклад IPFS, а повернутий хеш зберігається в блокчейні завдяки його незмінності. Сам же децентралізований контроль доступу на основі атрибутів з використанням смарт-контрактів має запобігати доступу неавторизованих користувачів до ресурсу даних.

Для вирішення задачі безпечного та ресурсоефективного сумісного використання даних з обмеженим доступом для хмарного середовища їх зберігання [3, 4] пропонується використання хаотичної системи доступу на основі смарт - карт, використовуваних в системі Інтернета речей (CADF-CSE).

Але, не зважаючи на велику кількість запропонованих рішень гарантувати відсутність загроз даним неможливо. Тому гострота розглянутих проблем обробки даних з обмеженим доступом і сьогодні є актуальною науковою задачею. Розробка нових методів та засобів, покращення ефективності існуючих з метою забезпечення цілісності даних на базі побудови гарантовано замкненого контуру їх безпеки, що і є метою цієї роботи.

З метою оперативного доступу дані з обмеженим доступом пропонується розмістити в хмарному сховищі в шифрованому вигляді. Це значно підвищує безпеку самих даних, але породжує іншу проблему - при здійсненні операцій обробки даних їх попередньо треба розшифровувати. Якщо це робити з використанням хмарних сервісів, то це створює загрозу втрати їх конфіденційності, оскільки вони клієнтом не контролюються. Якщо це робити на стороні клієнта, то виникає проблема пошуку необхідного блоку в масиві зашифрованих даних. Більшість розглянутих схем передбачають пошук по входженнях значень бітових згорток хеш-функцій в масив шифрованих даних, що часто призводить до видачі хибних даних, що в свою чергу, зменшує продуктивність їх обробки.

З метою підвищення продуктивності пошукових операцій в масиві зашифрованих даних пропонується схема роботи, заснована на розділенні масиву

даних перед шифруванням на блоки встановленої довжини (рисунок 1), кожному з яких ставиться у відповідність набір пошукових атрибутів (ключових слів):

$$M = \{B1, B2, \dots, Bn\} \quad [1]$$

де:  $M$  – множина блоків даних вихідного масиву даних,  $Bn$  – відповідний блок масиву даних, де  $n$  - ідентифікатор блоку.

$$Vi = \{A1, A2, \dots, An\} \quad [2]$$

де:  $Vi$  – множина пошукових атрибутів  $i$ -го блоку даних,  $A1$  -  $n$  -  $n$ -й пошуковий атрибут.

Множини пошукових атрибутів кожного блоку разом з його ідентифікатором зберігаються в локальній базі даних (блокчейні) корпоративної мережі.

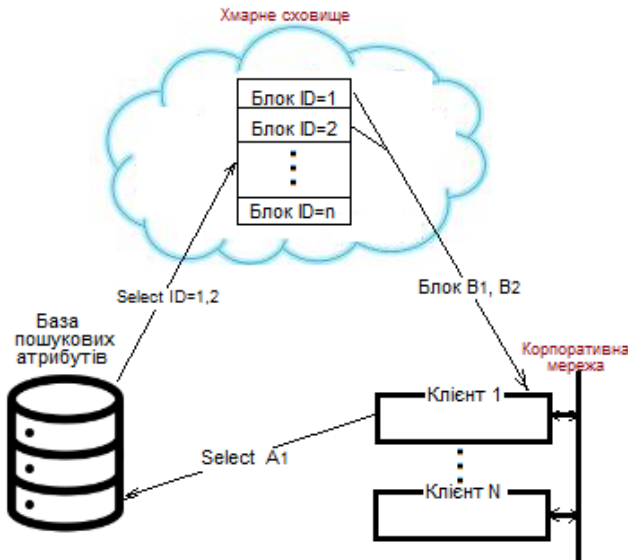


Рисунок1 – Схема пошуку даних в хмарному сховищі з локальною базою пошукових атрибутів

Пошук даних зводиться до визначення множини ідентифікаторів блоків в локальній базі по заданих ключових словах і наступної їх виборки з хмарного сховища і передачі відповідному клієнту корпоративної мережі.

Застосування розробленого методу збільшує ефективність пошуку даних з обмеженим доступом, при цьому гарантуючи їх конфіденційність.

Для підтвердження результатів роботи планується провести експерименти, де буде застовано описану систему пошуку даних з метою підтвердження її ефективності.

### **Перелік посилань**

1. Chandrakant P. Navdeti; Indrajit Banerjee; Chandan Giri. Privacy preservation and secure data sharing scheme in fog based vehicular ad-hoc network / Journal of Information Security and Applications, Volume 63, December 2021, Page 103014
2. Kunpeng Liu; Chenfei Wang; Xiaotong Zhou. Decentralizing access control system for data sharing in smart grid \ High-Confidence Computing, volume 3, Issue 2, June 2023, 100113
3. Muhammad Tanveer; Ali Kashif Bashir; Bander Alzahrani. CADF-CSE: Chaotic map-based authenticated data access/sharing framework for IoT-enabled cloud storage environment / Physical Communication, Volume 59, August 2023, p. 102087
4. Tengfei Zheng; Yuchuan Luo; Tongqing Zhou; Zhiping Cai. Towards differential access control and privacy-preserving for secure media data sharing in the cloud / Computers & Security, Volume 113, February 2022, p 102553
5. Xiaojie Zhao; Shangping Wang; Yaling Zhang; Yu Wang. Attribute-based access control scheme for data sharing on hyperledger fabric /Journal of Information Security and Applications Volume 67, June 2022, Page 103182
6. Yipeng Zou; Tao Peng; Guojun Wang; Entao Luo; Jinbo Xiong. Blockchain-assisted multi-keyword fuzzy search encryption for secure data sharing / Journal of Systems Architecture, Volume 144, November 2023, p 102984



УДК 004.4

Тоцький О.П.

*Київський національний університет імені Тараса Шевченка*

## МЕТОДИ ОБРОБКИ КАРДІОГРАМ

*Проведено попередній поверхневий огляд ключових понять електрокардіографії, а також ознайомлення з процесом формування електрокардіограми. Розглянуті існуючі методи обробки часових сигналів, а саме перетворення Фур'є та вейвлет-аналіз.*

*In this paper I conduct a preliminary superficial review of the key concepts of electrocardiography, as well as familiarization with the process of forming an electrocardiogram. Existing methods of processing time signals, namely Fourier transform and wavelet analysis, are considered.*

Проблема серцево-судинних захворювань, які призводять до значного числа захворювань і смертей, стає все важливішою в сучасному медичинському світі. Вирішення цієї проблеми через раннє діагностування та ефективне лікування різноманітних кардіологічних недугів виглядає все більш необхідним. Особливої ваги набуває автоматизований аналіз великого обсягу даних електрокардіографії.

Сьогодні для аналізу електрокардіографічних сигналів (ЕКС) часто використовуються методи Фур'є. Але вейвлет-перетворення дозволяють отримати більш вичерпну, точну інформацію з меншими обчислювальними витратами порівняно з перетвореннями Фур'є. Вейвлети відзначаються більшою ефективністю у представленні локальних характеристик сигналів порівняно з іншими спектральними методами.

### **Поняття електрокардіограми, процес формування ЕКГ**

Електрокардіограма (ЕКГ) записує електричні активності серця, оцінює правильність ритму серця, його частоти, виявляє порушення внутрішньосерцевої провідності, дозволяє проаналізувати кровопостачання серцевого м'яза в стані спокою, а також виявити збільшення камер серця (передсердь та шлуночків).

Людське серце складається з чотирьох камер (відділів): двох передсердь та шлуночків, - послідовне скорочення кожної з них фіксується на ЕКГ у вигляді відхилень від ізолінії. Такі відхилення називають «зубцями» і називають латинськими літерами *P*, *Q*, *R*, *S*, *T*. Зубці, розташовані вище ізолінії називаються позитивними, нижче – негативними. Розрізняють зубці: *P*, *Q*, *R*, *S*, *T*. Зубці *P*, *R*, *T* – спрямовані вгору, а зубці *Q*, *S* – вниз.

В загальному процес формування електрокардіограми можна описати так: формується імпульс збудження у синусовому вузлі. Далі відбувається збудження передсердь та формування  $R$ -зубця. Після цього реєструється інтервал  $P-Q$ . Збуджується міокард шлуночків та записується  $QRS$ -комплекс. Згасається збудження та відновлюється вихідний стан, з'являється сегмент  $S-T$  і  $T$ -зубець.

### Дослідження існуючих методів обробки часових сигналів

Дані електрокардіограми є неперервним сигналом, які для обробки на комп'ютері потрібно перевести сигнал в цифрову форму. Один із способів зробити це - рівномірно по часу виміряти значення сигналу на певному проміжку часу і ввести отримані значення амплітуд в комп'ютер. Якщо робити вимірювання досить часто, то за отриманим дискретним сигналом можна буде досить точно відновити вигляд вихідного безперервного сигналу

Будь-яка безперервна функція може бути розкладена в інтеграл Фур'є. Функція представляється у вигляді суми «ряду» синусоїд з різними амплітудами, де коефіцієнти (амплітуди) при синусоїдах називаються спектром функції. У відносно гладких функцій спектр швидко убуває (з ростом частоти коефіцієнти швидко прямують до нуля). Для відносно «ламаних» функцій спектр убуває повільно, тому що для подання розривів і «зламів» функції потрібні синусоїди з великими частотами.

Розкладання сигналів в ряди Фур'є мають ряд недоліків, які привели до появи швидкого перетворення Фур'є і стимулювали розвиток вейвлет-перетворення. Основні з них:

– обмежена інформативність аналізу сигналів в зв'язку з тим, що в частотній області немає чіткого виявлення особливостей сигналів по всьому частотному діапазону спектра;

– перетворення Фур'є не дає уявлення про локальні особливості сигналу, а відображає глобальні відомості про частоти. Немає можливості аналізувати частотні характеристики сигналу в певний момент часу.

Вейвлет – це «маленька хвиля», енергія якої кінцева і локально сконцентрована в часі. Вейвлети використовуються для представлення сигналів аналогічно тому, як ряди Фур'є використовують синусоїду для розкладання сигналу. При вейвлет-розкладанні всі функції виходять з однієї шляхом її зрушень і розтягувань по осі часу.

Способи представлення результатів вейвлет-перетворення можуть бути ріноманітними. Вейвлет-спектр виглядає як поверхня в тривимірному просторі. Вид цієї поверхні відображає зміни у часі компонентів різного масштабу. Замість тривимірного зображення часто використовують або проекцію поверхні на площину із зображенням ізорівнів, або картини локальних екстремумів поверхонь, який визначає структуру локалізації максимумів і мінімумів аналізованого сигналу.

Обґрунтування застосування вейвлетів для виділення QRS-комплексу полягає в тому, що вейвлет-перетворення є гарним інструментом для аналізу перехідних, нестационарних явищ або, іншими словами, може характеризувати локальну регулярність сигналів.

### Перелік посилань

1. Electrocardiography – [Електронний ресурс] – Режим доступу до ресурсу: <https://en.wikipedia.org/wiki/Electrocardiography>
2. Wavelet-Based Analysis of Heart-Rate-Dependent ECG Features [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6932565/>.
3. Wavelet Analysis in Impedance Rheocardiography – [Електронний ресурс] – Режим доступу до ресурсу: [https://www.researchgate.net/publication/323807406\\_Wavelet\\_Analysis\\_in\\_Impedance\\_Rheocardiography](https://www.researchgate.net/publication/323807406_Wavelet_Analysis_in_Impedance_Rheocardiography)
4. The Fast Fourier Transform in Analysis of the Normal Phonocardiogram – [Електронний ресурс] – Режим доступу до ресурсу: [https://web.archive.org/web/20190504035038id\\_/https://www.jstage.jst.go.jp/article/ihj1960/20/3/20\\_3\\_333/\\_pdf](https://web.archive.org/web/20190504035038id_/https://www.jstage.jst.go.jp/article/ihj1960/20/3/20_3_333/_pdf)

УДК 004.4

Уваров В.С., Чабан О.Р., Манзюк Е.А.

*Хмельницький національний університет*

## **МЕТОД ДІАГНОСТИКИ ЗАХВОРЮВАНЬ СЕРЦЯ НА ОСНОВІ АНАЛІЗУ ЗОБРАЖЕНЬ, ОТРИМАНИХ МЕТОДОМ МАГНІТНО-РЕЗОНАНСНОЇ ТОМОГРАФІЇ**

*Створена та реалізована система для діагностики захворювань серця за допомогою аналізу зображень отриманих з магнітно-резонансної томографії (МРТ) з високою точністю, використовуючи нейромережеві підходи та інтелектуальний аналіз даних. У рамках дослідження використовувалися методи, які ґрунтуються на навчанні нейромереж на прикладах зображень серця пацієнта, а також методи, що використовують аналіз зображень для виявлення аномалій та відхилень в роботі серця. У розробленій системі існують механізми візуалізації та інтерпретації результатів нейромережі. Це може включати в себе відображення та пояснення ключових зон аномалій або патологічних змін на МРТ-зображеннях, виділення певних анатомічних особливостей та вказівників, які призвели до діагнозу.*

*A system has been developed and implemented for the diagnosis of heart diseases using high-precision analysis of images obtained from magnetic resonance imaging (MRI) with the utilization of neural network approaches and intelligent data analysis. Within the research framework, methods were employed that relied on training neural networks on examples of both healthy and heart disease-afflicted patients, as well as methods that utilized data-driven image analysis to detect anomalies and deviations in heart function. In the developed system, there are mechanisms for visualizing and interpreting the neural network's results. This may include displaying and explaining key areas of anomalies or pathological changes on MRI images, highlighting specific anatomical features and indicators that led to the diagnosis.*

Серцево-судинні захворювання протягом багатьох років залишаються однією з провідних причин смертності у всьому світі. У сучасному світі, особливо в розвинених країнах, це питання стає надзвичайно актуальним для системи охорони здоров'я [2, 3]. В цьому контексті особливе значення приділяється методам візуалізації, які відіграють ключову роль у наданні точних діагнозів вчасно.

Для оцінки стану серця та його функціонування використовуються різні методи візуалізації, такі як ультразвукове дослідження, електрокардіографія та магнітно-резонансна томографія (МРТ). Ці методи вимагають об'єктивних та ефективних інструментів аналізу роботи серця. Особливо важливим завданням є визначення об'єму лівого шлуночка серця, що дозволяє вчасно виявляти можливе

збільшення серця, що може виникнути внаслідок серцевої недостатності. Лівий шлуночок відповідає за перекачування крові до великої частини організму, і тому його функція є вирішальною для загальної оцінки роботи серця [1, 5].

Наукові дослідження, які проводяться в цій галузі, спрямовані на аналіз зображень серця, отриманих за допомогою МРТ, з метою покращення діагностики та контролю за серцевими захворюваннями.

Оцінка функції серця вимагає особливих підходів, і однією із ключових задач є точне визначення об'єму лівого шлуночка серця [4]. Це має важливе значення, оскільки збільшення лівого шлуночка може свідчити про розвиток серцевої недостатності. Робота лівого шлуночка полягає в перекачуванні крові до значної частини організму.

У запропонованій системі спочатку проводиться передпроцесінг, що включає в себе операції обрізки та повторного відбору частини зображення. Ця послідовність дій призводить до отримання обробленого зображення, готового до подальшої передачі у мережу. Наступним етапом є пропускання цього зображення через навчену мережу, що призводить до виділення піксельного маркування міокарда та визначення пікселів фону (тобто всі пікселі, які не відносяться до міокарда).

Після цього проводиться пост-обробка отриманого маркування, результатом якої є формування контуру сегментованого міокарда та його подальше поєднання з вихідним зображенням. Ця система розроблена для потенційних користувачів, які мають намір використовувати її для виділення контуру міокарда на зображеннях.

Зображення спочатку піддається процедурі ресемплінгу, а потім проходить через підготовлену мережу для виділення центрального контуру, що оточує лівий шлуночок серця. Отримана сегментація має ті самі розмір та роздільну здатність, що й вихідне зображення, і контури відображаються поверх нього.

Ця мережа відзначається своєю повністю згортковою структурою, яка складається з двох ключових компонентів: кодувальної та декодувальної частин мережі. Кожен кодер співпрацює зі своїм відповідним декодером, створюючи потужний механізм для точного виділення контуру міокарда. Ця система призначена для користувачів, які мають намір використовувати її для медичних досліджень та діагностики, і вона допомагає автоматизувати та полегшити процес виділення контуру серця на зображеннях.

Кодери включають два або три згорткових блоки, кожен з ядрами згортувального шару розміром 3 x 3. Після кожного такого блоку слідує шар пакетної нормалізації та шар ReLU для активації. По завершенні кожного згорткового блоку застосовується шар макс-пулінгу з вікном розміром 2 x 2 та кроком 2, що призводить до зменшення розмірності карти ознак. Важливим є те, що

кількість каналів ознак подвоюється після кожної дискретизації знижувальною функцією.

Індекси, які отримуються під час операцій макс-пулінгу, зберігаються та використовуються в декодерах. Декодери, в певному розумінні, можна розглядати як дзеркальні версії кодерів, але вони включають де-згорткові шари для розширення розмірності карти ознак, використовуючи індекси макс-пулінгу, отримані на етапі кодування.

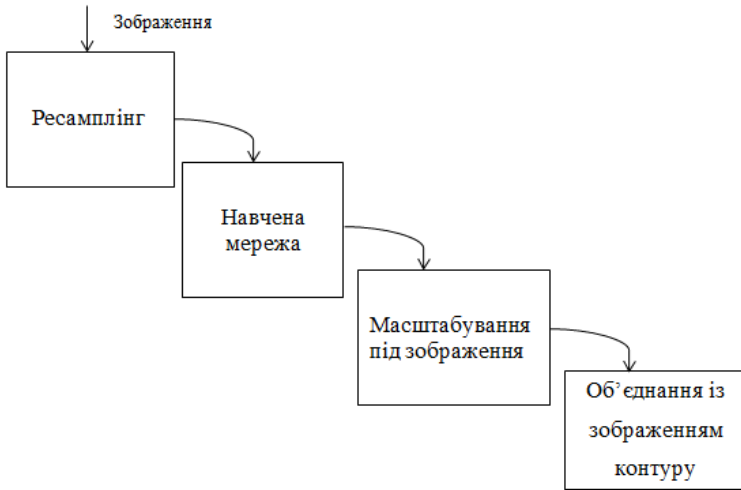


Рисунок 1 – Ілюстрація етапів роботи запропонованої системи для сегментації міокарда

Архітектура є модифікованою версією архітектури U-net, але відрізняється тим, що у кодерах завжди використовуються лише два блоки згорткових шарів. Важливою особливістю є те, що кількість каналів ознак залишається постійною, це відрізняє її і робить менш вимогливою до використання пам'яті ресурсів.

У результаті застосування глибокого навчання була створена модель для сегментації лівого шлуночка серця, що вдалося здійснити основну мету проекту. Ця модель продемонструвала хороші досягнення, успішно сегментуючи міокард у багатьох складних випадках, включаючи ситуації, коли присутні папілярні м'язи. Важливо зазначити, що мережі навчилися не лише визначати контури за інтенсивністю, але й розрізняти важкі сценарії, такі як поява темних ділянок у лівому шлуночку, і успішно інтегрують ці області у сегментацію лівого шлуночка.

Це демонструє важливість процесу навчання, де ознаки, що можуть бути важко реалізовані вручну в моделі, легко інтегруються через навчання. Мережа демонструє консистентну здатність виділяти ендокард, незалежно від наявності чи відсутності папілярних м'язів, що підкреслює її універсальність. Модель також проявляє інваріантність до масштабу та впорядковує сегментацію міокарда на зображеннях різного розміру. Однак, варто зауважити, що зовнішні межі, як правило, визначаються більш точно у випадках з меншими розмірами.

### Перелік посилань

1. Barrett M., Boyne J., Brandts J., Brunner-La Rocca H.-P., De Maesschalck L., De Wit K., Dixon L., Eurlings C., Fitzsimons D., Golubnitschaja O. Artificial intelligence supported patient self-care in chronic heart failure: a paradigm shift from reactive to predictive, preventive and personalised care. *Epm Journal*. 2019. Vol. 10. Pp. 445–464.
2. Biofeedback D. Biofeedback: an overview in the context of heart-brain medicine. *Cleveland Clinic journal of medicine*. 2008. Vol. 75. Pp. S31.
3. Johnston B. W., Barrett-Jolley R., Krige A., Welters I. D. Heart rate variability: Measurement and emerging use in critical care medicine. *Journal of the Intensive Care Society*. 2020. Vol. 21, No. 2. Pp. 148–157.
4. Kwon J., Kim K.-H., Jeon K.-H., Lee S. E., Lee H.-Y., Cho H.-J., Choi J. O., Jeon E.-S., Kim M.-S., Kim J.-J. Artificial intelligence algorithm for predicting mortality of patients with acute heart failure. *PloS one*. 2019. Vol. 14, No. 7. Pp. e0219302.
5. Sonawane A. R., Aikawa E., Aikawa M. Connections for matters of the heart: network medicine in cardiovascular diseases. *Frontiers in Cardiovascular Medicine*. 2022. Vol. 9. Pp. 873582.

УДК 004.4

Федоренко В.В., Пасічник О.А., Скрипник Т.К.

*Хмельницький національний університет*

## **ТЕХНОЛОГІЯ БЛОКЧЕЙН У СФЕРІ РЕЄСТРАЦІЇ МАЙНОВИХ ПРАВ**

*Технологія блокчейн ґрунтується на створенні двох списків даних, де окремі елементи, відомі, як блоки, поєднуються в ланцюжок завдяки криптографії. Блокчейн забезпечує відкрите зберігання потрібної інформації, забезпечуючи незмінність даних і збереження конфіденційності особистої інформації. Важливо відзначити, що блокчейн можна розглядати, як безмежну цифрову книгу економічних транзакцій, яку можна використовувати для фінансових операцій і обробки практично будь-яких даних, що мають велику цінність.*

*Блокчейн – це інноваційна технологія, що активно застосовується в різних галузях, таких як економіка, фінанси, медицина, правова сфера та інші. Проте використання блокчейну та смарт-контрактів в сфері нерухомості досі залишається недостатньо дослідженим. В цьому дослідженні розглядаються переваги та недоліки використання блокчейну та смарт-контрактів, і пропонується безпечна система для укладення угод, пов'язаних з орендою та продажем нерухомості, з використанням цих технологій.*

*Blockchain technology is based on the creation of two lists of data, where individual elements, known as blocks, are linked together in a chain using cryptography. The blockchain provides open storage of the necessary information, ensuring data integrity and maintaining the confidentiality of personal information. It is important to note that the blockchain can be viewed as a limitless digital ledger of economic transactions that can be used for financial transactions and processing of almost any data of great value.*

*Blockchain is an innovative technology that is actively used in various industries, such as economics, finance, medicine, legal, and others. However, the use of blockchain and smart contracts in the real estate sector is still insufficiently researched. This study examines the advantage and disadvantages of using blockchain and smart contracts, and proposes a secure system for concluding real estate transactions using these technologies.*

З розвитком новітніх технологій та постійними ризиками викриття чи несанкціонованого доступу до даних перестає мета забезпечити цілісність даних у сфері реєстрації майна, одним з найкращих це технологія блокчейн ...

Блокчейн – це інноваційна децентралізована система зберігання даних, що фактично представляє собою електронний журнал транзакцій, угод, контрактів та різноманітної інформації, який побудований на послідовних записах. Однією з основних переваг цієї технології є те, що дані не централізовано зберігаються на одному центральному сервері.

Технологія блокчейн спирається на важливий принцип групування всіх транзакцій у блоки,



використовуючи складні математичні алгоритми. Ці блоки об'єднуються в послідовний ланцюжок і криптографічно зв'язуються між собою. Ключовим елементом кожного блоку є його хеш – це унікальний цифровий підпис, який ґрунтується на інформації з попереднього блоку.

Підсумовуючи, можна виділити наступні основні переваги використання технології блокчейн:

1. У технології блокчейн відкритість та безпека є ключовими аспектами. Інформація щодо транзакцій, угод та смарт-контрактів доступна для загального перегляду, але неможливість змін чи втручання у ці дані гарантується. Подробиці про учасників процесу залишаються конфіденційними, і кожен користувач блокчейн має унікальний ключ - набір криптографічних записів, які не лише забезпечують надійність системи, але й захищають інформацію від потенційних хакерських атак. В контексті нерухомості ця перевага стає особливо корисною, оскільки фінансові операції між учасниками можуть бути чітко ідентифіковані, при цьому не потрібно розголошувати особисті дані;

2. Неможливість підробки: Кожен блок в блокчейні є незмінним, що запобігає будь-якій можливості підробки чи фальсифікації даних;

3. Стійкість до вторгнень: Через одночасне оновлення реєстру на всіх комп'ютерах в мережі технологія блокчейн надійно захищає дані від можливих вторгнень та змін;

4. Гарантований рівень довіри: Високий рівень довіри в операціях та обміні конфіденційною інформацією робить технологію блокчейн популярною для застосування в різних галузях, включаючи сферу нерухомості.

5. Децентралізація – рівність і різноманітність системи робить її майже неможливою для злому або пошкодження;

6. Необмеженість – це важлива особливість технології блокчейн є те, що теоретично її ланцюжок може бути безмежно розширений шляхом додавання будь-якої кількості блоків. Це означає, що система може безперервно розвиватися та розширюватися, не обмежуючись кількістю блоків. Така можливість створює безмежні перспективи застосування технології блокчейн у різних галузях, забезпечуючи масштабовану та надійну інфраструктуру для реєстрації та відстеження транзакцій і даних.

Для забезпечення надійності та безпеки майнових транзакцій, використання смарт-контрактів у технології блокчейн є оптимальним рішенням. Смарт-контракти представляють собою спеціальні протоколи, які записуються у вигляді програмного коду і функціонують у децентралізованому реєстрі, який керується комп'ютерною мережею. Зазвичай вони визначають та перевіряють умови контракту.

Блокчейн-додатки ґрунтуються на революційній моделі розробки масштабованих систем, яка спирається на використання децентралізованих додатків. Важливим прикладом цієї моделі є біткоїн, який вперше представив новий підхід до створення системи з відкритим вихідним кодом. Його архітектура базується на однорангових вузлах, де дані зберігаються у зашифрованому вигляді. Крім того, інші проекти, такі як Ethereum, Omni і Sage Network, також застосовують

цю модель, запропоновану розробниками біткоїна, для створення децентралізованих додатків.

Мережа блокчейн представляє собою мережу вузлів, кожен з яких має розгорнутий Ethereum-клієнт і з'єднується з іншими вузлами. Цей компонент відповідає за виконання смарт-контрактів та обробку різних транзакцій між користувачами системи. Блокчейн та смарт-контракти взаємодіють так: смарт-контракти – це фрагменти коду, що розміщені у блокчейні і виконують певні операції за умови задовільнення певних умов. Як тільки ці операції завершуються, вони стають сталими записами у мережі блокчейн і не піддаються змінам.

На Рисунок 1 можна побачити діаграму компонентів розробленої системи, призначеної для здійснення безпечних операцій з нерухомістю. Система складається із чотирьох основних частин: мережі блокчейн, веб-клієнта, серверної частини та реляційної бази даних.

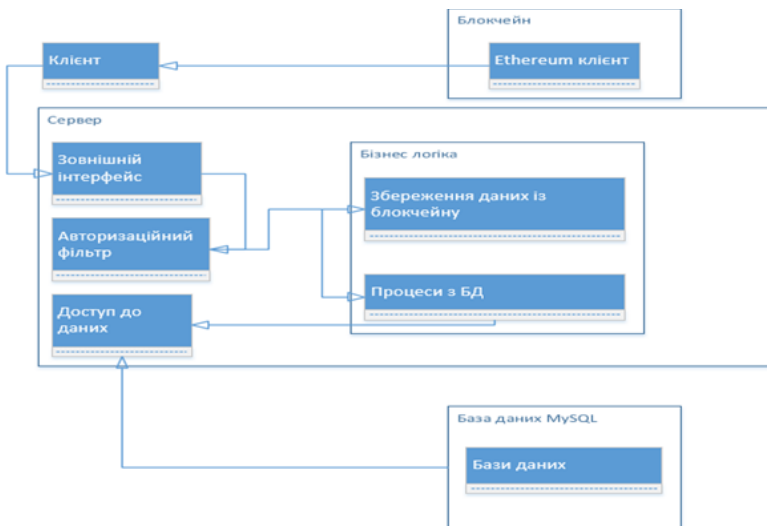


Рисунок 1 – діаграма компонентів системи для безпечних операцій з нерухомим майном

Реалізація смарт-контрактів базується на використанні мови програмування Solidity, яка є об'єктно-орієнтованою і була спеціально створена для ефективного створення смарт-контрактів, що функціонують на платформі Ethereum. Додатково для прискорення процесу розробки додатків використовуються різноманітні бібліотечні інструменти.

Веб-клієнт – це інтерфейс, який користувач використовує для взаємодії з системою. Функціональність веб-клієнта залежить від ролі користувача, який може виступати як орендар, орендодавець, продавець або покупець нерухомості. Усі взаємодії між клієнтом і мережею блокчейн здійснюються за допомогою набору

бібліотек Spring Boot, які дозволяють виконувати різні дії, такі як передача даних з одного облікового запису на інший, читання та запис даних зі смарт-контрактів, створення смарт-контрактів.

Реалізація Spring Boot дає змогу взаємодіяти з Ethereum через HTTP за допомогою JSON RPC-викликів. Це означає, що веб-клієнт може надсилати запити до окремих вузлів Ethereum та здійснювати читання та запис даних в блокчейні. Для підключення до вузлів мережі, основний об'єкт Spring Boot виступає як певний "міст" між клієнтом і блокчейном і передає дані провайдеру, де розгорнута мережа блокчейн.

Система використовує метод аутентифікації на основі програмних токенів для перевірки ідентифікації користувачів. Після успішної аутентифікації, користувачі отримують спеціальний токен, який надає їм право доступу до конкретних ресурсів та веб-сервісів. Цей токен служить маркером, що підтверджує їхню ідентифікацію та дозволяє використовувати систему.

Отже, у сфері нерухомості, роль смарт-контрактів та платформи Ethereum виявляється критично важливою. Крім того, інший галузевий сегмент, який може пройти суттєві зміни завдяки технології блокчейн, це... Провівши аналіз усіх ризиків, що властиві сектору нерухомості, і попередньо розглянувши технологію блокчейн, ми приходимо до висновку, що смарт-контракти можуть істотно покращити, спростити і зробити більш доступними процеси оренди та купівлі нерухомості завдяки зберіганню всіх документів і даних на блокчейні. Важливим аспектом є те, що будь-яка інформація щодо транзакцій, платежів або договірних угод не може бути видалена з блокчейну, що помітно зменшує ризик зловживань і шахрайства.

### Перелік посилань

1. Все про типи та створення смарт-контрактів. [Електронний ресурс] Режим доступу: <https://merehead.com/ua/blog/how-develop-smart-contract/>
2. Застосування блокчейн у сфері нерухомості [Електронний ресурс] Режим доступу: <https://guland.com.ua/kryptovalyuta/blockchain/blokcheyn-v-nerukhomosti.htm>
3. Ethereum для Java розробників [Електронний ресурс] Режим доступу: <https://ethereum.org/ru/developers/docs/programming-languages/java/>Що таке смарт контракт [Електронний ресурс] Режим доступу: <https://www.ibm.com/topics/smart-contracts>
4. Десять видів смарт-контрактів на блокчейні [Електронний ресурс] Режим доступу: <https://www.techtarget.com/searchcio/feature/Examples-of-smart-contracts-on-blockchain>
5. Що таке смарт-контракт в блокчейн і як він працює [Електронний ресурс] Режим доступу: <https://www.investopedia.com/terms/s/smart-contracts.asp>
6. Як блокчейн працює. Крок-за-кроком [Електронний ресурс] Режим доступу: <https://www.britannica.com/money/how-smart-contracts-work>
7. Що таке смарт-контракт? [Електронний ресурс] Режим доступу: <https://www.coinbase.com/ru/learn/crypto-basics/what-is-a-smart-contract>
8. Створення і розгортання смарт-контрактів з Solidity [Електронний ресурс] Режим доступу: <https://www.baeldung.com/smart-contracts-ethereum-solidity>
9. Смарт-контракт і блокчейн технології [Електронний ресурс]. Режим доступу: <https://www.javatpoint.com/smart-contracts-in-blockchain-technology>

УДК 004.4

Хміль О.О, Праворська Н.І.

*Хмельницький національний університет*

## **ВЕБ-САЙТ БІРЖІ ФРІЛАНСУ**

*Сучасний ринок праці постійно змінюється, змінюючи звичні уявлення про робочі відносини та шляхи заробітку. Веб-сайт біржі фрілансу є центральним елементом цифрової екосистеми, де фахівці та замовники зустрічаються для виконання проектів та взаємодії. Ця платформа створює унікальну можливість обміну навичками, послугами та ідеями без географічних обмежень, створюючи нові шляхи співпраці та заробітку як для індивідуальних фахівців, так і для підприємств. Важливою складовою веб-сайтів біржі фрілансу є їхні функції відбору, взаємодії та забезпечення якості виконання проектів. Із постійним зростанням ринку, стає необхідним розглядати інноваційні підходи для підвищення ефективності вибору фахівців, забезпечення надійності та безпеки угод, а також покращення способів оцінки результатів. Створення веб-сайту біржі фрілансу відображає важливість адаптації до сучасних тенденцій у зайнятості та розвитку технологій, забезпечуючи гнучкість, комфорт та ефективність для всіх учасників цього динамічного екосистеми праці.*

*The modern labor market is constantly changing, changing the usual ideas about working relationships and ways of earning. A freelance exchange website is the centerpiece of a digital ecosystem where professionals and clients meet to complete projects and interact. This platform creates a unique opportunity to share skills, services and ideas without geographical limitations, creating new ways of collaboration and earnings for both individual professionals and enterprises. An important component of freelance exchange websites is their selection, engagement and project quality assurance functions. With the constant growth of the market, it becomes necessary to consider innovative approaches to increase the efficiency of the selection of specialists, ensure the reliability and security of transactions, as well as improve the methods of evaluating results. Creating a freelance exchange website reflects the importance of adapting to current trends in employment and technology development, ensuring flexibility, comfort and efficiency for all participants in this dynamic work ecosystem.*

Сьогоднішній світ зазнає постійні зміни у способах праці та найму. Зростання фрілансу та дистанційної роботи стає все більш актуальним. Платформи фрілансу стають ключовими для пошуку роботи та найму фахівців.

Метою роботи є створення веб-сайту біржі фрілансу, який дозволить забезпечити зручний простір для зустрічі фахівців та замовників. Він підтримуватиме гнучкість у виборі роботи чи фахівця, а також надаватиме

можливість відстеження рейтингу та зворотний зв'язок для покращення якості послуг.

Аналіз сучасних тенденцій у галузі фрілансу відображає наступні ключові аспекти:

– Зростання популярності фрілансу: Світова тенденція до збільшення кількості фрілансерів та споживачів їхніх послуг. Це стимулює попит на веб-сайти бірж фрілансу для полегшення пошуку роботи та найму фахівців.

– Розвиток багатофункціональних інструментів: Інструменти стають ключовим напрямком в сучасних веб-сайтах бірж фрілансу. Більшості інструментів спрямовані на полегшення взаємодії між фахівцями та замовниками, забезпечення високої продуктивності та якості виконання проектів.

– Автоматизація та швидкість: Спрощення процесу пошуку фахівців та проектів через розвиток алгоритмів співставлення, що зменшує час, потрібний для знаходження ідеального кандидата чи проекту.

На основі усього сказаного можливо сформуванати концепцію прогресивного веб-сайту для фріланс біржі, який орієнтований на вдосконалення комунікації між замовником і фрілансером та оптимізацію укладання договору.

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.

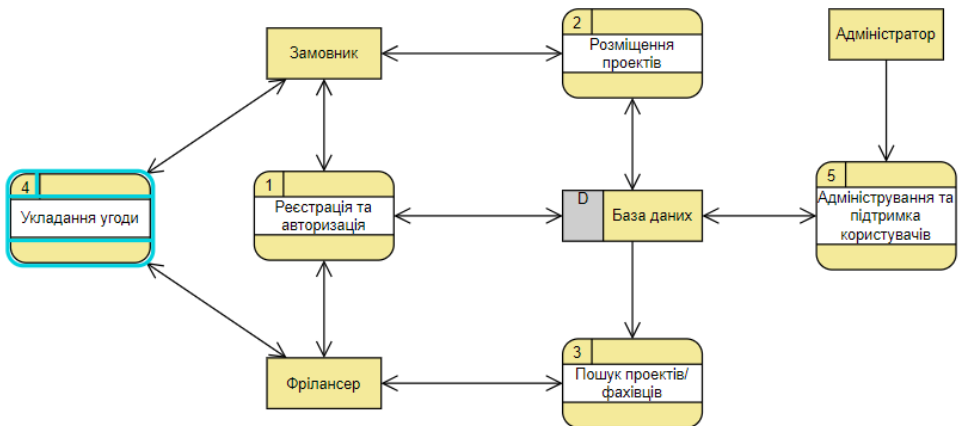


Рисунок 1 – DFD Діаграма

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 алгоритм отримання замовлення. У даній діаграмі зображено алгоритм, який є основним у взаємодії фрілансера та замовника на веб-сайті.

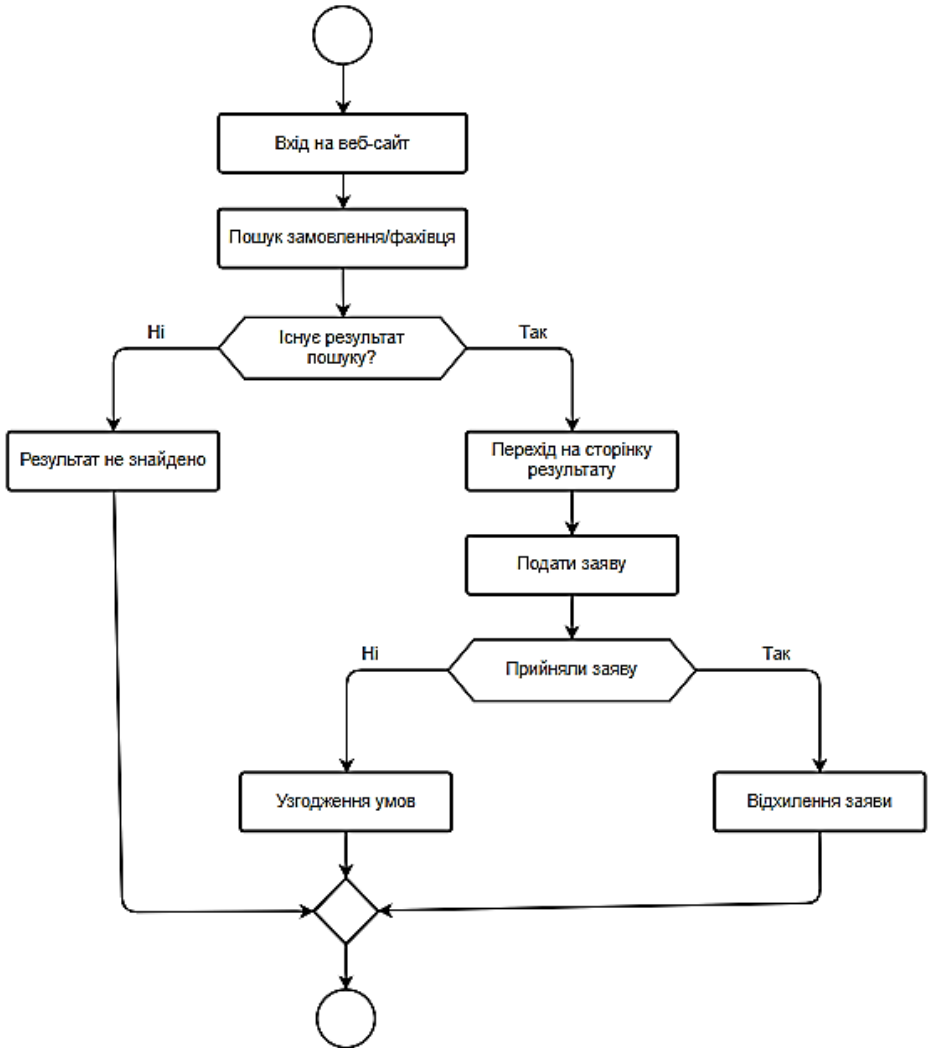


Рисунок 2 – Flowchart діаграма

Основні характеристики розроблюваного веб-сайту представляють собою:

1. Реєстрація та Профіль користувача: Можливість реєстрації для фахівців та замовників з можливістю створення та управління профілем, включаючи додавання інформації про навички, досвід роботи та портфоліо.

2. Пошук та Фільтрація: Функціонал для пошуку проєктів або фахівців за різними критеріями, використання фільтрів за галузями, областями навичок, термінами тощо.

3. Комунікація та Угода: Засоби спілкування, обговорення деталей проєктів, укладення угод та взаємодія між сторонами за допомогою чату та системи коментування.

4. Оцінка та Рейтинг: Механізми для оцінювання фахівців та замовників, системи збору відгуків та формування рейтингів для підвищення якості взаємодії та вибору кращих учасників.

Запропонований веб-сайт має потенціал стати одним з відомих бірж праці, де забезпечиться висока якість обслуговування, широкий вибір проєктів та фахівців у різних сферах. Це місце, де спільнота фахівців зможе розвивати свої навички, знаходити нові можливості для співпраці та отримувати доступ до широкого спектру професійних проєктів у реальному часі. Основними конкурентними перевагами цього веб-сайту будуть інноваційні рішення, які полегшать відбір найкращих кандидатів для проєктів, системи контролю якості та безпеки, що підвищать рівень довіри між учасниками, а також розгалужена система відгуків та рейтингів, яка сприятиме вибору найкращих фахівців для будь-яких завдань.

### **Перелік посилань**

1. Josh B. Freelancing Foundations: A Guide to Getting Started on Upwork / Burnett Josh - Independently published 2020. – 128 pages.
2. Alexandra F. Freelance Your Way to Freedom: How to Free Yourself from the Corporate World and Build the Life of Your Dreams 1st Edition / Fasulo Alexandra – Wiley 2022. – 272 pages .

УДК 004.4

Швайко В.К., Ільчишина Ю.В.

*Хмельницький національний університет*

## **МЕТОД ВИБОРУ ВИДУ СПОРТУ НА ОСНОВІ МОРФОФУНКЦІОНАЛЬНИХ ПОКАЗНИКІВ ЛЮДИНИ**

*Охарактеризовано сучасний стан залученості молоді до фізичної активності та занять спортом. Запропоновано алгоритм та метод розрахунку підбору виду спорту на основі морфофункціональних показників. Наведені середні значення для показників та їх вагові коефіцієнти.*

*The current state of youth involvement in physical activity and sports is characterized. An algorithm and a method of calculating the selection of a sport based on morphofunctional indicators are proposed. The average values for indicators and their weighting factors are given.*

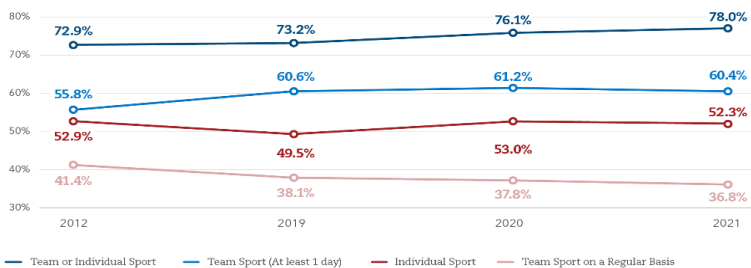
В останні роки в Україні спостерігається зниження рівня залученості дітей шкільного віку та підлітків до спортивних секцій (рисунок 1). Це пов'язано із глобальною пандемією Covid-19 у 2020-2021 роках, коли діти були змушені вести пасивний спосіб життя, а також із початком повномасштабного вторгнення російських військ на територію України.

За статистичними даними, отриманими у результаті соціологічного опитування, проведеного Фондом Фрідріха Еберта у 2017 році, 33% молоді віком 14–29 років займаються спортом у вільний час часто та дуже часто, 18% не роблять цього ніколи, а 46% зрідка або інколи. Регулярність занять знижується з віком — від 48% серед підлітків до 25% у 25–29 років [2].

У наших попередніх роботах [1,3] ми запропонували методику та концепцію системи підтримки прийняття рішень (СППР) щодо вибору спорту на основі морфофункціональних показників. Тому є актуальним розробити алгоритм та метод розрахунку підбору на основі середніх значень для показників та вагових коефіцієнтів.

Метою роботи є розробка автоматизованого виду спорту на основі вивчення морфофункціональних та соціально-психологічних показників, врахування рівня рухових можливостей дитини. Нашою цільовою аудиторією є молодь, а точніше діти шкільного віку. За статистикою найкращий вік для обрання спортивних секцій є 10-11 років, тому ми консультуємось з тренерами спортивних секцій підібрали основні необхідні нормативи для задачі на основі тих видів спорту, що культивуються в нашому місті. Загальні показники занять спортом серед дітей 6-12 років згідно [1] наведено на рисунку 1.





Source: Sports & Fitness Industry Association, 2021

Рисунок 1 - Загальні показники занять спортом серед дітей 6-12 років згідно [1]

Таблиця 1 – Середні показники нормативів для дітей (юнаків та дівчат) віком 10 та 11 років

№	Вид спорту/ Індикатор	Вагові коефіцієнти													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Баскетбол	0,3			0,15	0,05	0,2	0,15	0,05			0,1			
2	Бокс				0,1		0,2			0,3			0,15	0,25	
3	Вільна боротьба						0,1		0,25	0,3	0,2				0,15
4	Важка атлетика		0,5	-0,2		0,2				0,4	0,1				
5	Велоспорт	-0,2			0,45	0,4		-0,2				0,2		0,15	
6	Веслування		0,2	0,15					0,25	0,3					
7	Волейбол	0,1				0,25	0,15	0,1	0,15			0,05			
8	Гандбол		0,1		0,15	0,15	0,1		0,1	0,1	0,15				
9	Дзюдо		0,15		0,1	0,2			0,05	0,05	0,1	0,15	0,1	0,1	
10	Карате				0,1	0,05			0,1	0,25	0,2	0,15	0,15		
11	Кікбоксинг			0,15	0,05	0,05			0,1	0,2	0,1		0,2	0,15	
12	Легка атлетика (біг)	0,2			0,3	0,15		0,2				0,15		0,1	
13	Легка атлетика (стрибки)	0,2			0,2	0,25		0,2				0,1			
14	Легка атлетика (метання)		0,25	0,15			0,25		0,1	0,15					0,1
15	Панкратіон			0,15	0,05		0,1		0,15	0,25	0,05		0,2	0,05	
16	Пауерліфтинг	-0,1		0,35	-0,1		0,25		0,25	0,35					
17	Плавання	0,2	0,15	0,1	0,15			0,05	0,1		0,1				0,15
18	Регбі			0,15		0,25	0,1	0,1		0,15		0,25			
19	Самооборона			0,2			0,15			0,2	0,1	0,15	0,15	0,05	
20	Спортивна стрільба	-	-	-	-	-	-	-	-	-	-	-	-	-	-
21	Теніс					0,25	0,2	0,15	0,1			0,3			
22	Настільний теніс					0,15	0,2		0,1			0,25	0,3		
23	Тхеквондо					0,1	0,1		0,1	0,25	0,1	0,15	0,2		
24	Фехтування				0,15	0,1	0,1				0,1	0,2	0,25	0,1	
25	Футзал					0,2	0,15			0,1	0,1	0,3	0,15		
26	Футбол	0,15				0,3	0,15			0,1	0,1	0,2			
27	шахи			0,15	0,05		0,1								

Аналізуючи необхідні навички, ми систематизували важливість певного нормативу в межах конкретного виду спорту і розділили пріоритетність по коефіцієнтам. Це дозволить допомогти дітям шкільного віку здійснити найоптимальніший підбір видів спорту з тих, які культивуються в регіоні.

Наступним кроком буде доопрацювання нами кросплатформеного мобільного застосунку та імплементація отриманих в результаті дослідження даних в алгоритм. В майбутньому планується також розширення бази знань – тобто інформації по видах спорту, які культивуються в регіоні, збору інформаційних показників (індикаторів) для кожного виду спорту, збору тестових даних у вигляді морфофункціональних показників учня. Подальші дослідження спрямовані на даних та формування бази знань на бази даних та програмну реалізацію системи підтримки прийняття рішень щодо вибору виду спорту на основі морфофункціональних показників людини.

### **Перелік посилань**

1. Швайко В. К., Фесік З. Ю. Інформаційна система для вибору виду спорту на основі аналізу морфофункціональних показників людини. "Інформаційні технології та інженерія - 2023" (IT&I), 7-10 лютого 2023, Миколаїв, Україна, с. 28-29(доступ 03.11.2023)
2. Український спорт: вправи і результат URL: <https://tyzhden.ua/Society/212256> (доступ 03.11.2023)
3. Швайко В.К., Павлова О.О. Технологія підтримки прийняття рішень щодо вибору виду спорту на основі морфофункціональних показників людини. Актуальні Проблеми Комп'ютерних Наук (АПКН-2022), Хмельницький, Україна, 18-19 листопада 2022. Хмельницький: ХНУ, 2022. с.314-318 (доступ 03.11.2023)

УДК 004.4

Шебетко О.В., Кліменко В.І., Мазурець О.В.

*Хмельницький національний університет*

## **МЕТОД АДАПТИВНОГО ТЕСТУВАННЯ З ВИКОРИСТАННЯМ ПРОДУКЦІЙНИХ ПРАВИЛ**

*Розглянуто метод адаптивного тестування наявного рівня знань теоретичного навчального матеріалу з використанням продукційних правил, який призначений для перетворення даних користувача у вигляді множини тем навчального матеріалу, множини ключових слів теоретичного навчального матеріалу та тестових запитань у вихідні дані у формі оцінки рівня знань теоретичного навчального матеріалу. Також наведено відповідний програмний застосунок і досліджено ефективність його використання.*

*The method of adaptive testing of the existing level of knowledge of theoretical educational material using production rules is considered, which is designed to transform user data in the form of a set of topics of educational material, a set of keywords of theoretical educational material and test questions into output data in the form of an assessment of the level of knowledge of theoretical educational material. The corresponding software application is also given and the effectiveness of its use is investigated.*

В сучасному світі, де навчання і розвиток знань є ключовими факторами успіху, ефективні методи оцінки рівня знань студентів стають все більш важливими. Традиційні тести та екзамени, хоч і широко використовуються, не завжди здатні забезпечити індивідуалізоване оцінювання та зворотний зв'язок для кожного студента. Тож тестування має важливе значення у житті людей, студентів та у різних сферах життя, оскільки воно сприяє оцінюванню знань, визначенню компетентностей та вимірюванню успішності. Цей процес дозволяє виявляти сильні та слабкі сторони, вдосконалювати навички та досягати більших результатів [1].

Однак тестування має значення не лише у сфері освіти, але й у багатьох інших сферах життя. У бізнесі, наприклад, тестування використовується для оцінювання кандидатів під час процесу найму. Це дозволяє виявити їхні навички, здатності та придатність до виконання конкретних робочих обов'язків. Тестування також допомагає оцінити ефективність навчальних програм, перевірити знання своїх працівників та визначити потребу у додатковому навчанні [2].

Тестування також знайшло своє застосування у технологічних сферах, таких як розробка програмного забезпечення. Воно допомагає виявляти помилки та недоліки в програмах, забезпечує перевірку функціональності та відповідність вимогам. Тестування є важливою частиною процесу розробки програмного продукту та допомагає забезпечити його якість та надійність.

Прагнення автоматизувати процес формування тестових завдань спонукають до роздумів над штучним інтелектом та проблемами формалізації знань під час створення тестів. Традиційний підхід до створення засобів тестування зводиться до перенесення ручного тестування на комп'ютер, з використанням інформаційно-комунікаційних технологій замість паперової роботи. Це дає нам можливість керувати процесом формування тестів з великої кількості тестових завдань та автоматично перевіряти результати. Завдання, розроблені професіоналами, мають високу якість та зрозумілість. Однак значним недоліком такого підходу є висока складність самого процесу формування тестових завдань.

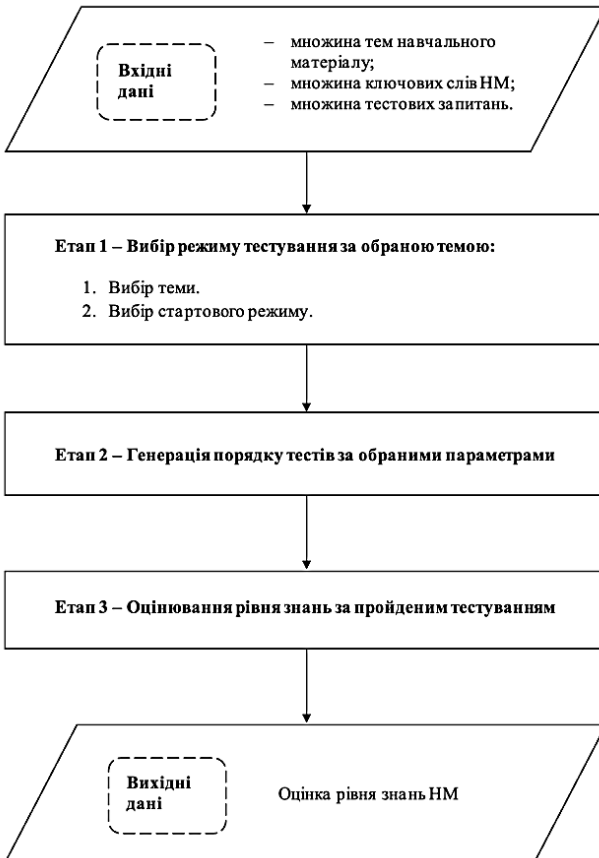


Рисунок 1 – Схема методу адаптивного тестування наявного рівня знань теоретичного навчального матеріалу

Метою роботи є розробка методу адаптивного тестування наявного рівня знань теоретичного навчального матеріалу з використанням продукційних правил та відповідної програмної реалізації на платформі .NET, яка призначена для двох груп користувачів, а саме: інженер із знань та кінцевий користувач, який проходить тестування.

Метод адаптивного тестування наявного рівня знань теоретичного навчального матеріалу з використанням продукційних правил призначений для перетворення даних користувача у вигляді множини тем навчального матеріалу, множини ключових слів навчального матеріалу НМ та тестових запитань у вихідні дані у формі оцінки рівня знань НМ [3, 4]. Схема кроків методу наведена на рисунку 1.

Першим етапом методу є вибір теми НМ з переліку запропонованих та стартового режиму тестування. Наступним етапом є генерація порядку тестових запитань за параметрами, які було обрано. З питань трьох рівнів складності, рандомно обирається 5. Два питання першого рівня (легкого), одне – другого (середнього) та два питання третього (важкого) рівня. Далі формується тестування, послідовність питань та їх складність залежить від обраного параметру на етапі 1. Після переходу з рівня 2 на рівень 1 під час тестування, відповідь на одне питання рівня 1 вибрана неправильно, то тестування завершиться, без можливості відповіді на друге. Адже для отримання мінімальної оцінки потрібно відповісти на усі питання рівня. І останній етап – це оцінювання рівня знань за темою НМ після проходження тестування.

Для відображення динамічних аспектів поведінки системи використовується діаграма діяльності. Ця діаграма, представлена у вигляді блок-схеми, демонструє логіку процедур, бізнес-процесів та потоків роботи шляхом зображення переходів між різними видами діяльності. Вона відображає як послідовні, так і одночасні дії, відображаючи логіку поведінки системи (алгоритм дій) та взаємодію декількох систем. На рисунку 2 наведено відповідну діаграму діяльності (Activity Diagram).

Для початку користувач обирає тему НМ та режим тестування, далі переглядає зміст НМ та ключові слова обраної теми. Потім розпочинає тест, якщо хоче. Якщо так, то він його проходить тестування та отримує результат. Потім користувач має можливість пройти тест знову, або вийти з тесту.

На основі вищеописаного методу адаптивного тестування наявного рівня знань теоретичного навчального матеріалу було спроектовано відповідну архітектуру інформаційної системи, що зображена на рисунку 3. Пропонована інформаційна система складається із ряду підсистем, що будуть розглянуті нижче.

*Підсистема вибору параметрів тестування.* Ця підсистема відповідає за обробку вибраної теми тестування та стартового режиму. Функції цієї підсистеми включають вибір теми навчального матеріалу для тестування, вибір режиму тестування (від найлегшого, від середнього, від найважчого) та перегляд вмісту обраної теми та переліку ключових слів.

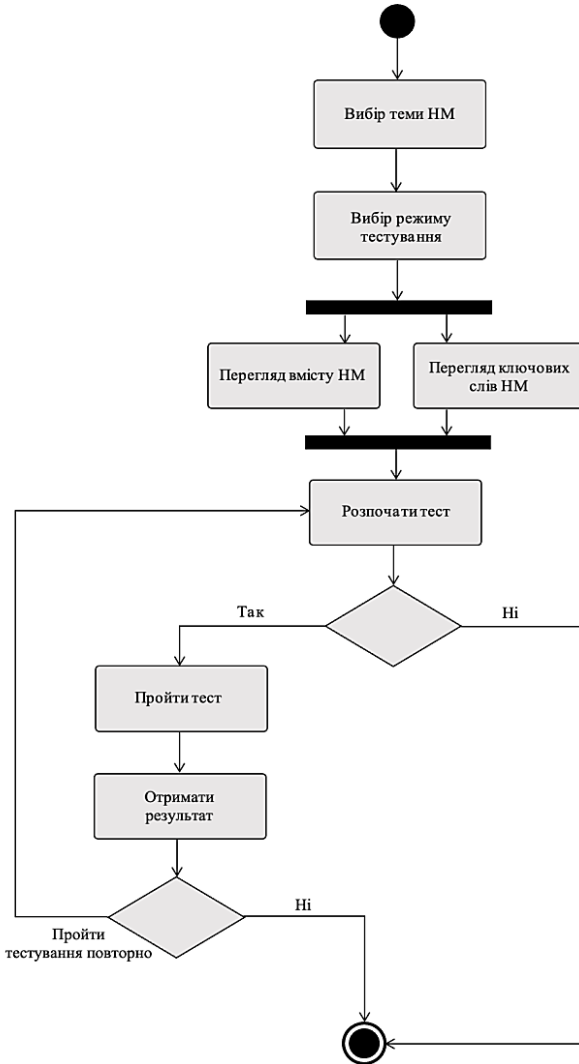


Рисунок 2 – Діаграма діяльності для адаптивного тестування наявного рівня знань теоретичного навчального матеріалу

*Підсистема генерації тестових завдань.* Дана підсистема відповідає за створення тестів залежно від рівня складності. Основні функції цієї підсистеми включають генерацію тестів з різним рівнем складності на основі продукційних

правил та генерацію варіантів питань у різних форматах (множинний вибір, одна відповідь і так далі).

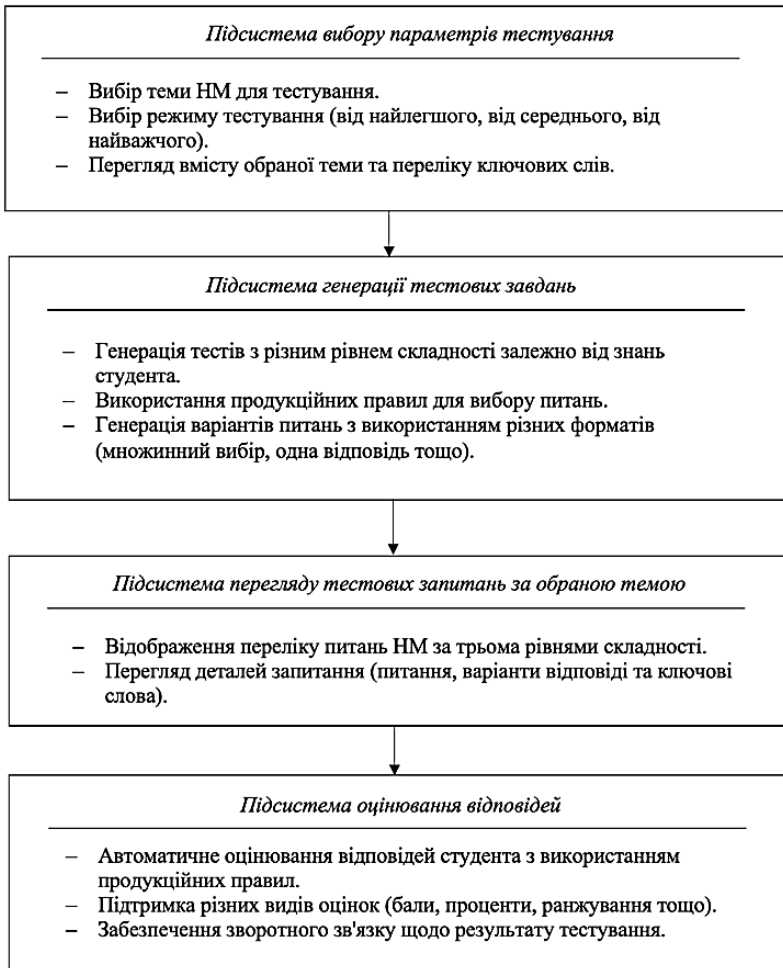


Рисунок 3 – Схема застосунку для адаптивного тестування наявного рівня знань навчального матеріалу

*Підсистема перегляду тестових запитань за обраною темою.* Функції цієї підсистеми включають перегляд переліку питань НМ за трьома рівнями складності (легкого, середнього, важкого), перегляд деталей запитання (питання, варіанти відповіді та ключові слова).

*Підсистема оцінювання відповідей.* Поточна підсистема відповідає за автоматичне оцінювання відповідей студента та надання зворотного зв'язку. Головні функції підсистеми включають автоматичне оцінювання відповідей студента на основі продукційних правил, підтримку різних видів оцінок (бали, відсотки, ранжування тощо) та забезпечення зворотного зв'язку студентів щодо результату тестування.

Отже, ці підсистеми разом забезпечують створення індивідуалізованої системи адаптивного тестування, яка дозволяє студентам ефективно навчатися та покращувати свої знання теоретичного навчального матеріалу.

Виконання поставлених задач відіграє одну з головних ролей в розробці інформаційної структури системи. Нижче на рисунку 4 наведено діаграму класів інформаційної системи.

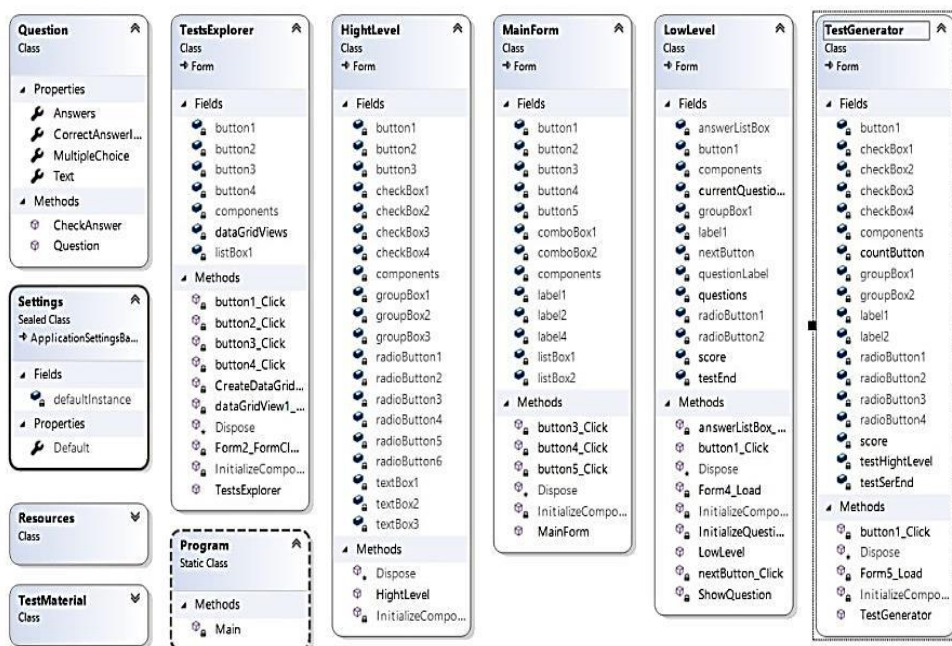


Рисунок 4 – Діаграма класів застосунку для адаптивного тестування наявного рівня знань навчального матеріалу

У класі `MainForm` реалізовано обробку обраної теми навчального матеріалу, вибору режиму тестування. Клас `TestGenerator` слугує для генерації тестових запитань різних рівнів складності. `TestsExplorer` – клас, у якому програмно створено відображення тестових питань обраного рівня складності та їх детальний опис. В



інших класах реалізоване тестування за різними алгоритмами: від найлегшого, від найважчого та від середнього.

Після запуску застосунку для адаптивного тестування наявного рівня знань навчального матеріалу, відкривається головне меню з вибором параметрів для початку проходження тестування (рисунок 5).

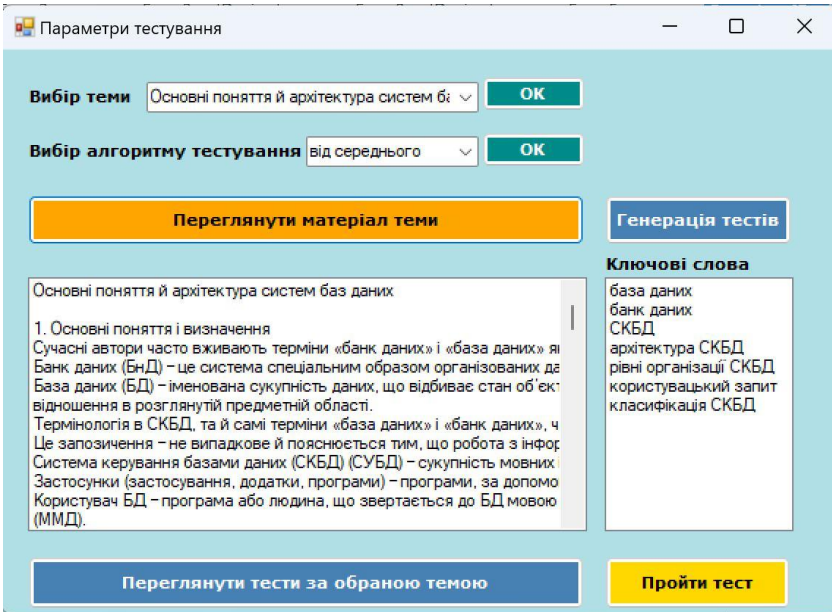


Рисунок 5 – Головне меню застосунку для адаптивного тестування наявного рівня знань навчального матеріалу

Переглянути тести за обраною темою можна обравши відповідну кнопку (рисунок 6).

Повернувшись на екран головного меню, можна розпочати тестування, за допомогою кліка на кнопку «Пройти тест». Далі з'явиться перше питання. Конкретна інструкція по відповіді на це питання буде знаходитись саме над ним. Користувач вибирає варіант відповіді, клацанням на активний кружечок та підтверджує свій вибір кліком на поле «Перейти до наступного запитання» (рисунок 7).

При вірній відповіді на питання, відображається наступне питання (зростаючи по складності вгору), при невірній відповіді засвідчується питання легше по складності.

При відповіді на останнє питання, програма автоматично вказує результат, наприклад: «Ви завершили тестування, оцінка 5», якщо правильно відповіли на всі

запитання (рисунок 8). Та «На жаль, не пройшли тестування», якщо не обрано жодної правильної відповіді (рисунок 9).

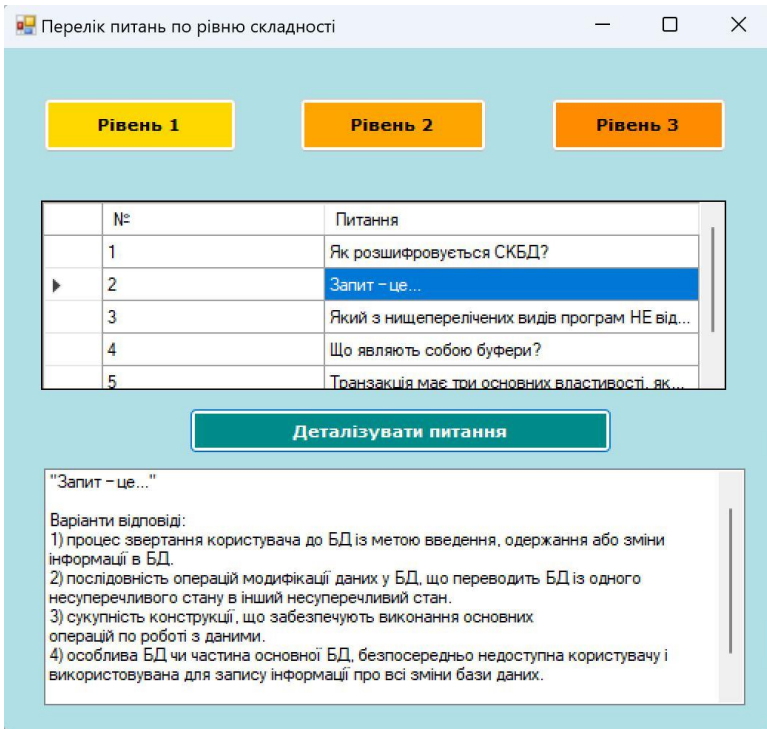


Рисунок 6 – Меню переліку запитань за рівнями складності

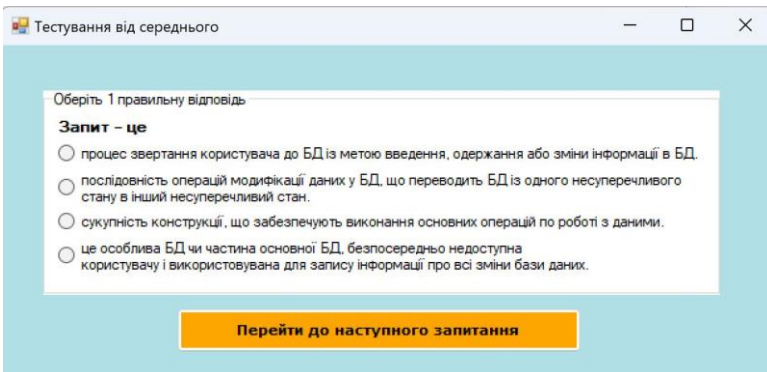


Рисунок 7 – Вигляд запитання після початку тестування

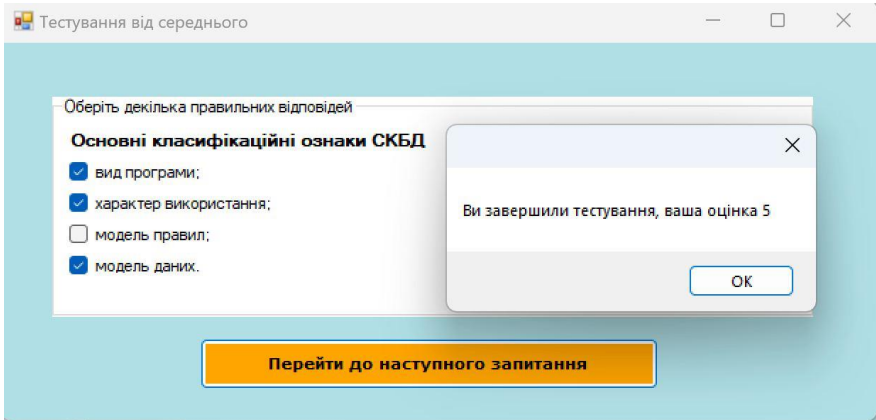


Рисунок 8 – Результат після успішного проходження тесту

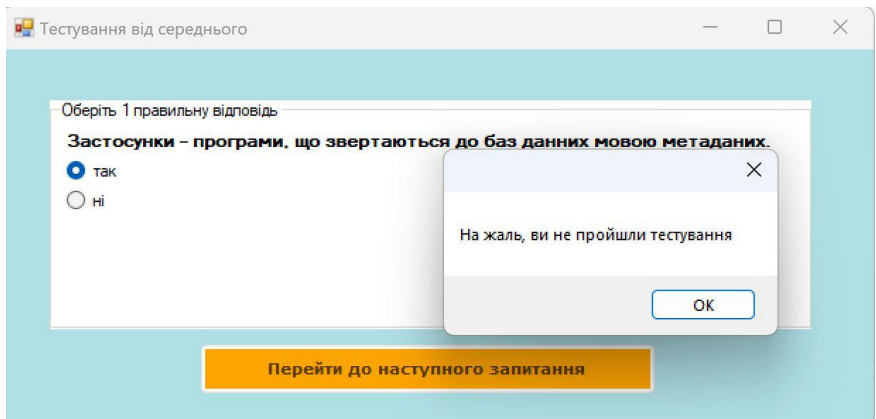


Рисунок 9 – Результат у випадку жодної правильної відповіді

Для дослідження створеного методу, було вирішено протестувати його на групі осіб та порівняти отриманий результат із результатами їхньої успішності з навчальної дисципліни. Спочатку було обрано тему навчального матеріалу з визначеної дисципліни, проведено тест та отримано оцінку з допомогою методу адаптивного тестування, результат показано на рисунку 10 і позначено помаранчевим кольором. Після цього було знайдено оцінки, які отримали студенти під час навчального процесу з обраної теми та внесено на діаграму синім кольором. Порівнявши отримані результати видно, що оцінки мають лише маленькі відхилення, окрім «Особи 4».

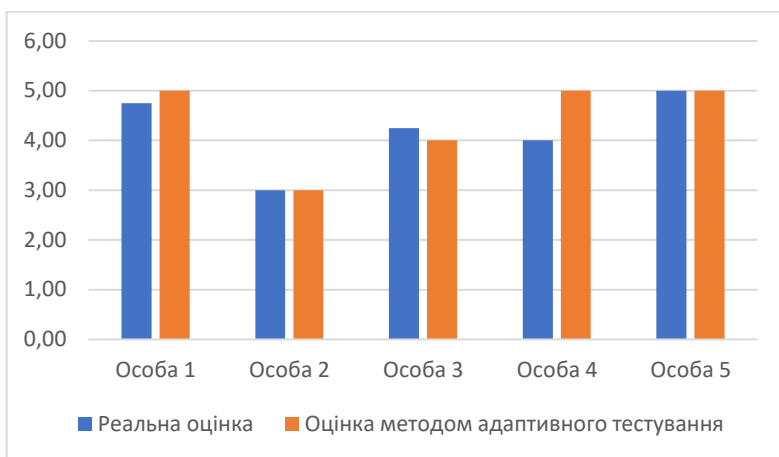


Рисунок 10 – Порівняння наявної та отриманої оцінки з використанням адаптивного методу тестування (ОК №1)

Аналогічно до попереднього дослідження, було проведено ще одне, однак за іншою темою навчального матеріалу. Результат зображено на рисунку 11.

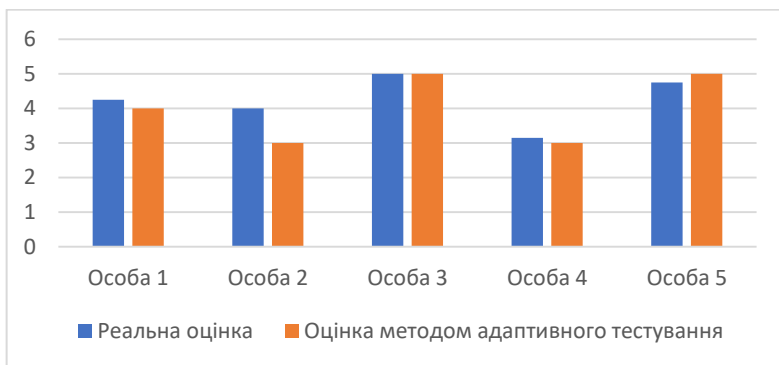


Рисунок 11 – Порівняння наявної та отриманої оцінки з використанням адаптивного методу тестування (ОК №2)

Провівши порівняння отриманих результатів, можна зробити висновок, що оцінки отримані двома способами співпадають, проте мають незначну похибку. Однак оцінки «Особа 2» не співпадають на один бал. Причиною цього є те, що адаптивне тестування глибше перевіряє знання і не дає змогу пропустити прогалини у вивченій темі, в той час як при реальному оцінюванні можуть попасти саме ті питання, які студент знає.

Для дослідження створеного програмного продукту, було вирішено протестувати його на певній групі осіб та порівняти отриманий результат із результатами їхньої успішності з навчальної дисципліни.

Спочатку було обрано тему навчального матеріалу з дисципліни «Проектування баз даних», проведено тест та отримано оцінку з допомогою методу адаптивного тестування, результат показано на рисунку 3.12 і позначено помаранчевим кольором. Після цього було знайдено оцінки, які отримали студенти під час навчального процесу з обраної теми та внесено на діаграму синім кольором.

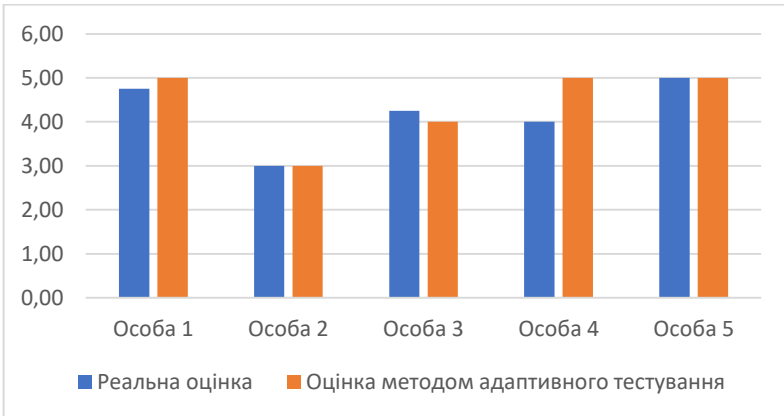


Рисунок 12 – Порівняння наявної та отриманої оцінки з використанням адаптивного методу тестування (ОК №3)

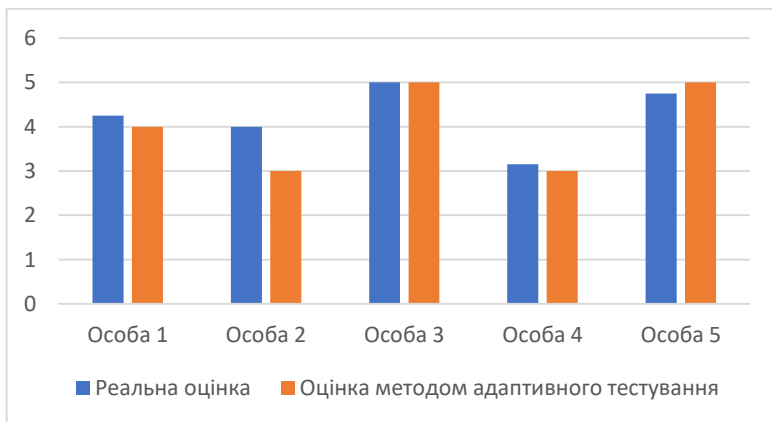


Рисунок 13 – Порівняння наявної та отриманої оцінки з використанням адаптивного методу тестування (ОК №4)

Після цього було знайдено оцінки, які отримали студенти під час навчального процесу з обраної теми та внесено на діаграму синім кольором.

Порівнявши отримані результати видно, що оцінки мають лише маленькі відхилення, окрім «Особи 4». Така неточність може бути спричинена рядом факторів, у данному випадку студент отримав меншу оцінку від викладача через невчасну здачу завдання.

Аналогічно до попереднього дослідження було проведено ще одне, однак за іншою темою навчального матеріалу. Результат зображено на рисунку 13.

Провівши порівняння отриманих результатів, можна зробити висновок, що оцінки отримані двома способами співпадають, проте мають незначну похибку.

Таким чином, було розглянуто метод адаптивного тестування наявного рівня знань теоретичного навчального матеріалу з використанням продукційних правил, який призначений для перетворення даних користувача у вигляді множини тем навчального матеріалу, множини ключових слів теоретичного навчального матеріалу та тестових запитань у вихідні дані у формі оцінки рівня знань теоретичного навчального матеріалу.

### **Перелік посилань**

1. Бармак О. В., Мазурець О. В. Інформаційна технологія гнучкого тестування рівня знань у середовищі MOODLE. Матеріали Всеукраїнської науково-практичної конференції з міжнародною участю «Сучасні інформаційні технології та інноваційні методики навчання: досвід, тенденції, перспективи». Тернопіль 2017. С.254-257.
2. Бармак О. В., Мазурець О. В. Інформаційна модель семантичної структури навчального курсу. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2018, №6, Т.1. С.92-97.
3. Мазурець О. В., Кліменко В. І., Скрипник Т. К. Автоматизоване формування тестових завдань для середовища MOODLE на основі онтології навчального матеріалу. Сучасні технології в механіці: Збірник наукових праць. Хмельницький. 2018. С.160-166.
4. Бармак О. В., Мазурець О. В., Кліменко В. І. Інформаційна технологія автоматизованого формування тестових завдань. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2017, №5. С.93-103.

УДК 004.4

Шевчук П.О., Молчанова М.О., Собко О.В.

*Хмельницький національний університет*

## **СИСТЕМА КЕРУВАННЯ ПРОДАЖАМИ ТОВАРІВ КОМП'ЮТЕРНОЇ ТЕХНІКИ З ВИКОРИСТАННЯМ ОБ'ЄКТНО-ОРІЄНТОВАНОГО ПІДХОДУ**

*Робота присвячена створенню системи керування продажами товарів комп'ютерної техніки з використанням об'єктно-орієнтованого підходу, призначена для керування, відслідковування, ведення обліку, замовлення, та купівлі товарів. Практична реалізація системи здійснена на базі об'єктно-орієнтованого підходу, що сприятиме легкому розширенню користувацького функціоналу.*

*The work is devoted to the creation of a sales management system for computer equipment using an object-oriented approach, designed for management, tracking, accounting, ordering, and purchase of goods. The practical implementation of the system is based on an object-oriented approach, which will facilitate easy expansion of user functionality.*

Система керування продажами товарів комп'ютерної техніки є незамінним інструментом для комерційних підприємств або постачальників, які займаються виробництвом цих товарів. В умовах сучасного ринкового середовища та стрімкого розвитку електронної торгівлі, де конкуренція стає все більш жорсткою та запеклішою, подібні програми надають підприємствам можливість автоматизувати процеси продажу, управління складом, обробки замовлень та багато інших аспектів торгівельної діяльності [1]. Вони є потужним інструментом для підприємств, незалежно від їх розміру та галузі, допомагаючи автоматизувати та оптимізувати процеси продажу, управління складом, відстеження покупок та взаємодію з клієнтами. Це дозволяє підприємствам миттєво отримувати оновлену інформацію про стан складу, замовлення клієнтів та фінансові показники [2].

Для функціонального опису системи спершу слід побудувати діаграму варіантів використання.

Діаграма варіантів використання є початковим концептуальним поданням або концептуальною моделлю системи у процесі її проектування і розробки. Для даного проєкту побудовано дві діаграми варіантів використання: перша діаграма відображає взаємодію з програмою у ролі користувача (рисунок 1), а друга – у ролі адміністратора (рисунок 2).

Також для візуалізації динамічних аспектів роботи системи керування продажами товарів комп'ютерної техніки було побудовано діаграму активності для адміністратора, схематично зображеної на рисунку 3.

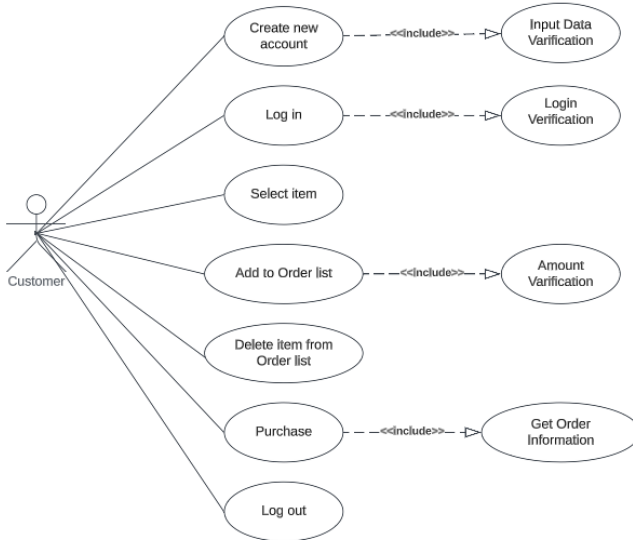


Рисунок 1 – Діаграма варіантів використання для користувача

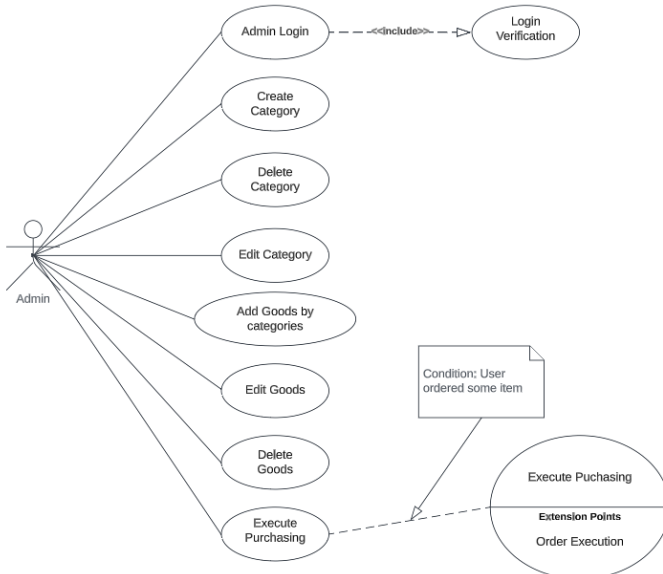


Рисунок 2 – Діаграма варіантів використання для адміністратора



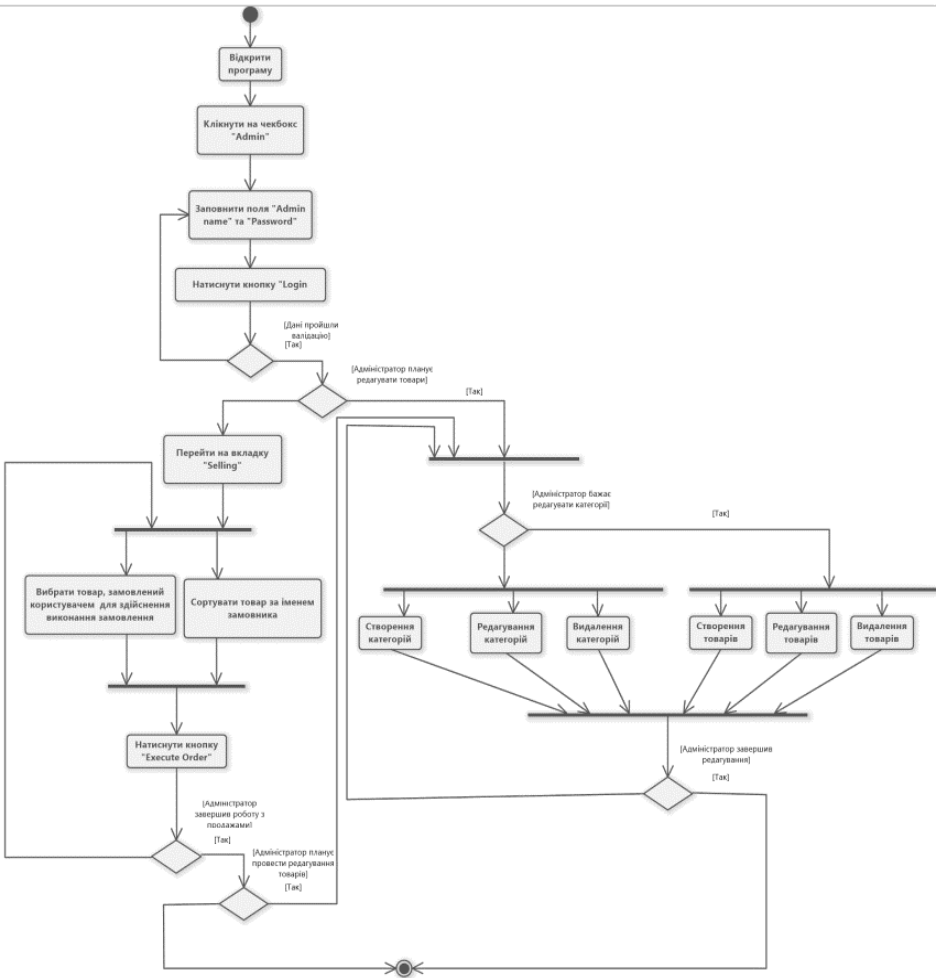


Рисунок 3 – Діаграма активності для адміністратора

Узагальнена схема системи замовлення товарів користувачем продемонстровано на рисунку 4. Модуль відповідає за інтерфейс, через який користувачі взаємодіють з системою. Він забезпечує зручний та інтуїтивно зрозумілий спосіб взаємодії з системою, де користувачі можуть створювати, редагувати замовлення, та купувати товари.

На основі розробленої структури інформаційної системи було створено діаграму класів, яка відображає структуру та взаємозв'язки класів, що будуть використовуватися в проєкті (рисунок 5).

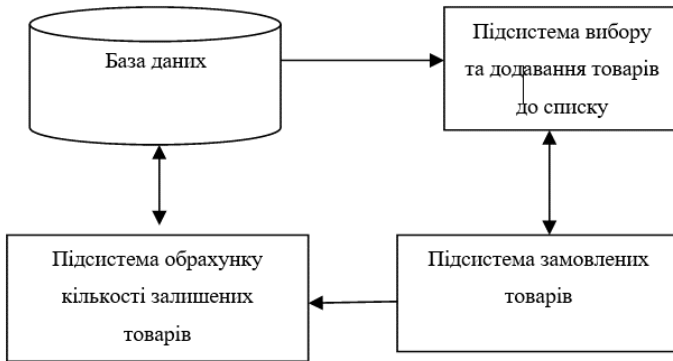


Рисунок 4 – Структура компонентів модулю замовлення товарів користувачем

Інтерфейс «IHelper» який служить для використання функціоналу реалізації підключення, та видозмінення баз даних, має такі властивості як «connection» та методи «population» та «sqlChange» які в інтерфейсі не мають реалізації. Класи. Тому «SQLCommandHelper» та «GoodsClass», який є похідним від попереднього, імплементують реалізацію від інтерфейсу «IHelper».

Статичний клас «FormActions» реалізує базову поведінку при взаємодії із застосунком такі як: «ClearTxts», «EmailValidator», «ExitForm», «ShowPas».

Класи «logForm», «regForm», «userMenu», «adminGoodsMenu», «adminCatMenu», «adminSellingForm», які є похідними від базового класу «Form», застосовуються для реалізації інтерфейсу застосунку як для користувача, так і для адміністратора. Також ці класи задіють певні правила взаємодії із системою.

За вищеописаною архітектурою інформаційної системи було розроблено програмний застосунок, інтерфейс якого наведено на рисунку 6.

Із рисунку 6 можна побачити що користувач має таблицю товарів та дані із товарів у наявності (додані адміністратором) та з правої частини список покупок самого користувача. Для купівлі товару спершу необхідно скласти список покупок. Для цього користувачу слід натиснути на бажаний товар із таблиці каталогу товарів.

Для зручності товари можна сортувати за ціною, кількістю, ім'ям, каталогом. Також для зручності додана можливість фільтрування товарів за категоріями. Отже після вибору товару користувач натискає на товар. Далі в полі «Amount» вводить кількість одиниць товару. Важливо що користувач може ввести тільки натуральне число та менше або рівне кількості на складі, в іншому ж випадку користувач отримає повідомлення про неможливість додачі товару до списку, оскільки вказане число є некоректним.

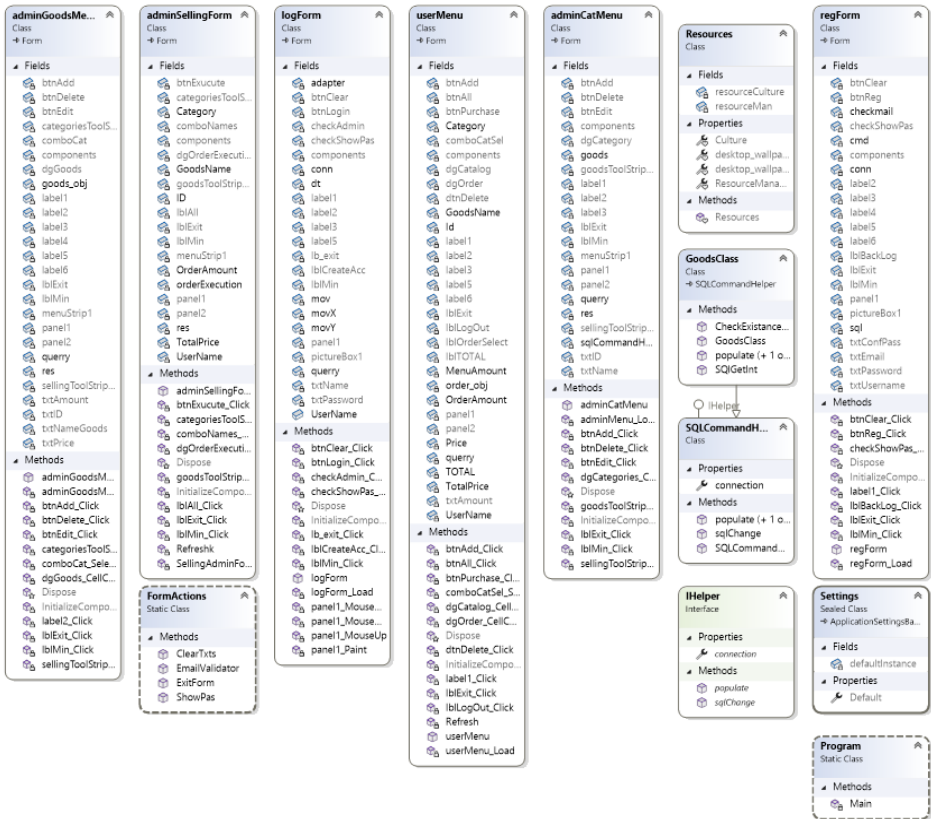


Рисунок 5 – Діаграма класів інформаційної системи

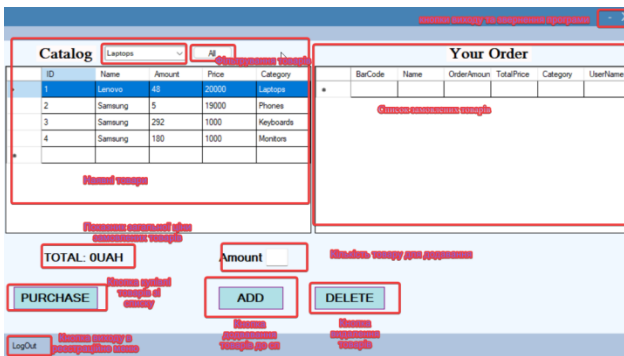


Рисунок 6 – Головне меню системи користувачів частини

Була створена система керування продажами товарів комп'ютерної техніки з використанням об'єктно-орієнтованого підходу, яка виконує основні функції пошуку, перегляду, замовлення та оплати товарів. Для реалізації системи було використано мову програмування C#, платформу розробки .Net Framework та середовище розробки Visual Studio.

Система має структуру, яка включає компоненти, такі як база даних, модуль пошуку, модуль замовлення, модуль оплати, модуль управління користувачами та інші. Кожен компонент виконує свої функції і спільно працює для забезпечення ефективної роботи системи.

### **Перелік посилань**

1. Wikipedia. Інформація про товари, та їх класифікації. URL: <https://uk.wikipedia.org/wiki/Товар>
2. Wikipedia. Споживач. URL: <https://uk.wikipedia.org/wiki/Споживач>

УДК 004.4

Якимчук Г.Б., Праворська Н.І.

*Хмельницький національний університет*

## **ПРОГРАМНИЙ ЗАСТОСУНОК ДЛЯ КЕРУВАННЯ ПРОЕКТАМИ**

*Управління проектами у сучасному світі є критично важливим для успіху організацій у різних галузях. Зміни в суспільстві та технологічний прогрес потребують постійного розвитку систем управління проектами. Ця робота є дослідженням та розробкою інноваційної системи управління проектами, яка враховує сучасні тенденції та потреби. Аналіз показує зростання популярності Agile методологій, розвиток інструментів та перехід до віддаленої роботи. Розробка системи спрямована на поліпшення планування, ресурсного менеджменту, моніторингу та комунікації в управлінні проектами, враховуючи потреби сучасного світу.*

*Project management in today's world is critical to the success of organizations in various industries. Changes in society and technological progress require continuous development of project management systems. This work is research and development of an innovative project management system that takes into account modern trends and needs. The analysis shows the growing popularity of Agile methodologies, the development of tools and the transition to remote work. The development of the system is aimed at improving planning, resource management, monitoring and communication in project management, taking into account the needs of the modern world.*

Управління проектами в сучасному світі є важливим складовим елементом ефективного функціонування організацій у різних галузях, від бізнесу та науки до громадських ініціатив. Ефективне планування, виконання та контроль проектів стає стратегічним завданням для досягнення успіху та конкурентоспроможності. Однак, у зв'язку з постійними змінами в суспільстві та технологічному прогресі, системи управління проектами також повинні постійно розвиватися та адаптуватися до цих змін.

Метою роботи є розгляд і дослідження питань, пов'язаних із розробкою і вдосконаленням систем управління проектами. Дослідження спрямоване на інтеграцію передових методологій та інноваційних технологій для створення більш ефективного програмного застосунку управління проектами, який відповідає сучасним потребам.

Аналіз сучасних тенденцій у галузі управління проектами відображає наступні ключові аспекти:

– Зростання популярності Agile методологій: Agile підходи до управління проектами, такі як Scrum та Kanban, все більше розповсюджуються завдяки їх гнучкості та спроможності швидко реагувати на зміни в умовах проекту. Agile дозволяє командам працювати більш ітеративно та відповідати на потреби клієнта.

– Розвиток багатофункціональних інструментів: Інструменти для управління проектами додають більше функцій, об'єднуючи в собі можливості для планування, моніторингу, комунікації та аналізу проектів. Це спрощує процес управління проектами та забезпечує доступ до всіх необхідних інструментів в одному місці.

– Зростання популярності віддаленої роботи в управлінні проектами: Віддалена робота стає стандартом у світі, що вимагає нових підходів до управління проектами, включаючи віддалену комунікацію та спільну роботу команд, що може бути викликом та одночасно перевагою для управління проектами.

На основі вищесказаного формується концепція розробки інноваційного програмного застосунку управління проектами, який орієнтований на вдосконалення та оптимізацію управління проектами.

В ході проектування вказаного застосунку було розроблено діаграму потоків даних (рисунок 1) та flowchart (рисунок 2) для демонстрації загальної роботи з застосунком.

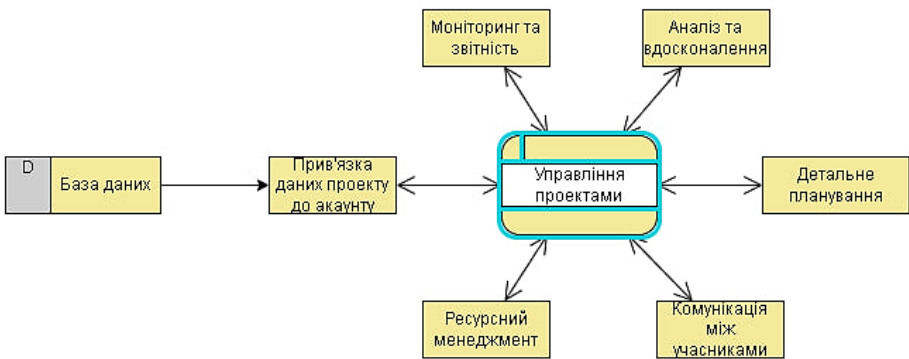


Рисунок 1 – DFD Діаграма

На діаграмі потоків даних (рисунок 1) показано основний функціонал, котрий виконуватиме застосунок та зв'язок з базою даних. Як представлено –

управління проектами включає в себе вищенаведені характеристики системи, які переходять в функціонал та взаємодіють між собою.

На наступній діаграмі (рисунок 2) можна більш детально побачити загальний алгоритм роботи з проектом від початку, а саме збору вимог, та включно до завершення виконання даного проекту. Також діаграма демонструє розгалуження в виконанні роботи, які періодично трапляються під час розробки.

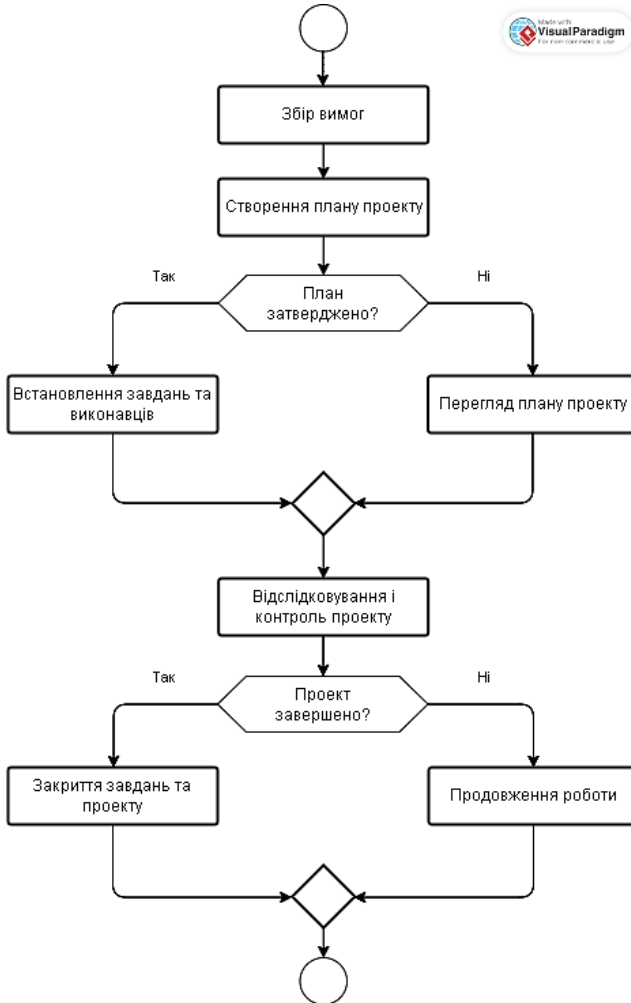


Рисунок 2 – Flowchart діаграма

Основні характеристики розроблюваного застосунку представляють собою:

1. Поліпшене планування: застосунок надає можливість створювати докладні та ефективні плани проєктів, враховуючи ресурси, терміни та завдання.

2. Ефективний ресурсний менеджмент: застосунок допомагає керувати ресурсами проєктів, включаючи людські та матеріальні ресурси, з метою забезпечення їх ефективного використання.

3. Моніторинг та звітність: застосунок надає засоби для постійного моніторингу стану проєктів та генерації звітів для аналізу продуктивності та досягнень.

4. Комунікація та співпраця: програма сприяє ефективній комунікації та співпраці між членами проєктних команд, забезпечуючи якісний обмін інформацією та робочими процесами.

5. Аналіз та вдосконалення процесів: застосунок надає інструменти для аналізу та оптимізації процесів управління проєктами, що спрямовані на підвищення продуктивності та якості управління проєктами.

Запропонований програмний застосунок має потенціал стати важливим інструментом для покращення управління проєктами, полегшуючи роботу організацій та сприяючи їхній конкурентоспроможності. Він може служити базовою платформою для інновацій та змін в управлінні проєктами, а також сприяти розвитку активної спільноти користувачів, що спільно вдосконалюють процеси управління проєктами. Загалом, ця розробка відкриває широкі перспективи для подальшого росту та вдосконалення у сфері управління проєктами.

### **Перелік посилань**

1. A Guide to the Project Management Body of Knowledge (PMBOK® Guide). Sixth Edition. USA. PMI, 2017. 66-67 p.
2. Пуліна Т. В. Можливості та перспективи управління проєктами на основі методології ISO 21500 / Т. В. Пуліна, Т. О. Фоміних, О. О. Соріна // Економічний простір. - 2017. - № 122. - С. 126-138.



УДК 004.4

Ялик В.І, Праворська Н.І.

*Хмельницький національний університет*

## **ПРОГРАМНИЙ ЗАСТОСУНОК ДЛЯ НАВЧАННЯ МАТЕМАТИЦІ УЧНІВ ПОЧАТКОВИХ КЛАСІВ З ВИКОРИСТАННЯМ ІНТЕРАКТИВНИХ ІГОР**

*В сучасному світі росте значення використання мобільних технологій у навчанні, особливо в початковій школі. Мобільні додатки стають все більш доступним та ефективним засобом покращення навчання та розвитку навичок учнів. Дослідження має на меті розробити та оцінити ефективність мобільного застосунку, призначеного для покращення математичних навичок учнів. Дана розробка пропонує інтерактивні завдання та уроки, спрямовані на стимулювання інтересу та мотивацію до вивчення математики. Дослідження відзначає роль мобільних технологій в сучасній освіті, особливо в контексті цифрової трансформації та зручного доступу до навчального матеріалу. Застосування гейміфікації в застосунку сприяє більш ефективному засвоєнню математичних концепцій, а також надає можливість для змагань та співпраці між учнями. Результати дослідження можуть бути корисними для освітніх установ, батьків та вчителів, які прагнуть покращити навчання та розвиток математичних навичок учнів у сучасному освітньому середовищі.*

*In today's world, the importance of using mobile technologies in education, especially in elementary school, is growing. Mobile applications are becoming an increasingly accessible and effective means of improving learning and developing students' skills. The research aims to develop and evaluate the effectiveness of a mobile application designed to improve students' mathematical skills. The application offers interactive tasks and lessons aimed at stimulating interest and motivation in learning mathematics. The study notes the role of mobile technologies in modern education, especially in the context of digital transformation and convenient access to educational material. Using of gamification in the application promotes more effective learning of mathematical concepts, and also provides an opportunity for competition and cooperation between students. The results of the study can be useful for educational institutions, parents and teachers who seek to improve the learning and development of students' mathematical skills in the modern educational environment.*

На сьогоднішній день використання мобільних технологій у навчанні, особливо в початковій школі, набуває все більшої ваги. Мобільні застосунки стають все більш доступними та ефективними інструментами для поліпшення навчання та розвитку навичок учнів. Дана робота спрямована на розробку та оцінку результативності мобільного додатка, який рекомендовано використовувати для вивчення математики учнями початкових класів.

Метою дослідження є розробка мобільного застосунку, призначеного для покращення рівня математичної грамотності та навичок учнів початкової школи. Додаток спрямований на надання інтерактивних математичних завдань та уроків, які зацікавлюють та мотивують учнів до активного навчання.

Використання застосунку буде спрямовано на покращення розуміння математичних концепцій та навичок розв'язування математичних завдань.

Результати дослідження можуть бути корисними для освітніх установ, батьків та вчителів, які бажають покращити навчання та розвиток математичних навичок учнів. Вони також підкреслюють важливість використання мобільних технологій, як інструмента для покращення навчання в сучасному освітньому середовищі.

Актуальність теми "Програмний застосунок для навчання математиці учнів початкових класів з використанням інтерактивних ігор" визначається кількома чинниками:

1. Цифрова трансформація в освіті: сучасна освіта стикається з різким зростанням інтересу до використання цифрових технологій у навчанні. Мобільні застосунки стають невід'ємною частиною цієї трансформації, особливо в початковій школі, де діти вже активно користуються смартфонами і планшетами.

2. Покращення математичної грамотності: математика є одним із ключових предметів у навчальному процесі. Розробка і впровадження мобільних застосунків, спрямованих на покращення математичної грамотності учнів початкової школи, має стратегічне значення для підвищення якості освіти.

3. Зручний доступ до навчального матеріалу: мобільні додатки надають можливість учням навчатися в будь-який час і в будь-якому місці. Це особливо корисно для підтримки самостійного навчання та вдома.

4. Розвиваючі ігри: використання гейміфікації в мобільних додатках дозволяє зробити навчання математики захоплюючим та цікавим для дітей. Ігровий підхід сприяє більш ефективному засвоєнню.

Отже даний програмний продукт розробляється з метою покращення математичної грамотності учнів початкової школи, використовуючи мобільні технології та гейміфікацію для того щоб зробити навчання більш цікавим та доступним.

Для цього даний застосунок буде виконувати наступні функції:

– навчання математиці: надаватиме навчальний матеріал для вивчення математики в початковій школі, включаючи основні арифметичні операції, геометричні поняття тощо;

– гейміфікація: заохочуватиме користувачів через ігровий підхід, використовуючи виклики, завдання та нагороди для стимулювання навчання;

- тести та вправи: надаватиме тести і вправи для перевірки розуміння матеріалу та закріплення навчальних навичок;
- моніторинг прогресу: дозволить користувачам відстежувати свій навчальний прогрес і досягнення;
- віддалений доступ: дозволить користувачам навчатися в будь-який час і в будь-якому місці завдяки мобільній платформі;
- змагання та співпраця: створюватиме можливості для змагань з іншими користувачами та спільного навчання.

Для більшої наочності того, які функції міститиме в собі розроблюваний мобільний додаток їх було відображено на функціональній діаграмі (Рисунок 1).

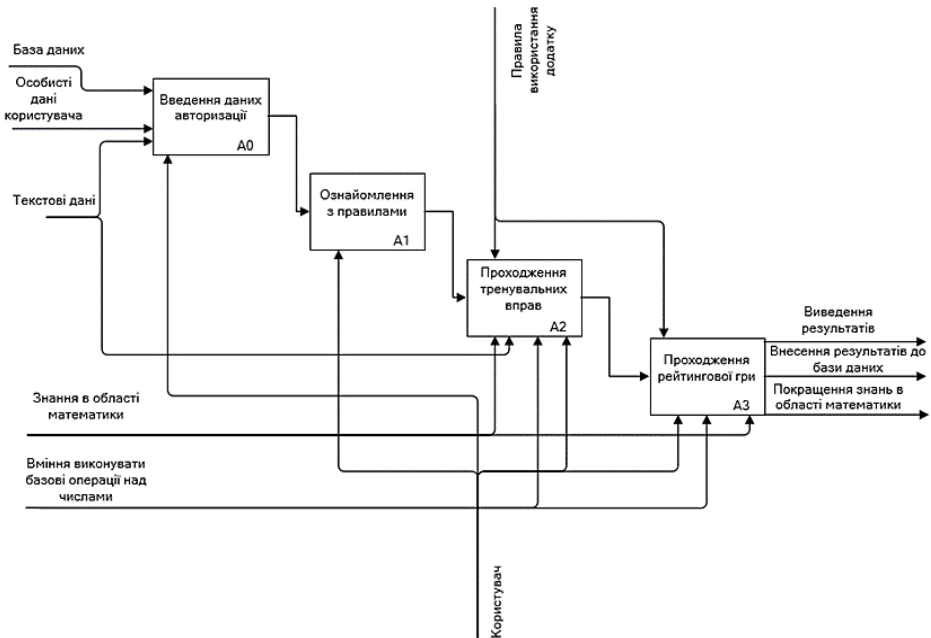


Рисунок 1 – Функціональна діаграма

На функціональній діаграмі (рисунок 1) показано основний функціонал, котрий виконуватиме застосунок, які дані для нього є вхідними, та що він повинен видавати як вихідні.

На діаграмі потоків даних (рисунок 2) відображено, як раніше показаний функціонал, взаємодіє з базою даних, а також яким чином це відбувається.

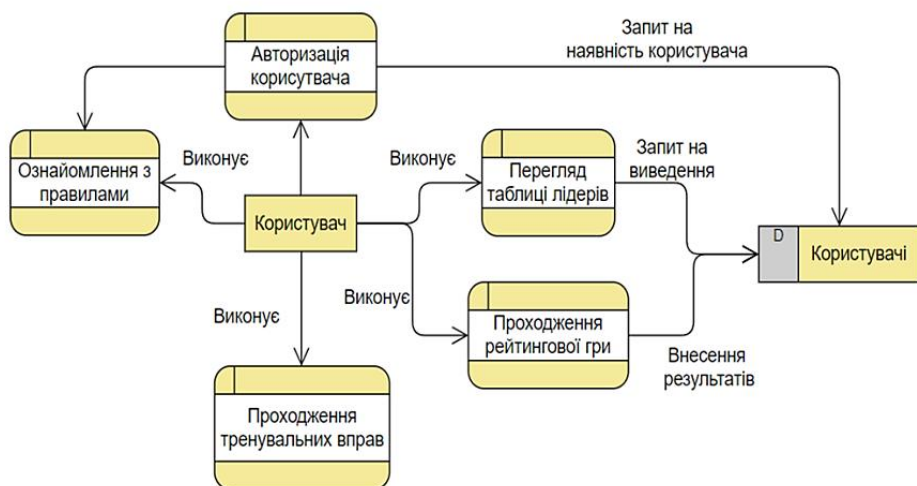


Рисунок 2 – Діаграма потоків даних

Підсумовуючи все вище вказане, запропонований мобільний застосунок для навчання математиці в початковій школі та його розробка є актуальними та важливими завданнями в сучасній освіті. Даний додаток спрямований на покращення математичної грамотності учнів, використовуючи інтерактивний підхід та гейміфікацію для стимулювання навчання. Це відповідає вимогам цифрової трансформації в освіті та сприяє покращенню рівня освіти в початковій школі.

### Перелік посилань

1. Jamie Madigan. Getting Gamers: The Psychology of Video Games and Their Impact on the People who Play Them. Madigan Jamie - Lanham.:Rowman & Littlefield Publishers, February 8, 2019. - 320p.
2. Percy Leed. Toys and Games: A Look at Then and Now (Read about the Past (Read for a Better World™)). Leed Percy – Minneapolis.: Lerner Publications™, August 1, 2023. – 24p.

УДК 004

Яресько А.Ю.

*Київський національний університет імені Тараса Шевченка*

## РОЗВИТОК ЦИФРОВИХ ПІДПИСІВ

*Проведено попередній поверховий огляд ключових історичних моментів у розвитку цифрових підписів, що сприяли поширенню та сьгоднішній популярності цифрових підписів. Розглянуто прикладний аспект розробки цифрових підписів, зокрема проаналізовано 3 алгоритми цифрових підписів: RSA, DSA та ECDSA.*

*In this paper I conduct a preliminary overview of the key historical moments in the development of digital signatures that contributed to the spread and today's popularity of digital signatures. The applied aspect of the development of digital signatures is considered. In particular three algorithms of digital signatures are analyzed: RSA, DSA, and ECDSA.*

Коли ми чуємо слово «підпис», то в перше ж чергу уявляємо підпис зроблений чорнилом на папері, але враховуючи стрімкий розвиток технологій на цьому нашій уявленні та знання про підписи не завершується. На рівні з фізичними підписами з'являються ще й підписи електронні (у тому числі і цифрові), що доволі швидко входять до повсякденного вжитку.

На сьгоднішній день електронні та цифрові підписи увійшли в наше життя на рівні фізичних підписів, у деяких моментах навіть здобули над ними перевагу.

Поняття цифрового підпису.

Цифровий підпис – це математична схема для перевірки автентичності цифрових повідомлень або документів. Дійсний цифровий підпис, якщо виконуються усі умови, дає одержувачу дуже високу впевненість, що повідомлення було створено відомим відправником (автентичність) і що повідомлення не було змінено під час передачі (цілісність) [1].

Ключові етапи розвитку цифрових підписів

1976: Опис ідеї схеми цифрового підпису Вітфілдом Діффі та Мартіном Хеллманом.

1977: Створення алгоритму RSA Рональдом Рівестом, Аді Шаміром і Леном Адлеманом.

1988: використання алгоритму RSA у Lotus Notes 1.0 для можливості здійснення цифрового підпису.

1999: запровадження можливості додавання цифрового підпису у форматі PDF.

2002: заснування SIGNiX, яке стало найпоширенішим хмарним програмним забезпеченням цифрового підпису

2008: формат файлу PDF стає відкритим стандартом для Міжнародної організації стандартизації (ISO) як ISO 32000. Включає цифрові підписи як невід'ємну частину формату[2].

## Принцип роботи цифрових підписів

Цифрові підписи засновані на криптографії з відкритим ключем, також відомої як асиметрична криптографія [4].

Схема цифрового підпису зазвичай складається з трьох алгоритмів:

- Алгоритм генерації ключів, який рівномірно випадковим чином вибирає закритий ключ із набору можливих закритих ключів. Алгоритм виводить закритий ключ і відповідний відкритий ключ.

- Алгоритм підпису, який за допомогою повідомлення та закритого ключа створює підпис.

- Алгоритм перевірки підпису, який, враховуючи повідомлення, відкритий ключ і підпис, приймає або відхиляє претензію повідомлення на автентичність.

За допомогою алгоритму відкритого ключа, наприклад Rivest-Shamir-Adleman або RSA, для реалізації цифрового підпису генеруються два ключі, створюючи математично пов'язану пару ключів: один приватний і один публічний [3].

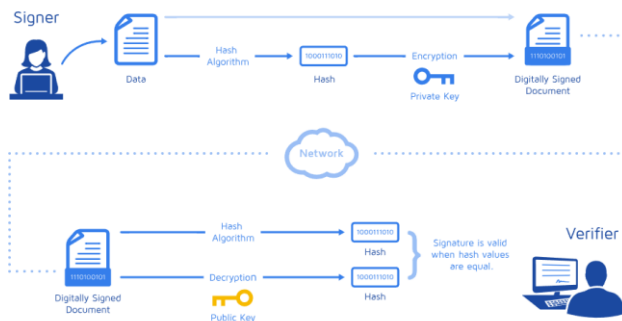


Рисунок 1 – Принцип роботи цифрового підпису [5]

## Алгоритм RSA

RSA (Rivest–Shamir–Adleman) – криптосистема з відкритим ключем, одна з найстаріших, яка широко використовується для безпечної передачі даних.

У криптосистемі з відкритим ключем ключ шифрування є відкритим і відрізняється від ключа дешифрування, який зберігається в таємниці (приватний). Користувач RSA створює та публікує відкритий ключ на основі двох великих простих чисел разом із допоміжним значенням. Прості числа тримаються в секреті. Повідомлення можуть бути зашифровані будь-ким за допомогою відкритого ключа, але можуть бути розшифровані лише тими, хто знає прості числа.

RSA є відносно повільним алгоритмом. Через це він зазвичай не використовується для безпосереднього шифрування даних користувача. Частіше RSA використовується для передачі спільних ключів для шифрування з симетричним ключем, які потім використовуються для масового шифрування-дешифрування [6].

## Алгоритм DSA

Алгоритм цифрового підпису (DSA) – це криптосистема з відкритим ключем і федеральний стандарт обробки інформації для цифрових підписів, заснований на математичній концепції модульного піднесення до степеня та задачі дискретного логарифмування. DSA є варіантом схем підпису Шнорра та Ель-Гамала.

Було випущено чотири редакції початкової специфікації. Остання специфікація: FIPS 186-4 від липня 2013 року. Специфікації FIPS 186-5 вказує, що DSA більше не буде схвалено для створення цифрових підписів, але може використовуватися для перевірки підписів, створених до дати впровадження цього стандарту.

Алгоритм DSA включає чотири операції: генерація ключа (що створює пару ключів), розподіл ключа, підписання та перевірка підпису.

## Алгоритм ECDSA

Це ще один алгоритм шифрування з відкритим ключем, призначений для створення електронного підпису та є модифікацією алгоритму DSA. Алгоритм ECDSA це асиметричний криптографічний алгоритм, що базується на еліптичних кривих.

Рівні міцності алгоритму впливають із задачі розв'язування дискретного логарифму в групі точок еліптичної кривої.

Алгоритми еліптичної кривої використовуються в TLS, PGP, SSH. Цей тип шифрування також використовується на біткойнах та інших блокчейн-платформах [7].

## Перелік посилань

1. What is Digital Signature: How it works, Benefits, Objectives, Concept [Електронний ресурс] – Режим доступу до ресурсу: <https://www.emptrust.com/blog/benefits-of-using-digital-signatures/>.
2. Infographic: The History of Digital Signature Technology [Електронний ресурс] – Режим доступу до ресурсу: <https://www.signix.com/blog/bid/108804/infographic-the-history-of-digital-signature-technology#:~:text=1977%3A%20Ronald%20Rivest%2C%20Adi%20Shamir,kind%20of%20primitive%20digital%20signature&text=1999%3A%20The%20ability%20to%20embed,makes%20digital%20signatures%20legally%20binding>
3. DEFINITION digital signature [Електронний ресурс] – Режим доступу до ресурсу: <https://www.techtarget.com/searchsecurity/definition/digital-signature>
4. Public-key cryptography [Електронний ресурс] – Режим доступу до ресурсу: [https://en.wikipedia.org/wiki/Public-key\\_cryptography](https://en.wikipedia.org/wiki/Public-key_cryptography)
5. Understanding digital signatures. What is a digital signature, and how can you create one? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq>
6. RSA Algorithm in Cryptography [Електронний ресурс] – Режим доступу до ресурсу: <https://www.geeksforgeeks.org/rsa-algorithm-cryptography/>
7. A Guide to Digital Signature Algorithms [Електронний ресурс] – Режим доступу до ресурсу: <https://dzone.com/articles/digital-signature-1>

УДК 004.9

Яшина В.А.

*Хмельницький національний університет*

## **ДИЗАЙН МОБІЛЬНИХ ЗАСТОСУНКІВ**

*Розглянуто задачу створення дизайну мобільних застосунків, що є обов'язковим етапом створення нового продукту. Але розробка UI/UX також може знадобитися при оновленні вже існуючої програми, або при її переміщенні на нові платформи. Типова розробка дизайну програми включає кілька ключових етапів: етап збору вступних та вимог до дизайну, відпрацювання архітектури та навігації у застосунку, розробка прототипів, створення деталізованих клікабельних прототипів, тестування дизайну прототипу, фінальний дизайн та розробка, підготовка до публікації, аналіз, правки та доопрацювання дизайну.*

*The task of creating a design of mobile applications, which is a mandatory stage of creating a new product, is considered. But UI/UX development may also be needed when updating an existing application or moving it to new platforms. A typical app design development includes several key stages: gathering input and design requirements, working out the app's architecture and navigation, prototyping, creating detailed clickable prototypes, testing the prototype design, final design and development, preparation for publication, analysis, editing and refinement design.*

Дизайн мобільних застосунків - це візуальне оформлення програми, а також створення структури, заснованої на логіці поведінки користувача. Іншими словами, це не лише зовнішній вигляд, а й зручність використання [1, 6].

Дизайн програми поділяється на UX та UI. UI-дизайнер створює візуальну частину програми, а UX-дизайнер – технічну. Під час розробки дизайну мобільних застосунків доцільно впроваджувати сучасні технології, слідкувати за трендами, а також приділяти увагу як зовнішньому вигляду, так і функціональним можливостям програми, щоб створити інтуїтивно зрозумілий інтерфейс. Так, будь-який користувач може легко розібратися в програмі.

Очевидно, що розробка дизайну є обов'язковим етапом створення нового продукту. Але розробка UI/UX також може знадобитися при оновленні вже існуючої програми, або при її переміщенні на нові платформи. Наприклад, якщо є програма під ОС Android, то випуск її версії для iOS вимагатиме нового дизайну, що відповідає гайдлайнам Apple. А якщо продукт існує досить довго, то йому рано чи пізно буде потрібен редизайн.

Типова розробка дизайну програми включає кілька ключових етапів [3].



1.Етап збору вступних та вимог до дизайну. Етапу створення дизайну передує етап дослідження – вивчення ринку, існуючих на ньому продуктів та потреб реальних чи потенційних споживачів. Лише тоді можна сформулювати концепцію продукту – описати його ринкову нішу, функціонал, монетизацію та сценарії використання. Без цього розробити дизайн програми неможливо.

2.Відпрацювання архітектури та навігації у застосунку. Архітектуру можна розглядати як сукупність блоків та екранів програми, їх ієрархію та взаємну узгодженість. Від архітектури безпосередньо залежить навігація в додатку, а отже, і зручність для кінцевого користувача. UX-фахівці формують навігацію та архітектуру виходячи зі сценаріїв використання програми. На цьому етапі дизайнери складають схеми та майнд-мапи програми, які є основою для перших макетів дизайну [3].

3.Розробка прототипів. Коли архітектура мобільного додатка узгоджена, розпочинається процес створення мокапів (макетів). По суті, це верхньорівневі приклади дизайну додатків, прототипи з мінімальною деталізацією, які допомагають визначити пріоритет і розташування елементів інтерфейсу на екрані. Макети обговорюються всередині команди та з клієнтом, їх легко змінювати та доповнювати, тому на етапі прототипування можна швидко позначити найкращі рішення.

4.Наступний крок – створення деталізованих клікабельних прототипів – часто вони мають анімацію, клікабельні кнопки та інший інтерактив, необхідний для UX-тестування. Вони дозволяють тестувати та оптимізувати дизайн до того, як розпочнеться розробка.

На цьому етапі можна залучати і команду розробників - вони можуть оцінити дизайн мобільних програм з технічної точки зору, позначивши складність, вартість та терміни розробки.

5.Тестування дизайну прототипу. Інтерактивні прототипи дозволяють взаємодіяти з ними як з готовим додатком, а значить його можна показувати людям - реальним користувачам, фокус-групам. Це можливість протестувати дизайн програми на практиці, простежити шлях користувача, зібрати детальний зворотний зв'язок та зрозуміти, наскільки продукт підходить для цільової аудиторії. На цьому етапі розробки можна знайти неочевидні особливості поведінки користувачів та зробити продукт кращим.

6.Фінальний дизайн та розробка. Далі протестований і узгоджений прототип передається на "вдосконалення" дизайнерам, щоб зробити продукт привабливішим, виправити стилістику, з урахуванням фінального UI продукту. Після доопрацювань та фінального узгодження дизайн передають розробникам, які розробляють технічну частину.

7. Підготовка до публікації. Для публікації продукту знадобиться додатковий візуальний контент - іконки, скріншоти екранів, або навіть відео зі сценаріями використання. Від успішності цього контенту залежить перший відгук користувачів, а отже, і статистика завантажень.

8. Аналіз, внесення виправлень та доопрацювання дизайну. Коли проект перебуває на фінальній стадії, настає час аналітики – як правило, це передрелізний етап та перші показники після релізу. На цьому етапі команді надходять дані для оцінки успіхів і оптимізації програми, вивчаються сценарії користувача і проблеми. Це дозволяє довести дизайн програми до ідеалу, позначити подальший вектор розвитку.

### **Перелік посилань**

1. GoldwebSolutions. URL: <https://goldwebsolutions.com/uk/blog/shho-take-vajrfrejmwireframe-ta-dlya-chogo-vin-potriben-u-protsezi-rozrobki-sajtu-chi-dodatku> .
2. Посібник з Wireframing для початківця. URL: <https://webdesign.tutsplus.com/uk/articles/a-beginners-guide-to-wireframing--webdesign7399> .
3. Проектування і дизайн інтерфейсів. URL: <https://otakoyi.ua/dyzayn-interfejsiv-ui-ux>.
4. Загальносистемні принципи та етапи створення програм. Життєвий цикл програмного виробу. [Електронний ресурс] – URL: <http://lib.mdpu.org.ua/e-book/vstup/L7.htm>.
5. Simon Butler, Michel Wermelinger, Yijun Yu, and Helen Sharp. 2009. Relating Identifier Naming Flaws and Code Quality: An Empirical Study. In Proceedings of the Working Conference on Reverse Engineering (WCRE). 31–35.
6. ISO/IEC 9126-1:2001. Software engineering – Software product quality – Part 1: Quality model.

UDC 004.5, 004.415.53

Alpashkin M.I., Dmytriiev V.G., Romaniuk O.V.

*Vinnitsia National Technical University*

## **USABILITY TESTING AS AN IMPORTANT FACTOR IN THE DEVELOPMENT OF A SUCCESSFUL SOFTWARE PRODUCT**

*The article considers the importance of usability testing as a development aspect in the development of a digital product.*

According to UXCAM research, 88% of users are less likely to return after a bad user experience of software product [1]. If it is difficult for users to navigate the website, its structure is illogical, and it takes a lot of time to perform daily tasks using the website, then users start looking for an alternative to it.

To create a good product that will generate income, IT companies pay considerable attention to developing an effective user experience, because they understand that \$1 invested in user-friendly design yields \$100 in profit [2]. One of the important guidelines for its creation is usability testing.

Therefore, the purpose of the study is to analyze how usability testing helps to create a successful software product.

Usability testing is a testing method of website functionality, or any other digital product by observing how real users complete task and interact with it. Usually, in a test, participants will attempt common tasks while observers watch, listen, and make notes. The purpose of usability testing is to reveal areas where user get confused during the customer journey. Data derived from this research help to make the overall user experience better. Doing usability testing in the right way, at the right stage, with the right participants, helps minimize the chances of developing the wrong product. This, in turn, saves valuable time, money, and resources. In other words, when usability testing is done early, at the paper prototype stage, it reveals problems that are easier and more cost-effective to solve. Conversely, when it is applied to a completed product, it provides insight into user success rates and task completion times.

Usability testing usually involves two different groups: end users and observers. Ideally, these two groups should not know each other, so that observers can collect more objective and unbiased data. When you set up a usability test, you create a scenario in which users have to complete a set of tasks that reflect what a new visitor to your website would do. These tasks can include actions such as registering, inviting a friend, or making a purchase. User researchers then recruit participants to form a focus group, which ideally consists of users who are representative of the product's target market. Participants attempt to complete these tasks in a controlled environment. While users work on these tasks,

observers closely monitor and evaluate their overall success in completing these tasks. They focus on identifying any usability issues that may arise. Observers may take notes during the observation or record the session on audio or video for later reference. Observers pay particular attention to areas where users are succeeding and areas where they are struggling. This information is invaluable to designers as it allows them to revise and improve their designs at a later stage.

Usability testing usually focuses on two types of products: websites and mobile applications. These products require different approaches and testing techniques, but the goal remains the same: to provide a user-friendly and intuitive interface for users.

Website testing involves checking all interface elements such as navigation, text, images, and forms. The main goal is to ensure that users can easily find information and complete tasks on your website. So, for example, the company Housing.com increased the popularity of using its functions by 20% after improving the search form [1].

Mobile applications have their own usability challenges, such as limited screen size, different interaction styles, and hardware limitations. According to the research,[3] users are 5 times more likely to abandon further use of a website if it is not optimized for mobile devices.

Mobile app testing involves checking how it works on different devices, screen resolutions, and operating systems, as well as taking into account the specifics of each platform.

Usability testing of online stores allows you to determine the reasons for the low level of sales, at what stage users have difficulties interacting with the online store, and also to offer solutions for solving the identified problems.

Usability testing is a key element of software development, as it helps to identify problems and improve the product based on user needs. Using a variety of methods, from interface testing to global assessments, allows you to provide a more detailed and comprehensive understanding of your product's usability. Conducting usability testing helps development teams identify and resolve issues, improving the usability and satisfaction of the product. As a result, this can lead to increased sales, customer loyalty, and market success for your product.

### **Link list**

1. Statistics To Impress Stakeholders 2023. URL:<https://uxcam.com/blog/ux-statistics/>
2. The Six Steps For Justifying Better UX. URL: <https://www.forrester.com/report/The-Six-Steps-For-Justifying-Better-UX/RES117708>
3. Know Your User – UX Statistics and Insights (with Infographic) URL: <https://www.toptal.com/designers/ux/ux-statistics-insights-infographic>



# АКТУАЛЬНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК 2023

ЗБІРНИК НАУКОВИХ ПРАЦЬ

*Комп'ютерна верстка:* **Олександр МАЗУРЕЦЬ,  
Марина МОЛЧАНОВА**

Підписано до друку 16.11.2023.  
Версія друку «APKN2023\_CorpusPaper v7mod1 Finita».

E-mail: [apkt.khnu@gmail.com](mailto:apkt.khnu@gmail.com)  
ХНУ. м. Хмельницький, вул. Інститутська, 11.