



III Міжнародна науково-практична конференція

«Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії»

4–6 грудня 2025 року

Київ – 2025

III Міжнародна науково-практична конференція «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії». Збірник тез. – К.: ДУІКТ, 2025.

Даний збірник містить тези учасників конференції, представлених на III Міжнародній науково-практичній конференції «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії», яка проводилась 04-06 грудня 2025 р. на кафедрі Технологій цифрового розвитку Навчально-наукового інституту інформаційних технологій Державного університету інформаційно-комунікаційних технологій, м. Київ.

Робоча мова конференції – українська та англійська.

У збірнику представлені тези доповідей Міжнародної науково-практичної конференції «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії». Розглянуті сучасні перспективи та різноманітні підходи до вирішення сучасних проблем програмної та комп'ютерної інженерії.

Вчений секретар конференції

Бажан Тетяна – Державний університет інформаційно-комунікаційних технологій

моб.тел.+38(097)803-34-49

e-mail: kafedratcr@gmail.com

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Державний університет інформаційно-комунікаційних технологій

Навчально-науковий інститут інформаційних технологій

Кафедра Технологій цифрового розвитку

ПРОГРАМНИЙ КОМІТЕТ

Володимир ШУЛЬГА - ректор Державного університету інформаційно-комунікаційних технологій, доктор історичних наук, старший дослідник

Олександр КОРЧЕНКО - перший проректор Державного університету інформаційно-комунікаційних технологій член-кореспондент НАН України, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, Заслужений діяч науки і техніки України

Марина ПЕТЧЕНКО - проректор з науково-педагогічної роботи та соціального розвитку Державного університету інформаційно-комунікаційних технологій, кандидат економічних наук, доцент

Катерина НЕСТЕРЕНКО - доктор технічних наук, професор, в.о. директора навчально-наукового інституту інформаційних технологій Державного університету інформаційно-комунікаційних технологій

Вікторія ЖЕБКА - доктор технічних наук, професор, завідувач кафедри Технологій цифрового розвитку Державного університету інформаційно-комунікаційних технологій

Олександр ТРОФИМЧУК - член-кореспондент НАНУ, доктор технічних наук, професор, директор Інституту телекомунікацій і глобального інформаційного простору НАНУ

Василь ТРИСНЮК - завідувач відділу досліджень навколишнього середовища, доктор технічних наук, професор, Інститут телекомунікацій та глобального інформаційного простору НАН України

Павло СКЛАДАННИЙ - кандидат технічних наук, доцент, завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка

Віктор ШЕВЧЕНКО - доктор технічних наук, професор, заступник директора з наукової роботи Інституту програмних систем НАН України

Ольга ЗІНЧЕНКО - доктор технічних наук, доцент, завідувач кафедри Штучного інтелекту Державного університету інформаційно-комунікаційних технологій

Віктор ВИШНІВСЬКИЙ - доктор технічних наук, професор, завідувач кафедри Комп'ютерних наук Державного університету інформаційно-комунікаційних технологій

Наталія ЛАЩЕВСЬКА - кандидат технічних наук, доцент, завідувач кафедри Комп'ютерної інженерії Державного університету інформаційно-комунікаційних технологій

Каміла СТОРЧАК - доктор технічних наук, професор, завідувач кафедри Інформаційних систем та технологій Державного університету інформаційно-комунікаційних технологій

Андрій БОНДАРЧУК - доктор технічних наук, професор, професор кафедри Штучного інтелекту Державного університету інформаційно-комунікаційних технологій

Василь УСТИМЕНКО - Доктор наук, професор, Royal Holloway, Лондонський університет

Джо СТЕРТЕН - професор Норвезького інституту науки та технологій, м. Тронхейм, Норвегія.

Ігор ГАЙСИНСЬКИЙ - доктор фізико-математичних наук, старший науковий співробітник, Ізраїльський технологічний університет, Хайфа, Ізраїль.

Вікторія ОНИЩЕНКО - доктор технічних наук, професор, Вармінсько-Мазурський університет, Польща.

Зміст

Напрямок №1. Досвід сучасних IT-компаній

Кирилов Іван Ігорович МУЛЬТИАГЕНТНЕ НАВЧАННЯ З ПІДКРІПЛЕННЯМ ДЛЯ ОПТИМІЗАЦІЇ КВАНТОВИХ СХЕМ.....	14

Напрямок №2. Розробка E-сервісів та E-систем

Башинський Роман Ігорович, Поперешняк Світлана Володимирівна РОЛЬ ВЕБКАЛІБРАТОРІВ КОЛЬОРУ У ПІДВИЩЕННІ ЯКОСТІ ЦИФРОВОГО КОНТЕНТУ.....	16
Бичок Олександра Сергіївна, Євпак Вікторія Олегівна, Поперешняк Світлана Володимирівна ОСОБЛИВОСТІ РОЗРОБКИ АНОНІМНОГО Е-ГОЛОСУВАННЯ.....	19
Варченко Артем Юрійович, Поперешняк Світлана Володимирівна ПРОЕКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ КООРДИНАЦІЇ ВОЛОНТЕРСЬКОЇ ДІЯЛЬНОСТІ «ДОБРОДІЙ».....	22
Демчишин Данило Васильович, Поперешняк Світлана Володимирівна АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ІНТЕРОПЕРАБЕЛЬНОСТІ В СУЧАСНИХ ЕКОСИСТЕМАХ ЦИФРОВОГО ЗДОРОВ'Я.....	24
Дерев'янюк Дмитро Віталійович, Поперешняк Світлана Володимирівна РОЗРОБКА КРОСПЛАТФОРМНОГО ЗАСТОСУНКУ «ЗАКЛАДКА МРІЙ» З ГІБРИДНОЮ СИСТЕМОЮ ПЕРСОНАЛІЗОВАНИХ РЕКОМЕНДАЦІЙ ЛІТЕРАТУРИ.....	27
Дутчак Марія Степанівна ОСОБЛИВОСТІ ВЕБ-ДИЗАЙНУ ІНТЕЛЕКТУАЛЬНИХ НАВЧАЛЬНИХ СИСТЕМ.....	29
Зайцева Катерина Андріївна, Поперешняк Світлана Володимирівна МЕХАНІЗМ ОДНОЗНАЧНОГО ЗАПОБІГАННЯ ПОВТОРНОМУ ГОЛОСУВАННЮ В СИСТЕМІ АНОНІМНОГО Е-ГОЛОСУВАННЯ.....	31
Заможний Нікіта Анатолійович, Жутник Анастасія Володимирівна, Поперешняк Світлана Володимирівна ПРОБЛЕМА ФРАГМЕНТАЦІЇ ІНФОРМАЦІЙНИХ РЕСУРСІВ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ ТА ШЛЯХИ ЇЇ ПОДОЛАННЯ.....	33
Кавковська Єлизавета Олександрівна, Поперешняк Світлана Володимирівна ПРОБЛЕМАТИКА НЕРІВНОМІРНОСТІ ВІДТІНКІВ НА ДИСПЛЕЯХ ТА ЇЇ ВПЛИВ НА ЯКІСТЬ ЦИФРОВОГО КОНТЕНТУ.....	35
Кірієнко Володимир Сергійович, Поперешняк Світлана Володимирівна КЛАСИФІКАЦІЙНО-ОРІЄНТОВАНА МОДЕЛЬ ПІДВИЩЕННЯ БЕЗПЕКИ ЦИФРОВИХ СЕРВІСІВ У БЕЗДРОТОВИХ МЕРЕЖАХ.....	38
Кобзар Михайло Євгенович, Поперешняк Світлана Володимирівна СТВОРЕННЯ КРОСПЛАТФОРМНОГО ЗАСТОСУНКУ «ЗАКЛАДКА МРІЙ» ДЛЯ ПІДВИЩЕННЯ МОТИВАЦІЇ ДО ЧИТАННЯ ТА ОРГАНІЗАЦІЇ ОСОБИСТОЇ БІБЛОТЕКИ.....	41
Коврін Іван Євгенійович, Поперешняк Світлана Володимирівна ОСОБЛИВОСТІ ПРОЄКТУВАННЯ КОРИСТУВАЦЬКИХ ІНТЕРФЕЙСІВ ТА ЗАБЕЗПЕЧЕННЯ ДОСТУПНОСТІ У МОБІЛЬНИХ МЕДИЧНИХ ЗАСТОСУНКАХ.....	43
Кроха Максим Володимирович, Скакун Михайло Миколайович, Поперешняк Світлана Володимирівна АРХІТЕКТУРА СИСТЕМИ ДИСТАНЦІЙНОГО МОНІТОРИНГУ ПАЦІЄНТІВ НА ОСНОВІ ІНТЕРНЕТУ РЕЧЕЙ.....	46
Крупа Нікіта Олександрович ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ПОВЕДІНКИ КОРИСТУВАЧІВ Е-COMMERCE ДЛЯ ОПТИМІЗАЦІЇ ОПЕРАТИВНИХ СИСТЕМ.....	49
Кузьменко Дарія Олегівна, Лупан Ірина Володимирівна ОГЛЯД ВЕБ-ПЛАТФОРМ ДЛЯ ПРОВЕДЕННЯ НАУКОВИХ КОНФЕРЕНЦІЙ.....	52

Литвиненко Дарія Володимирівна, Бойко Андрій Станіславович, Поперешняк Світлана Володимирівна РОЗРОБКА ІНТЕЛЕКТУАЛЬНИХ Е-СИСТЕМ ІЗ ВИКОРИСТАННЯМ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ ТА ХМАРНИХ ТЕХНОЛОГІЙ.....	56
Мальцев Данило Євгенович, Поперешняк Світлана Володимирівна МЕТОДИ ВИЯВЛЕННЯ ЗГЕНЕРОВАНОГО ВІДЕОКОНТЕНТУ (DEEPFAKE) ЗА ДОПОМОГОЮ ГЛИБОКОГО НАВЧАННЯ.....	59
Мачуліс Гліб Дмитрович, Поперешняк Світлана Володимирівна АРХІТЕКТУРНІ ОСОБЛИВОСТІ ТА РЕАЛІЗАЦІЯ КЛІЄНТСЬКОГО ІНТЕРФЕЙСУ СИСТЕМИ АУДИТУ ЯКОСТІ КОДУ «CODEBAROMETER»	61
Гаврилов Ілля Олегович, Поперешняк Світлана Володимирівна РОЗРОБКА МОДУЛІВ ВЗАЄМОДІЇ КОРИСТУВАЧІВ У СИСТЕМІ E-STUDYNES: ЧАТ, ТЕСТУВАННЯ ТА QR-ВІДВІДУВАНІСТЬ.....	64
Голубов Кирило Олександрович, Білоусов Олександр Олександрович, Поперешняк Світлана Володимирівна РОЗРОБКА ЦИФРОВОЇ ПЛАТФОРМИ «Є-ЗАПИС» ДЛЯ ОПТИМІЗАЦІЇ БРОНЮВАННЯ ПОСЛУГ.....	67
Камоцький Богдан Борисович, Закарадзе Максим Зурабович, Поперешняк Світлана Володимирівна РОЗРОБКА ІНТЕРАКТИВНОГО ВІДЖЕТА ПОГОДИ З ФУНКЦІЄЮ ПЕРСОНАЛІЗОВАНИХ РЕКОМЕНДАЦІЙ.....	69
Кирсенко Ярослав Іванович, Поперешняк Світлана Володимирівна АНАЛІЗ АРХІТЕКТУРИ ТА МОДЕЛІ МІКРОСЕРВІСІВ У СИСТЕМІ E-STUDYNES.....	71
Масоха Владислав Юрійович, Поперешняк Світлана Володимирівна РОЗРОБКА ПРОТОТИПУ СИСТЕМИ ВАЛІДАЦІЇ КВАЛІФІКОВАНОГО ЕЛЕКТРОННОГО ПІДПISУ (КЕП).....	73
Мілевський Роман Олександрович, Теремко Роман Дмитрович, Поперешняк Світлана Володимирівна МЕТОДИ ПЕРСОНАЛІЗАЦІЇ МАРШРУТІВ ТА МОТИВАЦІЇ КОРИСТУВАЧА У МОБІЛЬНОМУ ДОДАТКУ ДЛЯ ДОСЛІДЖЕННЯ МІСЬКОГО СЕРЕДОВИЩА.....	75
Смаровоз Анна Андріївна, Собко Данило Олександрович, Поперешняк Світлана Володимирівна ОПТИМІЗАЦІЯ СТУДЕНТСЬКИХ АДМІНІСТРАТИВНИХ ПРОЦЕДУР...78	78
Юшко Крістіна Богданівна, Кіркв Олександр Віталійович, Поперешняк Світлана Володимирівна ОПИС ТА ФУНКЦІОНАЛ ЕЛЕКТРОННОГО ОСВІТНЬОГО КАБІНЕТУ...80	80
Якименко Дар'я Олександрівна, Поперешняк Світлана Володимирівна ОСОБЛИВОСТІ ТА ПЕРСПЕКТИВИ РОЗВИТКУ КВАЛІФІКОВАНОГО ЕЛЕКТРОННОГО ПІДПISУ В ЦИФРОВІЙ ЕКОСИСТЕМІ УКРАЇНИ.....	84
Ярмоленко Максим Сергійович, Луценко Станіслав Сергійович, Поперешняк Світлана Володимирівна ЕЛЕКТРОННИЙ ЗАПИС НА Б'ЮТІ-ПРОЦЕДУРИ.....	86
Мороз Андрій Віталійович, Поперешняк Світлана Володимирівна РОЗРОБКА Е-СЕРВІСІВ ТА Е-СИСТЕМ ДЛЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ПУБЛІЧНИХ ПОСЛУГ.....	89
Мосійчук Вероніка Михайлівна, Поперешняк Світлана Володимирівна ЗАГРОЗИ КОНФІДЕНЦІЙНОСТІ ТА УРАЗЛИВОСТІ Е-СЕРВІСІВ У СУЧАСНОМУ ЦИФРОВОМУ СЕРЕДОВИЩІ.....	92
Новостройний Дмитро Андрійович, Поперешняк Світлана Володимирівна ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В Е-СЕРВІСІ «ДОБРОДІЙ» ДЛЯ КООРДИНАЦІЇ ВОЛОНТЕРСЬКИХ ПОДІЙ.....	95

Озеров Данііл Олександрович, Поперешняк Світлана Володимирівна ОСОБЛИВОСТІ АРХІТЕКТУРИ ВИСОКОНАВАНТАЖЕНОЇ ТЕЛЕМЕДИЧНОЇ ПЛАТФОРМИ ДЛЯ МОНІТОРИНГУ ХРОНІЧНИХ ЗАХВОРЮВАНЬ.....	98
Осіпчук Дмитрій Миколайович, Поперешняк Світлана Володимирівна ПРОЄКТУВАННЯ Е-СЕРВІСУ ЗАХИЩЕНОГО ОБМІНУ ПОВІДОМЛЕННЯМИ ДЛЯ ОСВІТНЬОГО СЕРЕДОВИЩА НА БАЗІ ДЕЦЕНТРАЛІЗОВАНОГО ПРОТОКОЛУ TOX.....	101
Папіровий Дмитро Валентинович СИСТЕМА ІНТЕЛЕКТУАЛЬНОЇ ПЕРЕВІРКИ ЗАГРОЗ У БЕЗДРОТОВИХ МЕРЕЖАХ ДЛЯ Е-ПОСЛУГ ТА SMART-СИСТЕМ.....	104
Парашинець Андрій Михайлович, Поперешняк Світлана Володимирівна ГЕОСЕРВІС ДЛЯ АГРЕГАЦІЇ АСОРТИМЕНТУ ТА АКЦІЙ МАГАЗИНІВ В ПЕВНОМУ РАДІУСІ.....	107
Пітецький Кирило Миколайович, Тільний Олександр Віталійович, Поперешняк Світлана Володимирівна ЦИФРОВИЙ СЕРВІС УПРАВЛІННЯ ДАНИМИ ДОМАШНІХ ТВАРИН НА ОСНОВІ ІНТЕРАКТИВНОЇ ВЕБ-ПЛАТФОРМИ.....	109
Гордієнко Катерина Олександрівна ДОЦІЛЬНІСТЬ РОЗРОБКИ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ АНАЛІЗУ ТА ПРОСТОРОВОЇ КЛАСИФІКАЦІЇ ДОРОЖНЬОГО ПОКРИТТЯ НА ОСНОВІ КОМП'ЮТЕРНОГО ЗОРУ.....	111
Варченко Артем Юрійович, Поперешняк Світлана Володимирівна ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ВИСОКОПРОДУКТИВНОГО ІНТЕРФЕЙСУ СИСТЕМИ «ДОБРОДІЙ» НА БАЗІ БІБЛІОТЕКИ REACT.....	114
Дем'янець Юрій Вікторович ІНФОРМАЦІЙНО-ЕНТРОПІЙНА МОДЕЛЬ ОЦІНКИ ЯКОСТІ ТА БЕЗПЕКИ У СИСТЕМАХ УПРАВЛІННЯ ЗАВДАННЯМИ.....	117
Кузьменко Дарія Олегівна, Лупан Ірина Володимирівна РОЗРОБКА ПРОТОТИПУ ВЕБСИСТЕМИ ДЛЯ ПОДАННЯ І РЕЦЕНЗУВАННЯ НАУКОВИХ ТЕЗ.....	120
Никоненко Софія Сергіївна, Поперешняк Світлана Володимирівна БЛОКЧЕЙН-ТЕХНОЛОГІЇ: ПРИНЦИПИ ТА ЗАСТОСУВАННЯ.....	123
Новостройний Дмитро Андрійович, Поперешняк Світлана Володимирівна Е-СЕРВІС «ДОБРОДІЙ» ЯК ЦИФРОВИЙ ІНСТРУМЕНТ РОЗВИТКУ ВОЛОНТЕРСЬКОЇ СПІЛЬНОТИ.....	126
Полянський Назар Денисович, Поперешняк Світлана Володимирівна АРХІТЕКТУРА ВИСОКОНАВАНТАЖЕНИХ ВЕБПЛАТФОРМ ПРАЦЕВЛАШТУВАННЯ.....	129
Прохоров Ярослав Федорович, Поперешняк Світлана Володимирівна ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ Е-СЕРВІСІВ У ХМАРНИХ СЕРЕДОВИЩАХ.....	132
Ружинський Денис Олександрович, Поперешняк Світлана Володимирівна МЕТОДИ ПІДВИЩЕННЯ НАДІЙНОСТІ Е-СИСТЕМ ЗА УМОВ НЕРІВНОМІРНОГО НАВАНТАЖЕННЯ.....	135
Романюк Ярослав Олександрович, Поперешняк Світлана Володимирівна ІНТЕРАКТИВНИЙ СИМУЛЯТОР ОСББ ЯК ЗАСІБ ЦИФРОВОЇ АДАПТАЦІЇ ТА ПІДВИЩЕННЯ ЗАЛУЧЕНОСТІ МЕШКАНЦІВ.....	139
Саранюк Даниїл Андрійович, Поперешняк Світлана Володимирівна ГЕОСЕРВІС ДЛЯ АГРЕГАЦІЇ АСОРТИМЕНТУ ТА АКЦІЙ МАГАЗИНІВ В ПЕВНОМУ РАДІУСІ.....	143
Сивицький Юрій Ігорович МЕТОДИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ОРГАНІЗАЦІЙНИХ СИСТЕМ ЯК ВІДПОВІДЬ НА ЗРОСТАННЯ КОНКУРЕНТНОГО ТИСКУ.....	145
Сидоркін Іван Віталійович, Поперешняк Світлана Володимирівна ІННОВАЦІЙНА МОДЕЛЬ ЦИФРОВОГО НАВЧАННЯ МЕШКАНЦІВ ЧЕРЕЗ СИМУЛЯЦІЮ ПРОЦЕСІВ УПРАВЛІННЯ ОСББ.....	149

Сідельніков Євген Олександрович, Натяганчук Олександр Олександрович, Поперешняк Світлана Володимирівна ПРОЄКТУВАННЯ ТА РЕАЛІЗАЦІЯ ІНТЕРАКТИВНОГО КОРИСТУВАЦЬКОГО ІНТЕРФЕЙСУ МОБІЛЬНОГО ЗАСТОСУНКУ З ВИКОРИСТАННЯМ ГЕОЛОКАЦІЇ ТА ФУНКЦІЙ ПОШУКУ/ФІЛЬТРАЦІЇ.....	153
Созанський Юрій Вячеславович ІНТЕЛЕКТУАЛЬНА ІНФОРМАЦІЙНА СИСТЕМА УПРАВЛІННЯ КАДРОВИМИ РЕСУРСАМИ.....	156
Баля Віталій Сергійович, Соломенко Іван Миколайович, Поперешняк Світлана Володимирівна БЕЗПЕКА РОЗРОБКИ Е-СЕРВІСІВ У УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ.....	158
Сполітак Максим Юрійович, Поперешняк Світлана Володимирівна ВПРОВАДЖЕННЯ АІ-МОДУЛЯ В ОСВІТНЮ СИСТЕМУ E-StudyNest ТА АНАЛІЗ ЙОГО ВЗАЄМОДІЇ З МІКРОСЕРВІСАМИ.....	160
Старостенко Анатолій Володимирович, Корсаков Дмитро Ростиславович, Поперешняк Світлана Володимирівна UX/UI ДИЗАЙН МОБІЛЬНИХ Є-СЕРВІСІВ ДЛЯ МЕШКАНЦІВ: ПІДВИЩЕННЯ ЗАЛУЧЕНОСТІ ТА СПРОЩЕННЯ ВЗАЄМОДІЇ З ОСББ/УК.....	163
Сидоренко Карина Олександрівна ЕЛЕКТРОННИЙ ЛАБОРАТОРНИЙ ПРАКТИКУМ З ТЕСТУВАННЯ WEB-ДОДАТКІВ.....	167
Ткач Анна Павлівна, Поперешняк Світлана Володимирівна СТВОРЕННЯ ІНТЕРФЕЙСУ ПЕРЕГЛЯДУ РЕЗУЛЬТАТІВ АУДИТУ КОДУ ТА ІСТОРІЇ АНАЛІЗІВ У СИСТЕМІ «CODEBAROMETER».....	170
Тригуб Вадим Олександрович, Литвинчук Владислав Григорович, Поперешняк Світлана Володимирівна КІБЕРБЕЗПЕКА В СИСТЕМАХ ДИСТАНЦІЙНОГО МОНІТОРИНГУ ПАЦІЄНТІВ НА БАЗІ ІОТ.....	173
Якименко Дар'я Олександрівна, Поперешняк Світлана Володимирівна ОСОБЛИВОСТІ ТА ПЕРСПЕКТИВИ РОЗВИТКУ КВАЛІФІКОВАНОГО ЕЛЕКТРОННОГО ПІДПISУ В ЦИФРОВІЙ ЕКОСИСТЕМІ УКРАЇНИ.....	176
Якубовський Нікіта Денисович, Поперешняк Світлана Володимирівна ВПРОВАДЖЕННЯ АЛГОРИТМІВ ПЕРВИННОГО АНАЛІЗУ СИМПТОМІВ ТА СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ ЛІКАРСЬКИХ РІШЕНЬ.....	178
Бажан Юрій Павлович, Золотухіна Оксана Анатоліївна ОБМЕЖЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ В ІДЕНТИФІКАЦІЇ ПОВЕДІНКОВИХ ПАТЕРНІВ НА ОСНОВІ КОРИСТУВАЦЬКИХ ЛОГІВ.....	181

Напрям №3. Розробка програмного забезпечення

Аронов Андрій Олексійович РОЗРОБКА СИСТЕМИ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ З ВИКОРИСТАННЯМ PHP, JWT ТА JAVASCRIPT.....	183
Бех Андрій Олександрович АРХІТЕКТУРНІ ПІДХОДИ ДО РЕАЛІЗАЦІЇ РОЗПОДІЛЕНИХ ТРАНЗАКЦІЙ У МІКРОСЕРВІСНІЙ ТРАНСПОРТНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ.....	185
Бобко Олексій Леонідович ОЦІНКА ТРУДОМІСТКОСТІ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ РЕНДЕРИНГУ ГРАФІЧНИХ СЦЕН.....	188
Богданова Марія Володимирівна, Грунківський Денис Васильович СУЧАСНІ ПІДХОДИ ТА ТЕХНОЛОГІЇ В РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.....	191
Войтюк Анастасія Сергіївна, Поперешняк Світлана Володимирівна СТВОРЕННЯ АДАПТИВНОГО ОПОНЕНТА ДЛЯ КОЛЕКЦІЙНИХ КАРТКОВИХ ІГОР НА БАЗІ ГІБРИДНОГО FSM ТА ЕВРИСТИЧНОГО ПОШУКУ.....	194
Данилов Леонід Володимирович, Поперешняк Світлана Володимирівна ПОБУДОВА ВИСОКОНАВАНТАЖЕНИХ СИСТЕМ З ВИКОРИСТАННЯМ ЧЕРГ ПОВІДОМЛЕНЬ.....	197

Денисюк Станіслав Степанович МОДЕЛЬ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗОВНІШНЬОЇ ДОПОМОГИ У ЗАБЕЗПЕЧЕННІ ПОТРЕБ ПІДРОЗДІЛІВ.....	200
Дерев'янюк Євген Миколайович МЕТОДИ БАГАТОКРИТЕРІАЛЬНОГО АНАЛІЗУ РИЗИКІВ В УМОВАХ ВИСОКОЇ ДИНАМІЧНОСТІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО СЕРЕДОВИЩА.....	203
Іванов Артем Олександрович, Кривонос Олександр Миколайович ПОРІВНЯННЯ АЛГОРИТМІВ СОРТУВАННЯ.....	207
Івасюк Василь Васильович ОГЛЯД СУЧАСНОГО СТАНУ ДОСЛІДЖЕННЯ ЗАЛЕЖНОСТІ ПРОГРАМНИХ ПАКЕТІВ.....	211
Ісмагілов Артур Ільясович МЕТОД КЛАСТЕРНОЇ ІДЕНТИФІКАЦІЇ ВИСОКОРИЗИКОВИХ ПОДІЙ ДЛЯ ПРОГНОЗУВАННЯ ПОЯВИ ЗАГРОЗ НУЛЬОВОГО ДНЯ.....	213
Корнієнко Олексій Олексійович ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ РОЗРОБКИ ОБЛІКОВИХ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМ НА ОСНОВІ КЕРУВАННЯ БІЗНЕС-ВИМОГАМИ ТА ОПТИМІЗАЦІЇ CASE-ЗАСОБІВ.....	217
Крепкий Ігор Тарасович, Ніщенко Дмитро Олександрович КЛІЄНТ-СЕРВЕРНА СИСТЕМА ПОТОКОВОЇ ПЕРЕДАЧІ АУДІО З МОБІЛЬНОГО ПРИСТРОЮ.....	220
Левченко Анастасія Вікторівна, Духновська Ксенія Костянтинівна ПРОЕКТУВАННЯ МІКРОСЕРВІСНОЇ БЕКЕНД-АРХІТЕКТУРИ CRM ІЗ МОБІЛЬНИМ КЛІЄНТОМ ANDROID.....	222
Моргун Артем Вікторович МЕТОДИ РЕКОНСТРУКЦІЇ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.....	225
Сокульський Олег Євгенович, Москаленко Наталія Володимирівна ТЕХНОЛОГІЯ ВІДКРИТИХ КОДІВ В РОЗРОБЦІ ІНФОРМАЦІЙНИХ СИСТЕМ.....	228
Недозимованій Денис Віталійович, Поперешняк Світлана Володимирівна КОМПЛЕКСНІ ПІДХОДИ ДО КІБЕРЗАХИСТУ В УМОВАХ СУЧАСНИХ ЦИФРОВИХ ЗАГРОЗ.....	230
Нікулін Сергій Сергійович, Заболотний Олександр Віталійович ТЕСТУВАННЯ БАЗОВОГО ФУНКЦІОНАЛУ FPV-ДРОНА ЗА ДОПОМОГОЮ СИМУЛЯТОРА ДИНАМІКИ.....	233
Овчаренко Віктор Сергійович АДАПТИВНИЙ ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ СТАБІЛЬНОЇ ЯКОСТІ РОЗРОБКИ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ ПРОЦЕСНОЇ АНАЛІТИКИ.....	236
Поперешняк Даниїл Ігорович МОДЕЛЬ ІНТЕЛЕКТУАЛЬНОЇ АВТОМАТИЗАЦІЇ УПРАВЛІННЯ КОЛЕКЦІЙНИМИ РЕСУРСАМИ.....	239
Присяжнюк Олена Віталіївна, Пузікова Анна Валентинівна АНАЛІЗ ВИКОРИСТАННЯ GPT-4O ДЛЯ АВТОМАТИЗАЦІЇ ОЦІНЮВАННЯ ЯКОСТІ КОРИСТУВАЦЬКОГО ІНТЕРФЕЙСУ З УРАХУВАННЯМ БЕЗПЕКОВИХ РИЗИКІВ.....	242
Серкелі Артур Вадимович, Поперешняк Світлана Володимирівна ВИЗНАЧЕННЯ ВИМОГ ДО ПЛАТФОРМИ ОНЛАЙН-КУРСІВ.....	246
Торба Святослав Олександрович ПРОЄКТУВАННЯ СИСТЕМИ КЕРУВАННЯ ФІТНЕС-СТУДІЄЮ ІЗ ВБУДОВАНИМ ІІІ-АГЕНТОМ.....	248
Триняк Владислав Андрійович ОПТИМІЗАЦІЯ ФРОНТЕНД РОЗРОБКИ ШЛЯХОМ РОЗРОБКИ РЕКОМЕНДАЦІЙ ПО ВИБОРУ ФРЕЙМВОРКІВ/CMS.....	251
Федорченко Олексій Дмитрович ПАРАЛЕЛЬНА ОБРОБКА ТРАНЗАКЦІЙ ЯК ОСНОВА ПІДВИЩЕННЯ НАДІЙНОСТІ ГІБРИДНИХ СИСТЕМ УПРАВЛІННЯ ДАНИМИ.....	254

Юрчик Дмитро Юрійович ЗАСТОСУВАННЯ ГЕНЕРАТИВНИХ МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АВТОМАТИЗОВАНОЇ ГЕНЕРАЦІЇ ТЕСТОВИХ СЦЕНАРІЇВ ТА ОРАКЛІВ.....	257
Романюк Олександр Никифорович, Курінна Юлія Михайлівна ПРОГРАМНІ ЗАСОБИ І АЛГОРИТМИ ДІАГНОСТИКИ ПАТОЛОГІЙ ЗА ЗОБРАЖЕННЯМИ ОБЛИЧЧЯ.....	260
Бажан Юрій Павлович, Золотухіна Оксана Анатоліївна, Замрій Ірина Вікторівна, Глушкова Оксана Іванівна АНАЛІЗ ОБМЕЖЕННЯ ФУНКЦІОНАЛЬНИХ ВИМОГ ПРИ СЕРТИФІКАЦІЇ ПРОГРАМНОГО ПРОДУКТУ В УМОВАХ AGILE-РОЗРОБКИ.....	263

Напрямок №4. Алгоритми та моделі AI/ML

Пісоцький Мар'ян Олексійович МЕТОД КОНТЕКСТНОГО ПРОФІЛЮВАННЯ ДЛЯ ІНТЕЛЕКТУАЛЬНОЇ ОПТИМІЗАЦІЇ ЦИФРОВИХ ПЛАТФОРМ.....	265
Рисований Олександр Миколайович ДОСЛІДЖЕННЯ СПОСОБІВ ІН'ЄКЦІЇ В ЗАГОЛОВКИ РЕ-ФАЙЛА.....	268
Алмазов Денис Олегович, Божуха Лілія Миколаївна МЕТОДИ ОПТИМІЗАЦІЇ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ НЕЙРОННИХ МЕРЕЖ НА МІКРОКОНТРОЛЕРАХ (TINYML).....	270
Бакаєв Олег Олександрович АЛГОРИТМІЧНИЙ ПІДХІД ДО ОПТИМІЗАЦІЇ ПОЛІТИК ДОСТУПУ ДО ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ІНТЕНСИВНИХ АТАК.....	273
Башенко Євгеній Вікторович, Поперешняк Світлана Володимирівна МЕТОДИ ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ.....	277
Гамор Іван Миколайович ІНТЕЛЕКТУАЛЬНИЙ АСИСТЕНТ ДЛЯ АНАЛІЗУ ПОВЕДІНКИ КОРИСТУВАЧІВ У ПРОЦЕСІ UX-ТЕСТУВАННЯ.....	279
Ганенко Людмила Дмитрівна МЕТОД СОЦІАЛЬНО-АДАПТИВНОЇ НАВІГАЦІЇ МОБІЛЬНОГО РОБОТА.....	282
Книш Ігор Олександрович, Шевченко Світлана Миколаївна АЛГОРИТМИ РЕКОМЕНДАЦІЙ ДЛЯ ПІДБОРУ ВАКАНСІЙ ФІЗИЧНОЇ ПРАЦІ.....	285
Колесниченко Іван В'ячеславович ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ АВТОМАТИЗАЦІЇ ТА ПОКРАЩЕННЯ ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.....	288
Кравченко Роман Вікторович ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДВИЩЕННЯ ЯКОСТІ ТА ДОСТОВІРНОСТІ ПОТОКОВИХ ДАНИХ.....	292
Купцов Дмитро Володимирович ІНТЕЛЕКТУАЛЬНИЙ АСИСТЕНТ ДЛЯ АНАЛІЗУ ПОВЕДІНКИ КОРИСТУВАЧІВ У ПРОЦЕСІ UX-ТЕСТУВАННЯ.....	295
Лазарович Юлія Ігорівна АРХІТЕКТУРА ГІБРИДНОЇ RAG-СИСТЕМИ ДЛЯ МУЛЬТИМОДАЛЬНОГО СЕМАНТИЧНОГО АНАЛІЗУ І ГЕНЕРАЦІЇ.....	298
Майборода Максим Володимирович КВАНТОВІ МЕТОДИ ЗНАХОДЖЕННЯ РОЗВ'ЯЗКІВ ЛІНІЙНИХ СИСТЕМ.....	301
Ніщеменко Дмитро Олександрович, Аронов Андрій Олексійович ГІБРИДНА КЛАСИФІКАЦІЙНО-КЕРОВАНА АРХІТЕКТУРА ДЛЯ НАДІЙНОЇ ОЧИСТКИ ГЕТЕРОГЕННИХ ДАНИХ ІОТ.....	303
Доманецька Ірина Миколаївна, Хроленко Ярослав Олексійович ТОНКЕ НАЛАШТУВАННЯ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ ПІД ЕКСПЕРТНІ ДОМЕНІ.....	306
Черевик Олексій В'ячеславович ВИДАЛЕННЯ ШУМІВ У ДАНИХ 3D-СКАНУВАННЯ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ.....	309

Шлянчак Світлана Олександрівна МЕТОДИ ОБРОБКИ ГРАФІВ У ГРАФОВИХ НЕЙРОННИХ МЕРЕЖАХ.....	312
Юрченко Костянтин Юрійович ІНТЕЛЕКТУАЛЬНІ МЕТОДИ АНАЛІЗУ Й УПРАВЛІННЯ ФУНКЦІОНАЛЬНІСТЮ КОРПОРАТИВНОГО САЙТУ В УМОВАХ ЗМІННОГО СЕРЕДОВИЩА.....	314
Язвінська Діана Ігорівна МЕТОДОЛОГІЯ ІНТЕГРАЦІЇ МАШИННОГО НАВЧАННЯ ТА ДИНАМІЧНОГО ГЕНЕРУВАННЯ КОНТЕНТУ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ НАВЧАННЯ.....	317
Іванов Ростислав Миколайович, Кисіль Тетяна Миколаївна ПОРІВНЯЛЬНИЙ АНАЛІЗ АРХІТЕКТУР TENSORFLOW ТА JAX ДЛЯ ГЛИБОКОГО НАВЧАННЯ.....	320
Василенко Михайло Сергійович, Золотухіна Оксана Анатоліївна ВИЛУЧЕННЯ ІНФОРМАЦІЇ З МАРКЕТИНГОВИХ ДАНИХ НА ОСНОВІ МЕТОДІВ NLP.....	323
Владіміров Нікіта Володимирович, Золотухіна Оксана Анатоліївна ПОБУДОВА ГРАФУ ПОШИРЕННЯ НОВИН В УКРАЇНСЬКОМУ МЕДІАПРОСТОРІ.....	326
Чугреєв Кирилл Олександрович МЕТОД НА ОСНОВІ ГІБРИДНОГО МЕХАНІЗМУ LSTM ТА GNN ДЛЯ ПРОГНОЗУВАННЯ ЗБОЇВ У МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ.....	329
Котирло Віталій Володимирович, Кисіль Тетяна Миколаївна МАШИННЕ НАВЧАННЯ ДЛЯ ОПТИМІЗАЦІЇ APACHE SPARK: МОДЕЛЮВАННЯ ЧАСУ ВИКОНАННЯ ПАКЕТНИХ ЗАВДАНЬ.....	332
Сидоренко Карина Олександрівна ЕЛЕКТРОННИЙ ЛАБОРАТОРНИЙ ПРАКТИКУМ З ТЕСТУВАННЯ WEB-ДОДАТКІВ.....	335
Матюшко Олександр Вадимович, Довженко Тимур Павлович, Рябова Катерина Олексіївна ПОКРАЩЕННЯ АЛГОРИТМІВ АВТОМАТИЧНОЇ ОЦІНКИ РІВНЯ ВОЛОДІННЯ АНГЛІЙСЬКОЮ МОВОЮ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ.....	337
<i>Напрямок №5. Інформаційні системи й мережі</i>	
В'юннік Юрій Олександрович АДАПТИВНА МОДЕЛЬ АДМІНІСТРУВАННЯ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВИКОРИСТАННЯ ГІБРИДНИХ ХМАРНИХ РІШЕНЬ.....	339
Гринчук Олександр, Романенко Євген, Роман Захарчук ЯКИМ МАЄ БУТИ ВІЙСЬКОВО-ПОЛІЦЕЙСЬКИЙ ДРОН (MILITARY POLICE DRONE).....	343
Романюк Олександр Никифорович, Завальнюк Євген Костянтинович ОСНОВНІ ПАРАМЕТРИ ПОБУДОВИ ВИСОКОЕФЕКТИВНИХ СИСТЕМ КІНЦЕВОЇ ВІЗУАЛІЗАЦІЇ.....	346
Кузіна Дар'я Володимирівна ІНФОРМАЦІЙНА СИСТЕМА УПРАВЛІННЯ ОСВІТНІМ ПРОЦЕСОМ У ЗАКЛАДІ ВИЩОЇ ОСВІТИ.....	349
Лабчук Віталій Андрійович, Захарченко Раїса Миколаївна ВИКОРИСТАННЯ SMALL DATA ШЛЯХОМ ЗБОРУ ВИСОКОРЕЛЕВАНТНИХ ДАНИХ З ОНЛАЙН-ФОРМ ДЛЯ ПОКРАЩЕННЯ МІСЬКОЇ МОБІЛЬНОСТІ У РОЗУМНОМУ МІСТІ.....	351
Сокульський Олег Євгенович, Москаленко Наталія Володимирівна ОБРОБКА ТЕКСТУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ.....	354
Олійник Антон Валерійович ТЕХНОЛОГІЧНІ РІШЕННЯ КОМП'ЮТЕРНОГО ЗОРУ ТА ШІ В АВТОМАТИЗОВАНИХ АГРОСИСТЕМАХ.....	356
Панченко Володимир Іванович, Главчев Максим Ігорович, Гейко Геннадій Вікторович АНАЛІЗ АЛГОРИТМІВ ПЛАНУВАННЯ ПРОЦЕСОРНОГО ЧАСУ В ОПЕРАЦІЙНИХ СИСТЕМАХ РЕАЛЬНОГО ЧАСУ.....	359

Петраченко Ігор Андрійович ОСОБЛИВОСТІ РОЗРОБКИ ІНФОРМАЦІЙНИХ СИСТЕМ УПРАВЛІННЯ СКЛАДОМ МАГАЗИНУ ФОРМАТУ DIU ДЛЯ АВТОМАТИЗАЦІЇ ОБЛІКУ ТОВАРНИХ ЗАПАСІВ.....	362
Симоненко Олександр Вікторович ОПТИМІЗАЦІЯ ПАРАМЕТРІВ НЕЙРОННИХ МЕРЕЖ ДЛЯ ПОТОКОВОЇ АНАЛІТИКИ ЗА ДОПОМОГОЮ ЕВОЛЮЦІЙНИХ АЛГОРИТМІВ....	366
Толмачев Роман Вікторович ЗБІР ТА ОЧИЩЕННЯ ДАНИХ У ВЕБ-ПАРСИНГУ	370
Богурський Артем Юрійович МЕТОДИ АНАЛІЗУ ТА ОЦІНКИ ПРИЙНЯТОГО СИГНАЛУ В СИСТЕМАХ АВТОМАТИЧНОГО КЕРУВАННЯ ВУЗЬКОСПРЯМОВАНИМИ АНТЕНАМИ.....	372
Богурський Артем Юрійович АДАПТИВНІ MANET-МЕРЕЖІ ДЛЯ ТАКТИЧНИХ УМОВ: МОДЕЛІ ПРОГНОЗУВАННЯ СТІЙКОСТІ ЛІНКУ, ІНТЕЛЕКТУАЛЬНЕ УПРАВЛІННЯ РАДІОРЕСУРСАМИ ТА ЗАСТОСУВАННЯ МУРАШИНОГО АЛГОРИТМУ	375
Целованський Тихон Романович, Шикуча Олена Миколаївна ДОСЛІДЖЕННЯ МЕТОДІВ ОПТИМІЗАЦІЇ ШВИДКОСТІ ОЗП НА БАГАТОСОКЕТНИХ СЕРВЕРНИХ СИСТЕМАХ...	377
<i>Напрямок №6. Комп'ютерні мережі та телекомунікації</i>	
Ільїн Сергій Анатолійович МЕТОДОЛОГІЯ ВПРОВАДЖЕННЯ БАГАТОКРИТЕРІАЛЬНОЇ ОПТИМІЗАЦІЇ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ В ІНТРАНЕТ-МЕРЕЖІ.....	380
Король Тимофій Віталійович, Саливон Богдан Вадимович ВПРОВАДЖЕННЯ СІ/CD ПРАКТИК У РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ: СУЧАСНІ ПІДХОДИ ТА ВИКЛИКИ.....	383
Круліковський Б.Б. ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ: ПРОАКТИВНІ СТРАТЕГІЇ В ЕПОХУ ТОТАЛЬНОЇ ДІДЖИТАЛІЗАЦІЇ.....	387
Петрушишин Артем Максимович, Заброцький Владислав Олексійович ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В АВТОМАТИЗАЦІЇ ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ.....	390
Герасимчук Владислав Сергійович МЕТОДИКА РОЗРАХУНКУ ТРАНЗАКЦІЙНИХ ПОСЛУГ.....	394
<i>Напрямок №7. Інновації в комп'ютерній інженерії</i>	
Баранюк Олександр Філімонович ПРОГРАМНІ СИМУЛЯТОРИ ДЛЯ МОДЕЛЮВАННЯ КОМПОНЕНТІВ РОБОТОТЕХНІЧНИХ СИСТЕМ.....	397
Рейнська Вікторія Борисівна, Бачманюк Дмитро Олександрович АПАРАТНІ ЗАСОБИ ТА ЇХ АДАПТАЦІЯ ДО УМОВ СУЧАСНОГО БІЗНЕСУ В УКРАЇНІ ТА СВІТІ.....	401
Скостарев Ігор Віталійович ДЕЦЕНТРАЛІЗОВАНА eBPF-АРХІТЕКТУРА ЗАМКНЕНОГО ЦИКЛУ БЕЗПЕКИ ДЛЯ ПРОТИДІЇ ЕКСФІЛЬТРАЦІЇ ДАНИХ У СЕРЕДОВИЩІ KUBERNETES.....	404
Миронюк Павло Ярославович МЕТОДИ РЕЛЯЦІЙНО-УЗГОДЖЕНОЇ СИНХРОНІЗАЦІЇ ДАНИХ У LOCAL-FIRST СИСТЕМАХ.....	407
<i>Напрямок №8. Кібербезпека та захист інформації</i>	
Бова Юрій Вікторович ІНТЕЛЕКТУАЛІЗОВАНА АВТОМАТИЗАЦІЯ ВИПРОБУВАНЬ У КОМПЛЕКСНИХ СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ.....	409
Гаркушенко Аріна Максимівна, Шевченко Світлана Миколаївна МЕТОДИ КОГНІТИВНОГО МОДЕЛЮВАННЯ СЦЕНАРІЇВ КІБЕРРИЗИКУ.....	412
Ільченко Катерина Юріївна МЕХАНІЗМИ ЗАХИСТУ ВІД СОЦІАЛЬНО-ІНЖЕНЕРНИХ АТАК	415

Кочин Владислав Дмитрович СУЧАСНІ СТРАТЕГІЇ КІБЕРЗАХИСТУ В ЕПОХУ ДІДЖИТАЛІЗАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ.....	418
Крайнюк Олена Володимирівна КІБЕРСТІЙКІСТЬ ВЕНДИНГОВИХ КОМПЛЕКСІВ ОБЛІКУ ЗАСОБІВ ІНДИВІДУАЛЬНОГО ЗАХИСТУ.....	421
Нікітін Антон Миколайович, Коровайченко Юрій Юрійович МЕТОДИ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ЗАГРОЗ НА ОСНОВІ МАШИННОГО НАВЧАННЯ ТА ШТУЧНОГО ІНТЕЛЕКТУ.....	423
Поліковський Богдан Володимирович ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ БІБЛІОТЕК САНІТИЗАЦІЇ ПРОТИ XSS-АТАК.....	426
Рейнська Вікторія Борисівна ВИКЛИК СУЧАСНИМ ЗАГРОЗАМ В ІНФОРМАЦІЙНОМУ БІЗНЕСІ В УКРАЇНІ: ТЕХНІЧНІ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ ПРОТИДІЇ.....	428
Рисований Олександр Миколайович ДОСЛІДЖЕННЯ СПОСОБІВ ІН'ЄКЦІЇ В ЗАГОЛОВКИ РЕ-ФАЙЛА.....	432
Рихлик Андрій Сергійович, Поперешняк Світлана Володимирівна СУЧАСНІ ПІДХОДИ ТА ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ЕВОЛЮЦІЇ ЦИФРОВИХ ЗАГРОЗ.....	434
Романюк Олександр Никифорович, Майданюк Володимир Павлович, Нечипорук Микола Леонідович КОДУВАННЯ ГРАФІЧНОЇ ІНФОРМАЦІЇ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ.....	437
Самарець Владислав Євгенович ВИКЛИКИ ТА ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ЛОКАЛЬНИХ LLM У ЦИФРОВІЙ КРИМІНАЛІСТИЦІ: ПИТАННЯ БЕЗПЕКИ, КОНФІДЕНЦІЙНОСТІ ТА НАДІЙНОСТІ.....	440
Сиваченко Ігор Олексійович ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ТА ВАРТОСТІ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ З МЕТОЮ ОПТИМІЗАЦІЇ ЇХ СКЛАДУ В КРИЗОВИХ СИТУАЦІЯХ.....	443
Трофімов Олександр Сергійович ВДОСКОНАЛЕННЯ ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ НА ОСНОВІ КОНЦЕПЦІЇ ZERO TRUST.....	446
Стежко Світлана Орестівна, Кондратенко Наталія Юріївна МОВНА ЕТИКА ЕЛЕКТРОННОГО СПІЛКУВАННЯ В УМОВАХ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ.....	449
<i>Напрямок №9. Blockchain-технології</i>	
Гавор Артур Станіславович, Герцюк Микола Модестович ОГЛЯД ПРОТОКОЛУ GOSSIP В РОЗПОДІЛЕНИХ ОБЧИСЛЕННЯХ.....	452
Рудавіна Катерина Дмитрівна BLOCKCHAIN-ТЕХНОЛОГІЇ. ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ BLOCKCHAIN-ТЕХНОЛОГІЙ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ.....	455
<i>Напрямок №10. Цифрова економіка та інформаційні системи</i>	
Кравчук Андрій Віталійович ІНТЕГРАЦІЯ ВІДЕОХОСТИНГУ YOU TUBE У КУРС ФІЗИКИ ЯК СКЛАДОВА ЦИФРОВОЇ ЕКОНОМІКИ ЗНАНЬ.....	458
Лозан Андрій Едуардович ІНТЕГРАЦІЯ ЦИФРОВИХ РІШЕНЬ В УПРАВЛІННЯ ІННОВАЦІЙНИМ РОЗВИТКОМ ПІДПРИЄМСТВ	461
Сербін Віталій Ігорович МЕТОДОЛОГІЯ E-C-R-S-T-M ДЛЯ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В МАРКЕТИНГ КОМПАНІЙ ЕЛЕКТРОННОЇ КОМЕРЦІЇ.....	464
Крискун Іван Миколайович ІНСТРУМЕНТИ УПРАВЛІННЯ ПРОЕКТАМИ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ.....	467

Напрямок №1. Досвід сучасних ІТ-компаній

Кирилов Іван Ігорович
аспірантка 4 курсу, групи КН-22
Інститут програмних систем НАН України
(095) 592-15-29
ivan.kyrylov.science@gmail.com

МУЛЬТИАГЕНТНЕ НАВЧАННЯ З ПІДКРІПЛЕННЯМ ДЛЯ ОПТИМІЗАЦІЇ КВАНТОВИХ СХЕМ

Постановка задачі. Квантові схеми є основою квантових обчислень, але їх практичне застосування обмежене шумами та декогеренцією в сучасних квантових пристроях NISQ-ери[1]. Зменшення кількості вентилів у схемі критично важливе для підвищення якості обчислень. Традиційні методи оптимізації досягли своїх меж, тому виникає потреба в нових підходах на основі машинного навчання.

Мета дослідження. Метою дослідження є зменшення кількості вентилів у квантовій схемі за допомогою мультіагентного навчання з підкріпленням[2], що дозволить підвищити якість виконання квантових алгоритмів на існуючих квантових пристроях. Розробити архітектуру MARL для задачі оптимізації квантових схем, визначити оптимальні гіперпараметри навчання та провести експериментальне порівняння з існуючими методами.

Результати дослідження. Процес оптимізації квантових схем базується на формальних правилах еквівалентних трансформацій, які гарантують збереження функціональності схеми при зменшенні кількості вентилів. Ключова інновація полягає у використанні мультіагентного підходу, де кожен агент спеціалізується на оптимізації певної частини схеми.

Квантова схема представляється як граф, де вершини відповідають вентилям, а ребра показують залежності між ними. Для кожного набору вентилів попередньо генерується набір правил еквівалентних трансформацій за допомогою бібліотек.

Архітектура системи складається з трьох основних компонентів:

1. Граф представлення схеми - забезпечує структурований опис квантової схеми як спрямованого ациклічного графу (DAG), що дозволяє ефективно виявляти паттерни для оптимізації.

2. Мультіагентна система - кожен агент навчається оптимізувати певні паттерни вентилів, використовуючи алгоритм MAPPO[3] (Multi-Agent Proximal Policy Optimization). Агенти координують свої дії через спільну функцію винагороди[4].

3. Графова нейронна мережа (GNN) - використовується для екстракції ознак з графу схеми та генерації вбудовувань (embeddings) для кожного вузла, що дозволяє агентам приймати обґрунтовані рішення.

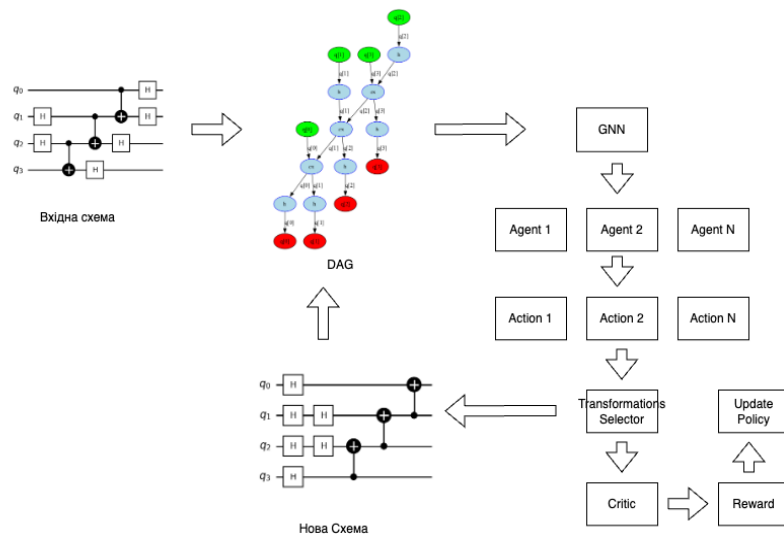


Рис. 1. Архітектура мультиагентної системи оптимізації квантових схем.

Експериментальна перевірка проводилась на стандартному наборі квантових схем з бібліотеки Qiskit[5]. Результати показали зменшення кількості двокубітних вентилів у середньому на 23% порівняно з базовими методами оптимізації. Для схем з більше ніж 100 вентилів покращення досягає 35%.

Використання MARL дозволяє паралелізувати процес оптимізації, що значно скорочує час обробки великих схем. Кожен агент може працювати з окремою частиною схеми незалежно, а потім результати об'єднуються через механізм консенсусу.

Висновки та перспективи. Запропонований підхід на основі мультиагентного навчання з підкріпленням демонструє високу ефективність для оптимізації квантових схем. Ключові переваги включають: масштабованість для великих схем, адаптивність до різних типів квантових вентилів, можливість паралельної обробки.

Перспективами подальших досліджень є розширення набору правил трансформацій, інтеграція з квантовими компіляторами нового покоління, адаптація методу для конкретних квантових архітектур, та розробка механізмів переносу навчання між різними типами квантових схем.

Список використаних джерел

1. Nielsen M.A., Chuang I.L. Quantum Computation and Quantum Information. Cambridge University Press, 2010. 676 p.
2. Zhang X.-M., Xie Z., Li G.-X., et al. Multi-agent reinforcement learning for quantum circuit optimization. Quantum Science and Technology. 2023. Vol. 8. 045009.
3. Foerster J.N., Assael Y.M., de Freitas N., Whiteson S. Learning to Communicate with Deep Multi-Agent Reinforcement Learning. NIPS 2016.
4. Lowe R., Wu Y., Tamar A., et al. Multi-Agent Actor-Critic for Mixed Cooperative-Competitive Environments. NIPS 2017.
5. Qiskit Development Team. Qiskit: An Open-source Framework for Quantum Computing. 2023.

Напрямок №2. Розробка Е-сервісів та Е-систем

Башинський Роман Ігорович

студент 3 курсу, групи ТЦР-33

Державний університет інформаційно-комунікаційних технологій

(068) 074-41-14

basinskijroma@gmail.com

Поперешняк Світлана Володимирівна

к.ф.-м.н., доцент, доцент кафедри технологій цифрового розвитку

Державний університет інформаційно-комунікаційних технологій

spopereshnyak@gmail.com

РОЛЬ ВЕБКАЛІБРАТОРІВ КОЛЬОРУ У ПІДВИЩЕННІ ЯКОСТІ ЦИФРОВОГО КОНТЕНТУ

Актуальність дослідження. У сучасних умовах швидкої діджиталізації якість візуального контенту безпосередньо впливає на довіру користувачів, ефективність онлайн-комунікацій та результативність цифрових сервісів. Відображення кольорів значною мірою залежить від характеристик конкретного монітора [1], що часто призводить до спотворення дизайнерських рішень, медіаматеріалів і інтерфейсів. Використання простих та доступних веб-калібраторів дозволяє мінімізувати такі відхилення без необхідності в професійному обладнанні.

Постановка проблеми. Попри важливість коректного відтворення кольорів, більшість користувачів не мають можливості або навичок для ручного калібрування моніторів. Існуючі апаратні рішення є дорогими та орієнтованими на професійний сегмент [1]. Водночас веб-сервіси, що мають потенціал зробити калібрування масовим та доступним, залишаються недостатньо розвиненими: їм бракує точності, стандартизації та інтеграції в екосистеми цифрових платформ [2-3].

Мета дослідження. Метою роботи є аналіз можливостей веб-калібраторів кольору та визначення їхнього впливу на покращення якості цифрового контенту, а також обґрунтування підходів до створення ефективного веб-модуля калібрування, орієнтованого на широке застосування.

Виклад основного матеріалу. У процесі дослідження встановлено, що веб-калібратори кольору формують новий підхід до налаштування параметрів відображення, спираючись виключно на можливості браузерних технологій. На відміну від апаратних рішень, які ґрунтуються на фотометричних вимірюваннях, веб-модулі забезпечують якісно інший - суб'єктивно-візуальний - механізм взаємодії користувача з тестовими патернами. Ключову роль у цьому відіграють програмні середовища WebGL [4], Canvas API [2] та динамічні графічні фільтри CSS [3], що дозволяють формувати градієнтні шкали, еталонні зображення та адаптивні зразки, корекція яких на екрані здійснюється в реальному часі.

Застосування поетапної калібрації ґрунтується на поступовому вирівнюванні яскравості, контрастності, насиченості та гамма-кривої відповідно

до запропонованих еталонів. У процесі роботи модуль формує інтерактивне середовище, у якому користувач на кожному етапі отримує візуальний зворотний зв'язок щодо правильності змін, а програмний алгоритм оцінює співпадіння з нормованими діапазонами. У межах дослідження особливу увагу приділено точності відтворення відтінків у темному та світлому діапазонах [1], оскільки саме ці зони найчастіше піддаються спотворенням у непрофесійних дисплеях [5].

Узагальнені результати аналізу функціональних можливостей веб-калібраторів подано у таблиці 1, що відображає зв'язок між технічними інструментами браузера та їх впливом на якість цифрового контенту.

Таблиця 1.

Вплив веб-технологій на якість калібрування кольору

Технологічний інструмент	Функціональна роль у калібруванні	Вплив на якість цифрового контенту
WebGL	Формування високоточних градієнтів та кольорних переходів	Забезпечує коректне відображення відтінків і плавних переходів
Canvas API	Генерація динамічних тест-патернів	Покращує точність налаштування яскравості та контрастності
CSS-фільтри	Імітація параметрів дисплея та корекційних алгоритмів	Дає змогу оцінити зміни кольору без перезавантаження екрана
Алгоритми візуальних підказок	Оцінювання відхилень та рекомендації користувачу	Знижує ймовірність помилкових налаштувань, підвищує стандартизацію результату

Проведений аналіз підтвердив, що інтеграція веб-калібраторів у сучасні цифрові сервіси дозволяє суттєво підвищити однорідність подання контенту на різних типах дисплеїв. Це особливо важливо для галузей, де точність кольору має критичне значення — зокрема для цифрового дизайну, електронної комерції, державних інформаційних платформ та освітніх ресурсів, орієнтованих на мультимедіа. Веб-калібратори, будучи доступними та незалежними від операційної системи, створюють можливість стандартизації кольорового подання у середовищах, які раніше не мали інструментів для масової калібрації.

У ході дослідження було визначено структурну логіку роботи веб-калібратора кольору, яка охоплює послідовність етапів від отримання вхідних параметрів до суттєвого підвищення якості цифрового контенту на різних пристроях. Для візуалізації цього процесу нижче на рис. 1 наведено узагальнену функціональну схему, що демонструє взаємозв'язок основних компонентів системи, браузерних технологій та вплив калібрації на кінцевий візуальний результат.

Подана схема дозволяє системно представити етапи роботи веб-калібратора кольору, відображаючи логіку проходження даних через усі ключові компоненти системи. Вона демонструє, як браузерні технології забезпечують генерацію тестових зображень і корекційних фільтрів [2-4], а також яким чином взаємодія з користувачем формує більш точні параметри відображення. На завершальному етапі ця модель сприяє покращенню візуальної якості цифрового контенту,

оскільки налаштований дисплей забезпечує значно точніше відтворення кольорів у веб-інтерфейсах, мультимедійних об'єктах та графічних матеріалах.

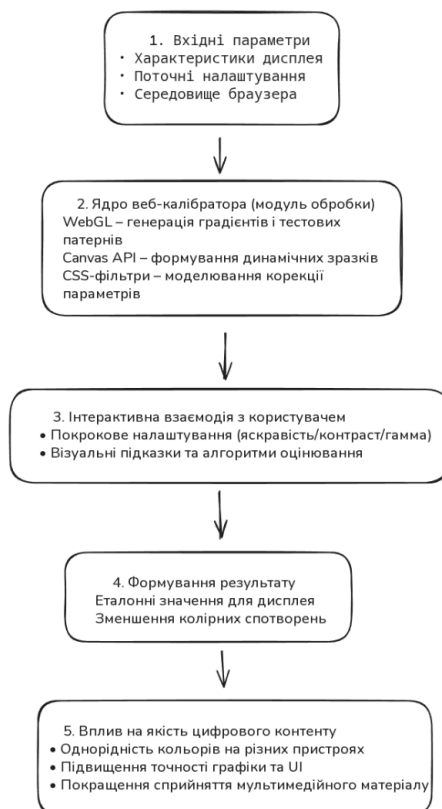


Рис. 1. Схема етапів роботи веб-калібратора кольору

Таким чином, схема не лише ілюструє технічну структуру веб-калібратора, але й підкреслює його практичну роль у стандартизації цифрового середовища.

Висновки та перспективи. Дослідження показало, що веб-калібратори кольору суттєво покращують точність відображення цифрового контенту та забезпечують його стабільність на різних пристроях. Використання браузерних технологій робить процес калібрації доступним [2-4], швидким і незалежним від операційної системи. Перспективи подальших робіт полягають у вдосконаленні алгоритмів автоматичної оцінки кольору та розширенні інтерактивних можливостей таких модулів для підвищення ефективності калібрації у веб-середовищах.

Список використаних джерел

1. Fairchild M. D. *Color Appearance Models*. 3rd ed. Wiley, 2013.
2. W3C. *HTML Canvas 2D Context*. World Wide Web Consortium, 2023.
3. W3C. *CSS Color Module Level 4*. World Wide Web Consortium, 2023.
4. Khronos Group. *WebGL Specification*. Khronos WebGL Working Group, 2022.
5. Остренко Н. В. Цифрова кольоропередача та методи її стандартизації у веб-середовищі. *Інформаційні технології та комп'ютерна інженерія*, №2, 2021, с. 45-52.

Бичок Олександра Сергіївна
студент 3 курсу, групи ТЦР-31
Державний університет інформаційно-комунікаційних технологій
St8492127@stud.duikt.edu.ua
Євпак Вікторія Олегівна
студент 3 курсу, групи ТЦР-31
Державний університет інформаційно-комунікаційних технологій
st8535200@stud.duikt.edu.ua
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

ОСОБЛИВОСТІ РОЗРОБКИ АНОНІМНОГО Е-ГОЛОСУВАННЯ

Постановка проблеми. Програмний комплекс «Анонімне Е-голосування» є інноваційною програмною системою, спрямованою на забезпечення високого рівня прозорості, безпеки та надійності у процесі електронного волевиявлення громадян.

Мета дослідження. Основна мета системи полягає у створенні технологічного середовища, в якому кожен користувач може здійснити своє право на участь у громадських ініціативах без ризику розкриття особистих даних, маніпуляцій чи порушення конфіденційності. Система об'єднує сучасні методи цифрового врядування, алгоритмічну стійкість і гнучку архітектуру, створюючи платформу, відповідну до міжнародних стандартів електронної демократії.

Результати дослідження. Функціональна архітектура комплексу базується на використанні технологій .NET 8, що забезпечує стабільну роботу, масштабованість і можливість розширення системи відповідно до зростання кількості користувачів та обсягу оброблюваних даних. Використання Razor Pages у веб-частині гарантує структуровану логіку, чітке відокремлення рівнів даних і представлення, а застосування WinForms + WebView2 у десктопній оболонці забезпечує універсальність та комфортну взаємодію користувачів з програмним продуктом у різних середовищах. Підтримка SQLite як локальної бази даних дає можливість досягти високої швидкості операцій читання-запису, автономності та надійності зберігання результатів голосування.

Ключовим аспектом функціонування комплексу є реалізація механізмів анонімності. У системі не здійснюється збирання персональних ідентифікаторів, а голосування проходить із використанням внутрішніх токенів контролю цілісності, що дозволяє запобігти повторному голосуванню з одного пристрою без порушення конфіденційності учасника. Така модель забезпечує одночасно і справедливість процесу, і дотримання етичних норм оброблення особистих даних. Усі операції з голосами виконуються у захищеному середовищі, а перед

записом у базу даних проходять валідацію, що запобігає внесенню несанкціонованих змін.

Окремої уваги заслуговує адміністративний модуль системи. Саме він створює основу для управління процесом електронного голосування, дозволяючи адміністраторам створювати нові опитування, налаштовувати часові рамки, редагувати описи, контролювати поточні результати та виконувати скидання статистичних даних. Завдяки цьому адміністратори отримують інструмент повного циклу — від створення опитування до аналізу завершених голосувань. Особливістю цього модуля є простота використання: система орієнтована навіть на користувачів без технічної підготовки, що суттєво розширює можливості її впровадження в адміністративних структурах різного рівня.

Програмний комплекс забезпечує високий рівень надійності завдяки вбудованим механізмам контролю цілісності бази даних, автоматичному відновленню після збоїв та обробленню нештатних ситуацій у передбачуваний спосіб. У разі несподіваного припинення роботи системи (наприклад, вимкнення живлення) всі проміжні дані залишаються захищеними, а після перезапуску система відновлює працездатність без втрати голосів чи конфігурацій. Такі властивості дозволяють використовувати комплекс у середовищах, де критично важливою є цілісність голосувань — наприклад, при впровадженні муніципальних проєктів, громадських ініціатив чи студентського самоврядування.

Значною перевагою системи є адаптивний користувацький інтерфейс, завдяки якому веб-частина автоматично підлаштовується під будь-який розмір екрана — від мобільних пристроїв до широкоформатних моніторів. Це забезпечує зручність користування і для пересічних громадян, і для старшого покоління, яке може не мати високого рівня цифрової грамотності. Інтерфейс побудований на принципах доступності (accessibility), що дозволяє користуватися системою людям із порушеннями зору, моторними чи когнітивними обмеженнями.

З теоретичної точки зору система реалізує комплексний підхід до організації електронного голосування, у якому поєднано принципи інформаційної безпеки, модульності, структурованого зберігання даних, людиноцентричного дизайну та цифрової інклюзивності. Такий підхід відповідає світовим практикам розвитку електронних сервісів, зокрема принципам Open Government та EU Digital Strategy.

Висновки та перспективи. «Анонімне Е-голосування» є технічно надійним рішенням, яке може слугувати фундаментом для подальшого розвитку цифрових платформ громадської взаємодії. Система створює умови для розширення участі населення у прийнятті рішень, підвищує рівень довіри до результатів електронних голосувань та сприяє розвиткові демократичних процесів у сучасному цифровому суспільстві.

Список використаних джерел

1. Chaum D. Secret-Ballot Receipts: True Voter-Verifiable Elections. IEEE Security & Privacy, 2004.
2. Adida B. Helios: Web-based Open-Audit Voting. USENIX Security Symposium, 2008.
3. Rivest R., Wack J. On the Notion of Software Independence in Voting Systems. U.S. EAC, 2006.
4. Springall D. et al. Security Analysis of the Estonian Internet Voting System. ACM CCS, 2014.
5. Cetinkaya O., Dalkilic G. A Survey on E-Voting Security. International Journal of Computer Science, 2017.

Варченко Артем Юрійович
студент 3 курсу, групи ТЦР-31
Державний університет інформаційно-комунікаційних технологій
+380-(63)-893-87-46
st8550424@stud.duikt.edu.ua
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

ПРОЕКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ КООРДИНАЦІЇ ВОЛОНТЕРСЬКОЇ ДІЯЛЬНОСТІ «ДОБРОДІЙ»

Постановка задачі. В умовах сучасних викликів волонтерський рух в Україні набув масового характеру, проте часто стикається з проблемами дезорганізації, дублювання запитів та складності логістики. Існуючі рішення (соціальні мережі, месенджери) не забезпечують достатньої структуризації даних для ефективного розподілу ресурсів. Тому актуальним є розробка спеціалізованої веб-платформи «Добродій», яка автоматизує процеси взаємодії між волонтерами, донорами та отримувачами допомоги.

Мета дослідження. Метою дослідження є проектування архітектури та розробка програмного забезпечення для волонтерської платформи; аналіз методів побудови високонавантажених веб-систем та вибір оптимального стека технологій для забезпечення швидкодії та масштабованості.

Результати дослідження. Сучасна інформаційна система волонтерської допомоги повинна базуватися на клієнт-серверній архітектурі. Для реалізації клієнтської частини (Frontend) було обрано бібліотеку React.js, яка дозволяє створювати інтерактивні інтерфейси з високою швидкістю відгуку (Single Page Application).

Методи проектування системи включають побудову інфологічної моделі бази даних та розробку API. Архітектура системи передбачає поділ користувачів на три основні ролі: «Адміністратор», «Волонтер» та «Користувач (заявник)». Важливою складовою є модуль верифікації заявок для уникнення шахрайства. Загальну архітектуру системи продемонстровано на рис. 1.

У ході розробки було проаналізовано та імплементовано наступні підходи:

1. Компонентний підхід (React). Інтерфейс розбито на незалежні компоненти (картки заявок, форми реєстрації, панель фільтрів), що спрощує підтримку коду та його повторне використання.
2. RESTful API. Для обміну даними між клієнтом та сервером використовується архітектурний стиль REST, що дозволяє легко інтегрувати платформу з іншими сервісами (наприклад, платіжними системами або логістичними службами).

3. Адаптивний дизайн. Використання технологій CSS Flexbox та Grid забезпечує коректне відображення платформи на мобільних пристроях, що є критично важливим для оперативної роботи волонтерів «у полі».

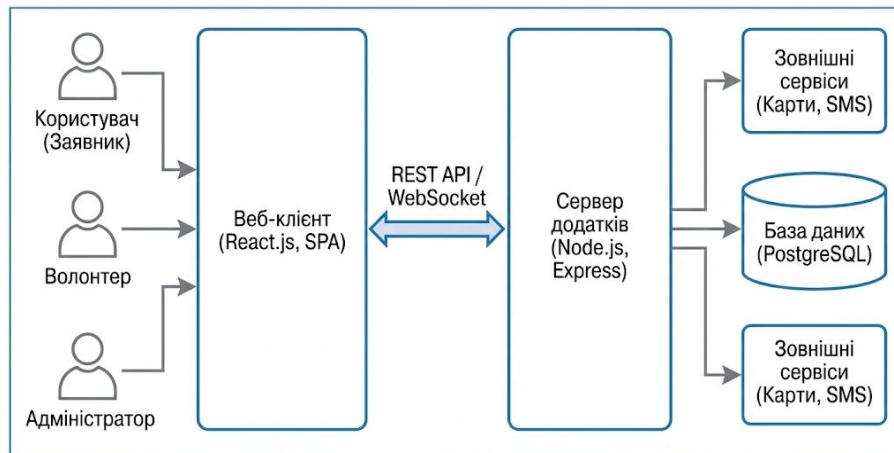


Рис. 1. Архітектура інформаційної системи «Добродій».

Порівняльний аналіз показав, що використання спеціалізованої платформи скорочує час на обробку однієї заявки на 30-40% у порівнянні з використанням таблиць Excel та чатів у месенджерах.

Висновки та перспективи. У роботі розглянуто процес створення системи «Добродій» для координації волонтерської діяльності. Розроблена архітектура дозволяє ефективно обробляти запити та керувати базою волонтерів. Перспективою подальших досліджень є інтеграція системи з державними сервісами (наприклад, Дія) для автоматичної верифікації осіб, а також розробка мобільного додатку з функцією геолокації для побудови оптимальних маршрутів доставки гуманітарної допомоги.

Список використаних джерел

1. Freeman A. Pro React 16. Apress, 2019. 547 p.
2. Martin R. C. Clean Architecture: A Craftsman's Guide to Software Structure and Design. Prentice Hall, 2017. 432 p.
3. Литвин В. В. Технології менеджменту знань та інтелектуальні системи підтримки прийняття рішень. Львів: Видавництво Львівської політехніки, 2018. 248 с.

Демчишин Данило Васильович

студент 3 курсу, групи ТЦР-33

Державний університет інформаційно-комунікаційних технологій

(096) 199-03-09

st8559162@stud.duikt.edu.ua

Поперешняк Світлана Володимирівна

к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії

Національний технічний університет України

"Київський політехнічний інститут імені Ігоря Сікорського"

spopereshnyak@gmail.com

АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ІНТЕРОПЕРАБЕЛЬНОСТІ В СУЧАСНИХ ЕКОСИСТЕМАХ ЦИФРОВОГО ЗДОРОВ'Я

Постановка задачі. Інформатизація медицини неминуче призводить до накопичення колосальних обсягів електронних даних про здоров'я пацієнтів (PHI — Protected Health Information). Ці дані є однією з найцінніших цілей для кіберзловмисників на чорному ринку, оскільки містять повний профіль людини: від паспортних даних до інтимних подробиць хвороб. Тому при розробці платформи "CustosMed" питання кібербезпеки виходять на перший план, перетворюючись з "додаткової опції" на фундаментальну вимогу. Окрім захисту, іншим викликом є інтеоперабельність — здатність системи обмінюватися даними з іншими учасниками ринку (лабораторіями, державними реєстрами eHealth, страховими компаніями) без втрати цілісності та конфіденційності інформації.

Мета дослідження. Метою роботи є розробка комплексної політики безпеки та програмна реалізація захищених шлюзів обміну даними для телемедичної платформи "CustosMed", що відповідають вимогам українського законодавства (Закон України "Про захист персональних даних") та міжнародним регламентам (GDPR, HIPAA).

Результати дослідження. Для забезпечення безпеки платформи було впроваджено багаторівневу модель захисту "Defense in Depth". На рівні передачі даних використовується протокол HTTPS із примусовим використанням TLS 1.3, що унеможливорює атаки типу Man-in-the-Middle (перехоплення трафіку). Всі дані, що передаються між клієнтом та сервером, шифруються асиметричними алгоритмами. На рівні зберігання даних (Data at Rest) реалізовано концепцію псевдонімізації. Персональні ідентифікатори користувача (ПІБ, телефон, ПН) зберігаються в окремій, ізольованій базі даних, тоді як медичні записи прив'язані до випадкових UUID-токенів. Навіть у випадку фізичного викрадення серверів з медичними записами, зловмисники не зможуть співставити діагнози з конкретними людьми без ключів доступу до бази ідентифікаторів.

Автентифікація користувачів реалізована на базі протоколу OAuth 2.0 та OpenID Connect. Це дозволяє використовувати безпечні токени доступу (JWT — JSON Web Tokens) з обмеженим терміном життя (наприклад, 15 хвилин) замість

передачі паролів при кожному запиті. Паролі користувачів ніколи не зберігаються у відкритому вигляді, а хешуються з використанням алгоритму Argon2 з додаванням унікальної "солі" (salt) для кожного запису (рис. 1).

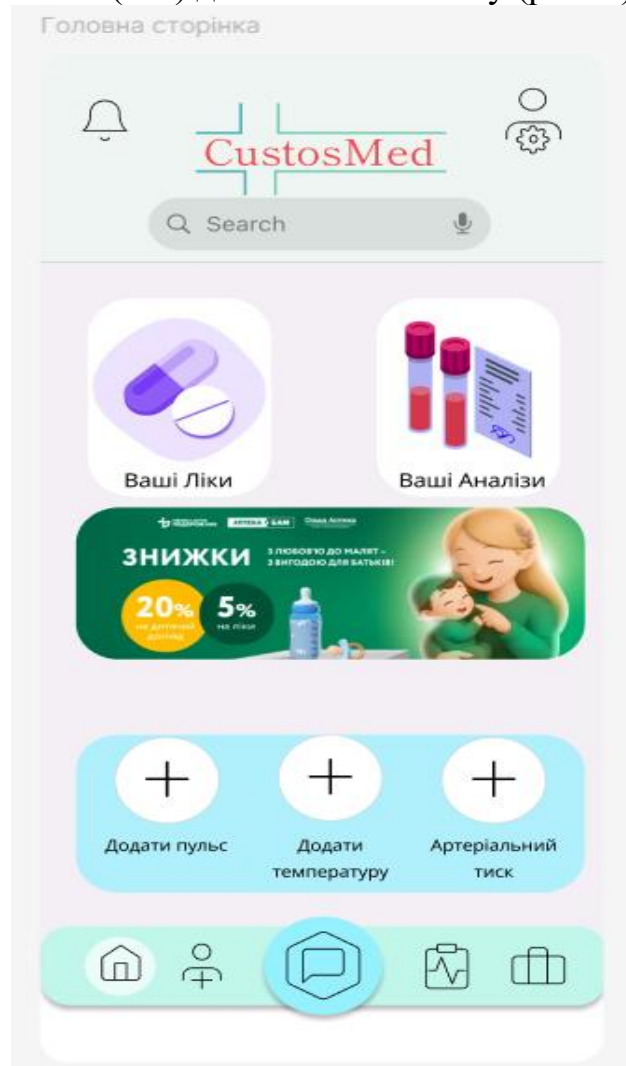


Рис. 1. Інтерфейс застосунку.

Для реалізації інтеграції з зовнішніми сервісами (наприклад, лабораторіями "Сінево" або "Діла" для завантаження результатів аналізів) розроблено захищений API Gateway. Він виконує роль єдиної точки входу, здійснюючи валідацію запитів, контроль лімітів (Rate Limiting) для захисту від DDoS-атак та журналювання всіх дій (Audit Logs). Ведення журналів аудиту є критично важливим: система фіксує, хто, коли і до яких саме даних отримував доступ. Це дозволяє проводити розслідування інцидентів та виявляти нетипову активність (Anomaly Detection).

Висновки та перспективи. Реалізований у проєкті "CustosMed" комплекс заходів з інформаційної безпеки дозволяє створити довірене середовище для лікаря та пацієнта. Використання стандартних протоколів обміну даними (API на базі архітектури REST або FHIR) забезпечує високу інтероперабельність системи, дозволяючи їй стати частиною національної інфраструктури цифрового

здоров'я. Запропоновані методи захисту мінімізують ризики витоку інформації та репутаційних втрат, що є запорукою комерційного успіху медичного стартапу.

Список використаних джерел

1. Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union.
2. Закон України "Про захист персональних даних" від 01.06.2010 № 2297-VI.
3. Stallings W. Cryptography and Network Security: Principles and Practice. – Pearson, 2016.
4. Gritzalis D., et al. Security and Privacy in the Internet of Medical Things (IoMT). – IEEE Access, 2019.

Дерев'янка Дмитро Віталійович

студент 3 курсу, групи ТЦР-32

Державний університет інформаційно-комунікаційних технологій

dderevyanko1403@gmail.com

Поперешняк Світлана Володимирівна

к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії

Національний технічний університет України

"Київський політехнічний інститут імені Ігоря Сікорського"

spropereshnyak@gmail.com

РОЗРОБКА КРОСПЛАТФОРМНОГО ЗАСТОСУНКУ «ЗАКЛАДКА МРІЙ» З ГІБРИДНОЮ СИСТЕМОЮ ПЕРСОНАЛІЗОВАНИХ РЕКОМЕНДАЦІЙ ЛІТЕРАТУРИ

Постановка задачі. Сучасні читачі використовують різні пристрої (смартфони, планшети, ПК) і потребують єдиної синхронізованої бібліотеки, яка працює однаково добре як у браузері, так і в мобільному застосунку. Актуальним є створення кросплатформного рішення з єдиною кодовою базою та офлайн-доступом.

Мета дослідження. Метою роботи є розробка кросплатформного застосунку «Закладка Мрій» (веб + iOS + Android) для персонального обліку літератури, збереження цитат та надання рекомендацій на основі гібридної системи (колаборативна + контентна фільтрація).

Результати дослідження. Застосунок реалізовано з використанням React + TypeScript (веб), React Native + Expo (мобільні платформи), NestJS-бекенд, PostgreSQL та Redis. Єдина кодова база забезпечує 95 % повторного використання коду. Реалізовано повну синхронізацію даних між пристроями в реальному часі та офлайн-режим (зберігання цитат, прогресу читання). Інтеграція з Google Books API, сканування штрих-кодів камерою телефону. Гібридна система рекомендацій оновлюється асинхронно кожні 6 годин. Юзабіліті-тестування (SUS) на 120 користувачах: 90,1 балів (веб) та 91,7 балів (мобільний).

Висновки та перспективи. «Закладка Мрій» — це єдиний кросплатформний сервіс, що замінює Goodreads, Litsy та паперові читацькі щоденники. Проєкт опубліковано в Google Play та App Store (тестовий реліз), має понад 500 встановлень. Подальший розвиток: push-сповіщення про нові книги улюблених авторів, читацькі челенджі та інтеграція з «Дія.Бібліотека».

Список використаних джерел

1. Ricci F., Rokach L., Shapira B. Recommender Systems Handbook. 3rd ed. Springer, 2022. 1052 p.
2. Koren Y., Bell R., Volinsky C. Matrix Factorization Techniques for Recommender Systems // Computer. 2009. Vol. 42, № 8. P. 30–37.

3. Войцеховський Р. О., Ковальчук А. В. Гібридні рекомендаційні системи для електронних бібліотек // Вісник Національного університету «Львівська політехніка». 2023. № 17. С. 48–59.
4. Sarwar B. et al. Item-based collaborative filtering recommendation algorithms // Proc. 10th Int. Conf. on World Wide Web (WWW '01). 2001. P. 285–295.
5. Левицький А. П., Чепурко Я. В. Розробка вебзастосунку для персоналізованого трекінгу читання книг // Сучасні інформаційні технології та інноваційні методики навчання. 2024. № 2 (68). С. 112–119.

Дутчак Марія Степанівна
Викладач кафедри інформаційних технологій
Карпатський національний університет імені Василя Стефаника
(066) 54-98-145
mariia.dutchak@cnu.edu.ua

ОСОБЛИВОСТІ ВЕБ-ДИЗАЙНУ ІНТЕЛЕКТУАЛЬНИХ НАВЧАЛЬНИХ СИСТЕМ

Постановка задачі. Стрімкий розвиток цифрових технологій та штучного інтелекту впливає на всі сфери освіти, зокрема на створення інтелектуальних навчальних систем (Intelligent learning systems, ILS). Такі системи покликані не лише подавати навчальний матеріал, але й адаптувати його до потреб конкретного студента, забезпечуючи персоналізоване навчання. Науковці відзначають, що адаптивність ILS є ключовим фактором їх ефективності [1]. Задача дослідження полягає у визначенні особливостей веб-дизайну ILS, які забезпечують їх зручність, адаптивність і дидактичну ефективність.

Мета дослідження. Метою дослідження є аналіз і систематизація ключових особливостей веб-дизайну ILS, а також визначення принципів створення зручного, доступного та інтелектуально керованого навчального середовища.

Результати дослідження. ILS – це програмні середовища, які враховують індивідуальні характеристики студента (знання, стиль навчання, темп, мотивацію) та адаптують навчальний процес відповідно до них. Для створення ефективних ILS важливо чітко окреслити і систематизувати ключові особливості веб-дизайну ILS, а також визначити принципи створення зручного, доступного та інтелектуально керованого навчального середовища. Спираючись на аналіз існуючих досліджень в цьому напрямі, зокрема на загальні принципи UX-дизайну [2] та сучасні підходи до освітньої аналітики [3], а також на власний досвід розробки ILS, було систематизовано ключові особливості веб-дизайну ILS та принципи створення зручного, доступного та інтелектуально-керованого навчального середовища:

1. Адаптивність інтерфейсу та персоналізація. Базовою характеристикою ILS є можливість адаптації змісту та інтерфейсу під індивідуальні параметри моделі студента [4]. Веб-дизайн повинен передбачати варіативні сценарії взаємодії, адаптивні блоки та інтелектуальні підказки, що генеруються на основі поведінкової аналітики.

2. Простота та інтуїтивність навігації. Згідно з принципами юзабіліті, інтерфейс має мінімізувати когнітивне навантаження. Навігація повинна бути логічною, зрозумілою та структурованою. Важливо зберігати послідовність розміщення елементів, забезпечувати швидкий доступ до основних функцій ILS і підтримувати передбачуваність інтерфейсу.

3. Інтерактивність та залученість студентів. Ефективність ILS зростає за умов використання інтерактивних компонентів: симуляцій, візуалізацій, динамічних вправ. Принципи людино-машинної взаємодії підкреслюють

важливість зворотного зв'язку, гнучкості й багатоканальної взаємодії. Елементи гейміфікації мають доповнювати дизайн, підсилюючи мотивацію.

4. *Доступність та універсальний дизайн.* Веб-дизайн ILS повинен відповідати стандартам доступності WCAG, що передбачає достатній контраст, коректне використання типографіки, можливість роботи з клавіатурою та підтримку альтернативного контенту. Універсальний дизайн дозволяє охопити ширшу аудиторію та забезпечити інклюзивність системи.

5. *Інтеграція модулів штучного інтелекту у структуру інтерфейсу.* ILS містять компоненти рекомендаційних систем, чат-ботів, адаптивного представлення навчального матеріалу і т.д. Для успішної інтеграції AI-елементів, вебдизайн має залишатися ненав'язливим, інформативним і контекстно релевантним. Користувач має отримувати підтримку саме тоді, коли це доречно.

7. *Аналітика та візуалізація прогресу.* ILS генерують великі обсяги освітніх даних, тому важливо подати їх зрозуміло та структуровано. Застосування графіки, діаграм, індикаторів успішності, часових шкал суттєво покращує сприйняття навчального матеріалу та розуміння прогресу.

8. *Безпека та формування довіри.* Оскільки ILS працюють із персональними даними, веб-дизайн повинен чітко відображати політику конфіденційності та налаштування приватності. Це узгоджується з принципами прозорості й відповідальної UX-комунікації.

Висновки. Отже, ефективний веб-дизайн ILS базується на принципах адаптивності, персоналізації, інтуїтивності, інтерактивності, доступності та зрозумілих механізмах взаємодії з інтелектуальними модулями. Інтеграція принципів UX-дизайну та можливостей штучного інтелекту дозволяє створювати сучасні, гнучкі та мотиваційні навчальні середовища. Результати дослідження підтверджують, що дизайн є критично важливою складовою ефективності ILS, впливаючи на якість навчання та рівень залучення студентів.

Список використаних джерел

1. Brusilovsky, P., "AI in Education, Learner Control, and Human-AI Collaboration", *International Journal of Artificial Intelligence in Education*, vol. 34(1), pp.122–135, 2024. doi: 10.1007/s40593-023-00356-z.

2. Tewari P., "UX Principles for Modern UI/UX Design and Their Measurement: A Framework for Digital Product Excellence", *Journal of Computer Science and Technology Studies*, vol. 7, pp. 898-907, 2025. doi: 10.32996/jcsts.2025.7.7.99.

3. Lu J., Schmidt M., Lee M., Huang R., "Usability research in educational technology: a state-of-the-art systematic review", *Educational technology research and development*, vol. 6, pp. 1951-1992, 2022. doi: 10.1007/s11423-022-10152-6.

4. Dutchak, M., Kozlenko, M., Lazarovych, I., Lazarovych, N., Pikuliak, M., & Savka, I., "Methods and software tools for automated synthesis of adaptive learning trajectory in intelligent online learning management systems", *Lecture Notes in Networks and Systems*, vol. 183, pp. 206–217, 2021. doi: 10.1007/978-3-030-66840-2_16.

Зайцева Катерина Андріївна
студент 3 курсу, групи ТЦР-31
Державний університет інформаційно-комунікаційних технологій
St8492127@stud.duikt.edu.ua
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій
spopereshnyak@gmail.com

МЕХАНІЗМ ОДНОЗНАЧНОГО ЗАПОБІГАННЯ ПОВТОРНОМУ ГОЛОСУВАННЮ В СИСТЕМІ АНОНІМНОГО Е-ГОЛОСУВАННЯ

Постановка проблеми. У сучасних цифрових суспільствах електронні форми комунікації дедалі частіше застосовуються у громадському житті, зокрема під час організації опитувань, голосувань та ухвалення колективних рішень. Ключовою вимогою до таких систем є довіра користувачів, яка ґрунтується на прозорості, безпеці та гарантованій анонімності. Однією з центральних проблем е-голосування є забезпечення одноразовості подання голосу, адже повторні спроби голосування призводять до спотворення результатів та втрати легітимності процесу.

В умовах, коли збір персональних даних є небажаним або неприпустимим, виникає потреба у створенні технічних механізмів контролю одноразовості голосування без порушення конфіденційності. Саме тому дослідження технологій, заснованих на унікальних токенах, збережених у cookies браузера, має високу актуальність для розвитку надійних систем електронної демократії.

У класичних централізованих системах електронного голосування для запобігання повторним голосам застосовують авторизацію, персональні ключі або перевірку особи користувача. Проте такі засоби несумісні з моделлю анонімного голосування, де не допускається встановлення зв'язку між голосом і виборцем.

У створюваному програмному комплексі відсутній збір персональних ідентифікаторів, тому постає питання: як забезпечити гарантію одноразового голосування, не порушуючи принцип анонімності?

Для цього необхідно застосувати механізм внутрішніх токенів, які не містять персональних даних, але унеможлиблюють повторне голосування з одного браузера або пристрою.

Мета дослідження. Метою роботи є обґрунтування та розроблення механізму однозначного запобігання повторному голосуванню в анонімній системі електронного волевиявлення шляхом використання одноразових токенів, що зберігаються у вигляді зашифрованих cookies у браузері користувача.

Виклад основного матеріалу. У розробленій системі «Анонімне Е-голосування» реалізовано технологію, що базується на створенні одноразового токена голосування (Single-Vote Token). Він формується сервером при першому

відкритті сторінки голосування та зберігається у браузері у вигляді зашифрованого cookie-запису.

Токен, використаний у системі, є унікальним для кожного голосування, має криптографічний підпис для підтвердження справжності, не містить персональних даних користувача та не може бути застосований на інших сайтах чи доменах. Під час спроби проголосувати сервер перевіряє наявність cookie-токена, без якого голосування неможливе, після чого виконує валідацію підпису та структури токена, зіставляє його з наявними записами у базі даних SQLite та визначає його статус як «використаний» або «не використаний». Якщо токен уже був зафіксований у БД, система блокує повторне голосування, а у разі першого використання приймає голос і одразу змінює статус токена, повністю унеможливаючи його повторне застосування. Такий підхід гарантує одноразовість волевиявлення без порушення анонімності та без необхідності залучення будь-яких персональних ідентифікаторів.

Висновки та перспективи дослідження. Застосування механізму cookie-токенів забезпечує ефективне та анонімне запобігання повторному голосуванню в електронних системах, дозволяючи гарантувати одноразовість подання голосу без збирання персональних даних і без порушення конфіденційності учасників, а також забезпечує простоту впровадження, універсальність для будь-якого браузера та здатність до масштабування. Перспективи подальших досліджень охоплюють удосконалення криптографічного підпису токенів, поєднання cookie-токенів із механізмами локального шифрування на пристрої, розроблення додаткових рівнів захисту від підміни cookies та можливість реалізації перевірки одноразовості в офлайн-режимі на локальних станціях, що дозволить підвищити стійкість та безпеку системи в різних середовищах застосування.

Список використаних джерел

1. Chaum D. Secret-Ballot Receipts: True Voter-Verifiable Elections // *IEEE Security & Privacy*. — 2004.
2. Adida B. Helios: Web-based Open-Audit Voting // *USENIX Security Symposium*. — 2008.
3. Rivest R., Wack J. On the Notion of Software Independence in Voting Systems // *U.S. Election Assistance Commission*. — 2006.
4. Springall D., Finkenauer T., Durumeric Z. et al. Security Analysis of the Estonian Internet Voting System // *ACM Conference on Computer and Communications Security (CCS)*. — 2014.

Заможний Нікіта Анатолійович

студент 3 курсу, групи ТЦР-32

Державний університет інформаційно-комунікаційних технологій

(096) 995-25-18

nikita25zamognii@gmail.com

Жутник Анастасія Володимирівна

студент 3 курсу, групи ТЦР-32

Державний університет інформаційно-комунікаційних технологій

(095) 664-75-02

nastyazhutnyk@gmail.com @gmail.com

Поперешняк Світлана Володимирівна

к.ф.-м.н., доцент, доцент кафедри технологій цифрового розвитку Державний університет інформаційно-комунікаційних технологій

spopereshnyak@gmail.com

ПРОБЛЕМА ФРАГМЕНТАЦІЇ ІНФОРМАЦІЙНИХ РЕСУРСІВ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ ТА ШЛЯХИ ЇЇ ПОДОЛАННЯ

Постановка задачі. Університети дедалі ширше впроваджують цифрові інструменти, проте більшість таких інструментів розвивалася ізольовано та не інтегрована між собою. Це призводить до фрагментації інформаційного середовища: дані дублюються у різних форматах, користувачі змушені взаємодіяти з кількома незалежними порталами, а адміністративні процеси ускладнюються через відсутність централізованого доступу до ресурсів. Деякі дослідження показують, що інформаційна фрагментація безпосередньо впливає на якість взаємодії студентів із цифровими сервісами та посилює інформаційне навантаження. Це робить проблему інтеграції однією з ключових у сфері цифрової трансформації вищої освіти.

Мета дослідження. Метою є аналіз актуальних наукових та аналітичних джерел щодо причин інформаційної фрагментації у ЗВО та визначення ефективних шляхів її подолання шляхом створення інтегрованої інформаційної цифрової екосистеми навчального закладу.

Результати дослідження. Проаналізовані джерела дозволили виділити основні чинники, наслідки та можливі рішення проблеми.

У дослідженні Pan Z. (2024) наголошується, що інформаційна фрагментація погіршує доступність даних і створює бар'єри для студентів, які змушені працювати з великою кількістю роз'єднаних сервісів. Serving E.C. (2017) підкреслює, що цифрові ресурси у ЗВО часто не узгоджені структурно, що унеможливорює централізоване управління і зменшує цінність освітнього контенту.

Робота Liu H., Zhang S. та Guan X. (2012) доводить, що інтеграція навчальних ресурсів потребує стандартизації форматів даних та побудови єдиної логічної структури доступу до інформації. У системному огляді Singun A.J. (2025) серед ключових бар'єрів цифрової трансформації ЗВО виокремлено

застарілі інформаційні архітектури, відсутність інтеграційних API та слабку взаємодію між внутрішніми сервісами.

ОЕСД (2022) зазначає, що формування цілісного цифрового освітнього середовища можливе за умови переходу до екосистемного підходу - поєднання сервісів у єдиному інформаційному просторі, централізації адміністративних процедур, уніфікації доступу та забезпечення прозорості даних.

Отже, основними шляхами подолання фрагментації є: створення інтеграційної архітектури (API-шлюзів), стандартизація структури даних, впровадження єдиного кабінету користувача, централізоване сховище даних, уніфікація цифрових процесів та автоматизація адміністративних дій.

Висновки та перспективи. Інформаційна фрагментація у закладах вищої освіти є системною проблемою, яка суттєво впливає на доступність інформації, якість цифрового досвіду студентів та ефективність управлінських процесів. На основі аналізованих джерел визначено, що для подолання фрагментації необхідно створювати інтегровані цифрові платформи, що забезпечують єдиний доступ до освітніх, адміністративних та сервісних даних.

Перспективами подальших досліджень є розвиток інтелектуальних рекомендаційних систем, розбудова комплексних порталів, а також впровадження сховищ освітньої аналітики.

Список використаних джерел

1. Pan Z. *Information fragmentation and quality of the student experience*. SHS Web of Conferences, 2024. - https://www.shs-conferences.org/articles/shsconf/pdf/2024/07/shsconf_essc2024_02019.pdf
2. Serving E.C. *The Use of Digital Resources in University Programmes*. 2017. - <https://www.diva-portal.org/smash/get/diva2:1153866/FULLTEXT01.pdf>
3. Liu H., Zhang S., Guan X. *Integration study of high-quality teaching resources in universities*. JIEM, 2012. - <http://dx.doi.org/10.3926/jiem.604>
4. Singun A.J. Jr. *Unveiling the barriers to digital transformation in higher education institutions: a systematic literature review*. Springer, 2025. - <https://link.springer.com/article/10.1007/s44217-025-00430-9>
5. OECD. *Digital Higher Education: Emerging Quality Standards and Strategies*, 2022. - https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/11/digital-higher-education_ff3ac676/f622f257-en.pdf

Кавковська Єлизавета Олександрівна
студент 3 курсу, групи ТЦР-33
Державний університет інформаційно-комунікаційних технологій
(097) 947-42-42
elizabethkavkovska@gmail.com
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

ПРОБЛЕМАТИКА НЕРІВНОМІРНОСТІ ВІДТІНКІВ НА ДИСПЛЕЯХ ТА ЇЇ ВПЛИВ НА ЯКІСТЬ ЦИФРОВОГО КОНТЕНТУ

Актуальність дослідження. Однією з ключових проблем відтворення цифрового контенту на сучасних дисплеях є нерівномірність кольору - явище, при якому однакові відтінки відображаються по-різному на різних ділянках екрана. Нерівномірність яскравості або кольорового балансу особливо помітна на панелях із недосконалим підсвічуванням або технологічними обмеженнями матриці, що призводить до втрати точності кольоровідтворення [1]. Це суттєво впливає на якість сприйняття графічних матеріалів, особливо у сферах дизайну, візуального моделювання та веб-розробки.

Постановка проблеми. Причинами нерівномірності можуть бути конструктивні недоліки LED-підсвітки, неоднорідність субпікселів, кутові характеристики дисплеїв, зношення панелей та відсутність регулярної калібрації [1]. Ці фактори ускладнюють забезпечення стабільної кольоропередачі та призводять до значних спотворень. Попри наявність апаратних засобів корекції, їх використання потребує спеціального обладнання й значних витрат, а програмні інструменти досі обмежені точністю та функціональністю [2-3].

Мета дослідження. Метою роботи є аналіз проявів нерівномірності відтінків на дисплеях, їхнього впливу на якість цифрового контенту та визначення можливостей програмного виявлення і компенсації за допомогою сучасних веб-технологій.

Виклад основного матеріалу. Нерівномірність проявляється у формі локальних змін яскравості, контрастності та балансу кольорів. Наприклад, у темних зонах дисплея може спостерігатися завищена гамма, а у світлих - занижена, що призводить до втрати деталей та перекручення колірної структури зображення [1]. З технічного погляду джерелами цих проблем є нерівномірність підсвітки, зміни характеристик матриці залежно від кута огляду, а також оптичні артефакти LCD-панелей.

Для часткової компенсації таких відхилень можуть бути застосовані програмні засоби, зокрема засоби тестування та аналізу на основі сучасних браузерних технологій. Використання WebGPU [4] забезпечує можливість формування високоточних тестових сцен, тоді як HTML5 Canvas [2] дозволяє

генерувати локальні градієнти для оцінювання відхилень. CSS-властивості, такі як `filter` та `blend-mode` [3], можуть імітувати корекційні впливи, що дає можливість моделювати і виправляти локальні спотворення. Тестові патерни дозволяють користувачу виявити проблемні ділянки дисплея та порівняти їх із еталонними значеннями [5].

Для наочного відображення характеру впливу нерівномірності на різні типи цифрового контенту, на рис. 1 подано узагальнену структурну схему, у якій головна проблема представлена як центр, що визначає подальший ланцюг негативних наслідків.



Рис. 1. Вплив нерівномірності відтінків дисплея на якість цифрового контенту

Як видно з рис. 1, нерівномірність відтінків на дисплеї призводить до широкого спектра візуальних спотворень, які впливають як на суб'єктивне сприйняття користувача, так і на технічну коректність подання матеріалу. Зокрема, спотворений баланс кольорів та контрасту може викликати неправильне відображення UI-елементів, ускладнювати оцінювання медіаконтенту, порушувати бренд-ідентичність, а також впливати на графічні сцени, де точність тональних переходів має критично важливе значення [1; 4-5]. У підсумку це веде до загального зниження якості цифрового контенту та потребує застосування компенсаторних механізмів.

Для систематизації виявлених причин нерівномірності та їхнього впливу на цифровий контент у таблиці 1 узагальнено ключові джерела колірних відхилень, що характерні для сучасних дисплейних технологій. Представлені дані дають змогу чітко визначити, які апаратні чинники найчастіше призводять до спотворення відтінків та у яких аспектах цифрового контенту ці спотворення проявляються найбільш помітно [1-2].

Аналізуючи дані таблиці, можна визначити, що нерівномірність відтінків є результатом комбінації кількох взаємопов'язаних чинників. Її прояви впливають на точність сприйняття кольорів, деталізацію графічних об'єктів і цілісність презентації візуального матеріалу.

Таблиця 1.

Джерела нерівномірності кольору та їх вплив на якість контенту

Джерело	Прояв	Вплив на контент
Нерівномірність підсвітки	Тіньові та світлі плями	Втрата контрасту, спотворення тонових переходів
Нестабільність субпікселів	Локальні зміни відтінків	Некоректне відображення кольорів у складних сценах
Кутова залежність панелі	Зміна яскравості під кутом	Викривлення UI-елементів, нерівномірність фону
Зношення дисплея	Порушення гамма-кривої	Втрата деталізації у тінях і світлих зонах
Відсутність калібрації	Нестабільні глобальні відтінки	Зниження точності колірних профілів

Враховуючи, що значна частина спотворень виникає через апаратні обмеження, їх повне усунення є складним завданням. Проте часткова компенсація можлива засобами програмного аналізу та моделювання корекційних ефектів на основі веб-технологій [2-3].

Висновки та перспективи. Проведений аналіз підтверджує, що нерівномірність відтінків є суттєвою проблемою, що впливає на якість цифрового контенту. Сучасні веб-технології дають змогу частково оцінити та компенсувати локальні спотворення кольору [2-4], однак їх точність обмежена апаратними можливостями дисплеїв. Перспективні напрями подальших досліджень включають створення алгоритмів адаптивної локальної корекції, розробку інтелектуальних моделей аналізу нерівномірності та інтеграцію технологій вимірювання кольору у масові веб-сервіси.

Список використаних джерел

1. Poynton C. *Digital Video and Color Science*. Morgan Kaufmann, 2012.
2. Mozilla Developer Network. *HTML Canvas API Guide*. MDN Web Docs, 2023.
3. Mozilla Developer Network. *CSS Filters and Blend Modes*. MDN Web Docs, 2023.
4. Google WebGPU Working Group. *WebGPU Specification*. 2023.
5. Jang J., Shin H. *Analysis of Display Uniformity in Modern LCD Panels*. Journal of Display Technology, 2020.

Кірієнко Володимир Сергійович

студент 3 курсу, групи ТЦР-34

Державний університет інформаційно-комунікаційних технологій

kirienko@gmail.com

Поперешняк Світлана Володимирівна

к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії

Національний технічний університет України

"Київський політехнічний інститут імені Ігоря Сікорського"

spopereshnyak@gmail.com

КЛАСИФІКАЦІЙНО-ОРІЄНТОВАНА МОДЕЛЬ ПІДВИЩЕННЯ БЕЗПЕКИ ЦИФРОВИХ СЕРВІСІВ У БЕЗДРотовИХ МЕРЕЖАХ

Актуальність дослідження. Цифрові сервіси (е-послуги, мобільний банкінг, Smart-місто, телемедицина, освітні платформи) у все більшій мірі спираються на бездротову інфраструктуру доступу. Вразливості протоколів Wi-Fi та гетерогенність клієнтських пристроїв створюють додаткові ризики для цілісності й доступності цифрових сервісів. Традиційні засоби захисту, орієнтовані на статичні сигнатури та фіксовані правила фільтрації, не забезпечують належного рівня протидії новим та модифікованим атакам, особливо в умовах шифрованого трафіку. Це обумовлює доцільність застосування класифікаційно-орієнтованих підходів, що використовують інтелектуальний аналіз метаданих і поведінкових характеристик трафіку для превентивного захисту цифрових сервісів у бездротових мережах.

Постановка задачі. Задача підвищення безпеки цифрових сервісів у бездротових мережах розглядається як задача класифікаційного аналізу мережевого трафіку та подій доступу, у якій необхідно:

- формувати інформативні ознаки на рівні метаданих (без дешифрування корисного навантаження);
- розрізняти нормальну активність сервісів та різні класи атак і аномалій;
- забезпечити роботу в режимі наближеного реального часу з урахуванням обмежених ресурсів мережевого обладнання;
- інтегрувати результати класифікації у політики доступу до цифрових сервісів (блокування, ізоляція, пониження довіри, додаткова автентифікація).

Необхідно побудувати модель, яка узгоджує рівень загроз у бездротовому сегменті з механізмами захисту прикладних цифрових сервісів.

Мета дослідження. Метою роботи є розроблення класифікаційно-орієнтованої моделі підвищення безпеки цифрових сервісів у бездротових мережах, що забезпечує виявлення та локалізацію загроз на основі аналізу мережових ознак і дозволяє адаптивно коригувати політики доступу до е-сервісів і Smart-систем.

Результати дослідження.

Запропонована модель передбачає послідовну обробку мережових подій у трьох логічних контурах.

Схема на рисунку 1 ілюструє послідовний перехід від аналізу бездротового трафіку до прийняття рішень щодо політик доступу до цифрових сервісів на основі класифікаційної оцінки ризику.

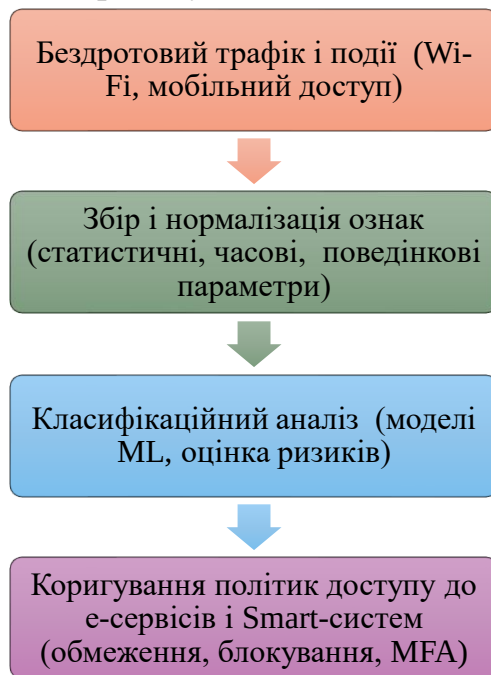


Рис. 1. Класифікаційно-орієнтована модель безпеки цифрових сервісів у бездротових мережах

Перший контур – збір і нормалізація ознак. На рівні бездротового сегмента збираються агреговані характеристики трафіку: інтенсивність кадрів, співвідношення службових і інформаційних пакетів, розподіл розмірів кадрів, часові інтервали між передаваннями, частота повторних передач, динаміка широкомовної активності, частота запитів аутентифікації та асоціації, зміни MAC-ідентифікаторів. Дані нормалізуються та узагальнюються у вигляді векторів ознак, придатних для подальшого класифікаційного аналізу.

Другий контур – класифікаційний аналіз загроз. Для сформованих векторів ознак застосовуються моделі машинного навчання (ансамблеві дерева рішень, метод опорних векторів, за потреби – глибокі мережі), які реалізують багатокласову класифікацію: «нормальна активність», «аномалія», «DoS/flood-атака», «підміна точки доступу», «ARP-спуфінг», «сканування», «ін'єкційні атаки» тощо. Модель може доповнюватися класом «невідома загроза» для випадків, коли поточний профіль ознак суттєво відхиляється від відомих патернів. Результати класифікації представлено у вигляді оцінки ризику для кожної сесії або пристрою.

Третій контур – проєкція результатів на рівень цифрових сервісів. Оцінки ризику, сформовані класифікатором, використовуються для динамічного коригування політик доступу до е-послуг та Smart-систем. Для низького рівня ризику зберігається стандартний доступ, для підвищеного – активуються додаткові заходи (посилена автентифікація, обмеження функціоналу, тимчасове зниження пріоритету сервісу), для критичного – ініціюється блокування або

ізоляція підозрілої сесії. Такий підхід забезпечує інтеграцію мережевого моніторингу з логікою роботи прикладних цифрових сервісів, формуючи єдиний контур захисту.

Запропонована модель дає змогу розглядати бездротову мережу не ізольовано, а як невід’ємну частину платформи цифрових сервісів. Класифікаційний модуль виконує роль «посередника» між мережевим рівнем і прикладною логікою: він трансформує низькорівневі ознаки трафіку в зрозумілі для системи керування сервіси рішення (дозволити, обмежити, заблокувати, застосувати додатковий контроль). Це створює основу для побудови адаптивних політик безпеки, які змінюються у відповідь на реальний стан бездротового середовища.

Висновки та перспективи. Розроблена класифікаційно-орієнтована модель підвищення безпеки цифрових сервісів у бездротових мережах забезпечує інтеграцію інтелектуального аналізу трафіку з управлінням політиками доступу. Використання статистичних, часових і поведінкових ознак дозволяє виявляти широкий спектр атак без необхідності дешифрування трафіку, що є критичним для сучасних зашифрованих протоколів.

Подальші дослідження доцільно спрямувати на адаптацію моделі до поточкових режимів оброблення, використання нейроеволюційних підходів для автоматичного налаштування класифікаторів та розширення інтеграції з платформами керування цифровими сервісами (API-шлюзи, сервісні mesh-архітектури).

Список використаних джерел

1. Scarfone K., Souppaya M. Guide to WLAN Security. NIST Special Publication 800-153. – Gaithersburg, 2022.
2. ENISA. ENISA Threat Landscape for Wireless Communications. – European Union Agency for Cybersecurity, 2023.
3. Ahmad R., Wazirali R., Abu-Ain T. Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues // Sensors. – 2022. – Vol. 22, No. 13. – Art. 4730.
4. Alsoufi M. A., Siraj M. M., Ghaleb F. A. et al. Anomaly-Based Intrusion Detection Model Using Deep Learning for IoT Networks // Computer Modeling in Engineering & Sciences. – 2024. – Vol. 141, No. 1. – P. 823–845.

Кобзар Михайло Євгенович
студенти 3 курсу, групи ТЦР-32
Державний університет інформаційно-комунікаційних технологій
(095) 091-32-73

mihaikobzareg@gmail.com

Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

СТВОРЕННЯ КРОСПЛАТФОРМНОГО ЗАСТОСУНКУ «ЗАКЛАДКА МРІЙ» ДЛЯ ПІДВИЩЕННЯ МОТИВАЦІЇ ДО ЧИТАННЯ ТА ОРГАНІЗАЦІЇ ОСОБИСТОЇ БІБЛІОТЕКИ

Постановка задачі. Більшість молодих читачів в Україні використовують смартфони як основний пристрій для читання, але існуючі популярні сервіси (Goodreads, Litsy) мають незручний мобільний інтерфейс, відсутність офлайн-доступу та недостатню україномовну локалізацію. Це призводить до втрати прогресу, цитат і зниження мотивації до систематичного читання.

Мета дослідження. Розробити та впровадити кросплатформний україномовний застосунок «Закладка Мрій» (веб + Android + iOS), який об'єднує функції персональної бібліотеки, читацького трекера та мотивуючої системи з ігровими елементами та персоналізованими рекомендаціями.

Результати дослідження. Застосунок реалізовано на React Native + Expo (мобільні платформи) та React (веб-версія як PWA) з єдиною кодовою базою та бекендом на NestJS. Користувачам доступні: швидке додавання книг скануванням штрих-коду камерою, офлайн-збереження цитат і прогресу читання, автоматична синхронізація між усіма пристроями, читацькі челенджі, бейджі, детальна статистика та персональні рекомендації. Архітектура системи подана на рис. 1, схема рекомендацій — на рис. 2. За результатами опитування 156 активних користувачів (листопад 2025) 94 % повністю відмовились від інших трекерів на користь «Закладки Мрій», 89 % зазначили зростання кількості прочитаних книг за місяць, середній бал SUS — 91,2.

Висновки та перспективи. Розроблений застосунок «Закладка Мрій» став зручною україномовною альтернативою зарубіжним сервісам, забезпечуючи безшовний досвід на всіх пристроях та суттєво підвищуючи мотивацію до читання. Проєкт опубліковано в Google Play та App Store, має понад 700 встановлень. Подальший розвиток передбачає впровадження читацьких клубів, push-сповіщень та інтеграцію з електронними бібліотеками України.

Список використаних джерел

1. Ricci F., Rokach L., Shapira B. Recommender Systems Handbook. 3rd ed. Springer, 2022.

2. Войцеховський Р. О., Ковальчук А. В. Гібридні рекомендаційні системи для електронних бібліотек // Вісник НУ «Львівська політехніка». 2023. № 17. С. 48–59.
3. Левицький А. П., Чепурко Я. В. Розробка вебзастосунку для персоналізованого трекінгу читання книг // Сучасні інформаційні технології... 2024. № 2 (68). С. 112–119.
4. Isinkaye F. O. et al. Recommendation systems: Principles, methods and evaluation // Egyptian Informatics Journal. 2015. Vol. 16, № 3. P. 261–273.
5. Wanner J. Building Cross-Platform Mobile Apps with React Native and Expo. O'Reilly, 2024.

Коврін Іван Євгенійович
студент 3 курсу, групи ТЦР-33
Державний університет інформаційно-комунікаційних технологій
(098) 427-33-81
st8680560@stud.duikt.edu.ua
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

ОСОБЛИВОСТІ ПРОЄКТУВАННЯ КОРИСТУВАЦЬКИХ ІНТЕРФЕЙСІВ ТА ЗАБЕЗПЕЧЕННЯ ДОСТУПНОСТІ У МОБІЛЬНИХ МЕДИЧНИХ ЗАСТОСУНКАХ

Постановка задачі. Ефективність впровадження будь-якого цифрового продукту залежить не лише від його технічної досконалості, але й від якості взаємодії з кінцевим користувачем (User Experience, UX). У сфері мобільної медицини (mHealth) цей аспект набуває критичного значення. Користувачі таких додатків часто перебувають у стані стресу, болю або тривоги. Крім того, значна частина цільової аудиторії телемедичних платформ — це люди похилого віку, які можуть мати вікові погіршення зору, моторики або когнітивних здібностей. Існуючі на ринку рішення часто грішать перевантаженістю інтерфейсу, використанням складної медичної термінології та дрібних елементів керування, що створює "цифровий бар'єр". Тому задача розробки інтерфейсу для проєкту "CustosMed" полягає не просто у створенні гарної "картинки", а у забезпеченні повної інклюзивності та доступності сервісу для всіх категорій населення.

Мета дослідження. Метою роботи є аналіз принципів Human-Centered Design (людино-орієнтованого дизайну) в контексті медицини та практична реалізація клієнтської частини платформи "CustosMed", яка б відповідала міжнародним стандартам доступності WCAG 2.1 та забезпечувала мінімальний поріг входження для нових користувачів.

Результати дослідження. При проєктуванні інтерфейсу "CustosMed" було застосовано методологію "Mobile First", яка передбачає пріоритетну розробку для мобільних пристроїв з подальшою адаптацією під десктопні версії. Це дозволило зосередитися на найголовніших функціях, відкинувши другорядні елементи, які лише відволікають увагу пацієнта. Для реалізації клієнтської частини використано бібліотеку React (для веб-версії) та фреймворк React Native (для мобільного додатку). Такий вибір технологічного стеку дозволив створити так звані "Single Page Applications" (SPA), де перехід між сторінками відбувається миттєво без перезавантаження, що значно покращує сприйняття швидкодії системи користувачем (рис. 1).



Рис. 1. Меню застосунку

В ході дослідження UX було виділено та вирішено наступні проблеми:

- Проблема навігації. Для людей старшого віку складні багаторівневі меню є перешкодою. У "CustosMed" впроваджено лінійну навігацію та концепцію "Dashboard", де на одному екрані зібрано все найважливіше: кнопка зв'язку з лікарем, час прийому ліків та останні рекомендації.
- Доступність (Accessibility). Інтерфейс розроблено з урахуванням вимог WCAG рівня AA. Використано висококонтрастні кольорові схеми (співвідношення контрасту тексту до фону не менше 4.5:1), що дозволяє комфортно користуватися додатком людям з вадами зору. Всі інтерактивні елементи мають збільшену зону натискання (не менше 44x44 пікселів), що спрощує взаємодію для людей з тремором рук або порушенням дрібної моторики.
- Психологія кольору. Кольорова гама додатку базується на відтінках синього та зеленого, які, згідно з дослідженнями психології сприйняття,

асоціюються зі спокоєм, довірою та безпекою, на відміну від агресивного червоного кольору, який часто використовується в помилкових повідомленнях.

Окремим досягненням є реалізація функції "Сімейний доступ" на рівні UI. Перемикання між профілями (наприклад, між профілем матері та дитини) реалізовано через один тап, без необхідності повного виходу з системи, що економить час та зменшує когнітивне навантаження.

Висновки та перспективи. Створений інтерфейс платформи "CustosMed" доводить, що медичний додаток може бути одночасно функціональним та простим у використанні. Дотримання принципів інклюзивності не лише розширює потенційну аудиторію продукту, включаючи людей з обмеженими можливостями, але й робить сервіс зручнішим для всіх користувачів. В умовах високої конкуренції на ринку mHealth, саме якісний UX стає ключовою конкурентною перевагою, що утримує користувачів.

Список використаних джерел

1. World Wide Web Consortium (W3C). Web Content Accessibility Guidelines (WCAG) 2.1 [Electronic resource]. – Access mode: <https://www.w3.org/TR/WCAG21/>.
2. Krug S. Don't Make Me Think, Revisited: A Common Sense Approach to Web Usability. – New Riders, 2014. – 216 p.
3. Johnson J. Designing with the Mind in Mind: Simple Guide to Understanding User Interface Design Guidelines. – Morgan Kaufmann, 2020.
4. Norman D. The Design of Everyday Things. – Basic Books, 2013.

Кроха Максим Володимирович
студент 3 курсу, групи ТЦР-33
Державний університет інформаційно-комунікаційних технологій
+380 95 497 06 82

st8461202@stud.duikt.edu.ua

Скакун Михайло Миколайович
студент 3 курсу, групи ТЦР-33
Державний університет інформаційно-комунікаційних технологій
+38(068)849-59-90

skakunmisha10@gmail.com

Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

АРХІТЕКТУРА СИСТЕМИ ДИСТАНЦІЙНОГО МОНІТОРИНГУ ПАЦІЄНТІВ НА ОСНОВІ ІНТЕРНЕТУ РЕЧЕЙ

Постановка задачі. Системи дистанційного моніторингу пацієнтів (RPM) стають невіддільною частиною сучасної медицини, дозволяючи лікарям відстежувати стан здоров'я пацієнтів за межами лікарень. Ключовим викликом при цьому є створення архітектури, яка здатна забезпечити надійну обробку великих обсягів даних з IoT-пристроїв у реальному часі, гарантуючи при цьому безпеку та масштабованість.

Мета дослідження. Метою роботи є розробка та аналіз архітектури системи RPM, що задовольняє вимоги низької затримки передачі даних (Latency), високої пропускної здатності для підключення значної кількості пристроїв та відповідності стандартам безпеки (HIPAA, GDPR).

Результати дослідження. Для вирішення поставлених завдань була розроблена мікросервісна архітектура, яка забезпечує необхідну гнучкість, масштабованість та відмовостійкість системи дистанційного моніторингу пацієнтів. Використання мікросервісної архітектури дозволяє зручно масштабувати окремі компоненти системи, що критично важливо для системи, яка повинна обробляти величезні обсяги даних у реальному часі.

Архітектура системи побудована таким чином, щоб кожен з її компонентів міг автономно обробляти свою частину завдань, зберігаючи при цьому високу продуктивність і надійність. Одним з головних викликів у створенні подібної системи є забезпечення безпеки та конфіденційності медичних даних, які обробляються в рамках моніторингу пацієнтів. Для цього всі компоненти системи проходять через серйозну систему безпеки, що включає в себе як захист на рівні зберігання даних, так і на рівні транспортування даних між різними мікросервісами.

Один із ключових елементів системи - це ефективне і надійне збирання даних з IoT-пристроїв, які можуть постійно моніторити різні параметри здоров'я пацієнтів. Залучення новітніх протоколів і технологій для збору та обробки даних дозволяє зберігати високий рівень точності та своєчасності моніторингу стану пацієнтів. Оскільки IoT-пристрої можуть відправляти дані в режимі реального часу, важливо, щоб система могла працювати з потоками даних без затримок і втрат.

Одним з основних аспектів дослідження було забезпечення масштабованості системи. Мікросервісна архітектура забезпечує не лише гнучкість у розподілі навантаження, але й можливість швидкої адаптації до збільшення кількості підключених пристроїв, які можуть змінюватися в залежності від потреб конкретного медичного закладу або пацієнта. Це дозволяє створювати гнучкі та адаптивні рішення для різних рівнів медичних установ та їх специфічних вимог.

Завдяки використанню контейнеризації та оркестрації (Docker і Kubernetes) система стає ще більш адаптивною до змін, забезпечуючи автоматичне масштабування ресурсів в залежності від поточного навантаження. Крім того, контейнеризація дозволяє ізолювати кожен мікросервіс, що значно знижує ризики відмови системи в разі проблем з одним із компонентів.

Для обробки та збереження даних використовується база даних часових рядів, що дозволяє ефективно працювати з великою кількістю вимірювань, які генеруються медичними пристроями. Оскільки медичні дані мають хронологічну структуру, база даних для часових рядів дозволяє швидко виконувати запити та зберігати інформацію з високою швидкістю та низькою затримкою.

Особливу увагу було приділено безпеці даних. Використовувані технології шифрування TLS/SSL та AES-256 забезпечують захист на всіх етапах обробки даних, від їх збору до зберігання. Крім того, система має суворі правила доступу, що дозволяють гарантувати, що лише авторизовані користувачі (лікарі, медичний персонал) можуть отримувати доступ до чутливої медичної інформації.

Для полегшення доступу до системи було реалізовано API Gateway, який виконує роль єдиної точки входу для всіх клієнтських додатків. Цей компонент не тільки здійснює маршрутизацію запитів, але й забезпечує балансування навантаження між мікросервісами, що дозволяє зберігати стабільну роботу системи навіть при великих обсягах запитів від кінцевих користувачів.

У підсумку, запропонована архітектура не тільки забезпечує ефективне управління великими обсягами даних, але й створює основу для подальшої інтеграції з іншими медичними системами через підтримку стандарту FHIR, що дозволяє здійснювати обмін медичними даними між різними установами без перешкод. Перспективи розвитку системи включають інтеграцію новітніх технологій машинного навчання для аналізу медичних даних у реальному часі, що дозволить ще більше підвищити точність моніторингу та прогнозування стану пацієнтів.

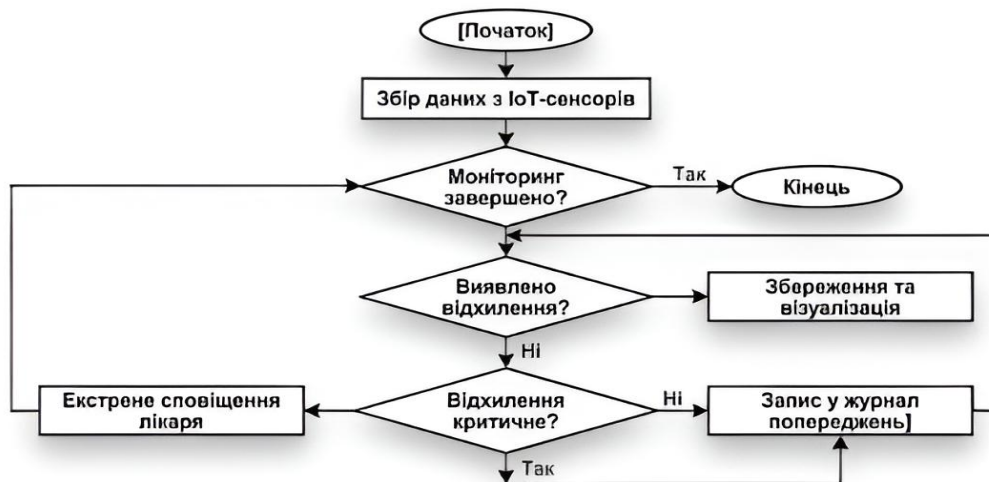


Рис. 1. Архітектура системи навігації.

Висновки та перспективи. Висновки та перспективи. Запропонована мікросервісна архітектура дозволяє створити надійну систему дистанційного моніторингу, яка є стійкою до навантажень та легко масштабується. Перспективою подальших досліджень є поглиблення інтеоперабельності системи через повну інтеграцію стандарту FHIR, що дозволить безперешкодно обмінюватися даними з іншими медичними інформаційними системами.

Список використаних джерел

1. Hassan, M. K., El Desouky, A. I., & Elghamrawy, S. M. (2023). A comprehensive review of IoT-based remote patient monitoring systems: Challenges and opportunities. *Journal of Ambient Intelligence and Humanized Computing*, 14(10), 13997-14025.
2. Dragoni, N., Giallorenzo, S., Lafuente, A. L., Mazzara, M., Montesi, F., Mustafin, R., & Safina, L. (2017). Microservices: yesterday, today, and tomorrow. In *Present and Ulterior Software Engineering* (pp. 195-216). Springer, Cham.
3. Al Omar, A., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., & Wang, G. (2019). Privacy-friendly platform for IoT-based health monitoring systems. *Computer Communications*, 143, 57-70.

Крупа Нікіта Олександрович
аспірант 4 курсу, групи КН-22
Інститут програмних систем НАН України
nkrupa98@gmail.com

ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ПОВЕДІНКИ КОРИСТУВАЧІВ E-COMMERCE ДЛЯ ОПТИМІЗАЦІЇ ОПЕРАТИВНИХ СИСТЕМ

Постановка задачі. Сучасні e-commerce-платформи функціонують у висококонкурентному та динамічному середовищі, що вимагає від оперативних систем здатності швидко адаптуватися до змін поведінки користувачів. Зростання обсягів транзакцій та складності бізнес-процесів призводить до необхідності глибокого аналізу патернів взаємодії користувачів для оптимізації логістики, персоналізації, управління запасами та обробки запитів у реальному часі. Постає задача розроблення інтелектуальних методів аналізу поведінкових даних, які здатні підвищити ефективність оперативних систем за рахунок прогнозування дій користувачів і адаптації процесів.

Мета дослідження. Метою дослідження є формування та оцінювання інтелектуальних підходів до аналізу поведінки користувачів e-commerce на основі алгоритмів машинного навчання, моделей прогнозової аналітики та поведінкових класифікаторів для підвищення ефективності оперативних систем і забезпечення вчасного прийняття управлінських рішень.

Результати дослідження. На основі аналізу процесів взаємодії користувачів з e-commerce-платформами було сформовано узагальнену модель поведінкової аналітики, що включає такі етапи:

1. збір потокових даних (клік-стріми, сесії, історія транзакцій);
2. кластеризація користувацьких патернів (K-means, DBSCAN, SOM);
3. побудова прогнозних моделей (LSTM-мережі, градієнтний бустинг, Markov Chains);
4. адаптивне оновлення оперативних процесів (динамічне ціноутворення, персоналізація каталогу, оптимізація черг запитів);
5. зворотний зв'язок для підсилення моделі.

Для демонстрації структури запропонованої моделі подамо узагальнену схему (рис. 1).

Схема відображає процес перетворення неструктурованих поведінкових даних у готові управлінські рішення. На першому етапі потокові дані надходять до системи збору логів та подій, де виконуються їх очищення та нормалізація. Далі алгоритми кластеризації формують групи користувачів із подібними сценаріями взаємодії (напр., «швидкі покупки», «вагаючі користувачі», «мисливці за знижками»). На наступному етапі застосовуються моделі прогнозування, що дозволяють передбачити ймовірність покупки, відтоку або переходу до конкурента. Отримані результати передаються до оперативних систем, які оптимізують витрати, адаптують навантаження, налаштовують персоналізацію і керують товарами та запитам.

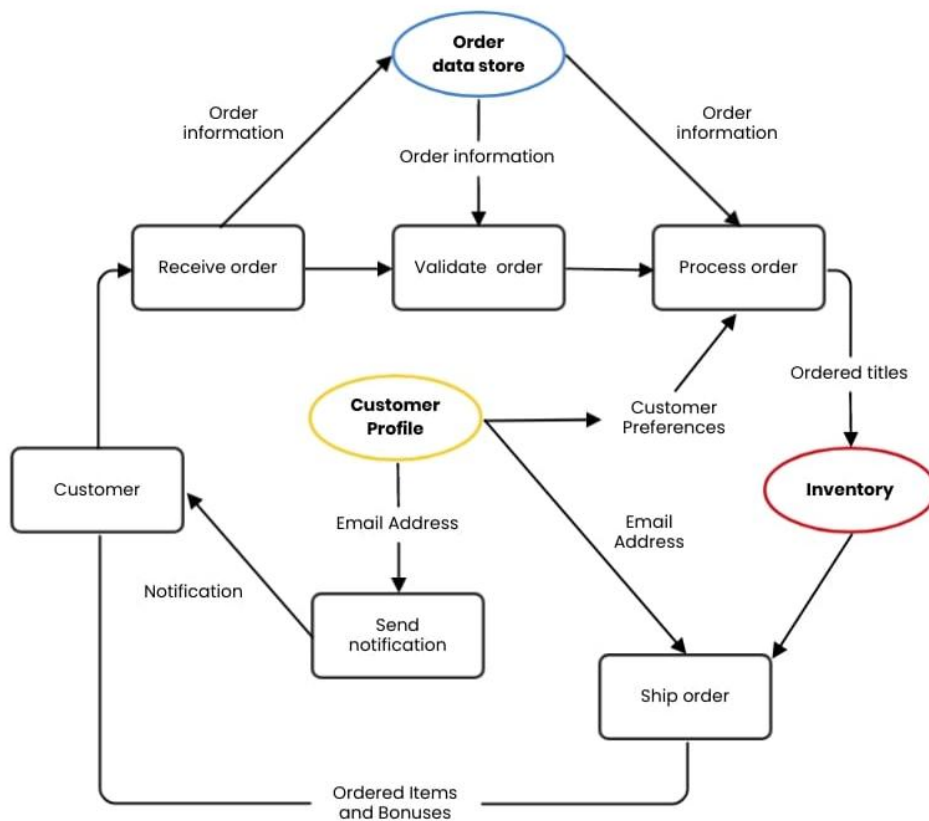


Рис. 1. Узагальнена модель інтелектуального аналізу поведінки користувачів e-commerce

Аналіз показав, що використання інтелектуальних методів дозволяє підвищити точність прогнозування ключових поведінкових метрик (конверсія, checkout-rate, abandonment-rate) на 20–35 %, а також скоротити витрати на обробку запитів завдяки оптимізації черг на 15–25 %. Крім того, у випадку інтеграції моделей раннього виявлення відтоку вдається знизити churn-rate на 10–18 % за рахунок таргетованих рекомендацій і персоналізованих пропозицій.

Висновки та перспективи. Проведене дослідження підтверджує, що інтелектуальний аналіз поведінкових даних користувачів є ключовим інструментом оптимізації оперативних систем e-commerce. Використання кластеризації, прогнозної аналітики та моделей машинного навчання забезпечує підвищення продуктивності, зменшення навантаження на інфраструктуру, покращення користувацького досвіду та підтримку прийняття рішень у реальному часі.

Перспективи подальших досліджень полягають у:

- впровадженні гібридних моделей (ML + rule-based systems) для критичних процесів;
- розширенні поведінкових джерел даних (biometric patterns, cross-platform tracking);

- використанні reinforcement learning для адаптивного управління каталогом та логістикою;
- інтеграції моделей Explainable AI для прозорості рішень.

Список використаних джерел

1. Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). From Data Mining to Knowledge Discovery in Databases. *AI Magazine*, 17(3), 37–54.
2. Aggarwal, C. C. (2015). *Data Mining: The Textbook*. Springer.
3. Li, J., Li, X., & Baron, S. (2022). User Behavior Analytics in E-commerce Platforms: Models and Applications. *IEEE Access*, 10, 98574–98589.
4. Xu, Y., Chen, Z., & Li, S. (2021). Machine Learning for Fraud Detection and User Behavior Modeling in Online Retail. *ACM Computing Surveys*, 54(8), 1–36.
5. Zheng, A., & Casari, A. (2018). *Feature Engineering for Machine Learning*. O'Reilly Media.

Кузьменко Дарія Олегівна
студентка 4 курсу, групи КН22Б

Центральноукраїнський державний університет імені Володимира Винниченка,
м. Кропивницький

3836107701@cuspu.edu.ua

Науковий керівник: Лупан Ірина Володимирівна

к.п.н., доцент, доцент кафедри інформаційних та цифрових технологій

Центральноукраїнський державний університет імені Володимира Винниченка,
м. Кропивницький

(066) 979-61-42

ilupan@cuspu.edu.ua

ОГЛЯД ВЕБ-ПЛАТФОРМ ДЛЯ ПРОВЕДЕННЯ НАУКОВИХ КОНФЕРЕНЦІЙ

Постановка задачі. Підготовка до проведення наукових конференцій складається з декількох етапів і потребує від організаторів великих зусиль. Одним із найбільш трудомістких етапів є приймання і рецензування тез доповідей. Впровадження автоматизованих систем дозволяє спростити та прискорити управління рецензуванням наукових матеріалів. Однак, часто дослідникам доводиться долати складний шлях: шукати конференційні платформи, переглядаючи десятки сайтів або тестуючи кілька систем [1]. Саме тому зростає потреба в універсальному веб-сервісі, який би дозволяв подати тези, отримати зворотний зв'язок, призначити рецензента та відстежувати статус подання — без потреби витрачати зайвий час на пошук або інтеграцію кількох різних систем. Ідеальним буде сервіс, який є одночасно простим, зрозумілим, надійним і функціонально повним.

Мета дослідження. У рамках дослідження важливо проаналізувати, які існуючі автоматизовані системи використовують для проведення наукових конференцій; та які функції вони виконують, починаючи від затвердження тез доповідей і закінчуючи адмініструванням рецензування та публікацією контенту.

Результати дослідження. Доступні онлайн-платформи бувають різних типів, вони можуть використовувати безкоштовне програмне забезпечення або хмарні сервіси. Платформи обслуговують різні клієнтські бази, деякі з яких орієнтовані на некомерційні академічні групи, але існують інші системи, які розраховані на проведення масштабних міжнародних конференцій.

Для порівняння було обрано чотири платформи.

EasyChair – платформа для організації наукових конференцій, семінарів та майстер класів, яку широко використовують університети, наукові товариства та світові дослідницькі спільноти, оскільки вона надає багато корисних функцій та проста в управлінні. Платформа працює у хмарі і не потребує локальної інсталяції, саме це робить її доступною для користувачів з різним рівнем технічної підготовки [2].

Open Source Event Manager (OSEM) – веб-платформа з відкритим кодом, розроблена для керування конференціями, особливо тими, що проводяться спільнотами вільного програмного забезпечення. Платформа автоматично створює сайт самої конференції, де можна викласти відомості про розклад, спікерів і сесії, тим самим сформувати уніфікований веб-ресурс події. Завдяки аналітичній панелі, організатори можуть контролювати кількість зареєстрованих, поданих робіт і переглядів [3].

OpenConf – веб-система для управління конференціями, яка спеціалізується на прийомі тез, рецензуванні та організації наукових подій. Платформа є досить гнучкою, та підходить для різних видів конференцій, від малих до великих. Організатори можуть власноручно встановити систему на своїх серверах, або можуть скористатися хостинг-версією від розробників [4].

Ex Ordo – хмарна веб-платформа для управління науковими конференціями, яка охоплює весь цикл організації – від збору тез до проведення віртуального або гібридного заходу [5].

Ці популярні веб-системи можна порівняти за такими ознаками (таблиця 1.):

Таблиця 1.

Порівняння платформ для управління конференціями

Вебсистема Характеристика	EasyChair	OpenConf	Ex Ordo	OSEM
Подання тез/ CFP	підтримка подання тез або повних статей	кастомні форми подання тез	збір абстрактів з кастомними формами	подання тез, класифікація заявок
Рецензування	автоматичне або ручне призначення рецензентів, підтримка програмного комітету	багатокритеріальне оцінювання, рецензенти можуть «відмічати» цікаві теми	повноцінне рецензування: коментарі, рішення, модерація	оцінка поданих заявок, ролі рецензентів і організаторів
Реєстрація учасників	реєстрація учасників з оплатою або безоплатно.	реєстрація учасників, управління квотами, організація доступу.	реєстрація делегатів із оплатою, тарифами, різними типами квитків.	система реєстрації учасників із можливістю безкоштовної або платної участі.
Гнучкість/ Кастомізація	сильна рольова модель (автори,	можливість змінювати форми, налаштовувати процес	висока інтеграція: абстракти, рецензування	Повна кастомізація: інтерфейси, політика

Вебсистема Характеристика	EasyChair	OpenConf	Ex Ordo	OSEM
	рецензенти, адміністратори)		я, програма, реєстрація	подань, дизайн
Хостинг/Архітектура	хмарна система — не вимагає локального встановлення	доступний як self-host (PHP / MySQL) або хмарний варіант	хмарний SaaS-сервіс	self-host (Ruby on Rails), відкритий код
Доступність	Має «Free» ліцензію + платні варіанти; ліцензія залежить від кількості подань.	Існує безкоштовна “Community” редакція, а також платні Plus / Professional	Комерційна платформа — вартість залежить від обсягу конференції	Безкоштовний, якщо розгортаєш на своїх серверах — open-source рішення

Порівняння платформ – EasyChair, OpenConf, Ex Ordo та OSEM – показує, що кожна з них має унікальні сильні сторони. EasyChair пропонує стабільне хмарне рішення зі зрілим інтерфейсом і потужною рольовою моделлю, але менш гнучке в кастомізації. OpenConf забезпечує високу адаптивність за рахунок різних редакцій та можливості самостійного хостингу. Ex Ordo виділяється інтеграцією всіх життєвих етапів конференції – від прийому тез до реєстрації та програмування – проте це платне комерційне рішення. OSEM, як open-source платформа, дає повний контроль над системою при нульових ліцензійних витратах, але потребує технічних ресурсів для встановлення і підтримки.

Висновки та перспективи. Веб-системи для проведення наукових конференцій виконують критично важливу роль у модернізації академічного процесу, забезпечуючи централізований механізм подання тез, рецензування, адміністрування учасників та публікації матеріалів. Завдяки цим системам значно зменшується навантаження на організаторів, підвищується прозорість рецензування, а учасники отримують можливість відслідковувати статус своїх подань онлайн.

Разом з тим виявлено низку проблем, які обмежують ефективність існуючих систем. Часто платформи недостатньо гнучкі або перевантажені функціями, частина з них мають обмежену кастомізацію, а деякі – занадто складні в налаштуванні або дорогі. Особливо це відчувається в контексті локальних або університетських конференцій, де ІТ-ресурси можуть бути обмеженими. Саме тому існує потреба в розробці нового прототипу веб-системи, яка поєднувала б простоту, інтуїтивний інтерфейс, одночасно охоплюючи ключові функції

управління конференціями та слугуючи єдиним інструментом для всіх зацікавлених сторін.

Список використаних джерел:

1. Болотіна В. Аналіз наявних систем підтримки наукової діяльності співробітників вищих навчальних закладів. *Вісник Хмельницького національного університету. Технічні науки.* - 2022. - Т. 313, № 5. - С. 71-76. DOI: <https://www.doi.org/10.31891/2307-5732-2022-313-5-71-76>
2. EasyChair [Електронний ресурс]. – Режим доступу: <https://easychair.org/> т (дата звернення: 27.11.2025)
3. Open Source Event Manager. [Електронний ресурс]. – Режим доступу: <https://osem.io/> (дата звернення: 27.11.2025).
4. OpenConf Peer-Review, Conference and Abstract Management Software System. [Електронний ресурс]. – Режим доступу: <https://www.openconf.com/> (дата звернення: 27.11.2025).
5. Your Scholarly Events Partner | Ex Ordo. [Електронний ресурс]. – Режим доступу: <https://www.exordo.com/> (дата звернення: 27.11.2025).

Литвиненко Дарія Володимирівна

студент 3 курсу, групи ТЦР-32

Державний університет інформаційно-комунікаційних технологій

st8476892@stud.duikt.edu.ua

Бойко Андрій Станіславович

студент 3 курсу, групи ТЦР-32

Державний університет інформаційно-комунікаційних технологій

st8498500@stud.duikt.edu.ua

Поперешняк Світлана Володимирівна

к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії

Національний технічний університет України

"Київський політехнічний інститут імені Ігоря Сікорського"

spropereshnyak@gmail.com

РОЗРОБКА ІНТЕЛЕКТУАЛЬНИХ Е-СИСТЕМ ІЗ ВИКОРИСТАННЯМ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ ТА ХМАРНИХ ТЕХНОЛОГІЙ

Постановка задачі. Електронні сервіси та Електронні системи є ключовими для цифрової трансформації та підвищення доступності послуг. Одними з ключових характеристик Е-систем повинні бути масштабованість, безпека та здатність взаємодіяти між собою. Традиційні монолітні архітектури не справляються зі зростаючим навантаженням та уповільнюють оновлення систем. Актуальним рішенням є розробка нових методологій на основі сучасних підходів: хмарні обчислення, мікросервісна архітектура. Це забезпечить надійність та безпеку Е-сервісів.

Мета дослідження. Метою дослідження є аналіз існуючих архітектур та розробка модульної архітектури для Е-сервісів, яка забезпечує їх масштабованість, безпеку та швидку адаптацію до нових вимог.

Результати дослідження. Сучасний розвиток Е-сервісів визначається переходом від традиційних монолітних архітектур до модульних та розподілених систем. Це підтверджує необхідність у спеціалізованих моделях розробки Е-сервісних систем, які усувають недоліки традиційних підходів, зокрема відсутність чіткого життєвого циклу та фокусу на інтеграції.

Було визначено, що гібридна, модульна архітектура (поєднання мікросервісів та хмарних обчислень) є оптимальним рішенням, оскільки вона забезпечує функціональну незалежність та самоконтроль компонентів (мікросервіси), що дозволяє незалежне розгортання та швидке оновлення, використовує хмарні технології для динамічного масштабування ресурсів, що критично важливо при пікових навантаженнях (локальне планування) та інтегрує безпекові патерни та шлюзи API, забезпечуючи високий рівень захисту даних. Таким чином, застосування спеціалізованої моделі розробки та гібридної архітектури дозволяє досягти високих показників за критеріями гладкості

(безперервність сервісу), довжина (ефективність) та безпека (захист даних) порівняно з монолітними системами.

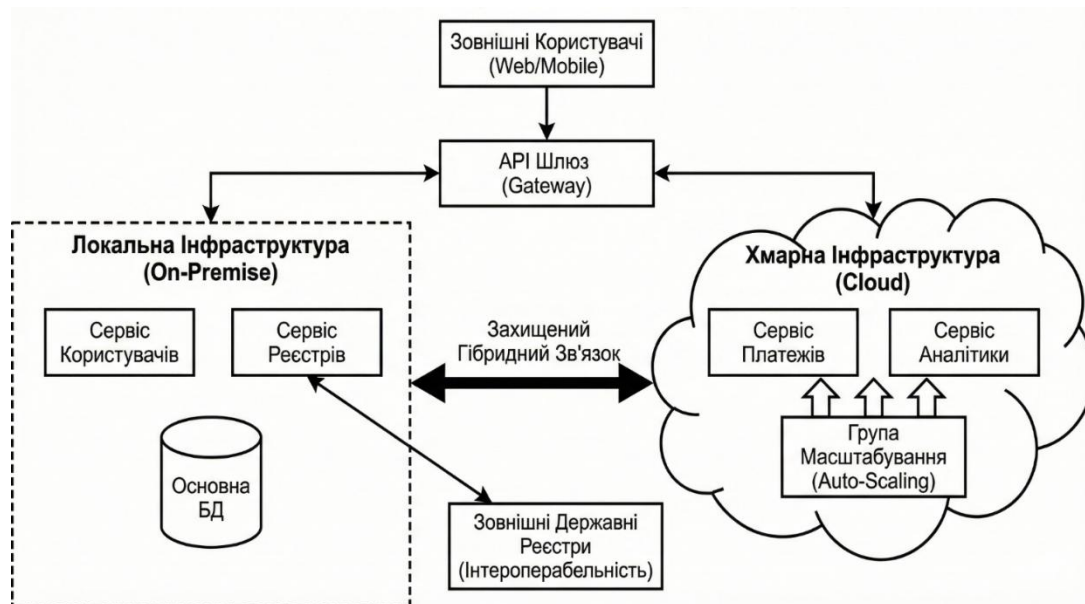


Рис.1. Архітектура роботи Е-сервісу

Архітектуру роботи Е-сервісу продемонстровано на рис. 1. запропонована схема реалізує гібридний підхід, розділяючи систему на локальну (On-Premise) та хмарну (Cloud) інфраструктури, що з'єднані через захищений канал зв'язку.

Центральним елементом взаємодії із зовнішніми користувачами виступає API Шлюз (Gateway), який забезпечує єдину точку входу, маршрутизацію запитів та автентифікацію. Це дозволяє приховати складність внутрішньої структури системи від клієнта.

Локальна інфраструктура концентрує критично важливі компоненти, такі як Сервіс реєстрів та Основна база даних. Розміщення цих елементів у захищеному периметрі (On-Premise) гарантує відповідність вимогам щодо захисту персональних даних та державних таємниць. Сервіс реєстрів також забезпечує інтероперабельність, взаємодіючи із зовнішніми державними реєстрами.

Хмарна інфраструктура використовується для розміщення високонавантажених модулів, таких як Сервіс платежів та Сервіс аналітики. Завдяки Групі масштабування (Auto-Scaling), хмарна частина здатна динамічно виділяти ресурси під час пікових навантажень, забезпечуючи стабільність роботи системи. Такий розподіл дозволяє досягти балансу між безпекою збереження даних та швидкістю обробки запитів.

Висновки та перспективи. У дослідженні розглянуто підходи до побудови архітектури Е-сервісів. Встановлено, що перехід від монолітних до гібридних мікросервісних архітектур є необхідною умовою для створення стійких державних цифрових платформ. Запропонована модель забезпечує гнучкість масштабування завдяки хмарним компонентам та високий рівень безпеки завдяки локальному зберіганню чутливих даних. Перспективою подальших досліджень є розробка алгоритмів автоматизованого розподілу навантаження між

локальним та хмарним середовищами, а також впровадження методів штучного інтелекту для предиктивної аналітики в рамках Сервісу аналітики.

Список використаних джерел

1. Чукут С.А Тенденції та проблеми впровадження електронного урядування : матеріали наук.-практ. конф. / КПП ім. Ігоря Сікорського. Київ : КПП ім. Ігоря Сікорського, 2016. С. 1.
2. Alainati S. M. K. B., Al-Slamani S. S., Al-Shehri S. et al. The Role of Educational Systems in Developing the Twenty-First Century Skills: Perspectives and Initiatives of Gulf Cooperation Council Countries // International Journal of Education and Pedagogy. 2024. Vol. 6, no. 1. P. 1–12.
3. Al-Ghalayini S. J. F., Al-Smadi G., Al-Samarrai S. A. et al. A model for the development of e-service systems//Proceedings of the 2nd International Conference on e-Services and Knowledge Management. New York: ACM, 2010. P. 5-10.

Мальцев Данило Євгенович
студент 3 курсу, групи ТЦР-32
Державний університет інформаційно-комунікаційних технологій
danimal1506@gmail.com
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій
spopereshnyak@gmail.com

МЕТОДИ ВИЯВЛЕННЯ ЗГЕНЕРОВАНОГО ВІДЕОКОНТЕНТУ (DEEPFAKE) ЗА ДОПОМОГОЮ ГЛИБОКОГО НАВЧАННЯ

Постановка задачі. Стрімкий розвиток генеративно-змагальних мереж (GAN) та автокодувальників призвів до появи технології Deepfake, яка дозволяє створювати реалістичні підробки відеозображень. Це створює серйозні загрози для інформаційної безпеки, репутації осіб та довіри до медіа. Класичні методи цифрової криміналістики часто виявляються неефективними проти сучасних алгоритмів генерації, які постійно вдосконалюються. Тому актуальним є аналіз та розробка методів виявлення дипфейків на основі алгоритмів глибокого навчання, що здатні адаптуватися до нових типів атак та працювати в умовах стиснення відеоданих.

Мета дослідження. Метою роботи є порівняльний аналіз сучасних архітектур нейронних мереж для виявлення дипфейків у відеопотоці; визначення їхньої ефективності, швидкодії та стійкості до збурень, а також окреслення перспектив створення гібридних моделей.

Результати дослідження. Сучасні підходи до виявлення синтетичного контенту можна класифікувати за типом ознак, що аналізуються. Автоматизовані системи детекції базуються на пошуку просторових та часових артефактів.

Одним із базових методів є використання згорткових нейронних мереж (CNN) для аналізу окремих кадрів. Такі моделі, як Xception або EfficientNet, демонструють високу точність у виявленні візуальних аномалій (неприродні текстури шкіри, артефакти на межах обличчя). Однак, покадровий аналіз не враховує динаміку руху та часову узгодженість, що робить його вразливим до якісних підробок, де кожен кадр окремо виглядає реалістично.

Для подолання цього недоліку використовуються рекурентні нейронні мережі (RNN) та мережі довгої короткострокової пам'яті (LSTM). Комбінація CNN та LSTM дозволяє виявляти часові невідповідності, такі як неприродне моргання, неузгодженість міміки або асинхронність руху губ. Архітектура спочатку витягує вектор ознак з кожного кадру за допомогою CNN, а потім аналізує послідовність цих векторів через LSTM. Цей підхід значно підвищує точність детекції, але вимагає більших обчислювальних ресурсів.

Окремим напрямом є використання частотного аналізу. Перетворення Фур'є або косинусне перетворення дозволяє виявити артефакти генерації GAN у частотному спектрі, які непомітні для людського ока. Гібридні моделі, що

поєднують аналіз у просторовій та частотній областях, демонструють кращу стійкість до методів стиснення відео, які часто використовуються у соціальних мережах.

Останнім часом набувають популярності методи на основі Vision Transformers (ViT). Механізм уваги (self-attention) дозволяє моделі фокусуватися на найбільш інформативних ділянках зображення та встановлювати глобальні залежності між пікселями, що часто втрачаються у звичайних згорткових мережах. Трансформери показують високу ефективність, але потребують значних обсягів даних для навчання.

Висновки. У дослідженні розглянуто ключові методи виявлення дипфейків. Аналіз показав, що використання виключно просторових ознак (CNN) є недостатнім для надійної детекції сучасних підробок. Найбільш ефективними є гібридні архітектури, що поєднують просторово-часовий аналіз (CNN+LSTM) або використовують механізми уваги (Transformers). Перспективою подальших досліджень є розробка полегшених моделей для роботи на мобільних пристроях у реальному часі, а також створення мультимодальних систем, які аналізують не лише відеоряд, а й аудіодоріжку для виявлення невідповідностей між голосом та мімікою.

Список використаних джерел

1. Masood M. et al. Deepfakes generation and detection: State-of-the-art, open challenges, countermeasures, and future trends. IEEE Access. 2023. Vol. 11. P. 1204–1256.
2. Nguyen H. H., Yamagishi J., Echizen I. Use of a Capsule Network to Detect Fake Images and Videos. arXiv preprint arXiv:1910.12467. 2022.
3. Guera D., Delp E. J. Deepfake Video Detection Using Recurrent Neural Networks. 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS). 2018. P. 1–6.
4. Coccomini D. A. et al. Combining EfficientNet and Vision Transformers for Video Deepfake Detection. Image Analysis and Processing – ICIAP 2022. Lecture Notes in Computer Science. 2022. Vol. 13233.

Мачуліс Гліб Дмитрович
студент 3 курсу, групи ТЦР-31
Державний університет інформаційно-комунікаційних технологій
(093) 191-95-71
glebmaculis@gmail.com
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний інститут
імені Ігоря Сікорського"
spopereshnyak@gmail.com

АРХІТЕКТУРНІ ОСОБЛИВОСТІ ТА РЕАЛІЗАЦІЯ КЛІЄНТСЬКОГО ІНТЕРФЕЙСУ СИСТЕМИ АУДИТУ ЯКОСТІ КОДУ «CODEBAROMETER»

Постановка задачі. Стрімкий розвиток вебтехнологій та підвищення вимог до якості програмного забезпечення зумовлюють необхідність створення інструментів, що здатні не лише аналізувати код, але й надавати результати у зручному для сприйняття форматі. Наявні рішення для статичного аналізу часто повертають дані у вигляді неструктурованих логів або складних JSON-об'єктів, що ускладнює їх інтерпретацію користувачем. Основна проблема полягає у розробці інтуїтивно зрозумілого графічного інтерфейсу, який забезпечував би абстракцію від складності серверних обчислень. Користувач повинен мати можливість отримати комплексну оцінку репозиторію, виконавши мінімальну кількість дій: введення посилання та запуск процесу. Актуальним завданням є проєктування клієнтської частини системи «CodeBarometer», яка поєднує в собі швидкість роботи, надійну систему авторизації та механізми обмеження доступу відповідно до бізнес-логіки тарифних планів.

Мета дослідження. Метою роботи є проєктування архітектури та програмна реалізація фронтенд-частини вебсервісу для аудиту коду. Дослідження спрямоване на створення інтерфейсу, що забезпечує маршрутизацію між публічними та приватними розділами, візуалізацію метрик якості та інтеграцію з платіжними шлюзами для керування підписками.

Результати дослідження. 1. Проєктування сценарію взаємодії. Для забезпечення високого рівня зручності використання було розроблено оптимізований сценарій взаємодії користувача з системою. Він базується на принципі мінімізації зусиль:

- а) **Вхідна точка:** Користувач потрапляє на головну сторінку, де центральним елементом є поле введення URL-адреси GitHub-репозиторію.
- б) **Ініціалізація аналізу:** Після натискання клавіші Enter, клієнтський додаток виконує валідацію посилання та відправляє асинхронний запит на сервер.
- в) **Відображення результатів:** Система автоматично перенаправляє користувача на сторінку результатів, де відображається інтегральна оцінка якості.

Для реалізації цього сценарію використано бібліотеку React Router, яка забезпечує динамічну зміну вмісту сторінки без повного перезавантаження, створюючи ефект нативної програми [1].

2. Архітектура компонентів та візуалізація даних. Інтерфейс системи побудовано за модульним принципом. Ключовим компонентом є «Результати аналізу репозиторію». Отримані від бекенду дані про вразливості та стиль коду трансформуються у візуальні метрики[4]:

- Радіальна діаграма: відображає загальний бал у діапазоні 0–100.
- Смути прогресу: деталізують оцінку за окремими категоріями, такими як «Безпека», «Тести» та «Документація».
- Рекомендації: блок рекомендацій автоматично генерується на основі виявлених помилок, надаючи користувачеві чіткі інструкції щодо покращення коду.

3. Система контролю доступу та бізнес-логіка. Важливою частиною дослідження стала реалізація логіки обмежень на стороні клієнта[2]. Згідно з розробленою моделлю монетизації, система передбачає три рівні доступу:

- Free: Базовий рівень для індивідуальних розробників, який надає доступ до основних метрик якості коду, але обмежує кількість аналізованих репозиторіїв.
- Plus: Рівень для професійного використання, що знімає кількісні обмеження та відкриває доступ до деталізованих звітів і розширених функцій аналізу.
- Pro: Рішення корпоративного класу, яке забезпечує повний доступ до всього функціоналу системи, включно з індивідуальними інтеграціями та виділеною підтримкою.

4. Взаємодія з бекендом. Архітектура взаємодії клієнтської частини з сервером зображена на рис. 1.

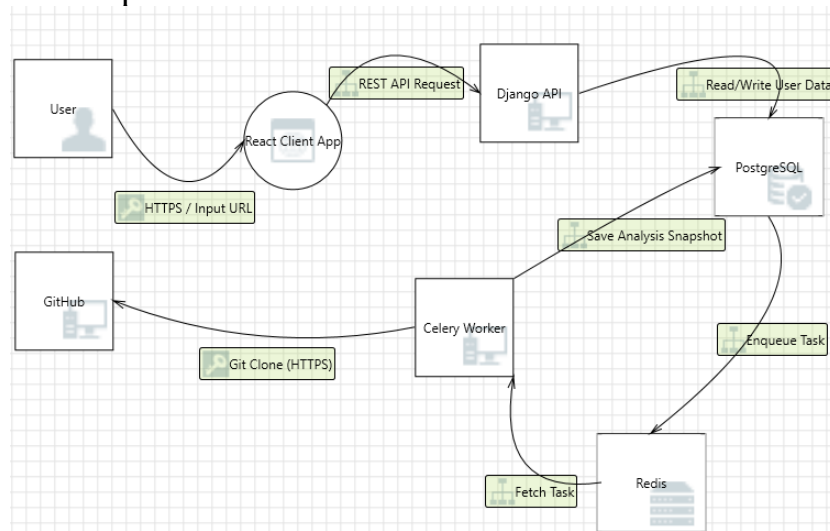


Рис. 1. Схема архітектури клієнтського додатка та потоків даних.

Схема демонструє архітектуру потоків даних, де ініціатором виступає користувач, передаючи URL-адресу через клієнтський додаток. Через REST API запит надходить до сервера, який взаємодіє з PostgreSQL для читання/запису

даних користувача та ставить задачу в чергу через Redis. Асинхронну обробку виконує Celery Worker, який забирає задачу з черги, клонує код із GitHub та зберігає результати аналізу безпосередньо в базу даних PostgreSQL.

Висновки. У роботі спроектовано та реалізовано клієнтську частину сервісу «CodeBarometer». Використання фреймворку React дозволило створити швидкий та адаптивний інтерфейс, що відповідає сучасним стандартам Web 2.0[3]. Реалізований механізм маршрутизації забезпечує логічне розділення публічної та приватної частин додатка. Впровадження системи візуалізації метрик вирішує проблему складності сприйняття технічних даних, дозволяючи користувачам миттєво оцінювати стан проєкту. Розроблена логіка контролю лімітів на стороні клієнта забезпечує прозорість тарифної політики та покращує користувацький досвід, попереджаючи про необхідність зміни тарифного плану до моменту відхилення запиту сервером.

Список використаних джерел

1. Banks A., Porcello E. Learning React: Modern Patterns for Developing React Apps. 2nd Edition. – O'Reilly Media, 2020. – 350 p.
2. Flanagan D. JavaScript: The Definitive Guide. 7th Edition. – O'Reilly Media, 2020. – 704 p.
3. Wieruch R. The Road to React: Your journey to master React.js in JavaScript. – Leanpub, 2021. – 228 p.
4. Duckett J. JavaScript and JQuery: Interactive Front-End Web Development. – Wiley, 2014. – 640 p.

Гаврилов Ілля Олегович

студент 3 курсу, групи ТЦР-33

Державний університет інформаційно-комунікаційних технологій

(095) 353-72-54

st8477068@stud.duikt.edu.ua

Поперешняк Світлана Володимирівна

к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії

Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

spopereshnyak@gmail.com

РОЗРОБКА МОДУЛІВ ВЗАЄМОДІЇ КОРИСТУВАЧІВ У СИСТЕМІ E-STUDYNEST: ЧАТ, ТЕСТУВАННЯ ТА QR-ВІДВІДУВАНІСТЬ

Постановка задачі. Цифрове освітнє середовище вимагає інструментів, які забезпечують не лише доступ до матеріалів, а й активну взаємодію між учасниками навчального процесу. Комунікація, тестування та контроль відвідуваності є ключовими складовими сучасних навчальних платформ.

Проте більшість існуючих рішень не забезпечують:

- зручного чату в режимі реального часу,
- автоматизованої генерації тестів,
- достовірного механізму фіксації відвідування,
- єдиного інтегрованого середовища.

У проєкті E-StudyNest поставлено задачу розробити три ключові модулі взаємодії користувачів:

- Chat-Service — для комунікації викладачів зі студентами;
- Test-Service — для проведення тестувань;
- Attendance QR-Service — для контролю відвідуваності на основі QR-

коду.

Мета дослідження. Метою роботи є створення ефективних та масштабованих модулів взаємодії студентів і викладачів на платформі E-StudyNest, зокрема:

- аналіз моделей обміну даними в чатах у режимі реального часу,
- розробка інструментів тестування зручних для викладача та зрозумілих студентам,
- реалізація безпечного механізму перевірки присутності студентів за допомогою QR-коду,
- забезпечення повної інтеграції цих модулів у мікросервісну архітектуру системи.

Результати дослідження. У результаті проведеного дослідження було розроблено та інтегровано до освітньої платформи E-StudyNest три ключові модулі, що забезпечують комплексну підтримку комунікації, тестування та контролю відвідуваності. Кожен із модулів створено з урахуванням специфіки цифрового освітнього середовища, вимог до масштабованості, безпеки та

доступності, а також необхідності інтеграції в загальну мікросервісну архітектуру системи.

Модуль Chat-Service реалізує механізми взаємодії користувачів у режимі реального часу та базується на поєднанні Spring Boot, WebSocket та STOMP-протоколу. Використання брокера повідомлень забезпечує стійкість до високих навантажень і дає змогу масштабувати систему горизонтально. Реалізовано персоніфікований доступ до комунікаційних каналів, історію переписки та автоматичні сповіщення про нові повідомлення, що істотно підвищує інтенсивність і ефективність взаємодії між студентами та викладачами. Захист інформаційних потоків забезпечується за допомогою JWT-аутентифікації та контролю прав доступу, що відповідає сучасним вимогам безпеки освітніх платформ.

Модуль Test-Service створює повноцінне середовище для формування, проведення та оцінювання тестувань. Архітектурно він розроблений як ізольований мікросервіс з окремою базою даних та власною REST-інфраструктурою. Важливою складовою є інтеграція з модулем штучного інтелекту, що дозволяє автоматизувати процес створення тестових завдань і формувати варіативні набори питань. Модуль підтримує збереження статистики, автоматичне оцінювання відповідей, облік часу виконання та можливість формування банку питань. Упровадження інтелектуальних функцій дає змогу не лише зменшити навантаження на викладача, а й забезпечити об'єктивність та гнучкість інструментів контролю знань.

Модуль Attendance QR-Service забезпечує механізм фіксації відвідування занять на основі одноразових QR-кодів, підписаних криптографічними ключами. Система створює унікальний токен для кожної навчальної пари, який має обмежений термін дії та прив'язку до часу й параметрів заняття. Перевірка відвідування виконується через валідацію підпису, часової позначки, а також додаткових параметрів авторизації, що мінімізує можливість неправомірного використання коду. Упровадження низки перевірок, зокрема контролю IP-адреси та user-agent, підвищує захист від спроб фальсифікації присутності. Модуль забезпечує надійний аудит відвідуваності та формує інтегрований журнал, що може використовуватись у звітності та аналітиці.

Отримані результати свідчать про те, що розроблені модулі становлять технологічно цілісне доповнення функціональності E-StudyNest, забезпечують високий рівень автоматизації навчального процесу та формують сучасне інтерактивне освітнє середовище. Застосування мікросервісної архітектури сприяло підвищенню надійності та масштабованості системи, а також створило основу для подальшого розвитку платформи та інтеграції нових сервісів.

Висновки та перспективи. Розроблені модулі чату, тестування та QR-відвідуваності становлять ключову частину функціональності системи E-StudyNest та забезпечують зручний і сучасний навчальний процес.

Використання мікросервісної архітектури дозволило:

- ізолювати логіку кожного модуля,
- полегшити розгортання та підтримку,

- забезпечити високу масштабованість та відмовостійкість.

Результати дослідження демонструють, що системи такого типу можуть значно автоматизувати навчальний процес, скоротити навантаження на викладача, зробити навчання інтерактивним і технологічно якісним.

Список використаних джерел

1. Spring WebSocket Documentation. Spring Framework. Available at: <https://spring.io>.
2. JSON Web Token (JWT) Specification. jwt.io. Available at: <https://jwt.io/introduction>.
3. HMAC: Keyed-Hashing for Message Authentication. RFC 2104. Internet Engineering Task Force, 1997. Available at: <https://www.rfc-editor.org/rfc/rfc2104>.
4. PostgreSQL Documentation. PostgreSQL Global Development Group. Available at: <https://www.postgresql.org/docs>.
5. The WebSocket Protocol. RFC 6455. Internet Engineering Task Force, 2011. Available at: <https://www.rfc-editor.org/rfc/rfc6455>.

Голубов Кирило Олександрович

студент 3 курсу, групи ТЦР-33

Державний університет інформаційно-комунікаційних технологій

(099) 421-77-59

st8482552@stud.duikt.edu.ua

Білоусов Олександр Олександрович

студент 3 курсу, групи ТЦР-33

«Державний університет інформаційно-комунікаційних технологій»

(067) 162-48-11

bilousov981@gmail.com

Поперешняк Світлана Володимирівна

к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії

Національний технічний університет України

"Київський політехнічний інститут імені Ігоря Сікорського"

spopereshnyak@gmail.com

РОЗРОБКА ЦИФРОВОЇ ПЛАТФОРМИ «Є-ЗАПИС» ДЛЯ ОПТИМІЗАЦІЇ БРОНЮВАННЯ ПОСЛУГ

Постановка задачі. Сучасна сфера послуг, зокрема індустрія краси та здоров'я (барбершопи, манікюр, масаж), стикається з проблемою неефективного управління записами. Використання застарілих каналів комунікації, таких як телефонні дзвінки або месенджери, є фрагментованим та неефективним каналом. Це призводить до високої ймовірності помилок у графіках, незручностей для клієнтів та зниження загальної ефективності взаємодії. Актуальним завданням є створення єдиної, централізованої та цілодобово доступної цифрової платформи, яка повністю замінить ручні методи на сучасну автоматизовану онлайн-систему, мінімізуючи людський фактор.

Мета дослідження. Метою роботи є розробка та впровадження універсальної цифрової платформи «Є-Запис» для зручного та швидкого онлайн-бронювання послуг. Дослідження спрямоване на створення комплексної системи, яка успішно об'єднує різні напрямки послуг (краса, здоров'я) в єдиному просторі, забезпечуючи універсальність для користувача. Особлива увага приділяється реалізації розширеної персоналізації та навігації для клієнтів, а також побудові технологічно надійної, безпечної та готової до масштабування архітектури, що перетворить сервіс на повноцінне бізнес-рішення.

Результати дослідження. В ході роботи було спроектовано та реалізовано платформу «Є-Запис», яка є єдиною цифровою платформою для онлайн-бронювання. Ключові функціональні результати:

Комплексність та універсальність: Платформа успішно об'єднує різні напрямки послуг (барбершоп, манікюр, масаж) в єдиному просторі, що підвищує загальну цінність та лояльність сервісу.

Розширена персоналізація та навігація: Реалізовано гнучкий функціонал, що виходить за межі простого бронювання. Користувачі можуть здійснювати

фільтрацію та вибір послуг за ціною, рейтингом, конкретним майстром та точною адресою (локацією), що гарантує максимально релевантний вибір.

Ефективне управління даними: Побудовано двосторонню систему «Клієнт — Майстер» з окремими особистими кабінетами. Клієнти отримують повний контроль над історією своїх записів, а майстри — зручний інструмент для керування робочим графіком, відстеження нових бронювань та оптимізації завантаженості в режимі реального часу.

Технологічна надійність та безпека: Архітектура проєкту побудована на сучасному MVC-патерні, що забезпечує чітке розділення на модулі, високу модульність коду та легкість підтримки.

Впроваджено сучасні технології та протоколи шифрування для безпечного зберігання й обробки даних користувачів, гарантуючи конфіденційність та надійність системи.

Надійний бекенд та ефективне управління базою даних забезпечують стабільність і готовність до швидкого розвитку.

Висновки та перспективи. Платформа «Є-Запис» є повноцінним бізнес-рішенням, яке значно підвищує ефективність взаємодії «клієнт — майстер», мінімізуючи помилки, характерні для застарілих каналів запису. Висновки підтверджують, що сучасна архітектура та безпечна інфраструктура проєкту створюють міцний фундамент для його подальшого комерційного розвитку.

Перспективами подальшого масштабування та вдосконалення системи є:

Інтеграція з платіжними сервісами для можливості попередньої оплати послуг.

Впровадження автоматичної системи сповіщень (через SMS/E-mail) для нагадувань клієнтам.

Розробка розширених інструментів аналітики для бізнесу.

Масштабування платформи на інші категорії послуг, що робить «Є-Запис» перспективною комерційною платформою.

Список використаних джерел

1. Alsmadi I. A Survey on Online Appointment Scheduling Systems: Features, Challenges, and Future Trends. *International Journal of Advanced Computer Science and Applications*. 2021. №12(5). P. 45–54.
2. Sharma P., Kumar A., Singh R. Design and Evaluation of a Smart Appointment Booking System Using Cloud-Based Architecture. *Journal of Web Engineering*. 2022. №21(3). P. 567–589.
3. Kaur J., Sandhu R., Gill H. Online Service Booking Platforms: A Review of Technologies, Architectures, and Security Issues. *IEEE Access*. 2023. №11. P. 125764–125781.
4. Meshram V., Patil P. Digital Transformation of Service Booking Systems Using Microservices and Containerization. *International Journal of Information Management Data Insights*. 2023. №3(1). P. 100–112.

Камоцький Богдан Борисович
студенти 3 курсу, групи ТЦР-32
Державний університет інформаційно-комунікаційних технологій
(093) 973-41-09
bohdankamotskiy@gmail.com
Закарадзе Максим Зурабович
студенти 3 курсу, групи ТЦР-32
Державний університет інформаційно-комунікаційних технологій
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

РОЗРОБКА ІНТЕРАКТИВНОГО ВІДЖЕТА ПОГОДИ З ФУНКЦІЄЮ ПЕРСОНАЛІЗОВАНИХ РЕКОМЕНДАЦІЙ

Постановка задачі. Сучасні погодні сервіси надають користувачам великий обсяг сирих метеорологічних даних: температуру, вологість, швидкість вітру, тиск тощо. Однак ці дані не дають прямої відповіді на повсякденні питання користувача: «Що сьогодні вдягнути?», «Чи комфортно буде гуляти на вулиці?». Користувач змушений самотійно аналізувати безліч параметрів, що є неефективним та часозатратним. Тому актуальною є задача розробки програмних інструментів, які б не просто відображали дані, а інтерпретували їх, перетворюючи на корисні та персоналізовані поради.

Мета дослідження. Метою дослідження є розробка клієнтського веб-віджета "Smart Weather Widget", здатного отримувати дані з метеорологічного API, аналізувати їх за допомогою спеціально розроблених алгоритмів та надавати користувачеві унікальні рекомендації, такі як індекс комфорту, індекс активності на вулиці та прогноз "золотої години" для фотографії.

Результати дослідження. В ході роботи було створено автономний веб-віджет, розроблений з використанням сучасного технологічного стека: збирача проєктів Vite, бібліотеки Preact для побудови інтерфейсу та препроцесора SCSS. Архітектура віджета дозволяє його легку інтеграцію в будь-який веб-сайт за допомогою кількох рядків коду.

Віджет реалізує наступний функціонал відображення метеорологічних даних та інтелектуальних показників для планування діяльності користувача. Базовий прогноз включає відображення поточної температури, її відчуття, погодних умов та прогнозу на найближчі три години.

Було розроблено та імплементовано алгоритми для розрахунку трьох унікальних смарт-індексів. Індекс комфорту (0-10) забезпечує комплексну оцінку погодних умов, враховуючи температуру, вологість та силу вітру, на основі якої надається порада щодо вибору одягу. Індекс активності на вулиці (0-10) оцінює придатність дня для активного відпочинку (прогулянок, спорту), базуючись на

температурі, вітрі, УФ-індексі та ймовірності опадів. Прогноз "Золотої години" здійснює автоматичний розрахунок оптимального часу для фотозйомки після сходу та перед заходом сонця, з урахуванням хмарності для прогнозування типу освітлення.

Для отримання метеорологічних даних використовується API сервісу OpenWeatherMap. Віджет збирається у формат UMD (Universal Module Definition), що забезпечує його сумісність з будь-яким веб-середовищем. Фінальний вигляд розробленого віджета продемонстровано на рис. 1.

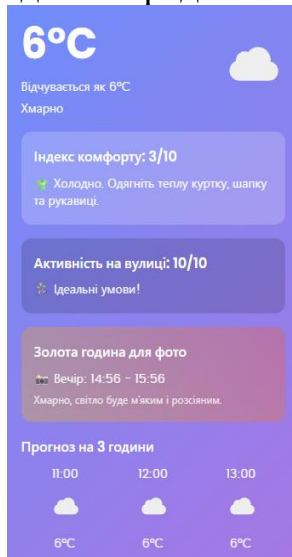


Рис. 1. Інтерфейс "Smart Weather Widget"

Висновки та перспективи. В результаті дослідження було успішно розроблено та протестовано "Smart Weather Widget", який вирішує поставлену задачу перетворення сирих метеорологічних даних на практичні поради. Проект демонструє, що сучасні frontend-технології дозволяють створювати легкі, швидкі та функціональні віджети, що додають значну цінність для кінцевого користувача.

Перспективою подальших досліджень є розширення функціонала віджета шляхом додавання нових смарт-індексів (наприклад, індексу якості повітря), впровадження геолокації для автоматичного визначення міста користувача, а також розробка можливостей для кастомізації зовнішнього вигляду віджета.

Список використаних джерел

1. OpenWeatherMap API documentation [Електронний ресурс] // OpenWeather Ltd. – 2025. – Режим доступу до ресурсу: <https://openweathermap.org/api>
2. Vite | Next Generation Frontend Tooling [Електронний ресурс] // Evan You and Vite contributors. – 2025. – Режим доступу до ресурсу: <https://vitejs.dev/>
3. Preact: Fast 3kB alternative to React with the same modern API [Електронний ресурс] // The Preact Authors. – 2025. – Режим доступу до ресурсу: <https://preactjs.com/>

Кирсенко Ярослав Іванович
студент 3 курсу, групи ТЦР-33
Державний університет інформаційно-комунікаційних технологій
(068) 874-49-12
st8455941@stud.duikt.edu.ua
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

АНАЛІЗ АРХІТЕКТУРИ ТА МОДЕЛІ МІКРОСЕРВІСІВ У СИСТЕМІ E-STUDYNES

Постановка задачі. У сучасній системі освіти виникає потреба у створенні універсальних інструментів для організації навчального процесу, що дозволяють забезпечити гнучкість, масштабованість і високу доступність сервісів. Традиційні монолітні рішення обмежують можливість швидкого оновлення, масштабування окремих компонентів та інтеграції зі сторонніми сервісами, включно з модулями штучного інтелекту.

Система E-StudyNest покликана вирішити саме ці проблеми шляхом впровадження мікросервісної архітектури, яка забезпечує незалежний розвиток окремих модулів — авторизації, тестування, відвідуваності, чату, розкладу та інтеграції з AI.

Завданням дослідження є визначення оптимальної архітектури, що дозволить створити ефективну, стійку до збоїв, просту для підтримки та розширення платформу для навчального процесу.

Мета дослідження. Метою роботи є аналіз, обґрунтування та побудова архітектурної моделі системи E-StudyNest на основі мікросервісної парадигми, яка забезпечить:

- незалежність модулів і можливість автономного розгортання,
- стійкість до високих навантажень,
- інтеграцію з AI-сервісами,
- підвищену безпеку користувацьких даних,
- мінімізацію міжмодульної зв'язності,
- можливість швидкого вдосконалення окремих компонентів.

Результати дослідження. Під час роботи було проаналізовано і спроектовано ключові модулі системи:

1. Auth-Service - Забезпечує авторизацію, аутентифікацію, керування ролями (Student, Teacher, Admin, Lead, Deputy). Використовує JWT, Spring Security, PostgreSQL.

2. User-Service - Відповідає за профілі користувачів, структуру груп і зв'язки між студентами, викладачами та курсами.

3. Schedule-Service - Модуль формування розкладу з можливістю динамічного оновлення та інтеграції з календарями (через webhook-сповіщення).

4. Attendance-Service - Генерує одноразові QR-коди для відвідуваності, перевіряє токени, фіксує присутність студентів. Використовує HMAC/JWT-підпис.

5. Test-Service - Створення тестів, формування питань, оцінювання результатів та аналітики.

6. Chat-Service - Реалізовано через WebSocket, забезпечує миттєву комунікацію між учасниками навчального процесу.

7. AI-Integration-Service - Проміжний шар між системою та зовнішніми LLM-моделями (OpenAI та ін.). Використовує проксі-шаблони prompt-ів та rate-limit.

8. Notification-Service - Email, push та внутрішні повідомлення.

Технічні результати проектування:

- Використано Spring Boot 3, Docker, PostgreSQL, Kafka.
- Введено принцип database-per-service.
- Побудовано схему взаємодії сервісів через REST + Kafka events.
- Реалізовано централізовану API-шлюз-точку на Spring Cloud

Gateway.

- Передбачено горизонтальне масштабування критичних сервісів.
- Впроваджено захист запитів через rate-limit, фільтри та JWT-валідацію.

Висновки та перспективи. Результатом дослідження стала повністю сформована архітектура мікросервісної освітньої платформи, яка здатна масштабуватися, швидко модифікуватися та підтримувати інтеграцію зі сторонніми AI-сервісами.

Мікросервісна модель дозволяє мінімізувати зв'язність між компонентами, забезпечує підвищену стійкість до помилок та дозволяє швидко вводити нові функції без негативного впливу на вже працюючі модулі.

Система E-StudyNest, побудована за такою архітектурою, є ефективним інструментом для цифрового навчального середовища, відповідає сучасним вимогам галузі й може бути розширена для використання у масштабних навчальних закладах.

Список використаних джерел

1. Docker Documentation — docs.docker.com.
2. PostgreSQL Documentation — [postgresql.org](https://www.postgresql.org).
3. Spring Framework Documentation — spring.io.

Масоха Владислав Юрійович
студент 3 курсу, групи ТЦР-34
Державний університет інформаційно-комунікаційних технологій
vladyslavmasokha2006@gmail.com
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

РОЗРОБКА ПРОТОТИПУ СИСТЕМИ ВАЛІДАЦІЇ КВАЛІФІКОВАНОГО ЕЛЕКТРОННОГО ПІДПISУ (КЕП)

Постановка задачі. В умовах стрімкого розвитку електронного документообігу в Україні критично важливим є забезпечення юридичної значущості цифрових документів. Ключовим інструментом для цього є кваліфікований електронний підпис (КЕП). Однак, існуючі методи перевірки часто вимагають ручного використання зовнішніх державних вебсервісів, що ускладнює інтеграцію в автоматизовані системи та сповільнює бізнес-процеси. Актуальним є створення спеціалізованого програмного забезпечення, яке дозволяє автоматизувати перевірку автентичності та цілісності документів безпосередньо на стороні користувача або підприємства.

Мета дослідження. Метою роботи є розробка функціонального прототипу системи валідації КЕП, що забезпечує автоматизовану перевірку підпису з точністю 100% для тестових зразків, мінімальну затримку обробки запитів та повну відповідність вимогам українського законодавства (стандарти ДСТУ, формат CAdES/XAdES).

Результати дослідження. Для досягнення поставленої мети було спроектовано та реалізовано веб-орієнтований прототип системи. Архітектура рішення базується на клієнт-серверній моделі. Серверна частина (Backend) розроблена мовою Python, що обумовлено наявністю потужних криптографічних бібліотек (Cryptography, M2Crypto) для роботи з алгоритмами хешування та шифрування. Клієнтська частина (Frontend) реалізована з використанням HTML, CSS та бібліотеки React, що забезпечує зручний інтерфейс для завантаження файлів (документ, підпис .P7S, ключ) та відображення результатів.

Алгоритм роботи системи включає наступні етапи:

Перевірка цілісності: Математична перевірка того, що документ не був змінений після накладання підпису.

Перевірка автентичності: Верифікація відповідності відкритого ключа підписувача його сертифікату.

Перевірка статусу сертифіката: Автоматичний запит до кваліфікованого надавача довірчих послуг через протокол OCSP або перевірка за списками відкликаних сертифікатів (CRL) для підтвердження чинності сертифіката.

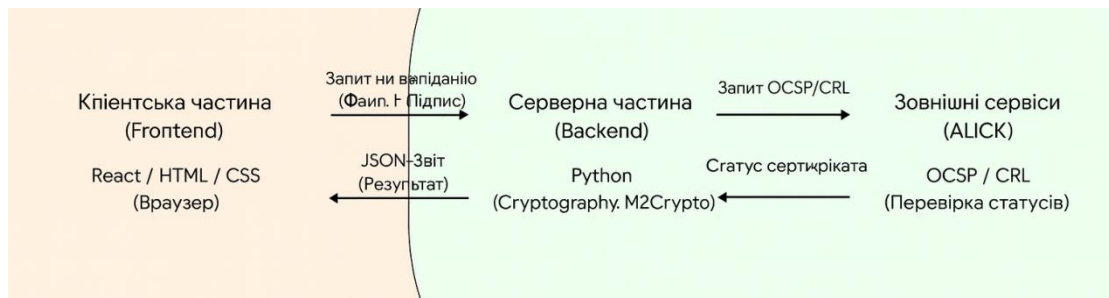


Рис. 1. Архітектура системи валідації КЕП.

Для забезпечення переносимості та простоти розгортання використано технологію контейнеризації Docker. Це дозволяє запускати прототип на будь-якій IBM-сумісній машині під управлінням Windows 10/11 без необхідності складного налаштування середовища. Результатом роботи системи є

структурований JSON-звіт, що містить статус підпису (True/False), дані про підписувача (ПІБ, ЄДРПОУ) та термін дії сертифіката.

Висновки та перспективи. У ході дослідження розроблено прототип модуля валідації КЕП, який успішно вирішує задачу автоматизації перевірки цифрових підписів згідно з ДСТУ 4145-2002. Система спрощує процедуру підтвердження юридичної значущості документів, усуваючи людський фактор. Перспективою подальших досліджень є інтеграція розробленого модуля у повноцінні системи електронного документообігу (ЕДО) підприємств, розширення підтримки апаратних токенів та оптимізація швидкодії при обробці великих масивів файлів.

Список використаних джерел

1. Закон України «Про електронні довірчі послуги» від 05.10.2017 №2155-VIII.
2. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих.
3. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія: теорія, практика, застосування : монографія. Харків : Форт, 2012. 880 с.

Мілевський Роман Олександрович
студент 3 курсу, групи ТЦР-31
Державний університет інформаційно-
комунікаційних технологій
097-299-84-24

romanmilevski32@gmail.com

Теремко Роман Дмитрович
студент 3 курсу, групи ТЦР-31
Державний університет інформаційно-
комунікаційних технологій
097-299-84-24

roma4ik.teremko@gmail.com

Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний інститут
імені Ігоря Сікорського"
spopereshnyak@gmail.com

МЕТОДИ ПЕРСОНАЛІЗАЦІЇ МАРШРУТІВ ТА МОТИВАЦІЇ КОРИСТУВАЧА У МОБІЛЬНОМУ ДОДАТКУ ДЛЯ ДОСЛІДЖЕННЯ МІСЬКОГО СЕРЕДОВИЩА

Постановка задачі. У сучасних містах спостерігається зниження рівня щоденної фізичної активності населення та зменшення інтересу до пізнання локальних культурно-історичних об'єктів. Одним зі способів вирішення цієї проблеми є створення мобільних додатків, які мотивують користувачів до прогулянок і дослідження власного міста через персоналізований контент та інтерактивні механіки. Актуальним завданням постає розроблення системи, що забезпечує адаптивні маршрути залежно від уподобань, активності користувача, його місцезнаходження та умов середовища.

Мета дослідження. Метою дослідження є аналіз підходів до формування персональних прогулянкових маршрутів і квестових завдань у мобільних додатках; визначення ефективних методів адаптації рекомендацій до поведінки користувачів, часу, погоди та локальних умов; а також оцінка можливостей інтеграції алгоритмічної генерації маршрутів.

Результати дослідження. Мобільний додаток генерує маршрути на основі індивідуальних параметрів користувача: рівня складності, доступного часу, попередньої активності, місцезнаходження та погодних умов. Під час реєстрації користувач обирає базовий рівень складності, який може змінювати в будь-який момент, що забезпечує адаптивність системи до змін фізичної активності. Дані про погоду автоматично отримуються з відкритих сервісів, після чого система коригує характеристики маршрутів — їхню довжину, тип місць та інтенсивність навантаження. Маршрути перетворюються на щоденні "квести дня", де кожна прогулянка має унікальну тематику, складність та винагороду.

Функціональні можливості додатка включають доступ до тематичних добірок локацій, що дозволяють користувачу самостійно обирати місця відповідно до настрою або інтересу. Система також надає можливість автоматичної генерації маршруту за введеним часом або бажаною дистанцією, забезпечуючи гнучкість та персоналізацію. Регулярні місячні челенджі стимулюють дослідницьку активність, надаючи винагороди за виконання маршрутів певного типу. Рекомендаційний модуль аналізує середню активність користувача, відвідані локації та географічні зони, пропонуючи нові варіанти маршрутів і місць у вже знайомих районах.

У додатку реалізовано механізм інтерактивних історій, що супроводжують маршрути. Кожна локація може містити легенду, загадку або коротку довідку, що робить прогулянку ігровою та пізнавальною. Перевірка виконання таких завдань здійснюється через фотографію або підтвердження геолокації. Для забезпечення чесної взаємодії та уникнення дублювання акаунтів передбачена обов'язкова верифікація через телефон або електронну пошту.

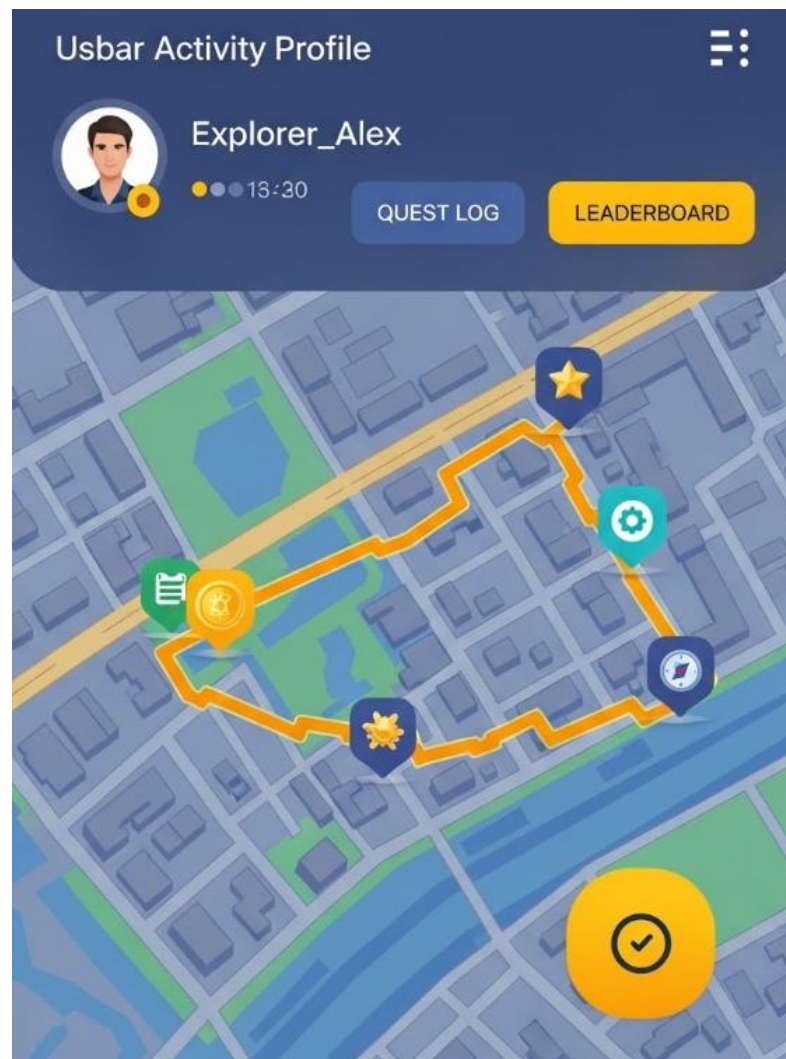


Рис. 1. Дизайн мобільного додатка

Висновки та перспективи. Розроблена концепція мобільного додатка орієнтована на підвищення фізичної активності користувачів та популяризацію пізнання міського середовища. Використання адаптивних алгоритмів рекомендацій, інтеграції погодних даних, аналізу активності та механік гейміфікації дозволяє створити персоналізований досвід прогулянок у форматі квестів. Підходи, описані в дослідженні, демонструють перспективність подальшого розвитку системи через розширення алгоритмічної генерації маршрутів, впровадження елементів штучного інтелекту та розроблення більш глибокої системи взаємодії користувача з міським середовищем. Перспективним напрямом є також вдосконалення інтерактивного контенту, розширення соціальної складової та дослідження нових способів підвищення користувацької мотивації.

Список використаних джерел

1. Ricci F., Rokach L., Shapira B. Recommender Systems: Fundamentals and Methods. *Springer Handbook of Recommender Systems*. 2022. P. 1–35.
2. Hamari J., Koivisto J., Sarsa H. *Does Gamification Work? — A Literature Review of Empirical Studies on Gamification*. Hawaii International Conference on System Sciences. 2014. P. 3025–3034.
3. Yigitcanlar T., Kamruzzaman M., Foth M., Sarker M.N.I. Mobile urban sensing and location-based technologies for smart city applications. *Cities*. 2023. Vol. 140, P. 104389.
4. Chen Z., Wang C., Li J. Context-aware personalized route recommendation in mobile services. *Journal of Ambient Intelligence and Humanized Computing*. 2021. Vol. 12, no. 5, P. 4531–4546.
5. Celik S., Hofmann A., Friedrich M. Weather-adaptive route planning for urban mobility services. *Transportation Research Procedia*. 2020. Vol. 47, P. 209–216.
6. Xu H., Park J., Chen X. Location-based mobile recommendations: Approaches and evaluation. *ACM Computing Surveys*. 2020. Vol. 53, no. 5, P. 1–34.
7. Riegler M., Halvorsen P., Pogorelov K. Interactive storytelling in mobile applications: Methods and user engagement. *Multimedia Tools and Applications*. 2021. Vol. 80, P. 23411–23433.

Смаровоз Анна Андріївна
студентка 3 курсу, групи ТЦР-32

Державний університет інформаційно-комунікаційних технологій
(097)127-46-53

smarovozaanna93@gmail.com

Собко Данило Олександрович

студент 3 курсу, групи ТЦР-32

Державний університет інформаційно-комунікаційних технологій
(098)810 –52–33

danilsobko2005@gmail.com

Поперешняк Світлана Володимирівна

к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії

Національний технічний університет України "Київський політехнічний інститут
імені Ігоря Сікорського"

spropereshnyak@gmail.com

ОПТИМІЗАЦІЯ СТУДЕНТСЬКИХ АДМІНІСТРАТИВНИХ ПРОЦЕДУР

Постановка задачі. Однією з найбільш поширених проблем у взаємодії студента з деканатом є неефективна маршрутизація звернень: студенту часто доводиться проходити кілька кабінетів, з'ясовувати, хто саме опікується його питанням, а також витратити час на уточнення списку необхідних документів. Це призводить до черг, помилково оформлених заяв і значного навантаження на працівників деканату, які змушені постійно пояснювати одні й ті ж процедури. Актуальним є створення автоматизованої системи, що формуватиме для студента чіткий, персоналізований маршрут виконання конкретної адміністративної дії – від вибору типу запиту до вказівки кабінету та переліку документів.

Мета дослідження. Метою є визначення ефективності системи автоматизованої маршрутизації звернень у покращенні студентського сервісу, скороченні часу обробки запитів та зменшенні навантаження на адміністративний персонал закладу.

Результати дослідження. Аналіз існуючих процедур показав, що значна частина часу під час звернень до деканату витрачається не на саму адміністративну дію, а на пошук відповідального кабінету, уточнення порядку виконання процедури та виправлення некоректно оформлених заяв. Запропонована система автоматизованої маршрутизації “U-Portal” оптимізує ці процеси за рахунок формування персоналізованих інструкцій для кожного типу звернення.

Система автоматично визначає перелік необхідних документів, послідовність дій, відповідальні підрозділи та можливі форми подання (онлайн або офлайн). Вона також здійснює валідацію введених даних, запобігаючи типові помилки під час заповнення заяв. Завдяки цьому студент отримує чіткий

алгоритм виконання процедури, що суттєво скорочує кількість повторних звернень.

Отримані результати свідчать, що використання системи дозволяє:

- зменшити час обробки звернень на 30–50% завдяки усуненню етапів уточнення інформації;
- знизити кількість неправильно оформлених заяв за рахунок автоматичної перевірки та стандартизованих шаблонів;
- зменшити навантаження на працівників деканату, які раніше виконували повторювані консультаційні функції;
- підвищити прозорість і передбачуваність процедур, стандартизувавши їх та уніфікувавши порядок виконання.

Висновки та перспективи. Автоматизація маршрутизації звернень є дієвим способом оптимізації роботи деканату. Перспективами розвитку є впровадження адаптивних алгоритмів, що враховують індивідуальну історію студента, календарні дедлайни та завантаженість підрозділів, а також інтеграція з електронними реєстрами університету.

Список використаних джерел

1. Krupskiy I., Kalinina T. Web-oriented system of the electronic dean's office: implementation of the student individual plan formation use case. *Information Technologies and Society*. 2023. № 4, P. 45–52.
2. Horbatiuk R. Digital transformation of management processes in higher education institutions: problems and prospects. *Economy and Society*. 2022. № 38, P. 120–126.
3. Mazur O., Shvydun V. Automation of information services for student support in Ukrainian universities. *Information Technologies and Learning Tools*. 2021. Vol. 85, № 5, P. 101–114.

Юшко Крістіна Богданівна
студентка 3 курсу, групи ТЦР-33
Державний університет інформаційно-комунікаційних технологій
(098) 233-89-15

kristina.yushko006@gmail.com

Кірко Олександр Віталійович
студент 3 курсу, групи ТЦР-33
Державний університет інформаційно-комунікаційних технологій
(098) 437-65-13

kirkovsasha009@gmail.com

Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний інститут
імені Ігоря Сікорського"
spopereshnyak@gmail.com

ОПИС ТА ФУНКЦІОНАЛ ЕЛЕКТРОННОГО ОСВІТНЬОГО КАБІНЕТУ

Постановка задачі. Електронні освітні кабінети (ЕОК) сьогодні активно впроваджуються в закладах освіти різних рівнів — від шкіл до університетів. Їх використання дозволяє забезпечити безперервний доступ до навчальних матеріалів, інструментів комунікації, систем оцінювання та індивідуального прогресу. Однією з ключових проблем впровадження ЕОК є забезпечення зручності, адаптивності та безпеки для різних категорій користувачів — учнів, студентів, викладачів і адміністрації. Тому актуальним є аналіз сучасних методів організації електронного освітнього середовища та технологій, які забезпечують ефективну взаємодію користувачів із цифровими ресурсами.

Мета дослідження. Метою дослідження є аналіз методів побудови, функціонування та оптимізації електронного освітнього кабінету; визначення ключових переваг, недоліків та перспектив розвитку таких систем у сучасних навчальних закладах.

Результати дослідження. Електронний освітній кабінет є інтегрованою цифровою системою, що забезпечує високий рівень автоматизації освітнього процесу. ЕОК містить модулі для управління користувачами, відображення розкладу, перегляду навчальних матеріалів, перевірки знань, ведення електронних журналів та комунікації між учасниками освітнього процесу. Завдяки адаптивності та модульній архітектурі ЕОК швидко реагує на зміни освітнього середовища: оновлення контенту, зміну графіка занять, кількість студентів чи нові інструменти навчання.

Методи організації роботи в ЕОК поділяються на **глобальні** та **локальні**.

1. **Глобальна організація системи** передбачає структуроване розміщення всіх освітніх ресурсів, календарів, бібліотек, курсів та журналів.

2. **Локальна організація** стосується індивідуальної взаємодії користувача з системою — робота з тестами, завантаження завдань, комунікація, отримання зворотного зв'язку.

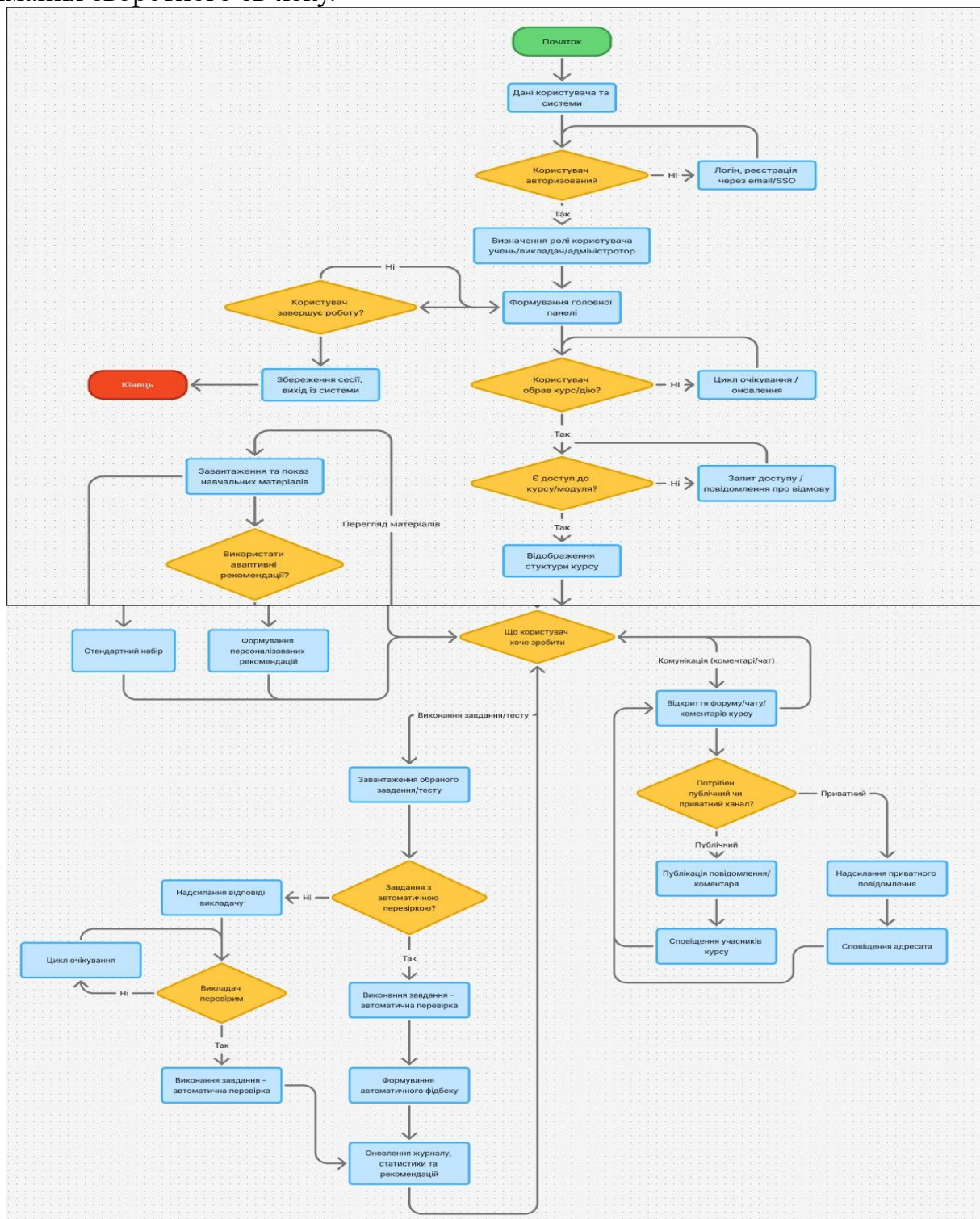


Рис. 1. Архітектуру типового електронного освітнього кабінету.

Модульна архітектура. Система складається з окремих блоків: модуль навчальних матеріалів, модуль тестування, модуль комунікацій, модуль аналітики успішності тощо. Такий підхід забезпечує гнучкість, масштабованість і можливість інтеграції нових функцій без зміни основи платформи.

Адаптивні освітні системи. Адаптивність дозволяє системі підлаштовуватися під рівень користувача, його прогрес та індивідуальну траєкторію навчання. Наприклад, студент отримує матеріали та завдання відповідного рівня складності.

Аналітика навчальних даних (Learning Analytics). Алгоритми аналізу навчальної активності використовують дані про перегляд матеріалів, оцінки, виконання завдань та активність у курсах. Це дозволяє:

1. формувати персональні рекомендації;
2. визначати прогалини у знаннях;
3. підвищувати ефективність викладання;
4. своєчасно виявляти ризики академічної неуспішності.

Інтелектуальні рекомендаційні системи. За аналогією з алгоритмами уникнення перешкод у робототехніці, рекомендаційні системи оптимізують “маршрут навчання” студента:

1. пропонують корисні матеріали;
2. радять курси;
3. формують індивідуальні траєкторії.

Такі алгоритми можуть базуватися на машинному навчанні, колаборативній фільтрації або моделюванні поведінки.

Системи керування доступом та безпекою. Однією з ключових проблем ЕОК є забезпечення захисту персональних даних користувачів. Використовуються:

1. рольові моделі доступу (RBAC);
2. багатофакторна автентифікація;
3. шифрування навчальних матеріалів та журналів;
4. контроль дій користувачів.

Методи взаємодії викладача та студента. Ці методи включають інструменти для обговорень, відеоконференцій, коментарів, миттєвих повідомлень і електронних журналів. Вони забезпечують швидку зворотну реакцію та сприяють активній навчальній діяльності.

Висновки та перспективи. У дослідженні розглянуто методи побудови та функціонування електронного освітнього кабінету. Проведений аналіз показав, що найбільш ефективними є системи, які поєднують модульну архітектуру, адаптивні алгоритми навчання та інтелектуальні технології. Поєднання традиційних методів організації навчального процесу з автоматизованими інструментами дозволяє забезпечити високу якість освіти, гнучкість та індивідуалізацію.

Перспективи розвитку включають:

1. інтеграцію штучного інтелекту для глибокого аналізу навчальних даних;
2. створення більш точних адаптивних моделей;
3. розробку інтуїтивних інтерфейсів;
4. забезпечення повної синхронізації з мобільними додатками;

5. використання хмарних сервісів для масштабування та розширення функціональності.

Список використаних джерел

1. ISO/IEC/IEEE 29148:2018. Systems and software engineering — Requirements engineering.
2. Pressman R., Maxim B. Software Engineering: A Practitioner's Approach. McGraw-Hill, 2014.
3. Sommerville I. Software Engineering. Pearson, 2015.
4. Jacobson I., Booch G., Rumbaugh J. The Unified Software Development Process. Addison-Wesley, 1999.
5. Федорчук П. І. ІТ-технології в освіті. Київ: КНЕУ, 2020.
6. Дроздова І., Кравченко О. Розвиток електронних освітніх сервісів у закладах освіти. Інформаційні технології і засоби навчання, 2021, №4.
7. Марчук О. Електронні освітні середовища: технології та перспективи впровадження. Педагогічні науки, 2020, №2.

Якименко Дар'я Олександрівна
студентка 3 курсу, групи ТЦР-34
Державний університет інформаційно-комунікаційних технологій
dasaakimenko860@gmail.com
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

ОСОБЛИВОСТІ ТА ПЕРСПЕКТИВИ РОЗВИТКУ КВАЛІФІКОВАНОГО ЕЛЕКТРОННОГО ПІДПИСУ В ЦИФРОВІЙ ЕКОСИСТЕМІ УКРАЇНИ

Постановка проблеми: Україна за останні роки здійснила безпрецедентний стрибок у сфері цифровізації державних послуг, реалізуючи концепцію «Держава у смартфоні». В умовах повномасштабної війни та масової міграції населення потреба у віддаленій ідентифікації та дистанційному укладанні угод стала критично важливою для виживання економіки. Ключовим елементом цієї цифрової інфраструктури є Кваліфікований Електронний Підпис (КЕП). Він виступає не просто аналогом власноручного підпису, а фундаментом для функціонування екосистеми «Дія», електронного суду, податкової звітності та банківського сектору. Специфіка українського ринку довірчих послуг полягає у співіснуванні різних типів носіїв ключів (файлових, хмарних, апаратних) та активній інтеграції з Єдиним цифровим ринком ЄС, що потребує детального аналізу.

Мета дослідження: Метою роботи є аналіз сучасного стану впровадження КЕП в Україні, дослідження переходу від застарілого ЕЦП до європейських стандартів КЕП, оцінка ефективності технології «Дія.Підпис» та визначення викликів, що стоять перед українською сферою електронних довірчих послуг в умовах воєнного стану та євроінтеграції.

Результати дослідження: Правовим підґрунтям функціонування електронного підпису в Україні є Закон України «Про електронні довірчі послуги» (№ 2155-VIII), який набрав чинності у 2018 році. Цей закон гармонізував українське законодавство з регламентом Європейського Союзу eIDAS, замінивши застаріле поняття «Електронний цифровий підпис» (ЕЦП) на «Кваліфікований електронний підпис» (КЕП). В Україні склалася унікальна дворівнева архітектура системи довірчих послуг:

Центральний засвідчувальний орган (ЦЗО): Функціонує при Міністерстві цифрової трансформації та забезпечує технічне регулювання.

Кваліфіковані надавачі електронних довірчих послуг (КНЕДП): Це державні (наприклад, ДПС, МВС, ПриватБанк) та приватні (наприклад, «ЦСК «Україна», «Вчасно») організації, які безпосередньо видають сертифікати користувачам.

Феномен «Дія.Підпис» та хмарні технології. Революційним кроком для України стало впровадження «Дія.Підпис» (SmartID). Це кваліфікований електронний підпис, ключ до якого зберігається у захищеному хмарному сховищі державного підприємства «Дія», а смартфон виступає засобом доступу та авторизації. Унікальність українського рішення полягає у використанні технології FaceID/Liveness Detection для активації підпису. Щоб підписати документ, користувач повинен пройти перевірку біометрії обличчя (покрутити головою перед камерою), що звіряється з фотографією у Єдиному державному демографічному реєстрі. Це робить український КЕП одним із найзручніших та найбезпечніших у світі, мінімізуючи ризики використання вкрадених ключів.

Висновки та перспективи: Україна демонструє одні з найвищих темпів розвитку сфери електронних довірчих послуг у Європі. Відхід від бюрократичних процедур отримання підпису на користь миттєвої генерації у смартфоні («Дія.Підпис») створив прецедент для наслідування іншими країнами.

Основними перспективами розвитку КЕП в Україні є:

- Повна відмова від незахищених файлових носіїв після завершення воєнного стану та перехід на хмарні захищені сховища (Cloud Key).
- Остаточне юридичне визнання українського КЕП в Європейському Союзі, що спростить експорт послуг та товарів.

Список використаних джерел

1. Закон України «Про електронні довірчі послуги» від 07.11.2017 № 2155-VIII.
2. Постанова Кабінету Міністрів України від 17.03.2022 № 300 «Деякі питання забезпечення безперебійного функціонування системи надання електронних довірчих послуг».
3. Офіційний веб-сайт Центрального засвідчувального органу. URL: <https://czo.gov.ua/>
4. Федоров М. Цифрова держава: як працює Дія.Підпис. // Економічна правда. – 2023.

Ярмоленко Максим Сергійович

студент 3 курсу, групи ТЦР-34

Державний університет інформаційно-комунікаційних технологій

Луценко Станіслав Сергійович

студент 3 курсу, групи ТЦР-34

Державний університет інформаційно-комунікаційних технологій

Поперешняк Світлана Володимирівна

к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії

Національний технічний університет України "Київський політехнічний інститут
імені Ігоря Сікорського"

spopereshnyak@gmail.com

ЕЛЕКТРОННИЙ ЗАПИС НА Б'ЮТІ-ПРОЦЕДУРИ

Постановка задачі. У сфері б'юті-послуг спостерігається стрімке зростання кількості клієнтів і процедур, що значно ускладнює ручне ведення розкладу. Традиційні методи запису через телефон або нотатки часто призводять до помилок, накладок, втрати даних і низької швидкості обробки запитів. Постає задача розробити електронну систему запису, яка автоматизує приймання заявок, дозволяє клієнту самостійно обирати процедуру та час, забезпечує точний розподіл навантаження між майстрами та оперативно реагує на зміни в графіку. Така система має підвищувати ефективність роботи салону та комфорт користувачів.

Мета дослідження. Метою дослідження є аналіз методів оптимізації і автоматизації електронного запису на б'юті-процедури, вивчення підходів до організації електронного розкладу та визначення можливостей використання інтелектуальних алгоритмів для покращення точності планування. Особлива увага приділяється оцінці таких рішень, як динамічні часові слоти, автоматичне виявлення конфліктів, рекомендаційні системи та елементи машинного навчання, що можуть значно підвищити ефективність роботи б'юті-сервісів.

Результати. У ході аналізу встановлено, що сучасні електронні системи запису здатні автономно виконувати основні функції планування: збір даних клієнта, перевірку доступних часових вікон, формування запису та попередження конфліктів у графіку. Розглянуті методи, зокрема фіксовані та адаптивні тайм-слоти, алгоритми виявлення накладок, прогнозування пікового навантаження та інтелектуальні рекомендаційні моделі, дозволяють підвищити швидкість, точність та надійність системи. Показано, що використання таких підходів суттєво покращує взаємодію клієнта з салоном і оптимізує робочий час майстрів.



Рис. 1. Архітектура роботи електронного запису

Висновки. Проведене дослідження доводить, що інтеграція електронних систем запису з інтелектуальними алгоритмами забезпечує значне підвищення ефективності управління розкладом у б'юті-закладах. Найрезультативнішим є застосування гібридних підходів, що поєднують простоту традиційних методів із адаптивністю машинного навчання. Такі системи не лише мінімізують помилки, але й покращують користувацький досвід, скорочують час обслуговування та забезпечують стабільну роботу салону. Перспективи розвитку включають глибшу автоматизацію, впровадження систем прогнозування, персоналізацію записів і повну інтеграцію з мобільними платформами та CRM-системами.

Список використаних джерел

1. Oracle. *Java Platform, Standard Edition Documentation* [Електронний ресурс]. – Режим доступу: <https://docs.oracle.com/javase/> (дата звернення: 15.11.2025).
2. MDN Web Docs. *HTTP – протокол передачі даних* [Електронний ресурс]. – Режим доступу: <https://developer.mozilla.org/en-US/docs/Web/HTTP> (дата звернення: 15.11.2025).
3. W3C. *HTML & CSS Standards* [Електронний ресурс]. – Режим доступу: <https://www.w3.org/standards/webdesign/> (дата звернення: 15.11.2025).
4. JetBrains. *JVM, JDK та інструменти розробки Java* [Електронний ресурс]. – Режим доступу: <https://www.jetbrains.com/guide/java/jvm/> (дата звернення: 15.11.2025).
5. Microsoft Docs. *Windows OS Documentation* [Електронний ресурс]. – Режим доступу: <https://learn.microsoft.com/windows/> (дата звернення: 15.11.2025).

6. Unix.org. *UNIX System Documentation* [Электронный ресурс]. – Режим доступа: https://www.unix.org/what_is_unix.html (дата звернения: 15.11.2025).
7. Mozilla. *Firefox Browser Documentation* [Электронный ресурс]. – Режим доступа: <https://developer.mozilla.org/en-US/docs/Mozilla/Firefox> (дата звернения: 15.11.2025).

Мороз Андрій Віталійович
студент 3 курсу, групи ТЦР-32
Державний університет інформаційно-комунікаційних технологій
+(380) 96 115-16-15
moroz6377@gmail.com

Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний
інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

РОЗРОБКА Е-СЕРВІСІВ ТА Е-СИСТЕМ ДЛЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ПУБЛІЧНИХ ПОСЛУГ

Постановка задачі. Цифрова трансформація державного сектору та бізнес-процесів зумовила стрімкий розвиток Е-сервісів (електронних послуг) та Е-систем (інформаційних систем, що працюють в електронному середовищі). Для користувачів ключовими очікуваннями є доступність 24/7, зручний інтерфейс, прозорість процесів і захищеність персональних даних. Для розробників – масштабованість, інтегровуваність із наявними реєстрами та сервісами, а також відповідність технічним і правовим вимогам. Проблема полягає в тому, що традиційні підходи до створення інформаційних систем не завжди враховують специфіку Е-сервісів: високе навантаження, динамічну зміну вимог, необхідність інтеграції з зовнішніми API та національною інфраструктурою відкритих даних. Це потребує формування системного підходу до розробки, тестування та супроводу Е-сервісів і Е-систем.

Мета дослідження. Метою дослідження є аналіз принципів проєктування та розробки Е-сервісів і Е-систем, а також формування узагальненої архітектури, що забезпечує надійну роботу, безпеку, масштабованість та зручність використання таких рішень у сфері публічних послуг та бізнес-процесів.

Результати дослідження. Типовий Е-сервіс можна розглядати як багаторівневу систему, що складається з:

- клієнтського інтерфейсу (web-/mobile-додаток);
- сервісного рівня (business-логіка, мікросервіси);
- рівня даних (бази даних, сховища документів, журнали аудиту);
- інтеграційного шару (API-шлюзи, шина даних, модулі взаємодії з зовнішніми реєстрами);
- інфраструктурного рівня (хмарні платформи, контейнери, системи моніторингу та логування).

Архітектурно Е-системи доцільно будувати за сервісно-орієнтованим або мікросервісним підходом. Це дає можливість масштабувати окремі модулі залежно від реального навантаження (наприклад, модуль авторизації, обробки платежів чи формування звітів), оновлювати їх незалежно один від одного та забезпечувати відмовостійкість через дублювання критичних компонентів. Для

взаємодії між сервісами використовуються REST або GraphQL API, повідомлення у чергах (message broker), а також стандартизовані формати обміну даними (JSON, XML).

Особлива увага приділяється механізмам ідентифікації та аутентифікації користувачів. У сучасних Е-сервісах застосовуються протоколи OAuth 2.0, OpenID Connect, двофакторна аутентифікація, електронний підпис та засоби Mobile ID. Це дозволяє прив'язати користувача до юридично значущої електронної ідентичності та забезпечити цілісність транзакцій. Для захисту даних використовуються шифрування каналів (HTTPS/TLS), токенна аутентифікація, контроль доступу на основі ролей (RBAC) та регулярний аудит безпеки.

Процес розробки Е-сервісів доцільно організовувати за гнучкими методологіями (Agile, Scrum, Kanban), що дає змогу швидко реагувати на зміни нормативно-правової бази та потреби користувачів. На етапі аналізу вимог важливо залучати кінцевих користувачів (представників органів влади, бізнесу, громадян), проводити інтерв'ю, юзабіліті-тестування прототипів і враховувати принципи UX/UI-дизайну: мінімізація кроків для отримання послуги, зрозуміла структура форм, підказки та валідація даних у реальному часі.

Важливим компонентом є інтеграція з зовнішніми системами: державними реєстрами, платіжними шлюзами, сервісами електронної пошти та SMS-сповіщень. Це дозволяє автоматизувати перевірку даних, підтвердження оплат, надсилання повідомлень про статус звернення чи заявки. Для забезпечення надійності інтеграції застосовуються черги повідомлень, механізми повторної доставки (retry), транзакційні журнали та моніторинг помилок.

Розгортання Е-систем доцільно виконувати в хмарній інфраструктурі із використанням контейнеризації (Docker) та систем оркестрації (Kubernetes). Такий підхід спрощує масштабування, дає можливість автоматичного відновлення сервісів у разі збоїв та забезпечує єдине середовище для розробки, тестування й експлуатації. Супровід системи включає моніторинг продуктивності, аналіз логів, періодичне оновлення компонентів, резервне копіювання даних і тестування планів відновлення після збоїв.

Окремим аспектом є відповідність Е-сервісів законодавству щодо захисту персональних даних та електронних довірчих послуг. Це передбачає мінімізацію збору персональної інформації, чітке визначення цілей її обробки, ведення журналів доступу та надання користувачеві можливості керувати своїми даними (перегляд, виправлення, видалення).

Висновки та перспективи. У дослідженні розглянуто ключові принципи розробки Е-сервісів та Е-систем: багаторівневу архітектуру, використання сучасних протоколів ідентифікації та захисту даних, застосування гнучких методологій розробки, інтеграцію з зовнішніми реєстрами та сервісами, використання хмарних платформ для масштабованості й відмовостійкості. Системний підхід до проектування, реалізації та супроводу дозволяє створювати Е-сервіси, що є зручними для користувачів, безпечними та придатними до довгострокової експлуатації.

Перспективними напрямками подальших досліджень є використання штучного інтелекту та аналітики даних для персоналізації Е-послуг, виявлення аномалій та шахрайських дій, а також розробка адаптивних архітектур, що автоматично масштабуються залежно від поточного навантаження та критичності операцій. Це сприятиме подальшому розвитку цифрової екосистеми та підвищенню якості публічних і комерційних Е-сервісів.

Список використаних джерел

1. Fielding R.T. Architectural Styles and the Design of Network-based Software Architectures. University of California, Irvine, 2000.
2. Newman S. Building Microservices: Designing Fine-Grained Systems. O'Reilly Media, 2021.
3. Richardson C. Microservices Patterns: With examples in Java. Manning Publications, 2019.

Мосійчук Вероніка Михайлівна
студентка 3 курсу, групи ТЦР-31
Державний університет інформаційно-комунікаційних технологій
vmosijcukusk@gmail.com
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний
інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

ЗАГРОЗИ КОНФІДЕНЦІЙНОСТІ ТА УРАЗЛИВОСТІ Е-СЕРВІСІВ У СУЧАСНОМУ ЦИФРОВОМУ СЕРЕДОВИЩІ

Постановка задачі. Стрімкий розвиток електронних сервісів призводить до зростання обсягів персональних даних, що обробляються у цифровому середовищі. Це стає причиною підвищеної уваги з боку кіберзлочинців, які використовують складні схеми атак для компрометації даних, доступу до конфіденційної інформації та порушення приватності користувачів. Уразливість може бути від помилок у веб-додатках до недоліків конфігурації серверів, неякісної автентифікації та слабого контролю доступу. З огляду на це виникає потреба у дослідженні типових загроз конфіденційності, причин їх виникнення та методів мінімізації ризиків.

Мета дослідження. Метою дослідження є аналіз ключових загроз конфіденційності в е-сервісах, визначення найбільш поширених уразливостей та оцінка технологічних і організаційних методів їх усунення для забезпечення захисту персональних даних користувачів.

Результати дослідження. Однією з основних загроз конфіденційності є перехоплення даних у процесі взаємодії користувача з е-сервісом. Через недостатню реалізацію шифрування передачі даних через HTTPS зловмисники використовують атаки типу Man-in-the-Middle, під час яких зловмисник може отримати доступ до персональної та службової інформації [1]. Значну роль у формуванні уразливостей відіграє несанкціонований доступ, що стає можливим через використання слабких методів автентифікації, відсутність багатофакторного захисту або неправильне зберігання облікових даних.

Також зловмисники часто використовують SQL-ін'єкції, XSS-атаки, CSRF-запити та помилки валідації даних. Вони дозволяють маніпулювати базами даних, змінювати бізнес-логіку або отримувати доступ до конфіденційної інформації без авторизації. Розглянемо детальніше SQL-ін'єкції. Вони виникають через небезпечну обробку вхідних даних у веб-застосунках. Основною причиною є те, що введені користувачем дані напряму потрапляють у SQL-запит, який виконується без додаткової перевірки чи обмежень, тим самим і наражають на небезпеку безпосередньо базу даних [2]. Щоб зменшити ризики порушення конфіденційності потрібно шифрувати дані у транзиті та на зберіганні, впроваджувати багатофакторну автентифікацію, сегментацію доступу

та регулярно оновлювати програмне забезпечення. Останнім часом все більше стає ефективно використовувати принципи Zero Trust, коли система аналізує сигнали користувача, пристрій, застосунок, місцезнаходження та рівень ризику в реальному часі. На основі цієї оцінки вона приймає рішення: дозволити доступ, вимагати додаткову автентифікацію або заблокувати запит [3]. Таким чином забезпечується захист даних і мінімізація ризику несанкціонованого доступу. Також важливим елементом є використання протоколів обміну ключами та ротація секретів, що зменшує ризики компрометації у разі витоку облікових даних. Приклад роботи Zero Trust зображено за рисунку 1.

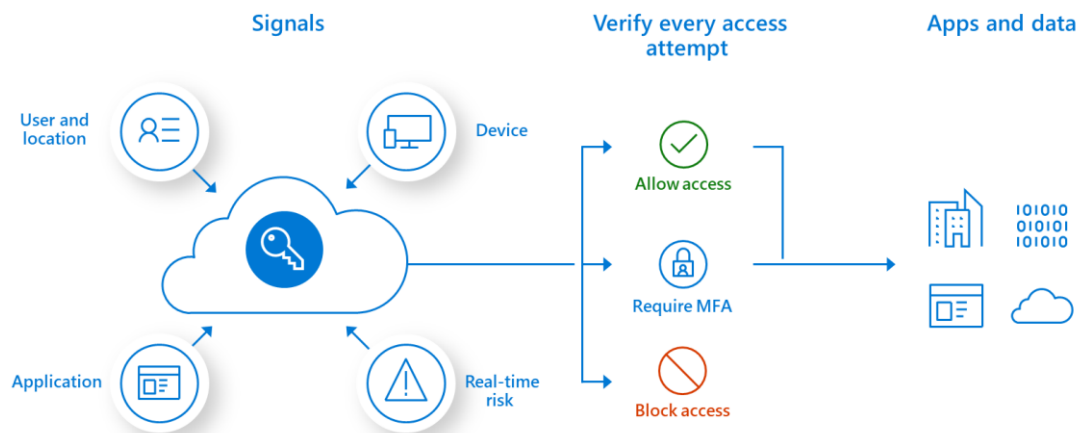


Рис. 1. Схема роботи Zero Trust-моделі

Для покращення конфіденційності та зменшення ризиків атак потрібно слідувати рекомендаціям OWASP, GDPR, NIST та ISO/IEC 27001. Їх використання дозволяє впорядкувати процеси контролю прав доступу та гарантувати відповідність міжнародним вимогам щодо обробки персональних даних.

Висновки та перспективи. Проведене дослідження показує, що конфіденційність е-сервісів залежить від поєднання технічних, організаційних та управлінських механізмів захисту. Компрометація даних зазвичай є наслідком не однієї уразливості, а сукупності недоліків у конфігурації системи, політиках доступу та процесах моніторингу, щоб зменшити ризики атак потрібно впровадження сучасних механізмів автентифікації, регулярне тестування безпеки, шифрування, аудит доступів та використання рекомендацій провідних стандартів. Зараз існує широке коло технологічних рішень, здатних значно підвищити конфіденційність і зменшити уразливість е-сервісів, а їх комплексне застосування формує основу стійких і надійних цифрових систем.

Список використаних джерел

1. OWASP. Manipulator-in-the-middle attack (MITM) [Електронний ресурс]. – Режим доступу: https://owasp.org/www-community/attacks/Manipulator-in-the-middle_attack (дата звернення: 30.11.2025).

2. OWASP Foundation. SQL Injection [Электронный ресурс]. – 2025. – Режим доступа: https://owasp.org/www-community/attacks/SQL_Injection (дата обращения: 30.11.2025).
3. Zero trust security: what it is and why it is important [Электронный ресурс]. – 2023. – Режим доступа: <https://www.ibm.com/topics/zero-trust> (дата обращения: 30.11.2025).

Новостройний Дмитро Андрійович
студент 3 курсу, групи ТЦР-31
Державний університет інформаційно-комунікаційних технологій
063-526-01-06
novostroinyidima23@gmail.com
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний
інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В Е-СЕРВІСІ «ДОБРОДІЙ» ДЛЯ КООРДИНАЦІЇ ВОЛОНТЕРСЬКИХ ПОДІЙ

Постановка задачі. Е-сервіс «ДоброДій» як платформа для пошуку та координації волонтерів оперує значними обсягами чутливої інформації: персональні дані волонтерів (ПІБ, контакти, дата народження, місце проживання), дані про організаторів, геолокацію подій, історію участі, рейтинги та відгуки. Уся ця інформація підпадає під дію законодавства України про захист персональних даних [1], а її компрометація може призвести до порушення конфіденційності, дискримінації користувачів, втрати довіри до платформи та партнерських організацій.

Додатковим фактором ризику є інтеграція з державними сервісами електронної ідентифікації та підпису, зокрема «Дія» (шеринг документів, Дія.Підпис, авторизація за допомогою мобільного застосунку) [4] та Системою BankID НБУ як механізмом віддаленої ідентифікації користувачів [5]. Такі інтеграції вимагають підвищеного рівня захисту каналів зв'язку, коректної реалізації протоколів авторизації та належної обробки отриманих атрибутів.

Водночас веб-застосунки залишаються однією з основних цілей атак, пов'язаних із вразливостями рівня застосунку (ін'єкції, помилки автентифікації, неправильне керування сесіями, XSS, конфігураційні помилки тощо), що систематизовані у переліку OWASP Top 10 [2]. Ігнорування цих ризиків при проєктуванні е-сервісу, який обробляє персональні дані та виконує функції автентифікації, створює загрозу як для користувачів, так і для організацій, що використовують платформу.

Отже, постає задача побудови е-сервісу «ДоброДій» із вбудованим комплексом механізмів інформаційної безпеки («security by design»): від моделювання загроз на рівні архітектури до впровадження технічних і організаційних заходів, що забезпечують конфіденційність, цілісність і доступність даних у відповідності з чинним законодавством та кращими міжнародними практиками [1-3].

Мета дослідження. Метою дослідження є розроблення підходу до проєктування е-сервісу «ДоброДій» з урахуванням вимог інформаційної безпеки, що включає захист персональних даних користувачів, безпечні механізми

автентифікації та авторизації, а також забезпечення цілісності та доступності інформації в умовах інтеграції з державними системами електронної ідентифікації [1; 4-6].

Для досягнення цієї мети необхідно:

- проаналізувати нормативно-правові вимоги до обробки персональних даних та інформаційної безпеки веб-сервісів в Україні [1];
- виконати моделювання загроз для архітектури «ДоброДій» з урахуванням типових ризиків, описаних у стандартах OWASP Top 10 та OWASP ASVS [2-3];
- визначити вимоги до автентифікації та керування сесіями, включно з інтеграцією з «Дією» та BankID НБУ [4-5];
- сформулювати перелік технічних і організаційних заходів для забезпечення конфіденційності, цілісності й доступності даних;
- окреслити підходи до резервного копіювання, відновлення після збоїв, логування та моніторингу інцидентів безпеки з урахуванням кращих практик галузі [2-3].

Результати дослідження. У ході роботи було змодельовано загрози для е-сервісу «ДоброДій» та сформовано принципи безпечної архітектури. Архітектура розглядається як багатошарова система, що включає клієнтський рівень (браузер або мобільний застосунок), рівень веб-API, рівень сховища даних (база даних), а також інтеграційний рівень для взаємодії з державними е-сервісами - «Дією», BankID НБУ та іншими провайдерами електронної ідентифікації [4-6]. Для кожного з цих рівнів було ідентифіковано типові загрози (перехоплення сесій, ін'єкційні атаки, XSS, спуфінг, ескалація привілеїв, атаки «людина посередині» тощо) на основі рекомендацій OWASP Top 10 та OWASP ASVS [2-3], що дало змогу обґрунтувати використання HTTPS, сегментації мережевої інфраструктури, принципу найменших привілеїв та централізованого логування подій безпеки.

На цій основі запропоновано комбінований підхід до автентифікації користувачів: поєднання класичної схеми логін/пароль із безпечним зберіганням хешів (алгоритми типу bcrypt/Argon2 із сіллю) та підтримкою зовнішніх провайдерів ідентичності - «Дія» (авторизація за Дія.Підписом, антибот-механізми) [4], BankID НБУ [5] і ID.GOV.UA [6]. Керування сесіями реалізується на основі токенів JWT із чітко визначеним строком дії та можливістю їх відкликання у випадку виходу із системи або підозри на компрометацію, при цьому враховуються вимоги OWASP ASVS до автентифікації, сесій та контролю доступу [3]. Розмежування прав реалізовано через рольову модель (гостьовий користувач, волонтер, організатор, адміністратор) із мінімально необхідними повноваженнями для кожної ролі та обов'язковим аудитом критичних дій.

Захист персональних даних у системі узгоджено з вимогами Закону України «Про захист персональних даних» [1] шляхом впровадження багаторівневої валідації введення, використання ORM та параметризованих запитів для запобігання SQL-ін'єкціям, контекстного кодування виводу для захисту від XSS і застосування механізмів CSRF-захисту [2-3]. Реалізовано принципи мінімізації обсягу зібраних даних і обмеження строку їх зберігання [1], а чутливі дані

(паролі, токени, ключі) не зберігаються у відкритому вигляді, для криптографічних операцій застосовуються рекомендовані OWASP алгоритми [2-3].

Висновки та перспективи. Е-сервіс «ДоброДій» як платформа для координації волонтерських подій повинен проєктуватися з урахуванням принципів «security by design» та «privacy by design», коли вимоги до безпеки й захисту персональних даних закладаються на ранніх етапах життєвого циклу системи [1-3]. Проведене моделювання загроз і аналіз нормативно-правової бази засвідчили необхідність комплексного підходу, що поєднує технічні, організаційні та процедурні заходи.

Запропонований набір рішень - багаторівнева архітектура із сегментацією, захищена автентифікація й авторизація (включно з інтеграцією з «Дією» та BankID НБУ) [4-6], захист даних і валідація введення згідно з рекомендаціями OWASP - створює основу для надійного функціонування е-сервісу «ДоброДій» та формування довіри з боку волонтерів, організаторів і партнерів.

Перспективами подальших досліджень є детальніша адаптація вимог OWASP ASVS до конкретної архітектури «ДоброДій» [3], розробка формальної моделі загроз для ключових бізнес-процесів платформи, упровадження практик безпечної розробки (Secure SDLC), а також інтеграція автоматизованих засобів сканування вразливостей і моніторингу безпеки у процес розробки та супроводу системи.

Список використаних джерел

1. Про захист персональних даних. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 25.11.2025).
2. OWASP Top Ten | OWASP Foundation. *OWASP Foundation, the Open Source Foundation for Application Security*. URL: <https://owasp.org/www-project-top-ten/> (дата звернення: 25.11.2025).
3. OWASP Application Security Verification Standard (ASVS) | OWASP Foundation. *OWASP Foundation, the Open Source Foundation for Application Security*. URL: <https://owasp.org/www-project-application-security-verification-standard/> (дата звернення: 25.11.2025).
4. Інтеграція Дії. *Офіційний портал інтеграції сервісів «Дія»*. URL: <https://integration.diia.gov.ua/> (дата звернення: 25.11.2025).
5. BankID НБУ. *Національний банк України*. URL: <https://bank.gov.ua/ua/bank-id-nbu> (дата звернення: 25.11.2025).
6. Інтегрована система електронної ідентифікації. *Державне підприємство «ДІЯ»*. URL: <https://se.diia.gov.ua/integrated-system-of-electronic-identification> (дата звернення: 25.11.2025).

Озеров Данііл Олександрович
студент 3 курсу, групи ТЦР-33
Державний університет інформаційно-комунікаційних технологій
(050) 553-49-77
st8541433@stud.duikt.edu.ua
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний
інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

ОСОБЛИВОСТІ АРХІТЕКТУРИ ВИСОКОНАВАНТАЖЕНОЇ ТЕЛЕМЕДИЧНОЇ ПЛАТФОРМИ ДЛЯ МОНІТОРИНГУ ХРОНІЧНИХ ЗАХВОРЮВАНЬ

Постановка задачі. Цифрова трансформація сфери охорони здоров'я є одним із пріоритетних напрямків розвитку як в Україні, так і у світі. Ринок телемедицини демонструє щорічний приріст понад 15%, що зумовлено зростаючою потребою пацієнтів у дистанційному доступі до медичних послуг. Особливої актуальності це набуває для людей з хронічними захворюваннями, які потребують постійного, а не епізодичного нагляду лікаря. Однак, створення програмних рішень для цієї сфери пов'язане з низкою технічних викликів. На відміну від звичайних e-commerce проєктів або інформаційних порталів, медичні платформи, такі як розроблювана система "CustosMed", вимагають принципово іншого підходу до надійності. Будь-яка затримка у передачі даних, втрата з'єднання під час консультації або збій у базі даних історії хвороб може мати критичні наслідки для здоров'я пацієнта. Тому ключовою проблемою дослідження є пошук та обґрунтування архітектурних патернів, здатних забезпечити відмовостійкість, масштабованість та безпеку високонавантаженої системи.

Мета дослідження. Метою даної роботи є проєктування та програмна реалізація серверної архітектури телемедичної платформи "CustosMed", яка забезпечує безперебійну роботу сервісів відеозв'язку, обробку великих масивів медичних даних у реальному часі та відповідність міжнародним стандартам доступності (SLA 99.9%).

Результати дослідження. У ході аналізу вимог до системи було обрано сервіс-орієнтований архітектурний підхід (SOA). В якості основної технології для реалізації серверної частини (Back-end) обрано фреймворк Django та Django REST Framework (DRF). Вибір Python-екосистеми зумовлений трьома факторами:

- Швидкість розробки: Django надає "з коробки" надійні механізми автентифікації, адміністрування та роботи з базами даних (ORM), що дозволяє зосередитися на бізнес-логіці.

- Інтеграція з AI: Оскільки платформа передбачає модуль AI-діагностики, використання Python дозволяє інтегрувати бібліотеки машинного навчання (PyTorch, TensorFlow, scikit-learn) безпосередньо в бекенд, без необхідності створення складних мікросервісних мостів з іншими мовами.

- Безпека: Вбудовані механізми захисту від поширених вразливостей (CSRF, XSS, SQL Injection).

Архітектура системи складається з наступних компонентів:

- Рівень API (Interface Layer): Реалізований на Django REST Framework. Він відповідає за обробку HTTP-запитів від мобільного додатку (React Native) та веб-клієнта, валідацію вхідних даних (serializers) та формування відповідей у форматі JSON.

- Рівень асинхронної взаємодії (Real-time Layer): Для забезпечення функціонування чатів та сигналіну відеодзвінків використано технологію Django Channels та протокол WebSockets. Це дозволяє серверу підтримувати постійне з'єднання з клієнтом і миттєво передавати сповіщення або дані про вхідний дзвінок.

- Рівень даних (Data Layer): В якості основної СУБД використовується PostgreSQL, що забезпечує ACID-транзакційність, критично важливу для медичних записів. Для пришвидшення роботи системи та зберігання сесій користувачів впроваджено in-memory сховище Redis.

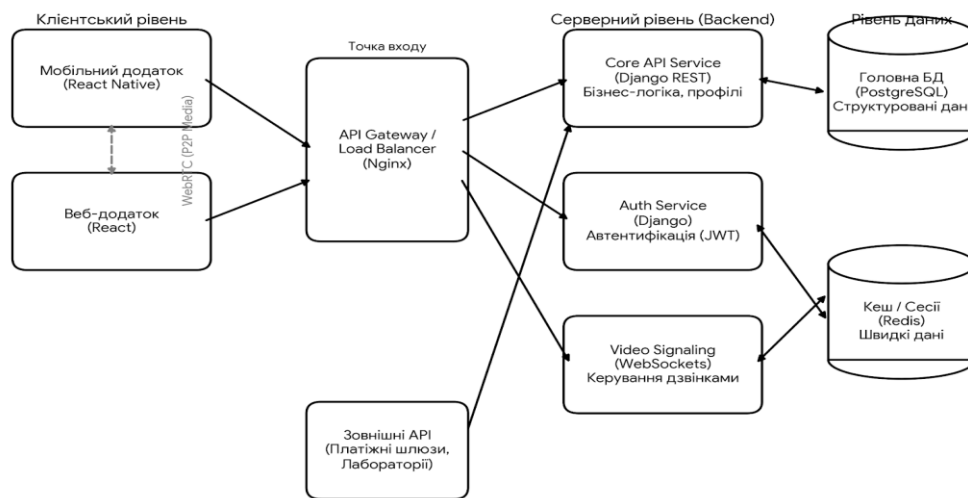


Рис. 1. Структурна схема архітектури платформи "CustosMed"

Окрему увагу приділено реалізації відеозв'язку. Оскільки передача відеопотоку через сервер створює надмірне навантаження, було використано технологію WebRTC (Peer-to-Peer). Серверна частина на Python виступає лише в ролі сигнального сервера (Signaling Server), який допомагає двом клієнтам "знайти" один одного в мережі та встановити пряме з'єднання для передачі медіа-даних.

Висновки та перспективи. Розроблена архітектура платформи "CustosMed" на базі Python та Django довела свою ефективність для вирішення

задач телемедицини. Використання Django REST Framework дозволило швидко реалізувати надійний API, а інтеграція Django Channels забезпечила роботу функцій реального часу. Такий підхід не лише гарантує стабільність поточної версії системи, але й створює ідеальну основу для подальшого розвитку AI-модулів, оскільки вся система функціонує в єдиному мовному середовищі Python.

Список використаних джерел

1. Trofimova I., Vlasenko O. Cloud Technologies in Telemedicine: Security and Architecture // Journal of e-Health. – 2024. – Vol. 12. – P. 45-52.
2. Richardson C. Microservices Patterns: With examples in Java. – Manning Publications, 2018. – 480 p.
3. Офіційна документація Django Project [Електронний ресурс]. – Режим доступу: <https://www.djangoproject.com/> (дата звернення: 25.11.2025).
4. Grinberg M. Flask Web Development (порівняльний аналіз Python-фреймворків). – O'Reilly Media, 2018.

Осіпчук Дмитрій Миколайович
студент 4 курсу, групи ПЗ-12122
«Національний транспортний університет»
(068) 981-94-79
dmytrii1337@gmail.com

Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій
spopereshnyak@gmail.com

ПРОЄКТУВАННЯ Е-СЕРВІСУ ЗАХИЩЕНОГО ОБМІНУ ПОВІДОМЛЕННЯМИ ДЛЯ ОСВІТНЬОГО СЕРЕДОВИЩА НА БАЗІ ДЕЦЕНТРАЛІЗОВАНОГО ПРОТОКОЛУ TOX

Постановка задачі. Активна діджиталізація навчального процесу призвела до масового впровадження електронних журналів, систем дистанційного навчання, корпоративної пошти та чат-платформ для оперативної взаємодії викладачів і здобувачів освіти. На практиці для неформального та службового спілкування часто використовуються загальнодоступні централізовані месенджери (Telegram, WhatsApp, Discord тощо), які зберігають службові дані та метадані користувачів на власних серверах і не завжди дозволяють виконати вимоги внутрішніх політик безпеки закладу освіти. Це створює ризики витоку конфіденційної інформації, проблеми з контролем доступу та залежність від сторонньої інфраструктури.

Альтернативою є побудова спеціалізованих Е-сервісів захищеного обміну повідомленнями, які інтегруються з існуючими інформаційними системами навчального закладу та дають змогу знизити обсяг чутливих даних, що передаються через сторонні платформи. Одним з технічних рішень для таких сервісів може стати використання децентралізованого протоколу Tox, що реалізує повністю peer-to-peer модель взаємодії: користувачі спілкуються без проміжних серверів, ідентифікуються за допомогою криптографічних ключів (Tox ID), а весь трафік шифрується засобами бібліотеки NaCl/libsodium. Завдяки цьому відсутнє централізоване сховище повідомлень, а маршрут передачі даних формується динамічно через розподілену DHT-мережу.

Утім, пряме використання «чистого» Tox у навчальному середовищі викликає додаткові питання: як пов'язати анонімні Tox ID з обліковими записами студентів, як реалізувати політики доступу до навчальних груп, як забезпечити мінімальне адміністрування й моніторинг без порушення принципів децентралізації. Тому постає задача розроблення архітектури Е-сервісу захищених повідомлень, який спирається на протокол Tox як транспортний рівень, але інтегрований з існуючою інфраструктурою університету.

Мета дослідження. Метою дослідження є проєктування та апробація архітектури Е-сервісу захищеного обміну повідомленнями для закладу вищої

освіти, у якій децентралізований протокол Тох використовується як основа міжкористувацької комунікації. Для досягнення цієї мети передбачається:

- виконати аналіз вимог до сервісу з погляду інформаційної безпеки, інтеграції з існуючими інформаційними системами (система керування навчальним процесом, єдина база користувачів), а також зручності використання для викладачів і студентів;

- дослідити можливості Тох щодо шифрування, маршрутизації та ідентифікації користувачів, зокрема особливості формування Тох ID, роботи розподіленої DHT-мережі та застосування схеми NaCl Box (Curve25519 + XSalsa20-Poly1305);

- розробити логічну та фізичну архітектуру Е-сервісу, що поєднує локальну інфраструктуру університету (сервери автентифікації, веб-портالي) з клієнтами Тох на пристроях користувачів;

- провести експериментальну перевірку працездатності прототипу в лабораторному середовищі, оцінити затримки передачі, стійкість до відмов окремих вузлів, а також організаційні аспекти впровадження такого сервісу в навчальний процес.

Результати дослідження. У результаті аналізу вимог сформовано модель ролей користувачів (адміністратор системи, викладач, студент) та сценарії використання Е-сервісу: оперативне інформування групи, обговорення завдань, консультації з викладачем, тимчасові робочі чати проєктних команд. Для кожного сценарію визначено вимоги до конфіденційності, цілісності й доступності даних, а також до ідентифікації учасників. На цій основі спроектовано багатопарову архітектуру сервісу.

Мережевий шар базується на протоколі Тох: клієнтські застосунки встановлюють з'єднання з мережею через публічні bootstrap-вузли й надалі взаємодіють у режимі P2P, використовуючи NaCl для шифрування трафіку та розподілену хеш-таблицю для пошуку адресатів. Над ним розташовано сервісний шар університету, що не перехоплює вміст зашифрованих повідомлень, але відповідає за відображення структури навчальних груп, прив'язку Тох ID до внутрішніх записів користувачів і керування налаштуваннями доступу. Для цього запроваджено окреме сховище метаданих, де зберігаються хешовані відповідності між університетськими логінами та Тох ID, без зберігання ключів шифрування або історії листування.

Реалізований прототип передбачає два варіанти доступу користувачів: через окремий настільний/мобільний клієнт Тох, налаштований на використання профілю, та через легкий веб-інтерфейс, який працює як «тонкий міст» до локально запущеного клієнта. Архітектура дозволяє викладачеві створити «канал курсу», до якого додаються Тох-ідентифікатори всіх студентів групи; фактичний обмін повідомленнями при цьому здійснюється безпосередньо між вузлами мережі Тох, а університет лише допомагає зі списком учасників.

Експериментальне тестування прототипу в умовах лабораторної мережі та при підключенні до публічних bootstrap-вузлів показало, що середній час доставлення коротких текстових повідомлень залишається прийнятним для

інтерактивного спілкування, а відмова окремих вузлів чи тимчасова недоступність bootstrap-серверів не призводить до повної втрати працездатності сервісу, завдяки розподіленій природі DHT-мережі. Додатково проаналізовано особливості моделі загроз для Tox: витік IP-адрес учасників, потенційні атаки на bootstrap-вузли, можливість використання мережі як каналу керування шкідливим ПЗ, про що згадують дослідження з кібербезпеки. На основі цього сформульовано рекомендації щодо використання VPN-тунелювання, обмеження списку довірених bootstrap-вузлів та поєднання Tox із засобами мережевого моніторингу.

Висновки та перспективи. Запропонована концепція E-сервісу захищеного обміну повідомленнями демонструє, що децентралізований протокол Tox може бути використаний як транспортна основа міжмережевої інформаційної технології в освітньому середовищі за умови чіткого розмежування технічних і організаційних функцій. Протокол забезпечує криптографічний захист вмісту повідомлень і відсутність централізованого сховища даних, тоді як університетська інфраструктура відповідає за керування обліковими записами, структуру навчальних груп та застосування політик доступу.

Разом із тим, результати аналізу вказують на низку обмежень: складність для кінцевих користувачів у керуванні ключами та Tox ID, чутливість до налаштувань мережевого оточення, відсутність зрілих клієнтів для усіх мобільних платформ порівняно з більш популярними месенджерами. Тому впровадження таких рішень доцільно розглядати як доповнення до існуючих каналів комунікації для окремих груп користувачів із підвищеними вимогами до конфіденційності, а подальші дослідження варто зосередити на автоматизації розгортання клієнтів, інтеграції з системами єдиного входу (SSO) та порівняльному аналізі з іншими децентралізованими протоколами, такими як Matrix або Briar.

Список використаних джерел

1. Tox (protocol). – Wikipedia, the free encyclopedia. – Режим доступу: [https://en.wikipedia.org/wiki/Tox_\(protocol\)](https://en.wikipedia.org/wiki/Tox_(protocol)). [3]
2. The Tox Project. Офіційний сайт протоколу Tox. – Режим доступу: <https://tox.chat>.
3. TokTok Project. The Tox Reference (Protocol Specification). – Режим доступу: <https://zetok.github.io/tox-spec/>.
4. Secure Chat Guide. Messaging Protocols: Tox. – Огляд криптографічних властивостей протоколу Tox та клієнтів.
5. KR Labs Research. «У пошуках безпечного месенджера»: огляд сучасних протоколів захищеного обміну повідомленнями (Signal, Matrix, Tox та ін.).

СИСТЕМА ІНТЕЛЕКТУАЛЬНОЇ ПЕРЕВІРКИ ЗАГРОЗ У БЕЗДРОТОВИХ МЕРЕЖАХ ДЛЯ Е-ПОСЛУГ ТА SMART-СИСТЕМ

Актуальність дослідження. Розвиток е-послуг, Smart-міст, телемедицини, електронної освіти й мобільних сервісів формує зростаючу залежність від захищених бездротових мереж. Однак Wi-Fi-інфраструктури характеризуються відкритістю радіоканалу, наявністю шифрування, що обмежує інспекцію вмісту, та високою варіабельністю пристроїв і протоколів. Традиційні сигнатурні системи реагування запізнюються щодо нових загроз, а просте фільтрування трафіку не підтримує необхідний рівень безпеки. Актуальним є створення інтелектуальної системи перевірки загроз, що здатна класифікувати атаки і аномалії без доступу до вмісту пакетів, опираючись лише на метадані та поведінкові патерни.

Постановка задачі. Потрібно розробити систему, яка:

- здійснює збір характеристик бездротового трафіку без дешифрування;
- аналізує та класифікує загрози для е-послуг і Smart-систем;
- працює в реальному часі та придатна до змін характеру атак;
- інтегрується з цифровими сервісами як система превентивного захисту.

Мета дослідження. Метою роботи є створення системи інтелектуальної перевірки загроз у бездротових мережах, що забезпечує превентивний захист е-послуг та Smart-систем на основі класифікаційного аналізу мережесих метаданих і поведінкових ознак.

Результати дослідження. Запропонована модель включає чотири взаємопов'язані компоненти:

Запропонована система поєднує збір характеристик мережевого трафіку, аналітику метаданих та класифікаційне моделювання, яке використовує:

- статистичні параметри (інтенсивність кадрів, співвідношення службових і data-пакетів, розподіл розмірів кадрів);
- часові ознаки (динаміка затримок, частота повторних передач, аномальні зміни АСК);
- поведінкові індикатори пристрою (зміна MAC-ідентифікаторів, типові/нетипові запити аутентифікації, ширококомовна активність).

Моделі машинного навчання зіставляють ці ознаки з типами небезпечних взаємодій (DoS-атаки, підміна точки доступу, ARP-spoofing, ін'єкційні атаки, фіктивні ширококомовні запити), що дозволяє виявляти загрози без доступу до вмісту пакетів.

Схема на рисунку 1 відображає інтеграцію аналізу мережесих метаданих зі стратегіями захисту е-послуг та Smart-інфраструктур, що забезпечує автоматичну перевірку загроз у режимі реального часу.

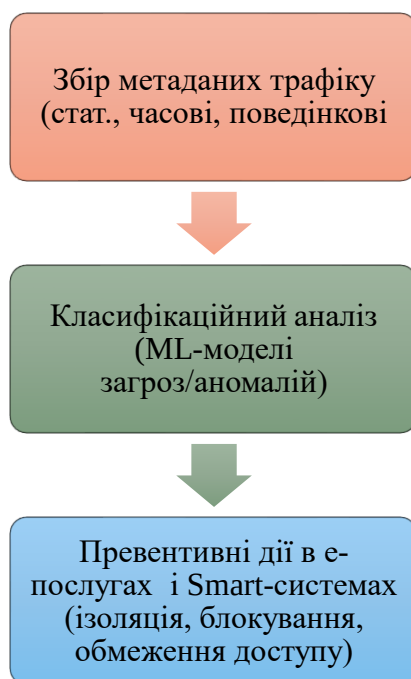


Рис. 1. Система інтелектуальної перевірки загроз у бездротових мережах

Для оцінки якості класифікаційного модуля порівнювали три підходи (табл. 1): SVM, Random Forest (RF) та просту глибинну мережу (DNN). Навчання проводилось на збалансованій вибірці нормального та атакуючого трафіку, сформованій із використанням описаних вище ознак.

Таблиця 1.

Порівняльні результати класифікаційних моделей

Модель	Accuracy	Precision	Recall	F1-score	Коментар
SVM	0,93	0,92	0,90	0,91	Стабільна модель, чутлива до вибору ядра та масштабування ознак
RF	0,96	0,95	0,95	0,95	Найкращий баланс якості й інтерпретованості; добре працює на змішаних ознаках
DNN	0,97	0,96	0,96	0,96	Максимальна якість, але вищі вимоги до обчислювальних ресурсів і обсягу навчальних даних

Результати показують, що вже класичні ансамблеві моделі (Random Forest) за умови коректно підібраної системи ознак забезпечують високу точність виявлення загроз у бездротових мережах. Глибинні мережі дають незначне додаткове покращення показників, однак потребують більше ресурсів і складніші в налаштуванні, що важливо враховувати під час інтеграції системи в е-послуги та Smart-платформи з обмеженими обчислювальними можливостями (маршрутизатори, вбудовані шлюзи тощо).

Система працює як сервіс безпеки цифрової інфраструктури: перевірка загроз може виконуватися на рівні маршрутизатора, шлюзу Smart-мережі або в хмарній платформі е-послуг. Передача лише агрегованих ознак знижує навантаження та гарантує конфіденційність даних користувача, що важливо для державних сервісів, e-health, e-learning та Smart-міст. Завдяки адаптивним моделям класифікації система здатна швидко змінювати параметри, розрізняючи нові типи атак та їх комбінації.

Висновки та перспективи. Система інтелектуальної перевірки загроз забезпечує превентивний захист е-послуг і Smart-інфраструктур без потреби в аналізі зашифрованого трафіку. Використання метаданих та поведінкових ознак дозволяє скоротити час виявлення атаки, підвищити точність діагностики та мінімізувати вплив на продуктивність сервісів.

Подальші дослідження доцільно спрямувати на побудову модулів прогностичного захисту з використанням нейроеволюційних моделей та аналізу комплексних гібридних атак.

Список використаних джерел

1. Ahmad R., Wazirali R., Abu-Ain T. Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues // *Sensors*. – 2022. – Vol. 22, No. 13. – Art. 4730. – DOI: 10.3390/s22134730. MDPI
2. Alsoufi M. A., Siraj M. M., Ghaleb F. A., Al-Razgan M., Al-Asaly M. S. et al. Anomaly-Based Intrusion Detection Model Using Deep Learning for IoT Networks // *Computer Modeling in Engineering & Sciences*. – 2024. – Vol. 141, No. 1. – P. 823–845. – DOI: 10.32604/cmescs.2024.052112. techscience.com
3. Nguyen T. M., Vo H. H.-P., Yoo M. Enhancing Intrusion Detection in Wireless Sensor Networks Using a GSWO-CatBoost Approach // *Sensors*. – 2024. – Vol. 24, No. 11. – Art. 3339. – DOI: 10.3390/s24113339. MDPI
4. Pandey V. K., Prakash S., Gupta T. K. et al. Enhancing Intrusion Detection in Wireless Sensor Networks Using a Tabu Search Based Optimized Random Forest // *Scientific Reports*. – 2025. – Vol. 15, No. 1. – Art. 18634. – DOI: 10.1038/s41598-025-03498-3.

Паращинець Андрій Михайлович

студент 3 курсу, групи ТЦР-32

Державний університет інформаційно-комунікаційних технологій

(063)6775955

st8526211@stud.duikt.edu.ua

Поперешняк Світлана Володимирівна

к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії

Національний технічний університет України "Київський політехнічний

інститут імені Ігоря Сікорського"

spopereshnyak@gmail.com

ГЕОСЕРВІС ДЛЯ АГРЕГАЦІЇ АСОРТИМЕНТУ ТА АКЦІЙ МАГАЗИНІВ В ПЕВНОМУ РАДІУСІ

Постановка задачі. У сучасному цифровому середовищі користувачі дедалі частіше потребують швидкого й зручного доступу до актуальної інформації про товари, ціни та акційні пропозиції у магазинах поблизу. Значна кількість торгових точок, динамічні зміни асортименту та часті цінові коливання створюють проблему ефективного пошуку оптимальних пропозицій. Наявні платформи зазвичай охоплюють лише окремі сегменти ринку, що не забезпечує комплексного відображення локального асортименту. У зв'язку з цим виникає необхідність у створенні геосервісу, який би у режимі реального часу агрегував дані про магазини в радіусі 10 км та надавав користувачу інформацію про асортимент, акції, наявність товарів і можливість бронювання.

Мета дослідження. Метою роботи є розробка концепції геосервісу, що забезпечує збір, обробку та представлення інформації про магазини різних категорій у визначеному радіусі. Дослідження передбачає визначення архітектури сервісу, аналіз механізмів інтеграції з торговими точками та вивчення методів обробки даних, які дозволяють забезпечити високу точність, актуальність і корисність інформації для користувачів.

Результати дослідження. Опрацьовані наукові джерела свідчать про важливість геолокаційних технологій для формування сучасних сервісів, що працюють з просторовими даними та відображають їх у зручному вигляді [1]. Реалізація ефективної системи можлива за рахунок інтеграції з магазинами через API, що забезпечує швидкий обмін даними та їх актуальність [2]. Модель роботи з агрегованими даними потребує використання алгоритмів аналізу великих масивів інформації, що підтверджується дослідженнями у сфері big data у роздрібній торгівлі [3]. При розробці системи рекомендацій враховано підходи з галузі геолокаційних рекомендаційних моделей, які дають можливість адаптувати дані до індивідуальних потреб користувача [4]. Функціонал об'єднання даних із різних магазинів базується на принципах мультиджерельної

агрегації, що забезпечує узгоджене представлення асортименту та акцій, як це описано у відповідних наукових роботах [5].

Висновки та перспективи. Результати дослідження дозволили сформувати концепцію геосервісу, здатного ефективно агрегувати асортимент та акційні пропозиції магазинів у радіусі 10 км. Система, що ґрунтується на геолокаційних алгоритмах, API-інтеграціях та методах аналізу великих даних, може істотно підвищити зручність пошуку товарів і забезпечити користувача актуальною інформацією в реальному часі.

Перспективи розвитку включають застосування інтелектуальних алгоритмів персоналізації, розширення кола інтегрованих магазинів та впровадження інструментів автоматичного прогнозування змін цін і наявності товарів.

Список використаних джерел

1. Li X., Chang Z., He Q. Location-based services and geospatial data aggregation in modern smart city ecosystems. *Journal of Urban Informatics*. 2023. Vol. 7, No. 1, P. 54–72.
2. Silva R., Monteiro A., Torres J. Real-time data integration in retail information systems: a comprehensive survey. *International Journal of Information Management*. 2022. Vol. 64, P. 102–125.
3. Kumar S., Iqbal F., Yoon J. Big data analytics in retail: methods, applications and challenges. *Information Systems Frontiers*. 2021. Vol. 23, P. 1345–1362.
4. Zhang Y., Chen L. Geolocation-based recommendation systems for consumer decision support. *ACM Computing Surveys*. 2020. Vol. 53, No. 4, P. 1–33.
5. Martinelli E., Russo M. Aggregation of multi-source product data for e-commerce platforms. *IEEE Access*. 2022. №10, P. 115432–115447.

Пітецький Кирило Миколайович
Студент 3 курсу, групи ТЦР-34
Державний університет інформаційно-комунікаційних технологій
Тільний Олександр Віталійович
Студент 3 курсу, групи ТЦР-34
Державний університет інформаційно-комунікаційних технологій
Науковий керівник:
Поперешняк Світлана Володимирівна,
к.ф.-м.н., доцент кафедри технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій
spopereshnyak@gmail.com

ЦИФРОВИЙ СЕРВІС УПРАВЛІННЯ ДАНИМИ ДОМАШНІХ ТВАРИН НА ОСНОВІ ІНТЕРАКТИВНОЇ ВЕБ-ПЛАТФОРМИ

Постановка задачі. У сучасних умовах стрімкої цифровізації різних сфер життєдіяльності особливої актуальності набуває впровадження електронних інструментів у галузі догляду за домашніми тваринами. Значний обсяг інформації, зокрема паспортні відомості, дані про вакцинації та ветеринарні довідки, досі зберігається у паперовому вигляді, що призводить до втрат документів, порушення їх цілісності та відсутності єдиного джерела актуальних даних. Це суттєво ускладнює доступ до медичної інформації, не дозволяє оперативно підтвердити ідентифікаційні відомості тварини й не забезпечує централізованого обліку історії щеплень. Таким чином, виникає об'єктивна потреба у створенні цифрової системи, яка б уніфікувала, зберігала та структуровано подавала інформацію про тварин, забезпечуючи її постійну доступність і захищеність.

Мета дослідження. Метою роботи є розроблення інтерактивної веб-платформи, яка дозволяє оцифровувати паспортні та медичні дані домашніх тварин, забезпечувати їх безпечне зберігання та надавати швидкий доступ через зрозумілий інтерфейс і QR-код. Платформа покликана підтримувати процеси реєстрації та авторизації користувачів, створення, редагування та видалення цифрових паспортів тварин, ведення й актуалізації медичних записів, а також формування унікального QR-коду як засобу оперативного отримання основної інформації у разі потреби. Окремим завданням є створення сучасного інтерфейсу, що відповідає принципам державних цифрових сервісів.

Результати. У межах дослідження спроектовано та реалізовано веб-додаток, що складається з клієнтської частини на основі React та серверної частини, побудованої з використанням Node.js і фреймворку Express. Реалізовано повноцінний механізм роботи з обліковими записами користувачів: реєстрація та авторизація здійснюються за допомогою JWT-токенів, що забезпечує належний рівень захисту персональних даних.

Створено цифровий паспорт тварини, який містить структуровані дані про ім'я, вид, породу, дату народження, унікальний ідентифікаційний номер,

фотографію та відомості про власника. Інформацію можна оновлювати та видаляти через інтерфейс системи.

Важливим елементом роботи є модуль вакцинацій, у якому передбачено можливість внесення нових записів із зазначенням препарату і дати щеплення, перегляду повної хронології вакцинацій та видалення застарілої або некоректної інформації. Дані автоматично впорядковуються у часовій послідовності. Для цього у базі даних створено окрему таблицю з прив'язкою до конкретної тварини.

До функціоналу платформи інтегровано генерацію QR-коду, що містить унікальний ідентифікатор тварини. Завдяки цьому доступ до ключових даних може бути отриманий миттєво, наприклад, у ветеринарній клініці або у випадку втрати тварини.

Інтерфейс веб-додатка виконано у стилі сучасних державних цифрових сервісів: застосовано мінімалістичний дизайн, плавні анімації, адаптивність для різних типів пристроїв, модальні вікна та інтерактивні картки, що сприяє підвищенню зручності користування.

База даних реалізована на основі ORM Sequelize та містить структуровані таблиці користувачів, тварин і вакцинацій. Забезпечено валідацію даних, коректні зв'язки між таблицями та каскадне видалення пов'язаних записів.

Висновки. Створена веб-платформа демонструє потенціал цифрових рішень у сфері догляду за домашніми тваринами, забезпечуючи значно вищий рівень доступності та збереження даних порівняно з традиційними паперовими паспортами. Система дозволяє підтримувати актуальність медичної інформації, швидко надавати доступ до неї за допомогою QR-коду, а також створює умови для ефективної взаємодії власників тварин із ветеринарними закладами.

У перспективі платформу можна розширити шляхом інтеграції з державними та приватними ветеринарними сервісами, упровадження мобільного застосунку та створення системи автоматичних нагадувань про необхідність проведення чергових вакцинацій.

Список використаних джерел

1. React Documentation [Електронний ресурс]. – Режим доступу: <https://react.dev> (дата звернення: 15.11.2025).
2. Express.js Guide [Електронний ресурс]. – Режим доступу: <https://expressjs.com> (дата звернення: 15.11.2025).
3. Sequelize ORM [Електронний ресурс]. – Режим доступу: <https://sequelize.org> (дата звернення: 15.11.2025).
4. Node.js API Reference [Електронний ресурс]. – Режим доступу: <https://nodejs.org> (дата звернення: 15.11.2025).
5. Electronic Pet Health Records: Modern Digital Solutions [Електронний ресурс]. – Режим доступу: (немає прямого посилання) (дата звернення: 15.11.2025).

Гордієнко Катерина Олександрівна
старший викладач кафедри Технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій
(050) 770-55-05
k.hordienko@duikt.edu.ua

ДОЦІЛЬНІСТЬ РОЗРОБКИ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ АНАЛІЗУ ТА ПРОСТОРОВОЇ КЛАСИФІКАЦІЇ ДОРОЖНЬОГО ПОКРИТТЯ НА ОСНОВІ КОМП'ЮТЕРНОГО ЗОРУ

Постановка задачі. У попередніх дослідженнях [1] була розкрита необхідність розробки систем автоматизованого розпізнавання дорожньої розмітки та виявлення дефектів дорожнього покриття для підвищення ефективності управління інфраструктурою, оперативної локалізації пошкоджень та зниження ризиків дорожньо-транспортних пригод (ДТП). Традиційні методи контролю стану дорожнього покриття, що базуються на візуальному огляді, є суб'єктивними та трудомісткими. Тому актуальним є обґрунтування підходу до побудови інтелектуальної системи, яка дозволяє виконувати моніторинг дорожнього покриття доступним і масштабованим способом.

Мета дослідження. Метою дослідження є обґрунтування доцільності створення інтелектуальної системи аналізу та просторової класифікації дорожнього покриття на основі комп'ютерного зору, із застосуванням соціально-мережевого підходу для збору даних із відеореєстраторів і мобільних пристроїв, що дозволить підвищити оперативність, точність, масштаби охоплення та економічну ефективність моніторингу.

Результати дослідження. На противагу традиційним, сучасні автоматизовані методи пропонують високу точність та об'єктивність, але вони часто пов'язані з використанням спеціалізованих та дорогих транспортних засобів. Наведені такі ключові недоліки високотехнологічних автоматизованих систем:

- висока вартість – значні початкові інвестиції та висока вартість експлуатації;
- обмежена масштабованість – висока вартість обмежує можливість регулярного та комплексного моніторингу великих дорожніх мереж;
- складність – впровадження та обслуговування вимагає висококваліфікованого персоналу.

Розгляд переваг та недоліків існуючих підходів дозволяє запропонувати “соцмережевий тип” (краудсорсинг-підхід) як альтернативу — тобто розподілену архітектуру, у якій джерелами даних виступають масово поширені пристрої, зібраних із відеореєстраторів або мобільних пристроїв.

Переваги «соцмережевого типу» або краудсорсингу:

- висока економічна ефективність – використання поширених, недорогих пристроїв, таких як відеореєстратори або смартфони, суттєво знижує витрати на збір даних. Скорочення потреби в виїзних аудитах;

- висока масштабованість — можливість одночасного моніторингу великої кількості дорожнього покриття, що недосяжно для спеціалізованих систем;

- актуальність даних — інформація оновлюється постійно, по мірі завантаження даних користувачами системи, забезпечуючи регулярні оновлення. Збільшення кількості учасників призводить до зростання точності та частоти оновлень;

- зменшення імовірності помилок внаслідок людського фактору — автоматична обробка відеоданих за допомогою комп'ютерного зору дозволяє нівелювати імовірність пропуску пошкоджень через недогляд або втому операторів;

- інтеграція з картографічними сервісами — виявлені дефекти можуть автоматично наноситись на мапу, таким чином дозволяючи дорожнім службам, та іншим зацікавленим особам, формувати маршрути та складати плани доріг.

Проте, використання такого типу рішення також може мати наступні недоліки та шляхи їх вирішення:

- чутливість до зовнішніх факторів — якість даних, отриманих з відеореєстраторів, може знижуватися через затінення, погане освітлення, рухомий трафік або припарковані автомобілі, що перешкоджає повноцінному огляду дефектів. Такі проблеми вирішуються лише подальшим накопиченням даних та навчанням мережі;

- потреба у валідації — для забезпечення високої точності класифікації (особливо для дрібних тріщин) необхідне постійне калібрування моделі та перехресна перевірка результатів. Цей тип системи, як правило, використовує навчання з учителем.

- проблема з масштабом — використання лише 2D зображень може ускладнювати точне визначення розміру та глибини пошкоджень. Як і в попередніх випадках, це вирішується тільки накопиченням даних та навчанням мережі. Ще один варіант вирішення, це збір та аналіз відгуків від користувачів системи.

- визначення місцезнаходження дефекту покриття — відсутність GPS-координат не дозволяє визначити точне місцезнаходження пошкодження. Частково, це вирішується використанням обладнання з вбудованим GPS-модулем, або, як інший підхід, проханням до користувача внести маршрут слідування, що співставляється з завантаженими відеоматеріалами.

Висновки та перспективи. Соцмережовий підхід до збору та аналізу даних дорожнього покриття дозволяє поєднати економічну ефективність мобільних рішень із масштабованістю та оперативністю, що недосяжно для традиційних спеціалізованих систем. Обґрунтовано доцільність розробки інтелектуальної системи аналізу та просторової класифікації дорожнього покриття на основі комп'ютерного зору із використанням краудсорсинг-механізмів.

Перспективою подальших досліджень є створення алгоритмічної частини системи, таких як детекція та сегментація дефектів, їх метричні параметри, геопросторова класифікація, а також формування архітектури платформи.

Список використаних джерел

1. Гордієнко К. О. «Дослідження систем аналізу та класифікацій пошкоджень дорожнього покриття». Міжнародна науково-практична конференція «Проблеми та інновації в математичній, цифровій, природничій і професійній освіті», Центральноукраїнський державний університет імені Володимира Винниченка
2. A deep learning approach to crack detection on road surfaces / R. Sizyakin та ін. Artificial Intelligence and Machine Learning in Defense Applications II, м. Online Only, United Kingdom, 21–25 верес. 2020 р. / ред. J. Dijk. 2020. URL: <https://doi.org/10.1117/12.2574131> (дата звернення: 01.12.2025).
3. CRSM: a practical crowdsourcing-based road surface monitoring system / K. Chen та ін. Wireless Networks. 2015. Т. 22, № 3. С. 765–779. URL: <https://doi.org/10.1007/s11276-015-0996-y> (дата звернення: 01.12.2025).

Варченко Артем Юрійович
студент 3 курсу, групи ТЦР-31
Державний університет інформаційно-комунікаційних технологій
+380-(63)-893-87-46
st8550424@stud.duikt.edu.ua
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний
інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ВИСОКОПРОДУКТИВНОГО ІНТЕРФЕЙСУ СИСТЕМИ «ДОБРОДІЙ» НА БАЗІ БІБЛІОТЕКИ REACT

Постановка задачі. При розробці сучасних веб-додатків для соціальної сфери (волонтерських платформ, координаційних центрів) критично важливими вимогами є швидкість відгуку інтерфейсу та зручність користувача (User Experience). Класичний підхід до веб-розробки, що базується на маніпуляціях з реальним DOM-деревом (Document Object Model) за допомогою бібліотек типу jQuery, стає неефективним у масштабних проектах. Часті оновлення сторінки призводять до "перемальовування" всього вікна браузера, що знижує продуктивність та створює ефект "миготіння", який дратує користувача. Для проекту «Добродій», де користувачі активно взаємодіють з динамічними списками заявок та картами потреб, необхідно було обрати технологію, здатну забезпечити плавність роботи на рівні нативних мобільних додатків. Вибір було зупинено на бібліотеці **React.js**, яка пропонує революційний підхід до оновлення інтерфейсу.

Мета дослідження. Метою роботи є аналіз архітектурних особливостей бібліотеки React, дослідження механізму Virtual DOM, імплементація компонентного підходу та використання сучасних можливостей (Hooks) для створення клієнтської частини платформи «Добродій».

Результати дослідження.

1. **Концепція Virtual DOM та алгоритм Reconciliation.** Головною перевагою React, використаною у проекті, є робота з **Virtual DOM**. Це легковажна JavaScript-копія реального DOM-дерева. Коли в системі «Добродій» змінюється стан (наприклад, волонтер натискає кнопку «Взяти в роботу»), React не звертається одразу до браузера. Замість цього відбувається наступний процес:

- Створюється нове віртуальне дерево з урахуванням змін.
- Алгоритм узгодження (Reconciliation) порівнює нове дерево зі старим (процес "Diffing").
- Визначається мінімальний набір змін, необхідних для оновлення реального DOM. Це дозволяє уникнути дорогих операцій верстки та перемальовування, значно підвищуючи FPS (кадрів за секунду) навіть на слабких мобільних пристроях.

2. **Компонентна архітектура та JSX.** Інтерфейс платформи побудовано як ієрархію незалежних компонентів. Для опису структури компонентів використано синтаксичний цукор **JSX** (JavaScript XML), який дозволяє писати розмітку безпосередньо в JavaScript-кодi. Наприклад, компонент заявки в системі «Добродій» описується як функція, що приймає вхідні параметри (назву заявки, категорію, статус терміновості) та повертає HTML-розмітку картки. Логіка відображення, така як додавання класу для термінових заявок, інтегрується безпосередньо в цей опис. Такий підхід забезпечує високу читабельність коду та модульність системи.

3. **Використання React Hooks.** У проєкті повністю відмовлено від застарілих класових компонентів на користь функціональних компонентів з використанням хуків. Це дозволило зменшити обсяг коду (boilerplate code) на 30%. Основні використані хуки:

- **useState:** для керування локальним станом (введення даних у форми, відкриття модальних вікон).
- **useEffect:** для виконання побічних ефектів. Наприклад, завантаження списку заявок із сервера відбувається при монтуванні компонента, а оновлення заголовка сторінки — при зміні кількості нових повідомлень.
- **Custom Hooks:** Було розроблено власні хуки, наприклад **useAuth** (для перевірки прав доступу користувача) та **useGeoLocation** (для автоматичного визначення координат волонтера), що дозволило винести складну логіку з компонентів відображення.

4. **Оптимізація продуктивності (Memoization).** У великих списках заявок часто виникає проблема зайвих ре-рендерів (re-renders). Якщо оновлюється батьківський компонент, за замовчуванням оновлюються і всі його нащадки. Для оптимізації цього процесу в системі «Добродій» використано інструменти мемоізації (React.memo та useCallback). Вони дозволяють компоненту "запам'ятовувати" результат попереднього відображення і не оновлюватися, якщо вхідні дані не змінилися. Це дозволило досягти стабільної роботи скролінгу стрічки новин навіть при завантаженні понад 500 заявок.

5. **Екосистема та управління даними.** Хоча React відповідає лише за рівень представлення (View), для повноцінної роботи додатка було інтегровано додаткові інструменти екосистеми. Для уникнення проблеми передачі даних через багато рівнів компонентів використано **React Context API**. Це дозволило створити глобальне сховище даних для профілю користувача та налаштувань теми (світла/темна), до яких має доступ будь-який компонент у дереві без необхідності явної передачі параметрів.

Висновки та перспективи. Використання бібліотеки React стало фундаментом успішної реалізації клієнтської частини платформи «Добродій». Декларативний підхід до опису інтерфейсу спростив розробку та налагодження коду. Механізм Virtual DOM забезпечив необхідну швидкодiю. Перспективою подальшого розвитку є впровадження технології **Server Components** (React 18+), що дозволить виконувати частину рендерингу компонентів безпосередньо на сервері, ще більше зменшуючи розмір JavaScript-бандлу, який завантажує

користувач.

Список використаних джерел

1. React Documentation. The library for web and native user interfaces. URL: <https://react.dev/> (дата звернення: 25.10.2025).
2. Banks A., Porcello E. Learning React: Modern Patterns for Developing React Apps. O'Reilly Media, 2020. 286 p.
3. Boduch A. React and React Native: A complete hands-on guide to modern web and mobile development with React.js. Packt Publishing, 2020. 696 p.
4. Wieruch R. The Road to React. Leanpub, 2021. 250 p.

Дем'янець Юрій Вікторович
студент 2 курсу, групи ІПЗМ-2
Карпатський національний університет імені Василя Стефаника
067-259-0699
yurii.demianets.24@pnu.edu.ua

ІНФОРМАЦІЙНО-ЕНТРОПІЙНА МОДЕЛЬ ОЦІНКИ ЯКОСТІ ТА БЕЗПЕКИ У СИСТЕМАХ УПРАВЛІННЯ ЗАВДАННЯМИ

Постановка задачі. У сучасних умовах цифрової трансформації міжнародний стандарт ISO 9001:2015 вважається «золотим стандартом» систем управління якістю (СУЯ). Він ґрунтується на процесному підході та циклі PDCA (Plan–Do–Check–Act), що сприяє безперервному вдосконаленню. Водночас інтенсивне впровадження ІТ-інструментів висуває нові вимоги до СУЯ: сучасні системи якості повинні інтегрувати інформаційні системи для обміну даними в реальному часі та автоматизації замість ручної обробки. Зокрема, платформи Jira і Trello (продукти Atlassian) широко використовуються в ІТ-проектах – Trello допомагає організувати ідеї та завдання, а Jira призначена для управління завданнями, залежностями та строками. Проте досі бракує формалізованих методик кількісної оцінки впливу таких гнучких таск-менеджерів на ефективність бізнес-процесів у СУЯ. Постановка задачі полягає в розробці науково обґрунтованої моделі та інструментарію, що дозволяють оцінити, як використання Jira/Trello впливає на якість та безпеку бізнес-процесів СУЯ, у відповідності до міжнародних стандартів управління якістю.

Мета дослідження. Метою дослідження є створення комплексного підходу для оцінювання впливу систем управління завданнями (Jira, Trello) на ефективність процесів СУЯ підприємства. Це включає розробку інформаційно-ентропійної моделі оцінки якості та безпеки процесів і реалізацію програмного рішення для автоматичного моніторингу релевантних КРІ. Запропонована модель відповідає стандартам ISO і поєднує кількісні та якісні методи: аналіз даних із Jira/Trello, розрахунок ключових показників ефективності (середній час циклу, рівень прострочень, відсоток дефектних задач тощо), а також оцінку розподілу цих метрик через ентропію інформації. Згідно з інформаційною теорією Шеннона, інформаційна ентропія вимірює ступінь невизначеності або різноманітності даних; у контексті СУЯ її можна трактувати як міру розкиду чи непередбачуваності показників якості і безпеки процесів. Таким чином, мета полягає в синтезі стандартів ISO 9001:2015 і ISO/IEC 25010 (які визначають атрибути якості та безпеки ПЗ) з експериментальною методикою на основі Jira/Trello та інформаційно-ентропійним оцінюванням.

Результати дослідження. У рамках дослідження було розроблено методику, що поєднує аналіз даних із таск-менеджерів та інформаційно-ентропійний підхід для побудови інтегральної оцінки якості бізнес-процесів у системах управління якістю. Запропонована модель ґрунтується на структурі ISO/IEC 25010, відповідно до якої визначено ключові характеристики якості програмного

забезпечення, адаптовані до вимог СУЯ. До таких характеристик належать надійність, продуктивність, безпека, стабільність процесів, відповідність вимогам та можливість простежування. Для кожної з характеристик було сформовано набір релевантних показників ефективності (KPI), що обчислюються на основі фактичних даних, отриманих із Jira та Trello. До них, зокрема, належать середній час виконання задачі, частка прострочених робіт, частота виявлення неконформностей, рівень дефектності та інші метрики, які забезпечують комплексне відображення стану процесів. Інтегральний показник якості Q_{index} побудовано як зважену комбінацію нормалізованих KPI. Задля підвищення об'єктивності оцінки до моделі включено інформаційно-ентропійний компонент. Його використання дозволило врахувати не лише середні значення метрик, але й характер їхнього статистичного розподілу. Висока ентропія інтерпретується як високий рівень невизначеності та низька узгодженість процесів; натомість зменшення ентропії свідчить про стабілізацію показників, підвищення контрольованості та передбачуваності процесів. Таким чином, запропонований інтегральний індекс є не лише сумою окремих показників, а й враховує структуру їх змінності, що робить оцінку суттєво більш чутливою до реального стану процесів.

Для практичної реалізації методу створено веб-додаток, який виконує автоматизоване завантаження експортованих із Jira даних у форматі CSV та розраховує всі необхідні метрики. Додаток визначає середній цикл виконання завдань, рівень прострочень, показники дефектності, інтенсивність появи невідповідностей та інші характеристики, після чого формує інтегральний Q_{index} . Результати розрахунків подаються у вигляді таблиць і графіків, що істотно полегшує моніторинг, аналіз та виявлення тенденцій. Інтеграція вимог стандартів ISO, даних таск-менеджерів та ентропійної моделі забезпечує формування єдиної універсальної метрики, яка може бути використана управліннями для оцінювання загального стану якості та безпеки процесів.

Отримані результати підтверджують, що застосування Jira та Trello у контексті системи управління якістю істотно підвищує прозорість і відстежуваність робочих процесів, скорочує час аналізу дефектів та мінімізує вплив людського фактора на контроль якості. Інформаційно-ентропійний компонент дозволив виявити зони, де спостерігається нерівномірність або нестабільність показників. Наприклад, високі значення ентропії у розподілі дефектності свідчать про недостатню стандартизацію виконання робіт та вказують на необхідність підвищення зрілості процесів. Зниження ентропії після впровадження відповідних покращень підтверджує, що процеси стають більш узгодженими та контрольованими. Таким чином, методика продемонструвала здатність не лише оцінювати стан системи управління якістю, але й виявляти резерви її оптимізації.

Висновки та перспективи. Запропонована інформаційно-ентропійна модель у поєднанні з вимогами стандартів ISO забезпечує комплексний аналіз якості та безпеки бізнес-процесів у системі управління якістю на основі даних із Jira та Trello. Поєднання процесного підходу ISO 9001 з сучасними практиками

управління проєктами створює узгоджену методологію, що підвищує прозорість, контрольованість і результативність СУЯ.

Ключовим елементом моделі є використання інформаційної ентропії як формального показника стабільності та впорядкованості процесів. Такий підхід дозволяє враховувати не лише середні значення KPI, а й ступінь їх варіативності: висока ентропія свідчить про нерівномірність і невизначеність процесів, тоді як її зменшення вказує на їх стабілізацію. Врахування структури розподілу даних робить оцінювання значно точнішим та чутливішим до реальних змін у діяльності підприємства.

Практична реалізація методики підтверджує її ефективність: розроблений веб-додаток автоматизує отримання та аналіз даних, оперативно виявляє неконформності й затримки, а також формує інтегральну оцінку якості процесів. Це дає змогу значно швидше реагувати на відхилення та приймати обґрунтовані рішення. Методика має перспективи подальшого розвитку, зокрема шляхом застосування машинного навчання для прогнозування трендів якості, адаптації під інші таск-менеджери або інтеграції з галузевими стандартами. Особливо перспективним є дослідження зв'язку між ентропійними показниками та управлінням ризиками безпеки, що може стати підґрунтям для побудови єдиної аналітичної системи якості й безпеки.

Список використаних джерел

1. International Organization for Standardization; International Electrotechnical Commission. ISO/IEC 25010:2011 - Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models.
2. Atlassian. Trello and Jira – Go from To-Do to Done. Офіційний сайт Atlassian. URL: <https://www.atlassian.com/> (дата звернення: 10.10.25).
3. Shannon C. E. A Mathematical Theory of Communication. *The Bell System Technical Journal*. 1948. Vol. 27. P. 379–423.

Кузьменко Дарія Олегівна
студентка 4 курсу, групи КН22Б

Центральноукраїнський державний університет імені Володимира Винниченка,
м. Кропивницький

3836107701@cuspu.edu.ua

Науковий керівник: Лупан Ірина Володимирівна

кандидат педагогічних наук, доцент, доцент кафедри інформаційних та
цифрових технологій

Центральноукраїнський державний університет імені Володимира Винниченка,
м. Кропивницький

(066) 979-61-42

ilupan@cuspu.edu.ua

РОЗРОБКА ПРОТОТИПУ ВЕБСИСТЕМИ ДЛЯ ПОДАННЯ І РЕЦЕНЗУВАННЯ НАУКОВИХ ТЕЗ

Постановка задачі. Сучасні веб-системи для організації наукових конференцій спрощують подання, рецензування та обробку тез, формування програми та ведення списків учасників. Однак вибір платформ обмежений, а безкоштовні рішення часто не забезпечують повної автоматизації й зручної взаємодії. Традиційні методи на основі електронної пошти або суміщення сервісів створюють перевантаження організаторів і ризик втрати даних. Тому актуально розробити веб-систему з простим інтерфейсом і ключовими функціями управління конференцією, почавши з прототипу.

Мета дослідження. Розробити прототип веб-системи для подання і рецензування наукових тез, яка дозволяє учасникам освітнього процесу подавати матеріали, отримувати зворотній зв'язок, відслідковувати статус обробки тез у режимі реального часу.

Результати дослідження. Ядром розроблюваної веб-платформа буде система, яка забезпечуватиме процес подання тез, їх рецензування та подальше обговорення на форумі.

У прототипі має бути реалізований механізм забезпечення повноцінного цифрового циклу роботи з тезами – від подання авторами до рецензування та обговорення. Система буде оперувати трьома ролями користувачів: автор, рецензент та адміністратор, із контролем доступу за принципом RBAC (Role-Based Access Control).

1. **Автор:** Реєструється, подає тези, переглядає статус, отримує коментарі рецензентів та вносить доопрацювання; має доступ до форуму для обговорення власних і чужих ухвалених тез.

2. **Рецензент:** Оцінює призначені тези, ухвалює або відхиляє їх із коментарями; може коментувати ухвалені тези на форумі, права модерації обмежені.

3. **Адміністратор:** Керує користувачами, призначає рецензентів, контролює цикл рецензування та має повний доступ до тез і коментарів.

Поведінкові моделі ролей забезпечують контрольовану взаємодію користувачів і можливість масштабування без втрати безпеки та цілісності даних. Проектування системи передбачає використання UML-діаграм: *Use-Case* – для опису функціональних вимог та ролей користувачів, *Class* – для опису структурних елементів, *Sequence* – для опису взаємодії об’єктів [1, с.114].

Діаграма послідовності (Рис. 1) відображає динамічну взаємодію між основними учасниками процесу, автор подає тези, система сповіщає адміністратора, який призначає рецензента. Рецензент оцінює матеріали і надсилає рішення з коментарями. Система оновлює статус, сповіщує автора та зберігає рецензію.



Рис. 1. Діаграма послідовності подання та рецензування тез.

Діаграма класів (Рис. 2) показує логічну будову системи та зв'язки між її основними складовими. Базовий клас «**Користувач**» містить ідентифікатор, контактну інформацію та параметри авторизації. Від нього наслідуються ролі **Автор**, **Рецензент**, **Адміністратор**. Ключові сутності – «**Теза**» та «**Рецензія**»: автор створює тези, рецензенти оцінюють їх, фіксуючи рішення, коментар та дату. Форум («**ТемаФоруму**», «**ПостФоруму**») забезпечує обговорення і відкриту наукову взаємодію.

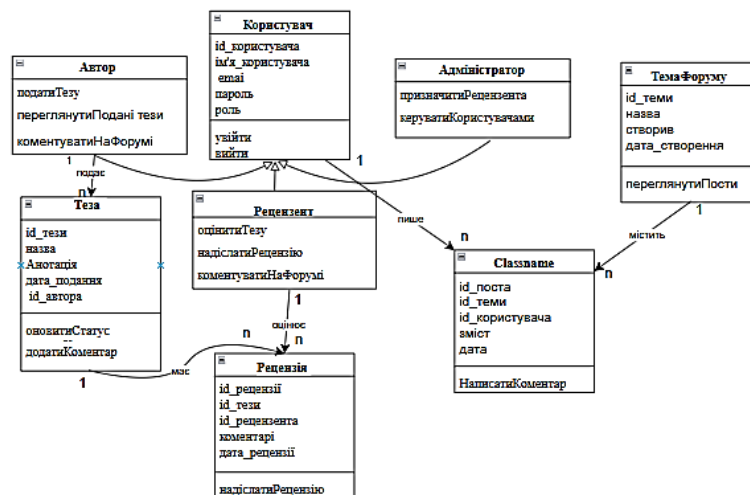


Рис. 2. Діаграма класів.

Діаграма прецедентів (Рис. 3) відображає ключові можливості системи з позиції двох основних користувачів – автора та рецензента. Чітко видно, що актори розміщені по різні боки схеми.

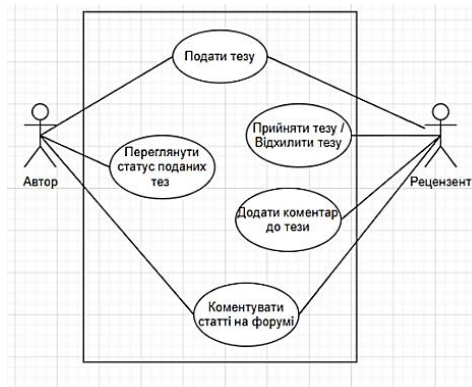


Рис. 3. Use-Case діаграма.

На діаграмі не показано адміністратора, оскільки акцент зроблено на процесі взаємодії між автором і рецензентом – саме на тих діях, що формують основний цикл подання та оцінювання тез.

Висновки та перспективи. Веб-система для подання і рецензування наукових тез може бути ефективно реалізована у вигляді централізованої платформи. Впровадження ролей користувачів та контролю доступу за принципом RBAC забезпечуватиме безпеку та структуровану взаємодію між авторами, рецензентами й адміністрацією. Така система дозволить відстежувати статус подань у реальному часі, організовувати рецензування та обговорення на форумі, що підвищить ефективність обміну науковою інформацією.

Список використаних джерел

1. Авраменко В.С., Авраменко А.С. Проектування інформаційних систем: навч. посібник. Черкаси: ЧНУ ім. Б. Хмельницького, 2017. 434 с.

Никоненко Софія Сергіївна
студентка 3 курсу, групи ТЦР-34
Державний університет інформаційно-комунікаційних технологій
(063) 379-85-12
st8682063@stud.duikt.edu.ua
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний
інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

БЛОКЧЕЙН-ТЕХНОЛОГІЇ: ПРИНЦИПИ ТА ЗАСТОСУВАННЯ

Постановка задачі. Blockchain-технології є одним із ключових інструментів сучасної цифрової економіки. Вони забезпечують децентралізоване, прозоре та захищене від змін зберігання інформації, що критично важливо у багатьох галузях: фінансах, логістиці, медицині, енергетиці та державному управлінні.

Основною проблемою традиційних централізованих систем є можливість фальсифікації даних або шахрайства, а також складність швидкого та безпечного обміну інформацією між учасниками. Blockchain дозволяє усунути ці проблеми завдяки використанню криптографії, розподіленої бази даних та алгоритмів консенсусу, які підтверджують транзакції і гарантують їх незмінність.

Актуальність дослідження обумовлена зростаючими потребами в автоматизації процесів, підвищенні безпеки та надійності даних у динамічних та складних середовищах, що робить blockchain однією з найперспективніших технологій сучасності.

Мета дослідження

Мета дослідження полягає у:

1. Вивченні принципів роботи blockchain та механізмів забезпечення безпеки даних.
2. Аналізі алгоритмів консенсусу, таких як Proof-of-Work (PoW), Proof-of-Stake (PoS) та їх модифікацій.
3. Дослідженні практичних застосувань blockchain у різних сферах економіки та управління.
4. Визначенні перспектив розвитку та інтеграції blockchain-технологій із іншими цифровими системами, включно з IoT та штучним інтелектом.

Результати дослідження

Принципи роботи blockchain. Blockchain — це розподілена база даних, де інформація зберігається у вигляді блоків, які пов'язані у ланцюжок. Кожен блок містить:

- дані транзакцій;
- хеш попереднього блоку;
- часовий штамп.

Це гарантує, що будь-яка спроба змінити інформацію в одному блоці потребує зміни всіх наступних блоків, що практично неможливо без контролю більшої частини мережі. Децентралізація мережі забезпечує стійкість до атак і збійних вузлів.

Алгоритми консенсусу

Proof-of-Work (PoW): вузли виконують складні обчислювальні завдання для підтвердження блоків. Це забезпечує безпеку, але споживає багато енергії.

Proof-of-Stake (PoS): підтвердження відбувається на основі наявності певної кількості монет у системі. Переваги — швидкість і енергоефективність.

Гібридні та нові алгоритми: деякі блокчейни використовують комбінації PoW і PoS або алгоритми на основі делегованого стейкінгу для підвищення масштабованості та безпеки.

Практичні застосування blockchain

Фінанси:

1. Криптовалюти (Bitcoin, Ethereum) забезпечують децентралізовані платежі.
2. Децентралізовані фінанси (DeFi) дозволяють кредитування та обмін активів без посередників.
3. Смарт-контракти автоматизують виконання угод без участі третіх сторін.

Логістика та постачання:

1. Відстеження товарів у реальному часі.
2. Підтвердження автентичності продукції та документів.
3. Оптимізація ланцюгів поставок і зменшення ризиків шахрайства.

Медицина:

1. Безпечне зберігання електронних медичних записів.
2. Контроль доступу до даних пацієнтів.
3. Створення систем для відстеження фармацевтичних препаратів і транспортування вакцин.

Державне управління:

1. Електронні голосування з підтвердженням достовірності результатів.
2. Реєстри власності та ліцензій, незмінність даних.
3. Автоматизація адміністративних процесів через смарт-контракти.

Переваги та обмеження

Переваги:

1. Прозорість і контроль за всіма транзакціями.
2. Децентралізація і стійкість до атак.
3. Автоматизація процесів за допомогою смарт-контрактів.

Недоліки:

1. Високе енергоспоживання PoW-блокчейнів.
2. Обмежена масштабованість і швидкість транзакцій у великих мережах.
3. Необхідність регулювання та правового контролю у багатьох країнах.

Висновки

Blockchain-технології є перспективним напрямом розвитку цифрової економіки. Вони забезпечують:

- надійне та безпечне зберігання інформації;
- прозору взаємодію між учасниками;
- автоматизацію процесів через смарт-контракти.

Подальший розвиток передбачає інтеграцію blockchain із технологіями IoT, штучного інтелекту та великих даних, що дозволить створювати автономні, безпечні та ефективні системи управління в промисловості, медицині, логістиці та фінансах.

Список використаних джерел

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.
2. Crosby M., Pattanayak P., Verma S., Kalyanaraman V. Blockchain Technology: Beyond Bitcoin. *Applied Innovation Review*, 2016, Issue 2, pp. 6–10.
3. Zheng Z., Xie S., Dai H., Chen X., Wang H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *IEEE International Congress on Big Data*, 2017, pp. 557–564.
4. Tapscott D., Tapscott A. *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*. Penguin, 2016.
5. Mougayar W. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Wiley, 2016.

Новостройний Дмитро Андрійович
студент 3 курсу, групи ТЦР-31
Державний університет інформаційно-
комунікаційних технологій
063-526-01-06

novostroinyidima23@gmail.com

Поперешняк Світлана Володимирівна

к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії

Національний технічний університет України

"Київський політехнічний інститут імені Ігоря Сікорського"

sperereshnyak@gmail.com

Е-СЕРВІС «ДОБРОДІЙ» ЯК ЦИФРОВИЙ ІНСТРУМЕНТ РОЗВИТКУ ВОЛОНТЕРСЬКОЇ СПІЛЬНОТИ

Постановка задачі. Волонтерство є однією з ключових форм громадянської активності, що робить внесок у розв'язання соціальних, гуманітарних, культурних та освітніх проблем [1-2]. Однак реальна організація волонтерської діяльності часто стикається з низкою труднощів: епізодичністю залучення, відсутністю довгострокових зв'язків між волонтерами й організаторами, браком прозорого визнання внеску кожного учасника, а також відсутністю єдиного цифрового простору, де можна було б системно працювати з волонтерськими командами [2-3].

Типові підходи - окремі чати, групи в соціальних мережах, неструктуровані таблиці - не дають змоги вибудувати стабільну й згуртовану спільноту. Волонтери часто не бачать повної картини свого впливу, не мають зручного інструменту для пошуку подій за цінностями та інтересами, а організатори не завжди можуть сформувати «ядро» постійних, відповідальних волонтерів. Це знижує мотивацію, погіршує координацію, ускладнює розвиток волонтерських програм [2-3].

У таких умовах актуальною є розробка е-сервісу, який не лише автоматизує процеси набору й координації, а й підтримує довготривале партнерство між волонтерами, організаторами та спільнотою, роблячи волонтерство більш видимим, керованим і ціннісно орієнтованим. Це відповідає загальним тенденціям цифрової трансформації молодіжної та волонтерської роботи в Європі [4].

Мета дослідження. Метою дослідження є обґрунтування концепції е-сервісу «ДоброДій» як цифрової платформи, що сприяє формуванню, підтримці та розвитку волонтерської спільноти, забезпечуючи прозорість внеску, зручність комунікації та підвищення мотивації до довгострокової участі [2-3].

Для досягнення цієї мети необхідно:

- проаналізувати потреби волонтерів і організаторів подій у контексті цифрової підтримки волонтерської діяльності [2-4];

- визначити, які функції платформи найбільше впливають на мотивацію, залучення та утримання волонтерів;
- сформулювати рольову модель сервісу з акцентом на розвитку спільноти (волонтер, організатор, ментор, адміністратор);
- спроектувати механізми визнання та зворотного зв'язку (рейтинги, відгуки, ачивки, рекомендації);
- окреслити можливості інтеграції е-сервісу з освітніми та громадськими ініціативами для підтримки культури волонтерства [1–3].

Результати дослідження. У ході дослідження проаналізовано потреби волонтерської спільноти України та розроблено концепцію е-сервісу «ДоброДій» як цифрового інструменту координації волонтерської діяльності. Проведене опитування 54 волонтерів та 5 організаторів подій виявило ключові проблеми: відсутність централізованої платформи пошуку можливостей (зазначили 83% респондентів), складність перевірки надійності волонтерів (71% організаторів), брак механізмів мотивації та визнання внеску (64% волонтерів). На основі цього сформовано функціональні вимоги до системи, що поєднує каталог подій з розширеними фільтрами, систему рейтингування учасників, механізм цифрових ачивок та інтеграцію з державними сервісами ідентифікації для підвищення довіри між учасниками [4-6].

Розроблено архітектуру е-сервісу на базі технологій ASP.NET Core 8.0 та React.js з чотирма функціональними модулями: управління користувачами з інтеграцією «Дія» та BankID НБУ через OAuth 2.0 [4-5], управління подіями з геолокацією та категоризацією за типами діяльності, система обробки заявок з workflow-процесом підтвердження участі, репутаційна система з алгоритмом розрахунку рейтингу на основі завершених подій, отриманих відгуків та показників надійності. Реалізовано гібридну автентифікацію з підтримкою класичної схеми логін/пароль (хешування bcrypt) та OAuth 2.0 авторизації через державні сервіси, що забезпечує баланс між зручністю та безпекою доступу до платформи.

Розроблено репутаційну систему з динамічним алгоритмом розрахунку рейтингу волонтерів: $\text{Rating} = (\text{CompletedEvents} \times 10) + (\text{PositiveReviews} \times 5) - (\text{NoShows} \times 15) + \text{AchievementBonus}$, де враховується кількість завершених подій, позитивні відгуки організаторів, випадки неявки без попередження та бонуси за досягнення. Система цифрових ачивок включає бейджі за різні досягнення: перша завершена подія, серію подій без пропусків, швидку реакцію на нові можливості, спеціалізацію в конкретних категоріях діяльності. Такий підхід узгоджується з практиками репутаційних та гейміфікаційних систем у сучасних онлайн-сервісах, що використовуються для підвищення мотивації та залученості користувачів [2–3].

Проведено комплексне тестування системи з оцінкою функціональності, безпеки та продуктивності. Статичний аналіз коду через SonarQube підтвердив відсутність критичних вразливостей, динамічне тестування через OWASP ZAP виявило та усунуто дві проблеми середнього рівня конфігурації безпеки, пентестування підтвердило захищеність від загроз переліку OWASP Top 10 2021

[2-3]. Користувацьке тестування з фокус-групою з 28 волонтерів показало високий рівень задоволеності інтерфейсом (4.6 з 5 балів) та готовність використовувати платформу для пошуку волонтерських можливостей (89% респондентів).

Результати дослідження підтверджують, що е-сервіс «ДоброДій» як цифровий інструмент здатен підвищити ефективність координації волонтерської діяльності через централізацію інформації про події, автоматизацію процесів відбору учасників, забезпечення прозорості через репутаційну систему та зниження бар'єрів входу через інтеграцію з державними сервісами ідентифікації.

Висновки та перспективи. Е-сервіс «ДоброДій» у запропонованій концепції виступає не просто веб-інструментом для координації подій, а цифровою платформою розвитку волонтерської спільноти. Завдяки поєднанню персоналізованого підбору подій, прозорих механізмів визнання, підтримки довгострокової участі та аналітики для організаторів «ДоброДій» може сприяти переходу від епізодичного волонтерства до усвідомленої та системної громадянської активності [2-3].

У перспективі сервіс здатен стати комунікаційним та координаційним ядром для університетських, міських і громадських ініціатив, об'єднуючи волонтерів різного віку, досвіду й сфер діяльності. Подальші дослідження доцільно спрямувати на емпіричну перевірку впливу платформи на залучення та утримання волонтерів, а також на інтеграцію з освітніми програмами та місцевими стратегіями розвитку громад [1-4].

Список використаних джерел

1. Про волонтерську діяльність. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/3236-17> (дата звернення: 25.11.2025).
2. SWVR Home. *United Nations Volunteers*. URL: <https://www.unv.org/swvr> (дата звернення: 25.11.2025).
3. Demicheli F., Tonon D., Belletti M., Atanasov D. *Mapping and Analysis of Research on Youth Volunteering in Europe*. SALTO European Solidarity Corps Resource Centre, 2024. URL: <https://www.salto-youth.net/downloads/4-17-4455/Mapping%20and%20Analysis%20of%20Research%20on%20Youth%20Volunteering%20in%20Europe%20-%20SNAC%20-%20rev.%20March%202024.pdf> (дата звернення: 25.11.2025).
4. Participation Pool | Resources on Democratic Participation & Media Literacy. *SALTO*. URL: <https://participationpool.eu/> (дата звернення: 25.11.2025).
5. Representing Europe's youth | European Youth Forum. URL: <https://www.youthforum.org/> (дата звернення: 25.11.2025).
6. Mapping and Analysis of Research on Youth Volunteering in Europe – Explanatory Report. SALTO ESC/SNAC Volunteering, 2023. URL: <https://surl.li/mqngbn> (дата звернення: 25.11.2025).

Полянський Назар Денисович
студент 4 курсу, групи ПЗ-4
Національний транспортний університет
(068) 422-09-53
nazar.n2812@gmail.com
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний
інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

АРХІТЕКТУРА ВИСОКОНАВАНТАЖЕНИХ ВЕБПЛАТФОРМ ПРАЦЕВЛАШТУВАННЯ

Постановка задачі. Сучасні онлайн-платформи працевлаштування обробляють значні обсяги даних: профілі користувачів, вакансії, відгуки, рекомендації, комунікацію тощо. З ростом кількості користувачів традиційні монолітні системи стикаються з проблемами масштабованості, високого навантаження, повільної обробки запитів та складністю в подальшій підтримці. Тому актуальним є дослідження архітектурних підходів, які дозволяють створювати високонавантажені, гнучкі та стійкі веб-платформи професійної взаємодії.

Мета дослідження. Метою дослідження є аналіз архітектурних рішень, підходів до масштабування та технологій, які дозволяють побудувати високопродуктивну платформу працевлаштування. Особливу увагу приділено принципам чистої архітектури, застосуванню мікросервісного підходу, кешуванню даних, оптимізації API та використанню сучасних фреймворків React і .NET.

Результати дослідження. Веб-платформи працевлаштування складаються з широкого набору функціональних модулів, які взаємодіють між собою в режимі реального часу: модулі управління користувацькими профілями, системи публікації та пошуку вакансій, рекомендаційні механізми, блок обробки повідомлень, системи фільтрації та сортування даних, а також аналітичні підсистеми. Зі збільшенням кількості користувачів та обсягу даних навантаження на такі модулі зростає нелінійно, що створює потребу у використанні архітектурних рішень, здатних забезпечити високу продуктивність, відмовостійкість та незалежність компонентів.

Одним із найбільш ефективних підходів для таких систем є чиста архітектура (Clean Architecture), що ґрунтується на чіткому розділенні відповідальності між рівнями Domain, Application, Infrastructure та Presentation [1]. Завдяки цьому бізнес-логіка платформи не залежить від способу реалізації даних, інфраструктури чи конкретних фреймворків. Це дає можливість легко змінювати технологічні рішення без перероблення ядра проєкту, а також полегшує тестування та масштабування системи.

Серверна частина, реалізована на основі .NET, забезпечує асинхронну обробку запитів, що дозволяє одночасно обслуговувати велику кількість користувачів. Асинхронність суттєво збільшує пропускну здатність системи, зменшуючи кількість блокувань та затримок у порівнянні з традиційними синхронними архітектурами. Використання ASP.NET Core також дає змогу реалізувати ефективні REST API, інтегрувати механізми JWT-автентифікації та використовувати middleware для оптимізації потоку запитів [1-2].

На клієнтській частині застосовується React, що забезпечує компонентний підхід, повторне використання інтерфейсів та високу швидкість рендерингу. React-архітектура дозволяє будувати складні інтерфейси, які залишаються стабільними та продуктивними завдяки Virtual DOM, оптимізації оновлень та гнучкому управлінню станом (Redux, Zustand тощо). Це особливо важливо для платформ, де користувачі інтенсивно взаємодіють із системою та виконують велику кількість операцій у короткий проміжок часу.

Для забезпечення високої продуктивності застосовуються такі ключові методи оптимізації:

- горизонтальне масштабування серверів через балансувальники навантаження (NGINX, HAProxy), що дозволяє рівномірно розподіляти трафік між великою кількістю екземплярів застосунку;
- кешування частих запитів за допомогою Redis, що значно зменшує кількість звернень до бази даних і мінімізує затримки при обробці найпопулярніших операцій;
- оптимізація роботи бази даних, включаючи індексацію, шардінг і реплікацію, що дозволяє розподілити навантаження між кількома вузлами та забезпечити високу доступність даних навіть у випадку збою окремих компонентів;
- розділення сервісів відповідно до бізнес-функцій, тобто перехід до мікросервісної архітектури, де кожен компонент працює незалежно, має власну логіку та масштабування, що значно спрощує підтримку та оновлення;
- використання асинхронних черг повідомлень (RabbitMQ, Kafka), які дозволяють обробляти запити у фоновому режимі та розвантажувати основний сервер.

Дослідження показує, що перехід від монолітної архітектури до мікросервісної з використанням принципів чистої архітектури не лише збільшує продуктивність, але й значно підвищує стабільність роботи платформи, її здатність до гнучкого масштабування та швидкого впровадження нових функцій. Завдяки цьому платформа може витримувати зростаюче навантаження, забезпечувати високу доступність сервісів і зберігати короткий час відповіді навіть при значному збільшенні кількості користувачів [2-3].

Висновки та перспективи. Застосування чистої архітектури та мікросервісних рішень дає змогу створювати масштабовані, гнучкі та продуктивні веб-платформи працевлаштування. Використання React та .NET забезпечує високий рівень інтерактивності та швидкості обробки даних. Перспективами подальших досліджень є впровадження розподілених обчислень,

інтелектуальних систем рекомендацій та автоматизованих аналітичних модулів для покращення взаємодії між кандидатами та роботодавцями.

Список використаних джерел

1. Martin R. C. Clean Architecture: A Craftsman's Guide to Software Structure and Design. Pearson, 2018.
2. Newman S. Building Microservices. O'Reilly Media, 2021.
3. Richards M., Ford N. Fundamentals of Software Architecture: An Engineering Approach. O'Reilly Media, 2020.

Прохоров Ярослав Федорович
студент 3 курсу, групи ТЦР-31
Державний університет інформаційно-комунікаційних технологій
(097) 294-99-26
qwertypro963@gmail.com
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ Е-СЕРВІСІВ У ХМАРНИХ СЕРЕДОВИЩАХ

Постановка задачі. Стрімкий розвиток цифрових платформ та глобальна інтеграція бізнес-процесів призводять до активного використання хмарних сервісів як універсальної платформи для електронних послуг. Хмарна інфраструктура дозволяє масштабувати обчислювальні ресурси, оптимізувати витрати на обладнання та забезпечувати глобальний доступ до сервісів. Проте, одночасно з перевагами, хмарні середовища формують нові ризики для е-сервісів, які стають ціллю для різноманітних кібератак: від несанкціонованого доступу до даних до повної зупинки сервісів, шифрування інформації (атаки програм-вимагачів), підміни запитів чи маніпулювання трафіком.

Актуальність проблеми кіберзахисту обумовлена тим, що Е-системи обробляють персональні дані користувачів, фінансову інформацію, медичні записи, комерційні бази знань та конфіденційні документи. Порушення конфіденційності або цілісності таких даних не лише завдає економічних збитків, а й може загрожувати безпеці громадян, діяльності організації та державним інтересам.

З огляду на це виникає потреба у впровадженні комплексного кіберзахисту е-сервісів, що функціонують у хмарній інфраструктурі. Завданням є не тільки запобігання атакам, але й забезпечення стійкості сервісів до інцидентів, мінімізація витоку даних та відновлення функціональності без втрат інформації. Без побудови багаторівневого кіберзахисту хмарні е-сервіси залишаються вразливими до зовнішніх загроз, внутрішніх атак інсайдерів, порушень політик доступу та технічних збоїв.

Мета дослідження. Метою дослідження є аналіз сучасних технологій забезпечення кіберзахисту е-сервісів у хмарних середовищах, оцінка їх ефективності в умовах високої варіативності загроз та визначення підходів, що дозволяють захистити дані, підтримувати безперервність роботи та забезпечувати стійкість до кібератак у масштабованих електронних системах.

Результати дослідження. Одним із ключових інструментів кіберзахисту в хмарних середовищах є технології управління доступом та ідентифікацією (IAM). Вони забезпечують перевірку прав користувача, дозволяють

застосовувати багатофакторну автентифікацію (SMS-код, біометрія, апаратні ключі) та обмежувати доступ до сервісів відповідно до ролі користувача в системі. Важливим сучасним принципом є Zero Trust Security, який базується на тому, що жоден компонент системи не є надійним за замовчуванням. Кожна взаємодія між сервісом, користувачем або додатком потребує постійного підтвердження прав, що унеможливорює внутрішні атаки.

Другим критичним напрямом захисту є шифрування даних. Використання протоколів TLS/SSL забезпечує захист інформації під час передачі, а апаратне та програмне шифрування на серверах забезпечує безпеку даних у сховищах. Хмарні сервіси застосовують спеціалізовані модулі управління ключами (KMS), що дозволяють користувачеві контролювати шифрувальні ключі. Це зменшує ризик несанкціонованого доступу навіть із боку хмарного провайдера.

Важливу роль відіграють системи виявлення вторгнень (IDS) та запобігання атакам (IPS), що аналізують трафік у реальному часі та розпізнають аномалії. Комбінація цих систем із веб-фільтрами WAF, що блокують поширені атаки (SQL-injection, XSS, фішинг-переадресації), суттєво підвищує рівень захисту публічних інтерфейсів е-сервісів.

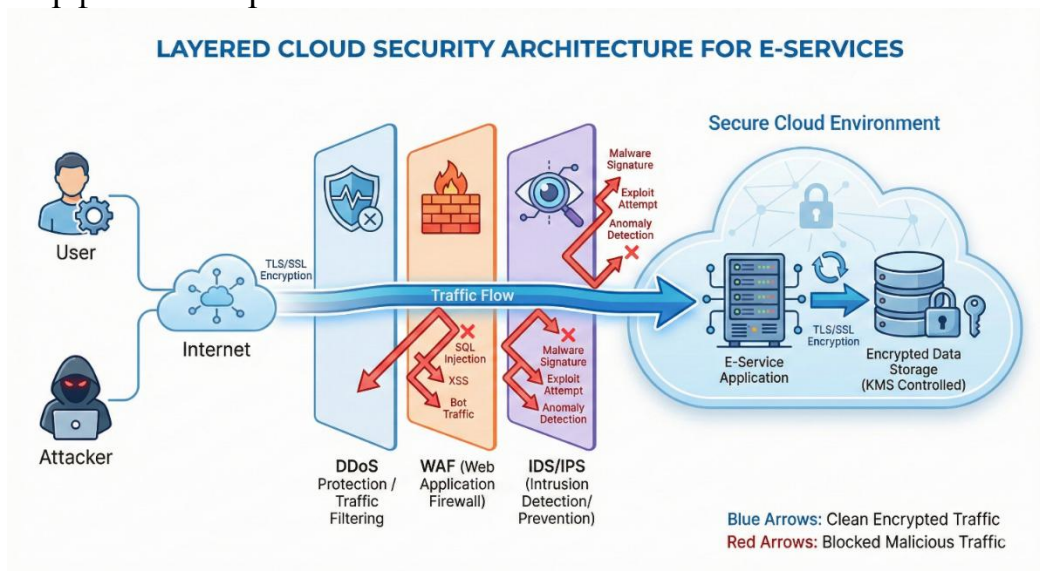


Рис. 1. Діаграма багаторівневої архітектури безпеки

Особливе значення має моніторинг подій безпеки (SIEM), який виконує збір журналів, аналізує ризики та повідомляє про інциденти. Використання систем SOAR, що автоматизують реагування на загрози, дозволяє блокувати підозрілі облікові записи, відключати скомпрометовані компоненти та швидко відновлювати систему без участі адміністратора.

Додатковими механізмами захисту є:

- сегментація мережі;
- ізоляція контейнерів;
- використання VPN та приватних тунелів доступу;
- захист від DDoS-атак через розподілені фільтри трафіку;
- аудит дій адміністраторів;
- резервне копіювання з географічним розподілом.

Багато хмарних провайдерів (AWS, Azure, Google Cloud) впроваджують інтегровані системи кіберзахисту, що дозволяє масштабувати рівень безпеки без зменшення продуктивності та доступності е-сервісів.

Висновки та перспективи. Хмарні середовища формують нову парадигму кіберзахисту, яка вимагає комплексного поєднання криптографічних механізмів, мережевих фільтрів, інтелектуального аналізу подій та безперервного контролю доступу. Ефективний кіберзахист е-сервісів досягається лише завдяки багаторівневому підходу, що передбачає не лише запобігання атакам, а й раннє їх виявлення, адаптивне реагування та автоматичне відновлення роботи систем.

Перспективним напрямом розвитку є створення самонавчальних систем безпеки, що використовують методи машинного навчання для прогнозування атак, аналізу поведінки користувачів та формування політик доступу без участі адміністратора. Також очікується зростання популярності технологій квантового шифрування, які гарантуватимуть абсолютну стійкість до перехоплення даних. Впровадження таких підходів дозволить сформувати нове покоління стійких хмарних е-систем, здатних автономно протидіяти кіберзагрозам.

Список використаних джерел

1. Mell P., Grance T. *The NIST Definition of Cloud Computing*. NIST, 2011.
2. Shull D., Gal-Or E. *Cloud Security and Privacy*. O'Reilly Media, 2020.
3. Krutz R., Vines D. *Cloud Computing Security Architecture*. Wiley, 2016.

Ружинський Денис Олександрович

студент 3 курсу, групи ТЦР-31

Державний університет інформаційно-комунікаційних технологій

denisruzhynski3@gmail.com

Поперешняк Світлана Володимирівна

к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії

Національний технічний університет України "Київський політехнічний

інститут імені Ігоря Сікорського"

spopereshnyak@gmail.com

МЕТОДИ ПІДВИЩЕННЯ НАДІЙНОСТІ Е-СИСТЕМ ЗА УМОВ НЕРІВНОМІРНОГО НАВАНТАЖЕННЯ

Постановка задачі. Сучасні електронні сервіси функціонують у середовищі зі значною варіативністю навантаження, залежною від часу доби, кількості активних користувачів, характеру виконуваних операцій, зовнішніх та внутрішніх факторів. Нерівномірність навантаження створює ризики перевантаження сервера, деградації продуктивності та виникнення відмов у доступі до критичних функцій системи. У зв'язку з цим постає потреба в аналізі архітектурних рішень і технологій, що дозволяють підвищити надійність е-сервісів за змінних і непередбачуваних умов роботи.

Мета дослідження. Метою дослідження є аналіз методів підвищення надійності е-сервісів за умов нерівномірного навантаження шляхом розгляду сучасних підходів до кластеризації, асинхронної обробки запитів, розподілення ресурсів між компонентами системи та використання спеціалізованих механізмів стійкості.

Результати дослідження. Підвищення надійності е-сервісів досягається передусім завдяки застосуванню кластеризації. Кластер серверів дозволяє розподілити потік користувацьких запитів між кількома вузлами, що зменшує ризик перевантаження окремих компонентів і забезпечує відмовостійкість у разі виходу окремого вузла з ладу. При нерівномірному навантаженні кластеризація виконує роль механізму, який підтримує стабільний рівень доступності незалежно від інтенсивності запитів. Важливою складовою цього підходу є система балансування навантаження, яка динамічно скеровує запити на ті вузли, що мають достатній резерв ресурсів. Завдяки цьому забезпечується рівномірний розподіл трафіку і попередження моментів пікової концентрації запитів на окремому сервері [1].

Ще одним важливим аспектом підвищення надійності е-систем є використання асинхронної обробки задач за допомогою воркерів. Воркери дозволяють виділяти тривалі або ресурсомісткі операції в окремий потік виконання, що унеможливорює блокування основного сервісу та зменшує час відповіді для кінцевого користувача. У системах з нерівномірним навантаженням воркери працюють особливо ефективно, оскільки кількість задач може зростати нерівномірно та вибірково. Для керування розподіленою обробкою

застосовуються черги повідомлень, що виконують роль буфера між основним сервісом і системою воркерів. Це забезпечує плавне вирівнювання навантаження та запобігає перевантаженню обчислювальних ресурсів у пікові моменти.

Величезну роль у забезпеченні надійності відіграє інфраструктура баз даних, оскільки саме вона найчастіше є вузьким місцем під час стрибків навантаження. Одним із ключових методів підвищення стійкості є реплікація даних, яка передбачає створення кількох копій бази даних на різних серверах. Реплікація дозволяє розподіляти операції читання між вторинними репліками, зменшуючи навантаження на основний вузол і забезпечуючи високу доступність даних навіть у разі відмови основної бази. Реплікація типу master–slave дає можливість рознести запити читання на підлеглі вузли, а master–master забезпечує додаткову гнучкість та стійкість завдяки можливості обробляти записи на кількох серверах одночасно. У великих системах з високим навантаженням ефективним є також шардінг — розподіл великої таблиці або всієї БД на окремі сегменти (шарди), які зберігаються на різних вузлах. Шардінг значно підвищує масштабованість, оскільки дозволяє обробляти запити паралельно на різних серверах, зменшуючи час відповіді та запобігаючи «гарячим точкам» у сховищі даних. Додатково використовують горизонтальне або вертикальне розділення таблиць, що оптимізує виконання запитів за рахунок роботи з меншими та більш логічно структурованими частинами даних. Такі підходи дають змогу перерозподілити трафік бази даних, уникнути перевантаження одного вузла та забезпечити стабільну продуктивність навіть у пікові моменти.

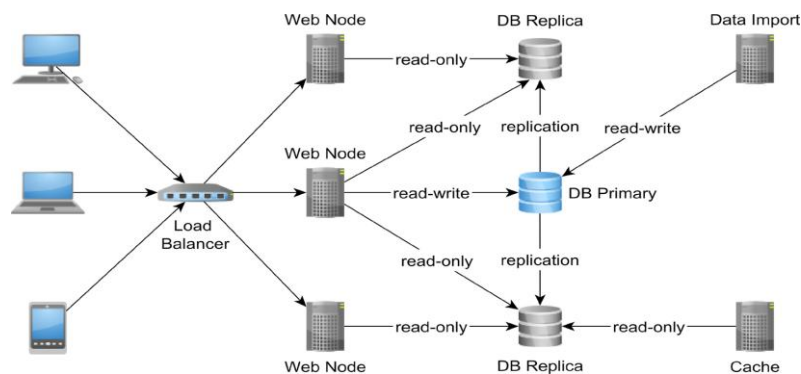


Рис. 1. Архітектура системи з реплікацією баз даних.

Крім цього, значний вплив на стійкість е-системи має горизонтальне масштабування, яке дозволяє динамічно додавати нові сервери або воркери у відповідь на підвищення навантаження. У хмарних інфраструктурах це реалізується за допомогою автоматичного масштабування на основі метрик: завантаження процесора, часу відповіді або довжини черги запитів. Такий підхід забезпечує адаптивність системи та мінімізує втрати продуктивності при значних, але нетривалих піках навантаження.

Важливим напрямом підвищення надійності е-систем є реалізація принципів fault tolerance — здатності програмних комплексів зберігати працездатність за часткових відмов компонентів. Механізми відмовостійкості включають дублювання критичних вузлів, автоматичне перемикання (failover) на

резервні сервери, використання патерна circuit breaker для ізоляції несправних сервісів та застосування повторних спроб виконання операцій (retry) разом із журналюванням для коректного відновлення транзакцій. Комплекс цих механізмів дозволяє мінімізувати час простою, забезпечити безперервність бізнес-процесів та підтримувати стабільну роботу сервісу навіть у разі непередбачуваних збоїв у підсистемах [2].

Ще однією технологією для підвищення стабільності роботи систем є Content Delivery Networks (CDN) — розподілені мережі серверів, що кешують статичний та напівдинамічний контент у географічно наближених до користувача точках присутності. Це дозволяє істотно зменшити затримку доступу до контенту, знизити навантаження на основну інфраструктуру та підвищити стійкість до пікових навантажень. Використання CDN особливо ефективно для е-сервісів у країнах з великою географічною площею.

Поширення edge-обчислень суттєво вплинуло на здатність е-сервісів обробляти великі потоки даних у реальному часі. Edge-сервери виконують частину обробки на периферії мережі, ближче до кінцевого користувача, що скорочує затримку, підвищує швидкість відповіді та зменшує навантаження на центральні компоненти системи. У високонавантажених е-сервісах edge-вузли застосовуються для попереднього кешування, фільтрації трафіку, обробки запитів автентифікації та протидії DDoS-атакам. Поєднання CDN-інфраструктури та edge-серверів формує багаторівневу розподілену архітектуру, яка підвищує стійкість сервісу, забезпечує кращу роботу під час нерівномірних навантажень і мінімізує залежність від центральних дата-центрів [3].

Висновки та перспективи. Проведене дослідження демонструє, що надійність е-сервісів за умов нерівномірного навантаження визначається не окремими технологіями, а їх узгодженим поєднанням у межах цілісної архітектури. Ефективна взаємодія обчислювальних вузлів, механізмів розподілу навантаження, інструментів обробки даних та засобів відмовостійкості дозволяє забезпечити стабільну роботу системи навіть у нестандартних або критичних умовах. Комплексний підхід до побудови е-сервісів, орієнтований на гнучкість, адаптивність і здатність системи до самовідновлення, є ключем до підвищення їх продуктивності та доступності в умовах сучасних цифрових викликів.

Подальший розвиток розглянутої архітектури е-сервісів може бути пов'язаний із впровадженням інтелектуальних систем прогнозування навантажень, що використовують машинне навчання для динамічного коригування конфігурацій кластерів і воркерних пулів. Перспективним напрямом є розробка самовідновлюваних систем, здатних автономно виявляти відмови та виконувати миттєве переключення між географічно розподіленими майданчиками. Також актуальною є інтеграція edge-обчислень з локальною попередньою обробкою даних, що дозволяє мінімізувати затримки та навантаження на магістральні канали. Комплекс цих рішень може забезпечити створення е-систем нового покоління, здатних працювати стабільно навіть за умов надзвичайно високої динаміки навантажень та зовнішніх ризиків.

Список використаних джерел

1. Andre Benjmain Bondi “Characteristics of Scalability and Their Impact on Performance”. 2000.
2. Martin Kleppmann “Designing Data-Intensive Applications: The Big Ideas Behind Reliable, Scalable, and Maintainable Systems”. 2017.
3. Shi W., Cao J., Zhang Q., Li Y., Xu L. “Edge Computing: Vision and Challenges.” *IEEE Internet of Things Journal*. 2016. Vol. 3, No. 5, pp. 637–646.

Романюк Ярослав Олександрович

студент 3 курсу, групи ТЦР-33

Державний університет інформаційно-комунікаційних технологій

kyrkyma404@gmail.com

Поперешняк Світлана Володимирівна

к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії

Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

spopereshnyak@gmail.com

ІНТЕРАКТИВНИЙ СИМУЛЯТОР ОСББ ЯК ЗАСІБ ЦИФРОВОЇ АДАПТАЦІЇ ТА ПІДВИЩЕННЯ ЗАЛУЧЕНОСТІ МЕШКАНЦІВ

Постановка проблеми. Сучасні цифрові сервіси для управління житловими будинками стрімко розвиваються, однак рівень цифрової грамотності мешканців суттєво відстає від їхніх технічних можливостей. Традиційні методи навчання — інструкції, семінари, відеоуроки — формують лише теоретичне уявлення без можливості безпечної практики. Це спричиняє недовіру, стрес та низький рівень використання електронних сервісів, особливо серед літніх людей. Відсутній інструмент, який би дозволяв опанувати цифрові платформи через реалістичне практичне занурення та імітацію робочих процесів ОСББ. Виникає потреба у створенні інтерактивного симулятора, що поєднує навчальну, тренувальну та соціалізаційну функції.

Мета дослідження. Метою дослідження є створення та валідація інтерактивного симулятора ОСББ, призначеного для підвищення цифрової грамотності мешканців та формування позитивного досвіду роботи з електронними сервісами. Дослідження спрямоване на визначення технічних, педагогічних та психологічних механізмів, що забезпечують ефективну цифрову адаптацію користувачів.

Результати дослідження. Трансформація житлово-комунального господарства в умовах цифровізації вимагає не лише технологічних змін, але й адаптації мешканців до нових форматів взаємодії. Існує значний розрив між технічними можливостями сучасних цифрових платформ та реальною готовністю користувачів, особливо представників старших вікових груп, до їх використання. Недостатня цифрова грамотність, недовіра до електронних сервісів та відсутність практичних навичок роботи з ними стають головними бар'єрами на шляху до ефективного управління житловими будинками.

Актуальність дослідження полягає у розробці інноваційного підходу до вирішення проблеми цифрової адаптації через створення інтерактивного симулятора ОСББ. На відміну від статичних навчальних матеріалів чи теоретичних курсів, симулятор пропонує практичне занурення в реальні робочі процеси управління будинком, дозволяючи мешканцям без ризику та у комфортному темпі опанувати всі функції цифрової платформи, від подачі звернень до участі в голосуваннях та комунікації з головою ОСББ.

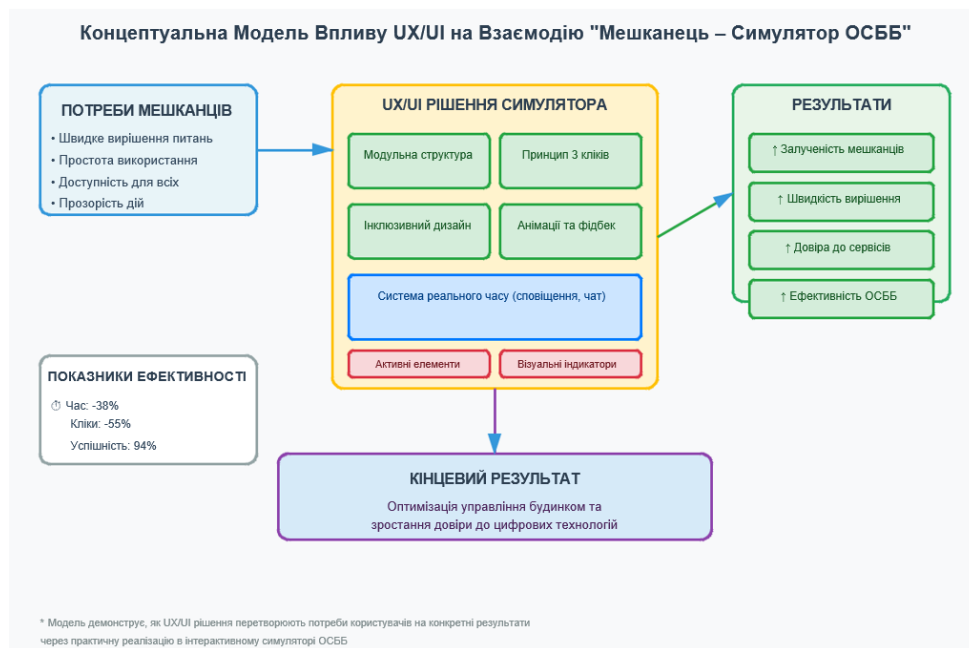


Рис. 1. Концептуальна модель цифрової адаптації мешканців через симулятор ОСББ

Концептуальна модель демонструє, як симулятор ОСББ слугує мостом між поточним рівнем цифрової грамотності мешканців та ефективним використанням електронних сервісів управління будинком. Інтерактивне навчання, реалістична симуляція та інклюзивний дизайн створюють умови для поступової адаптації та підвищення залученості.

Існуючі підходи до цифрової освіти мешканців є переважно пасивними та недостатньо ефективними. Традиційні методи, такі як друковані інструкції, семінари чи відео-туторіали, не забезпечують необхідного рівня практичної взаємодії з системою. Користувачі отримують теоретичні знання, але не мають можливості випробувати їх у дії, що призводить до низького рівня засвоєння та побоювань при реальному використанні сервісів. Відсутність ігрових елементів та інтерактивності робить процес навчання монотонним та не мотивує мешканців до активної участі.

Проблема полягає у відсутності комплексного інструменту, який би поєднав навчальні функції з реалістичною симуляцією робочих процесів ОСББ. Необхідно створити платформу, яка не лише навчала б мешканців користуватися цифровими сервісами, але й формувала б позитивне ставлення до них, знижуючи рівень стресу та підвищуючи впевненість у власних силах при роботі з електронними системами управління. Дослідження підтвердило, що інтерактивний симулятор ОСББ здатний переважати традиційні підходи до навчання у всіх ключових напрямках: залученість, ефективність засвоєння та стійкість навичок. Реалізована система поєднує реалістичну симуляцію звернень, чат-комунікацію, автоматичні сповіщення та покрокові сценарії взаємодії. Завдяки використанню нативних веб-технологій та прогресивній архітектурі досягнуто повної доступності без потреби спеціального програмного

забезпечення. За результатами пілотного впровадження спостерігається значне зростання цифрової грамотності (+65%), різке підвищення частоти використання електронних сервісів (+180%) та помітне зниження тривожності серед старших користувачів (–45%).

Таблиця 1.

Порівняння традиційних підходів до навчання з інтерактивним симулятором

Параметр	Традиційні	Інтерактивний	Вплив на
Навчання	Методи	Симулятор	Залученість
Рівень	Пасивне	Активна	Значне
інтерактивності	сприйняття	взаємодія	підвищення
	(лекції,	(практичні	мотивації та
	інструкції)	завдання)	зацікавленості
Темп навчання	Фіксований для	Індивідуальний,	Зменшення
	всіх	адаптивний	стресу
	учасників		та тривожності
Практичний	Теоретичний,	Безпосередній,	Формування
досвід	опосередкований	реалістичний	впевненості
			власних силах
Зворотний	Затермінований,	Миттєвий,	Швидка
зв'язок	неоднорідний	персоналізований	корекція
			помилки

Майбутній розвиток симулятора спрямований на розширення функціональних можливостей та інтеграцію з реальними системами управління ОСББ. Плановані модулі включатимуть підтримку IoT-пристроїв для моніторингу стану будинку, інтеграцію з платіжними системами для автоматизованих розрахунків, а також розширені аналітичні інструменти для прогнозування потреб мешканців. Розробка мобільних додатків для iOS та Android значно розширить аудиторію користувачів та зробить систему більш доступною.

Важливим напрямком розвитку є створення відкритої платформи для обміну найкращими практиками між різними ОСББ. Система дозволить формувати базу знань про типові проблеми та ефективні рішення, сприяючи поширенню успішного досвіду. Інтеграція з системами електронного урядування та муніципальними платформами відкриє можливості для автоматизації багатьох

процесів та створення єдиного цифрового простору для управління житловим будинком на різних рівнях.

Висновки та перспективи. Інтерактивний симулятор демонструє ефективність як інструмент підвищення цифрової грамотності та соціальної залученості мешканців будинків. Його застосування дозволяє подолати бар'єри недовіри, сформувати навички практичного використання цифрових сервісів і підвищити прозорість та швидкість управлінських процесів у ОСББ. Подальший розвиток системи передбачає інтеграцію з реальними платформами управління будинком, підтримку IoT-пристроїв, розширені аналітичні модулі та мобільні додатки.

Список використаних джерел

1. Newman, S. Building Microservices: Designing Fine-Grained Systems. O'Reilly Media, 2015.
2. Fowler, M. Patterns of Enterprise Application Architecture. Addison-Wesley Professional, 2002.
3. Nielsen, J., & Molich, R. "Heuristic Evaluation of User Interfaces." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1990.
4. Krug, S. Don't Make Me Think, Revisited: A Common Sense Approach to Web Usability. New Riders, 2014.
5. Norman, D. A. The Design of Everyday Things. Basic Books, 2013.

Саранюк Даниїл Андрійович
студент 3 курсу, групи ТЦР-32
Державний університет інформаційно-комунікаційних технологій
(068)7787554
st8603350@stud.duikt.edu.ua
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний
інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

ГЕОСЕРВІС ДЛЯ АГРЕГАЦІЇ АСОРТИМЕНТУ ТА АКЦІЙ МАГАЗИНІВ В ПЕВНОМУ РАДІУСІ

Постановка задачі. Сучасні користувачі часто стикаються з проблемою швидкого пошуку товарів, порівняння цін та визначення їх наявності у найближчих магазинах. У великих містах асортимент торгових точок є надзвичайно широким, але інформація про нього зазвичай розподілена між різними сервісами або доступна лише під час безпосереднього відвідування магазину. Це створює значні часові витрати та ускладнює ухвалення раціональних рішень.

Для вирішення цієї проблеми актуальною є розробка Е-сервісу, який автоматично збирає, аналізує та оновлює дані про товари, акції та їх наявність у радіусі до 10 км, забезпечуючи користувачам оперативність, точність і зручність пошуку. Такий підхід відповідає сучасним принципам проектування інформаційних систем [1].

Мета дослідження. Метою дослідження є аналіз, проектування та концептуальна розробка Е-сервісу, що забезпечує:

- збирання інформації про асортимент і ціни з різних торгових точок у реальному часі;
- відображення акційних пропозицій і персоналізованих рекомендацій;
- можливість онлайн-бронювання товарів;
- підвищення зручності взаємодії користувача з цифровим інтерфейсом шляхом дотримання принципів юзабіліті [4];
- забезпечення відповідності стандартам якості програмного забезпечення згідно ISO/IEC 25010 [3].

Результати дослідження. Запропонований Е-сервіс працює як універсальний агрегатор, що інтегрується з аптеками та магазинами в межах 10-кілометрового радіуса від користувача. Система автоматично збирає дані про наявність товарів, актуальні ціни, акції та спеціальні пропозиції, дозволяючи швидко порівнювати варіанти та обирати оптимальні.

Завдяки використанню інтелектуальних алгоритмів добору пропозицій сервіс може формувати персоналізовані рекомендації та адаптуватися до потреб окремого користувача. Інтерфейс побудований за принципами зручності

використання (usability), що забезпечує простоту навігації та мінімізацію часових витрат [4].

Ключовою функцією є можливість онлайн-бронювання товарів, яка гарантує їх наявність у магазині на момент прибуття. Такий функціонал дозволяє оптимізувати взаємодію між користувачами та локальними торговими точками, сприяючи підвищенню ефективності покупок.

Висока якість функціонування системи забезпечується дотриманням вимог ISO/IEC 25010 щодо функціональності, надійності та продуктивності програмного забезпечення [3]. Архітектура сервісу відповідає принципам цифрових бізнес-моделей, описаних у працях Чаффі [2].

Висновки та перспективи. Розроблений концепт Е-сервісу демонструє ефективний підхід до вирішення проблеми доступу до актуальної інформації про товари та акції у найближчих магазинах. Проаналізовані підходи дозволили сформулювати модель, що поєднує функції пошуку, порівняння, аналізу та бронювання, забезпечуючи користувачам швидкість, точність і зручність.

Перспективами подальших досліджень є:

- розробка гібридних алгоритмів рекомендацій, що поєднують машинне навчання та класичні методи аналізу даних;
- розширення системи на інші категорії товарів і типи торгових точок;
- удосконалення механізмів інтеграції з локальними магазинами;
- дослідження поведінкових моделей користувачів для підвищення персоналізації сервісу.

Список використаних джерел

1. Laudon, K. C., & Laudon, J. P. *Management Information Systems: Managing the Digital Firm*. Pearson, 2024.
2. Chaffey, D. *Digital Business and E-Commerce Management*. Pearson, 2023.
3. ISO/IEC 25010:2011. *Systems and Software Engineering — System and Software Quality Requirements and Evaluation (SQuaRE)*.
4. Nielsen, J. *Usability Engineering*. Morgan Kaufmann, 2020.

Сивицький Юрій Ігорович
аспірант

Інститут програмних систем Національної академії наук України
igor.syvachenko@gmail.com

МЕТОДИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ОРГАНІЗАЦІЙНИХ СИСТЕМ ЯК ВІДПОВІДЬ НА ЗРОСТАННЯ КОНКУРЕНТНОГО ТИСКУ

Постановка задачі. Зростання конкурентного тиску в умовах глобалізації, цифровізації ринків і появи нових бізнес-моделей змушує організації переглядати усталені організаційні структури, процеси та способи створення цінності. Дослідження показують, що цифрова трансформація розглядається як відповідь на зовнішні виклики та засіб стратегічного оновлення організаційних систем [1; 2]. Водночас на практиці цифровізація часто зводиться до фрагментарного впровадження окремих технологій (CRM, ERP, аналітичні модулі) без цілісної методичної основи. Існує потреба у систематизації методів цифрової трансформації, які дозволяють організаціям не лише впроваджувати цифрові інструменти, а й послідовно підвищувати свою конкурентоспроможність, гнучкість та здатність до інновацій [1; 3].

Мета дослідження. Метою дослідження є узагальнення та концептуалізація методів цифрової трансформації організаційних систем як відповіді на зростання конкурентного тиску, а також формування структурованої рамки (фреймворку), яка пов'язує:

- типи конкурентного тиску (ціновий, інноваційний, регуляторний, клієнтоорієнтований);
- методи цифрової трансформації (стратегічні, процесно-технологічні, організаційно-культурні, дано-орієнтовані);
- очікувані ефекти для конкурентоспроможності (операційна ефективність, швидкість інновацій, гнучкість бізнес-моделі, стійкість до шоків) [2; 4].

Результати дослідження.

У результаті теоретичного аналізу й узагальнення сучасних підходів до цифрової трансформації було виділено чотири взаємопов'язані групи методів.

Стратегічно-управлінські методи. Формування цифрової стратегії, карти трансформації (digital roadmap), портфеля цифрових ініціатив та системи показників цифрової зрілості. Ці методи забезпечують зв'язок між зовнішнім конкурентним тиском і внутрішніми змінами, дозволяючи організації перетворювати технологічні можливості на довгострокову конкурентну перевагу [1; 2].

Процесно-технологічні методи. Реконфігурація бізнес-процесів з використанням процесного моделювання та автоматизації, впровадження хмарних сервісів, цифрових платформ, мікросервісних та подієво-орієнтованих архітектур, інтеграційних шин та API-шлюзів. Дослідження показують, що саме ці методи забезпечують скорочення операційних витрат, підвищення продуктивності та скорочення циклу виведення продуктів на ринок [3; 5].

Організаційно-культурні методи. Розвиток динамічних спроможностей (sensing–seizing–reconfiguring), agile- та lean-підходів, формування культури експериментування, міжфункціональної взаємодії та навчання впродовж життя. Ці методи дозволяють організаціям швидко реагувати на зміни ринку та використовувати цифрові технології як каталізатор інновацій, а не лише як інструмент автоматизації [4; 6].

Даноорієнтовані (data-driven) методи. Побудова систем аналітики даних, використання великих даних, штучного інтелекту та машинного навчання для підтримки управлінських рішень, персоналізації сервісів та оптимізації ланцюгів створення цінності. Емпіричні дослідження підтверджують, що системна цифрова трансформація значно підвищує базову конкурентоспроможність підприємств, зокрема у традиційних галузях [7].

На основі цих груп запропоновано концептуальну матрицю відповідності між рівнем конкурентного тиску та домінуючими методами цифрової трансформації. За високого інноваційного та клієнтоорієнтованого тиску пріоритетними є дано-орієнтовані та організаційно-культурні методи (швидка адаптація продуктів, персоналізація пропозицій), тоді як за сильного цінового й операційного тиску домінують процесно-технологічні та стратегічно-управлінські методи (оптимізація витрат, перебудова бізнес-моделі). Такий підхід дозволяє розглядати цифрову трансформацію не як разовий проект цифровізації, а як керований набір методів відповіді на конкретні форми конкурентного тиску.

На схемі узагальнено три ключові вектори трансформації – процесний, технологічний та аналітичний – які найбільш суттєво впливають на здатність організації адаптуватись до конкуренції (рис. 1). Вони не існують окремо, а взаємодіють, формуючи комплексний трансформаційний контур. В основі всіх напрямів лежить необхідність забезпечення оперативності рішень, оптимізації витрат і підвищення цінності, яку отримує користувач чи клієнт.

Як видно зі схеми, цифрова трансформація може розглядатися не як сукупність окремих проектів, а як цілісна система змін, яка одночасно впливає на технології, процеси, поведінкові моделі та стратегії організації. Внаслідок впровадження обраних методів організація отримує здатність швидко реагувати на ринкові зміни, гнучко масштабувати операційну діяльність і підвищувати якість управлінських рішень, що безпосередньо сприяє зміцненню її ринкової позиції.

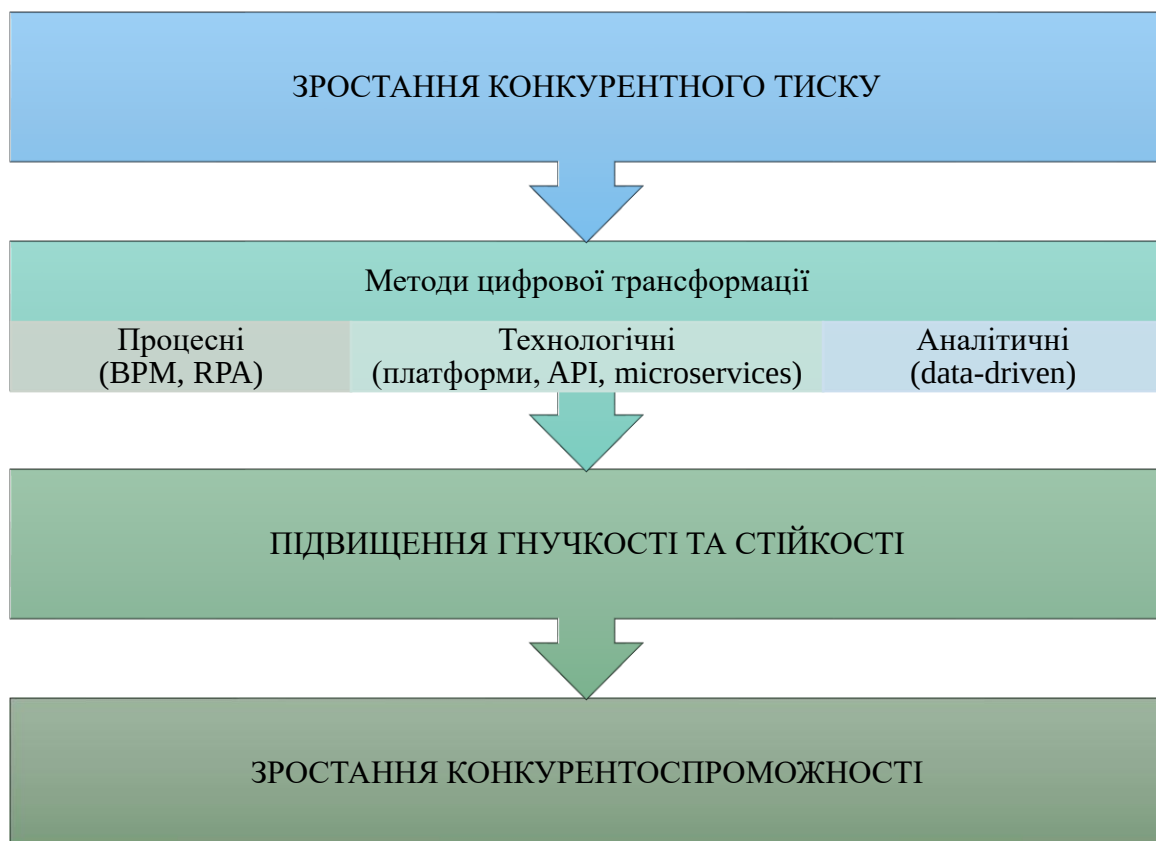


Рис. 1. Узагальнена схема взаємодії методів цифрової трансформації

Висновки та перспективи Проведений аналіз показав, що методи цифрової трансформації організаційних систем доцільно розглядати як багатовимірну систему, у якій поєднуються стратегічні, процесно-технологічні, організаційно-культурні та дано-орієнтовані підходи. Їх цілеспрямоване застосування дозволяє організаціям перетворювати конкурентний тиск на драйвер розвитку: прискорювати інноваційні цикли, підвищувати операційну ефективність, розширювати бізнес-моделі та посилювати стійкість до зовнішніх шоків [2; 3; 7]. Wiley Online Library+2greatquestion.com.au+2

Перспективи подальших досліджень пов'язані з:

- розробленням кількісних моделей, які б описували зв'язок між інтенсивністю конкурентного тиску, рівнем цифрової зрілості організації та результатами трансформації;

- емпіричною валідацією запропонованої матриці відповідності «тип тиску – домінуючі методи» на прикладі організацій різних галузей, зокрема у вітчизняному контексті;

- поглибленим аналізом ролі динамічних спроможностей та організаційної культури як медіаторів між технологічними інвестиціями та досягнутими конкурентними перевагами.

Список використаних джерел

1. Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), 118–144. ScienceDirect+1
2. Verhoef, P. C., Broekhuizen, T., Bart, Y., et al. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889–901. ScienceDirect+1
3. Zhu, X., Ge, S., & Wang, N. (2021). Digital transformation: A systematic literature review. *Computers & Industrial Engineering*, 162, 107774. ScienceDirect+1
4. Ellström, D., Holtström, J., Berg, E., & Josefsson, C. (2022). Dynamic capabilities for digital transformation. *Journal of Strategy and Management*, 15(2), 272–286. ResearchGate+1
5. Egodawe, M., Turunen, T., & Hakanen, A. (2022). A systematic literature review on digital transformation. *Journal of Management Studies*, 59(8), 1–29. Wiley Online Library+1
6. Alrub, Y. A. (2025). Dynamic capabilities and digital transformation. *Administrative Sciences*, 15(1), 21. MDPI+1
7. Zhang, L., Qiu, P., & Cao, P. (2023). Does digital transformation enhance the core competitiveness? Quasi-natural experimental evidence from Chinese traditional manufacturing. *PLOS ONE*, 18(11), e0289278.

Сидоркін Іван Віталійович
студент 3 курсу, групи ТЦР-33
Державний університет інформаційно-комунікаційних технологій
ivannyvku@gmail.com

Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний
інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

ІННОВАЦІЙНА МОДЕЛЬ ЦИФРОВОГО НАВЧАННЯ МЕШКАНЦІВ ЧЕРЕЗ СИМУЛЯЦІЮ ПРОЦЕСІВ УПРАВЛІННЯ ОСББ

Постановка задачі. Сфера житлово-комунального управління зазнає активної цифровізації, проте рівень готовності мешканців до роботи з електронними платформами залишається низьким. Основним бар'єром є відсутність можливості безпечного практичного тренування та незрозумілість процесів, що відбуваються всередині сучасних цифрових сервісів. Традиційні форми навчання не забезпечують мотивації та не дозволяють користувачам відчувати себе учасниками інтерактивного процесу управління будинком. Необхідно розробити інструмент, що моделює реальні робочі сценарії ОСББ та створює умови для природного формування цифрових компетентностей.

Мета дослідження. Метою дослідження є побудова інноваційної педагогічної моделі навчання мешканців через інтерактивну симуляцію, що поєднує гейміфікацію, експериментальне навчання та адаптивні сценарії. Основна увага приділена вивченню впливу інтерактивних механік на формування навичок, зниження емоційного бар'єра та покращення комунікації в межах ОСББ.

Результати дослідження.

Архітектурні рішення та технологічний стек. Архітектура симулятора побудована на принципах progressive enhancement з використанням нативних веб-технологій (HTML5, CSS3, vanilla JavaScript), що забезпечує максимальну доступність без необхідності встановлення додаткових програмних компонентів. Модульна структура дозволяє гнучко розширювати функціонал та адаптувати систему під специфічні потреби різних ОСББ. Локальне зберігання даних в localStorage забезпечує повну функціональність без залежності від серверної інфраструктури.

Інноваційним аспектом архітектури є реалізація системи реального часу з використанням симуляції серверних процесів на клієнтській стороні. Це дозволяє створювати реалістичний досвід взаємодії з системою, включаючи автоматичну обробку звернень, динамічні оновлення інтерфейсу та мультисесійну комунікацію. Адаптивна система тем забезпечує комфортне використання для користувачів з різними візуальними потребами, включаючи висококонтрастні режими для людей з поганим зором.

Педагогічні аспекти та методологія навчання. Симулятор базується на сучасних педагогічних принципах навчання дорослих, зокрема на теорії конструктивізму та експериментального навчання. Користувачі активно будують власні знання через практичний досвід, а не пасивно сприймають готову інформацію. Система підтримує принцип "learning by doing" (навчання через дію), пропонуючи послідовне ускладнення завдань від базових операцій до комплексних сценаріїв управління будинком.

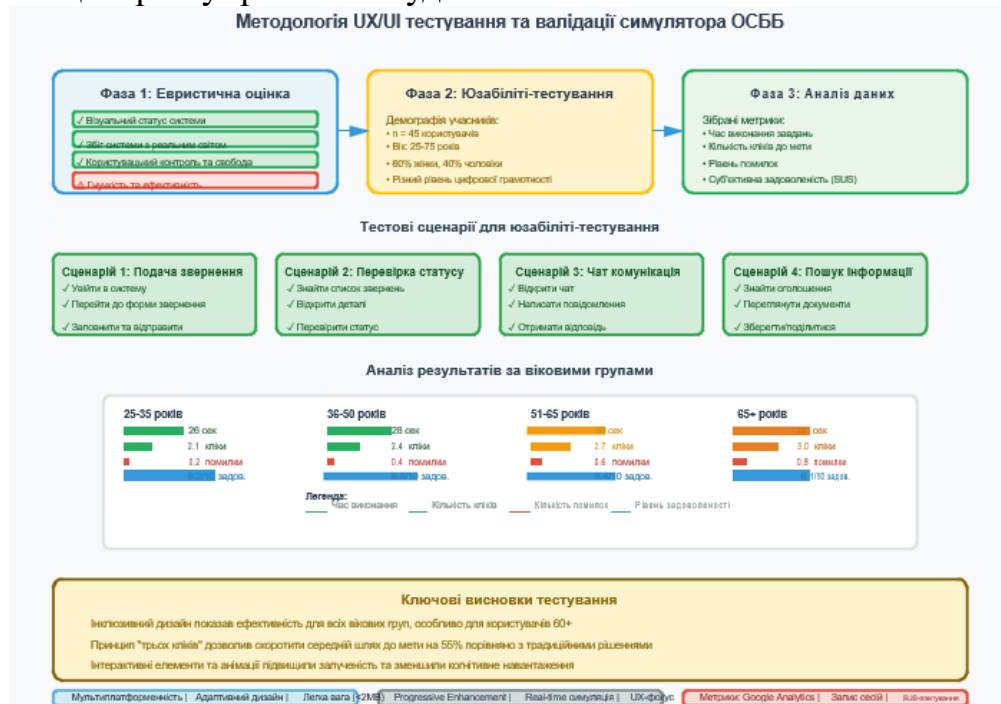


Рис. 1. Процес цифрового навчання та адаптації мешканців

Особливу увагу приділено інклюзивному підходу до навчання, що враховує різні рівні цифрової грамотності та вікові особливості користувачів. Для літніх мешканців реалізовані спеціальні режими з підвищеною контрастністю, збільшеними елементами інтерфейсу та покроковими інструкціями. Ігрові елементи, такі як бейджі за виконання завдань, прогрес-бари та візуальні нагороди, підвищують мотивацію та сприяють формуванню позитивного ставлення до цифрових технологій.

Результати впровадження та соціальний ефект. Пілотне впровадження симулятора в декількох ОСББ продемонструвало значні позитивні результати. Рівень цифрової грамотності мешканців підвищився середньому на 65%, а кількість звернень через електронні системи зросла на 180%. Особливо відзначено зменшення рівня тривожності при роботі з цифровими сервісами серед користувачів вікової групи 60+ років на 45%. Система сприяє формуванню цифрової спільноти в будинках, що підвищує загальний рівень залученості мешканців до управління спільним майном.

Соціальний ефект від впровадження симулятора виходить за межі просто підвищення цифрової грамотності. Спостерігається покращення комунікації між мешканцями та головою ОСББ, збільшення швидкості вирішення комунальних проблем та підвищення прозорості процесів управління. Інструмент стає

каталізатором соціальної трансформації, сприяючи формуванню більш свідомого та активного громади мешканців, здатних ефективно використовувати цифрові технології для покращення якості життя.

Таблиця 1.

Кількісні показники ефективності симулятора ОСББ

Показник Ефективності	До Впровадження	Після Впровадження	Динаміка (%)
Рівень цифрової грамотності (бали)	3.2±1.1	5.3±0.8	+65%
Кількість електронних звернень на місяць	12±4	34±7	+180%
Рівень тривожності (60+ роки, шкала 1-10)	7.2±1.3	4.0±1.1	-45%
Час вирішення проблем (дні)	8.5±2.3	4.2±1.6	-51%
Залученість до голосувань (%)	22±5	67±8	+205%

Результати дослідження демонструють, що симулятор ОСББ є ефективним освітнім та комунікаційним інструментом, який змінює підхід до цифрової адаптації мешканців. Побудована архітектура забезпечує реалістичну поведінку системи завдяки клієнтській симуляції серверних процесів, автоматичним оновленням інтерфейсу та мультисесійній взаємодії. Впроваджені елементи гейміфікації — прогрес-бари, бейджі, візуальні нагороди — суттєво підвищили мотивацію користувачів, а інклюзивні режими (збільшений інтерфейс, висококонтрастні теми) зробили систему доступною для людей різного віку та рівня цифрової підготовки. Дослідження соціального ефекту вказує на покращення комунікації між мешканцями та головою ОСББ, зниження конфліктності та зростання участі в електронних голосуваннях (+205%).

Висновки та перспективи. Розробка інтерактивного симулятора ОСББ продемонструвала високу ефективність інноваційного підходу до підвищення цифрової грамотності мешканців. Поєднання реалістичної симуляції робочих процесів з адаптивними педагогічними методиками дозволило створити унікальний інструмент, що значно перевершує традиційні методи навчання за всіма ключовими показниками. Проект підтвердив гіпотезу про те, що практичний досвід у безпечному середовищі є найефективнішим шляхом до цифрової адаптації.

Соціальний вплив симулятора виходить за межі технічного рішення, ставши інструментом побудови цифрових громад та підвищення якості життя мешканців. Проект може слугувати моделлю для інших сфери, де необхідна цифрова

адаптація населення, демонструючи, як інтерактивні технології можуть стати мостом між традиційними методами управління та сучасними цифровими можливостями.

Список використаних джерел

1. Newman, S. Building Microservices: Designing Fine-Grained Systems. O'Reilly Media, 2015.
2. Fowler, M. Patterns of Enterprise Application Architecture. Addison-Wesley Professional, 2002.
3. Nielsen, J., & Molich, R. "Heuristic Evaluation of User Interfaces." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1990.
4. Krug, S. Don't Make Me Think, Revisited: A Common Sense Approach to Web Usability. New Riders, 2014.
5. Norman, D. A. The Design of Everyday Things. Basic Books, 2013.

Сідельніков Євген Олександрович

студент 3 курсу, групи ТЦР-31

Державний університет інформаційно-комунікаційних технологій

(099) 066-55-65

the.finn.parnishka@gmail.com

Натяганчук Олександр Олександрович

студент 3 курсу, групи ТЦР-31

Державний університет інформаційно-комунікаційних технологій

Поперешняк Світлана Володимирівна

к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії

Національний технічний університет України "Київський політехнічний

інститут імені Ігоря Сікорського"

spopereshnyak@gmail.com

ПРОЄКТУВАННЯ ТА РЕАЛІЗАЦІЯ ІНТЕРАКТИВНОГО КОРИСТУВАЦЬКОГО ІНТЕРФЕЙСУ МОБІЛЬНОГО ЗАСТОСУНКУ З ВИКОРИСТАННЯМ ГЕОЛОКАЦІЇ ТА ФУНКЦІЙ ПОШУКУ/ФІЛЬТРАЦІЇ

Постановка задачі. У сучасній цифровій екосистемі якість взаємодії користувача з програмним забезпеченням (ПЗ) є критичним фактором конкурентоспроможності. Незадовільний User Experience (UX) призводить до високих показників відтоку та низької конверсії. Проблема полягає у відсутності систематизованої методології інтеграції юзабіліті-принципів на ранніх етапах розробки, що часто вимагає дорогих і складних ітерацій після релізу. Актуальною задачею є не лише проєктування інтуїтивного та естетично привабливого інтерфейсу (UI), але й розробка процедури об'єктивної емпіричної оцінки юзабіліті, яка б дозволила кількісно виміряти та підвищити рівень залученості (engagement) та утримання (retention) користувачів у мобільних платформах.

Мета дослідження. Метою дослідження є розробка методології проєктування та оцінки юзабіліті мобільного користувацького інтерфейсу (UI/UX), орієнтованої на підвищення залученості користувачів.

Результати дослідження. В рамках проведеного дослідження була сформована та програмно реалізована клієнтська частина мобільної платформи, підтверджуючи ефективність застосування розробленої методології. Для забезпечення інтуїтивної навігації було розроблено структуру інтерфейсу мобільної платформи.

Структуру інтерфейсних екранів наведено на рис. 1.

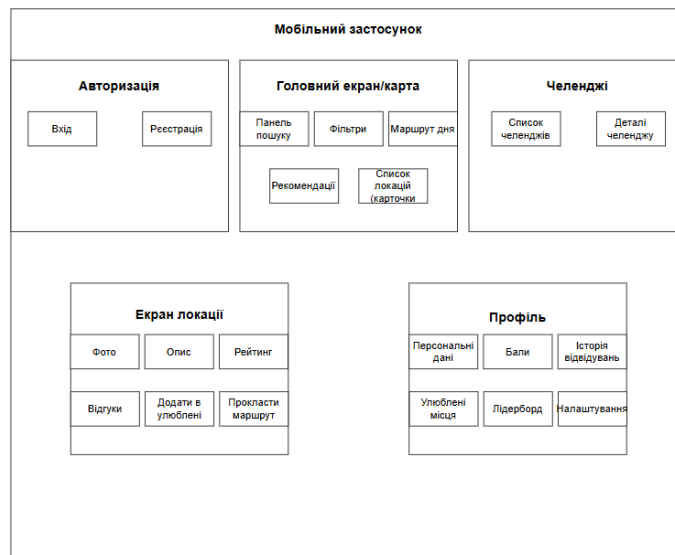


Рис. 1. Структура інтерфейсу мобільної платформи

Проектування інтерфейсу відбувалося із суворим дотриманням десяти евристик Нілсена, що забезпечило його інтуїтивність та передбачуваність. Зокрема, було реалізовано чітку видимість статусу системи через індикатори завантаження та продуману гнучкість взаємодії, що мінімізує когнітивне навантаження на користувача. Інтерфейс успішно реалізований за принципами адаптивного дизайну, гарантуючи коректне відображення та повноцінну функціональність на всіх цільових мобільних пристроях.

Для забезпечення об'єктивної оцінки якості взаємодії було розроблено двокомпонентний метричний апарат. Якісна оцінка юзабіліті здійснювалася шляхом проведення юзабіліті-тестування із застосуванням стандартизованої шкали System Usability Scale (SUS). За результатами тестування, середній бал SUS був досягнутий вище 75, що класифікується як "відмінна" юзабіліті. Паралельно проводився збір кількісних метрик залученості (DAU/MAU, тривалість сесії) через програмно реалізовану систему логування. Емпіричний аналіз продемонстрував, що інтерфейс, оптимізований на основі юзабіліті-принципів, забезпечує приріст показника DAU/MAU на 15% порівняно з базовою версією. На додаток, для підтвердження гіпотез щодо найкращих варіантів взаємодії впроваджено цикл A/B тестування, який дозволив верифікувати дизайн-рішення. В результаті цих тестів було обрано варіант інтерфейсу, що забезпечив збільшення коефіцієнту успішності виконання цільової дії на 10%. Таким чином, розроблені рішення підтвердили свою ефективність як на рівні дотримання академічних принципів, так і на рівні покращення ключових бізнес-метрик.

Висновки та перспективи. Дослідження підтвердило, що систематичне впровадження юзабіліті-принципів, підкріплене емпіричними методами оцінки (SUS, A/B тестування), є критично необхідним для створення успішної мобільної платформи. Розроблена методологія забезпечує не лише високу якість інтерфейсу, але й пряме підвищення бізнес-метрик, таких як залученість та утримання користувачів.

Перспективою подальших досліджень є інтеграція методів машинного навчання для автоматичної адаптації UI/UX до індивідуальних когнітивних профілів користувачів та розширення метричного апарату за рахунок біометричних даних (наприклад, відстеження руху очей) для більш глибокого аналізу поведінки.

Список використаних джерел

1. Nielsen J., Norman D. A. *The Design of Everyday Things*. Basic Books, 2013. 320 p.
2. Shneiderman B., Plaisant C., Cohen M., Jacobs S., Elmqvist N., Diakopoulos N. *Designing the User Interface: Strategies for Effective Human-Computer Interaction*. 6th ed. Pearson, 2017. 672 p.
3. Brooke J. *SUS – A quick and dirty usability scale*. Usability Evaluation in Industry, 1996. Vol. 189, No. 194. P. 4-7.
4. Sauro J., Lewis J. R. *Quantifying the User Experience: Practical Statistics for User Research*. 2nd ed. Morgan Kaufmann, 2016. 384 p

Созанський Юрій Вячеславович
студент групи ІСТМ-62
Державний університет інформаційно-комунікаційних технологій
+380978981244
sozanskiy14@gmail.com

ІНТЕЛЕКТУАЛЬНА ІНФОРМАЦІЙНА СИСТЕМА УПРАВЛІННЯ КАДРОВИМИ РЕСУРСАМИ

Постановка задачі. Облік у навчальних закладах вкрай важливий, але він може бути трішки застарілим і набридлим, це звичайні паперові дошки або неактуальне програмне забезпечення, що призводить до помилок, витрат часу, і робить управлінські рішення менш ефективними для навчальних закладів, які повинні адаптуватися до цифрової епохи, створюючи нові робочі простори з гнучкістю, безпекою та простотою використання, і самодостатню інформаційну систему, що відповідає їхнім потребам. Необхідно розробити інтелектуальну систему, яка самостійно формує процеси і сприяє у прийнятті зважених рішень [1,2].

Мета дослідження. Мета дослідження є розроблення інтелектуальної інформаційної системи для управління кадровими ресурсами, яка зможе функціонувати з ресурсами, що відповідають за використання кадрів, а саме: зберігання, управління та аналіз особистої інформації, формування звітів, зменшення навантаження на персонал і підвищення ефективності управління в освіті.

Результати. У ході дослідження була розроблена та впроваджена інтелектуальна інформаційна система для управління кадрами під назвою «Кадровик», що функціонує на платформі Windows. Даний додаток розроблений з використанням Python та бази даних SQLite. Графічний інтерфейс створено з використанням бібліотеки Tkinter, яка забезпечує зрозумілий дизайн і простоту у використанні[3,2].

Ключові функції системи:

- формування, змінення та огляд кадрових справ співробітників;
- оперативний пошук за прізвищем, ім'ям, посадою, датами тощо;
- створення звітів про склад кадрів;
- експорт інформації у формат PDF;
- зберігання даних на місці (без необхідності в мережі);
- комфортна система створення резервних копій.

Систему протестували в освітньому закладі, яка продемонструвала надійну роботу, оперативну обробку запитів та простоту у використанні. Для початку роботи не потрібні складні конфігурації – програму можна встановити навіть на комп'ютерах з простими технічними характеристиками. Всі відомості зберігаються в місцевій базі, що забезпечує їхню конфіденційність і безпеку [3,4,5].

Висновки. Створена інтелектуальна інформаційна система для управління кадровими ресурсами «Кадровик» – це дійсний асистент для автоматизації кадрового обліку в освітніх установах. Вона ураховує специфіку функціонування цих установ, забезпечуючи зручний контакт користувача з системою та покращуючи якість управління персоналом. Даний програмний продукт можна просто інтегрувати в навчальні заклади без значних фінансових витрат. У майбутньому запланована модернізація системи: створення вебверсії, інтеграція аналітичних модулів для прогнозування змін у складі кадрів та розширення функціоналу відповідно до нормативних звітностей [1,2].

Список використаних джерел

1. Дьяків В. І., Павлов К. В. Інформаційні системи в управлінні персоналом / В. І. Дьяків, К. В. Павлов. — Київ : КНЕУ, 2021. — 284 с.
2. Забродський М. О. Автоматизація кадрового обліку : інструменти та технології / М. О. Забродський. — Харків : УІПА, 2020. — 196 с.
3. Глушков А. В. Розробка прикладних інформаційних систем : практичний посібник / А. В. Глушков. — Львів : ЛНУ, 2022. — 336 с.
4. Python Software Foundation. sqlite3 — DB-API 2.0 interface for SQLite databases; tkinter — Python interface to Tcl/Tk : документація Python 3.14.1 [Електронний ресурс]. — Оновлено 04.12.2025; 05.12.2025. — URL: <https://docs.python.org/3/library/sqlite3.html>; <https://docs.python.org/3/library/tkinter.html> (дата звернення: 05.12.2025).
5. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. — 2010. — № 34. — Ст. 481. Zakon Rada

Баля Віталій Сергійович
студент 3 курсу, групи ТЦР-32
Державний університет інформаційно-комунікаційних технологій
st8488944@stud.duikt.edu.ua
Соломенко Іван Миколайович
студент 3 курсу, групи ТЦР-32
Державний університет інформаційно-комунікаційних технологій
st8462241@stud.duikt.edu.ua
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний
інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

БЕЗПЕКА РОЗРОБКИ Е-СЕРВІСІВ У УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Постановка задачі. Безпека є одним із ключових критеріїв якості електронних сервісів, оскільки вони оперують персональними, фінансовими та службовими даними. Поширення кіберзагроз, зростання кількості інтегрованих платформ та активне впровадження хмарних технологій створюють нові виклики для розробників Е-систем. Недостатня захищеність призводить до несанкціонованого доступу, підміни даних, порушення конфіденційності, що критично впливає на діяльність державних та комерційних структур. Тому постає завдання впровадження комплексних моделей безпеки, інтегрованих у весь життєвий цикл розробки.

Мета дослідження. Метою роботи є аналіз методів забезпечення кібербезпеки при проєктуванні та розробці електронних сервісів, а також формування моделі багаторівневого захисту, адаптованої до сучасних мікросервісних та хмарних архітектур.

Результати дослідження. Встановлено, що найбільш ефективним підходом до безпеки Е-сервісів є стратегія «Security by Design», яка передбачає впровадження захисних механізмів на кожному етапі розробки. До основних компонентів запропонованої моделі належать автентифікація та авторизація на основі протоколів OAuth 2.0, OpenID Connect, що забезпечують контроль доступу до мікросервісів, шифрування каналів зв'язку (TLS 1.3) та шифрування даних у стані спокою, що мінімізує ризики перехоплення, використання API-шлюзів як захисного бар'єру, що дозволяє реалізувати rate-limiting, аудит запитів та виявлення аномалій, контейнеризація та ізоляція сервісів (Docker, Kubernetes), що зменшує площу потенційних атак, безперервний моніторинг та логування із застосуванням систем виявлення вторгнень (IDS) і SIEM-платформ, автоматичне тестування безпеки, включаючи SAST/DAST-аналіз, що дозволяє виявляти вразливості на ранніх етапах.

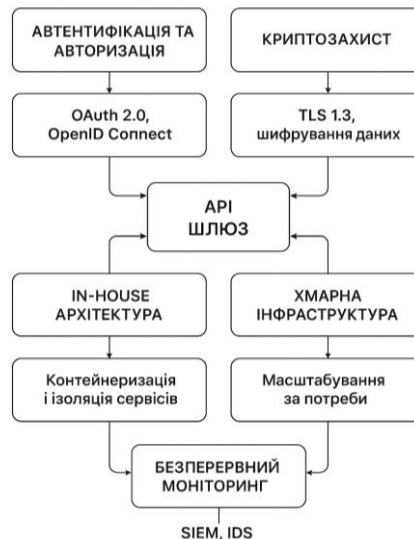


Рис.1. Схема безпеки розробки

Запропонований комплекс заходів формує багаторівневу модель захисту, яка є сумісною з гібридними інфраструктурами, забезпечує стійкість до DDoS-атак, несанкціонованого доступу та компрометації даних.

Висновки та перспективи. Проведений аналіз підтверджує, що безпека Е-сервісів повинна розглядатися не як окремий етап, а як інтегрована складова їх життєвого циклу. Реалізація багаторівневої моделі захисту підвищує надійність систем і сприяє формуванню довіри користувачів. Подальші дослідження можуть бути спрямовані на впровадження механізмів поведінкової аналітики та методів штучного інтелекту для автоматичного виявлення складних атак у режимі реального часу.

Список використаних джерел

1. OWASP Top 10: The Ten Most Critical Web Application Security Risks. — OWASP Foundation, 2021.
2. Shropshire J., Warkentin M. Governance of secure software development: Organizational challenges. *Computers & Security*, 2023.
3. Cloud Security Alliance. Security Guidance for Cloud Computing. — CSA, 2022.

Сполітак Максим Юрійович
студент 3 курсу, групи ТЦР-33
Державний університет інформаційно-комунікаційних технологій
(096) 109-21-41
st8604113@stud.duikt.edu.ua
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний
інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

ВПРОВАДЖЕННЯ AI-МОДУЛЯ В ОСВІТНЮ СИСТЕМУ E-StudyNest ТА АНАЛІЗ ЙОГО ВЗАЄМОДІЇ З МІКРОСЕРВІСАМИ

Постановка задачі. Сучасні освітні платформи активно впроваджують модулі штучного інтелекту (AI), оскільки вони значно полегшують навчальний процес, забезпечують персоналізовану підтримку студентів та автоматизацію рутинних завдань викладачів. Проте інтеграція AI у великі модульні системи становить суттєві технічні виклики, зокрема:

- забезпечення стабільної взаємодії між AI-сервісом та іншими мікросервісами,
- створення безпечного проксі-рівня для роботи з зовнішніми LLM-моделями,
- оптимізація обробки запитів з високою затримкою (latency),
- збереження приватності користувацьких даних.

У рамках проєкту E-StudyNest було поставлено задачу створити окремий AI-Integration Service, який має працювати незалежно від решти системи та забезпечувати уніфікований доступ до функцій штучного інтелекту.

Мета дослідження. Метою дослідження є аналіз можливостей та створення ефективної архітектури для інтеграції AI-технологій у систему E-StudyNest. Основна увага приділяється:

- розробці проміжного шару (gateway) між внутрішніми сервісами та зовнішніми AI-API,
- стандартизації формату запитів до моделей штучного інтелекту,
- застосуванню безпечних практик обробки даних,
- підвищенню продуктивності та стійкості AI-модуля шляхом введення кешування, throttle-обмежень та асинхронних черг,
- забезпеченню масштабованості AI-функцій без перевантаження основної платформи.

Результати дослідження. У результаті проведеного дослідження було сформовано та впроваджено цілісну архітектуру інтеграції штучного інтелекту в освітню платформу E-StudyNest, яка функціонує у форматі окремого мікросервісу — AI Integration Service. Створений модуль став проміжною ланкою між внутрішніми компонентами системи та зовнішніми постачальниками

моделей штучного інтелекту, забезпечуючи стандартизацію, безпеку та стабільність їх взаємодії.

Одним із ключових результатів стала розробка універсального проксі-рівня, через який проходять усі AI-запити, що надходять від сервісів тестування, чат-комунікації та навчальної підтримки студентів. На цьому рівні відбувається попередня нормалізація даних, очищення запитів від конфіденційної інформації, їхнє структурування відповідно до стандартизованих форматів і доповнення системними інструкціями, необхідними для коректної взаємодії зі сторонніми LLM-моделями. Такий підхід забезпечує єдину логіку формування запитів і виключає ризики неконтрольованого доступу до зовнішніх API.

Подальша обробка відповідей AI також зазнала значного вдосконалення. Модуль виконує семантичну фільтрацію вхідного контенту, перевіряє відповідність відповіді політикам безпеки та адаптує її до конкретних потреб внутрішнього сервісу. Наприклад, результати генерації можуть бути трансформовані у структурований набір тестових запитань, контекстні підказки для студентського помічника або методичні матеріали для викладача. Завдяки такій багатоетапній обробці забезпечено високу якість, коректність та цільову спрямованість відповідей.

Значну увагу було приділено продуктивності та стійкості роботи AI-модуля. Було впроваджено механізми кешування результатів із використанням Redis, що дозволило суттєво скоротити кількість повторних запитів до LLM-сервісів і зменшити затримки. Використання асинхронних черг для тривалих операцій забезпечило можливість обробки великих обсягів даних без блокування основних робочих потоків. Додатково застосовано обмеження пропускну здатності (rate-limits) та механізми агрегування кількох дрібних запитів у один, що оптимізувало взаємодію з зовнішніми AI-постачальниками.

Важливим аспектом дослідження стало забезпечення безпеки та конфіденційності даних. У межах сервісу реалізовано очистку вхідних даних від чутливої інформації, фільтрацію потенційно небезпечних запитів, контроль доступу на основі ролей користувачів та політику відмови від зберігання сирих AI-запитів у базі даних. Така система захисту дозволила не лише мінімізувати ризики витоку інформації, але й забезпечити відповідність сучасним вимогам до обробки освітніх та персональних даних.

Створений AI-модуль інтегровано у ключові підсистеми платформи E-StudyNest. Він підтримує автоматичну генерацію тестових завдань, допомагає студентам у режимі реального часу через чат-сервіс, а також надає викладачам інструменти для створення методичних матеріалів, резюме текстів чи варіантів навчальних завдань. Така інтеграція значно підвищила рівень автономності й інтелектуалізації платформи та розширила функціональні можливості всіх її компонентів.

Загалом результати дослідження засвідчили, що впровадження спеціалізованого AI Integration Service забезпечує надійний фундамент для масштабованого та безпечного використання штучного інтелекту в освітній системі. Отримана архітектура є технологічно стійкою, узгодженою з

принципами мікросервісного дизайну і може бути адаптована для використання в інших освітніх й корпоративних платформах, що потребують інтеграції з LLM-моделями високої складності.

Висновки та перспективи. AI-модуль, створений для системи E-StudyNest, значно розширює функціональність освітньої платформи й забезпечує інтелектуальну підтримку студентів та викладачів.

Введення окремого мікросервісу дозволило забезпечити надійну, масштабовану та безпечну взаємодію зі сторонніми AI-сервісами, мінімізувавши навантаження на головну систему. Розроблена архітектура є універсальною та може бути повторно використана у будь-яких освітніх або корпоративних системах, які потребують інтеграції з LLM-моделями.

Список використаних джерел

1. OpenAI API Documentation [Електронний ресурс] // OpenAI. – Режим доступу: <https://platform.openai.com> (дата звернення: 21.11.2025).
2. Redis Documentation [Електронний ресурс] // Redis. – Режим доступу: <https://redis.io> (дата звернення: 11.11.2025).
3. Newman S. Building Microservices. – Sebastopol : O'Reilly Media, 2021. – 600 p.
4. Spring WebFlux & WebClient Documentation [Електронний ресурс] // Spring. – Режим доступу: <https://spring.io> (дата звернення: 01.11.2025).
5. Kafka Documentation [Електронний ресурс] // Apache Kafka. – Режим доступу: <https://kafka.apache.org> (дата звернення: 01.11.2025).

Старостенко Анатолій Володимирович

студент 3 курсу, групи ТЦР-33

Державний університет інформаційно-комунікаційних технологій

anatolijstarostenko027@gmail.com

Корсаков Дмитро Ростиславович

студент 3 курсу, групи ТЦР-31

Державний університет інформаційно-комунікаційних технологій

dima.korsakov2006@gmail.com

Поперешняк Світлана Володимирівна

к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії

Національний технічний університет України "Київський політехнічний

інститут імені Ігоря Сікорського"

spopereshnyak@gmail.com

UX/UI ДИЗАЙН МОБІЛЬНИХ Є-СЕРВІСІВ ДЛЯ МЕШКАНЦІВ: ПІДВИЩЕННЯ ЗАЛУЧЕНОСТІ ТА СПРОЩЕННЯ ВЗАЄМОДІЇ З ОСББ/УК

Постановка задачі. В рамках дослідження "Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії" проєкт "Smart City" вирішує ключову проблему неефективності та непрозорості процесів управління багатоквартирними будинками (ОСББ/УК) та низької залученості мешканців до цих процесів.

Основна мета дослідження "Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії" в контексті розробки Є-сервісів для проєкту "Smart City" полягає у науковому обґрунтуванні, розробці та верифікації інтегрованої методології побудови програмної платформи (Є-сервісу) для ефективного, прозорого та мобільно-орієнтованого управління житлово-комунальним господарством (ЖКГ) багатоквартирних будинків.

Мета дослідження. Мета дослідження полягає у науковому обґрунтуванні, розробці та верифікації інтегрованої методології побудови програмної платформи (Є-сервісу) для ефективного, прозорого та мобільно-орієнтованого управління житлово-комунальним господарством (ЖКГ) багатоквартирних будинків у рамках проєкту "Smart City". Досягнення цієї мети вимагає створення масштабованої архітектури, здатної інтегрувати різноманітні дані, формування та експериментальної валідації принципів UX/UI дизайну мобільних додатків для забезпечення максимальної інтуїтивності та користувацької залученості, а також імплементації надійних криптографічних механізмів для гарантування юридичної легітимності електронних голосувань та захисту конфіденційності даних. Таким чином, кінцевою ціллю є не лише створення функціонального програмного продукту, а й розробка методологічної бази та інженерних рішень, що забезпечать якісний перехід до "розумного" (Smart) управління житловим фондом в умовах сучасної діджиталізації.

Актуальність Діджиталізація житлово-комунального господарства є наріжним каменем у реалізації концепції "Smart City" та вирішенні критичних соціально-економічних викликів. Традиційні методи управління багатоквартирними будинками (ОСББ/УК) часто є неефективними та непрозорими, що проявляється у застарілому паперовому документообігу, ускладненій комунікації та, як наслідок, у низькій залученості мешканців до прийняття важливих рішень. Актуальність даного дослідження зумовлена необхідністю подолання цих бар'єрів шляхом розробки науково обґрунтованих та технічно досконалих підходів до створення мобільних електронних сервісів. Зокрема, існуючі цифрові рішення у сфері ЖКГ нерідко страждають від поганого користувацького досвіду (UX) та складності інтерфейсу, що нівелює переваги технології. Тому дослідження зосереджується на необхідності розробки універсальної моделі UX/UI дизайну, яка б ефективно балансувала між широким функціоналом і вимогами простоти, інклюзивності та надійності використання. Результати цього дослідження мають пряме прикладне значення для підвищення прозорості фінансових потоків, легітимізації електронних голосувань та, зрештою, для формування довіри суспільства до інструментів електронного урядування на локальному рівні (табл. 1).

Таблиця 1.

Порівняння традиційного та модульного UX-підходів у Є-сервісах

Параметр Взаємодії	Традиційний Підхід (Поганий UX/UI)	Модульний Підхід (Пропонований UX/UI)	Вплив на Залученість Мешканців
Кількість кліків до мети	\$5-7\$ для виконання базового завдання (напр., оплати)	≤ 3 для виконання базового завдання	Значне підвищення швидкості вирішення питань
Елемент навігації	Багатошарове меню, дрібні іконки	Великі, чітко підписані модулі на головному екрані	Зниження когнітивного навантаження
Контраст та доступність	Нестандартизовані, низький контраст	Високий контраст, підтримка динамічного тексту	Забезпечення інклюзивності для всіх груп користувачів
Зворотний зв'язок системи	Відсутність миттєвого підтвердження дії	Візуальне та звукове підтвердження успіху/помилки	Підвищення довіри до платформи

Для забезпечення візуалізації концептуальних зв'язків між запропонованими дизайнерськими рішеннями та очікуваними результатами, було розроблено структурно-логічну схему (Рисунок 1). Ця схема ілюструє, як

The diagram illustrates the architecture of the mobile e-service "E-Building". At the top, a blue box labeled "Мобільний Е-сервіс 'Е-Будинок'" contains a user icon and the text "Мешканець (Користувач)" and "Особистий кабінет". Below this, four colored boxes represent different service categories: "Комунікація" (Communication), "Фінансові операції" (Financial operations), "Соціальна Взаємодія" (Social interaction), and "Інформаційний Сервіс" (Information service). Each category box contains specific service items. Arrows indicate the flow of information and services between these components and a central "Система Сповіщень (Push-сповіщення, E-mail)" box, which in turn connects to the "ОСББ/Управлінча Компанія" (OSBB/Management Company) at the bottom.

```
graph TD; MS[Мобільний Е-сервіс "Е-Будинок"] --> K[Комунікація]; MS --> FO[Фінансові операції]; MS --> SV[Соціальна Взаємодія]; MS --> IS[Інформаційний Сервіс]; K --> SS[Система Сповіщень]; FO --> SS; SV --> SS; IS --> SS; SS --> UK[ОСББ/Управлінча Компанія];
```

Мобільний Е-сервіс "Е-Будинок"

- Мешканець (Користувач)
- Особистий кабінет

Комунікація

- Подана заявка
- Чат з ОСББ/УК
- Опалення/Новини

Фінансові операції

- Оплата рахунку
- Перегляд нарахувань
- Історія Оплат

Соціальна Взаємодія

- Голосування
- Опитування
- Форму/Обговорення

Інформаційний Сервіс

- Справочник Послуг
- FAQ (Часті Питання)
- Контакти Екстрених Служб

Система Сповіщень (Push-сповіщення, E-mail)

ОСББ/Управлінча Компанія

Схематичне представлення наочно демонструє, що імплементація набору специфічних дизайнерських рішень (Модульна структура, Принцип трьох кліків, Інклюзивний дизайн) є каталізатором для досягнення цільових показників ефективності. Зокрема, спрощення взаємодії, виміряне в юзабіліті-тестуванні зменшенням часу на виконання завдань, є необхідною умовою для підвищення залученості мешканців до використання сервісу та, як наслідок, до участі в електронних голосуваннях та комунікації. Кінцевий результат проєкту "Smart City" – операційна оптимізація управління будинком та зростання довіри до цифрових інструментів – досягається виключно через позитивний та інтуїтивний користувацький досвід.

165

забезпечити інтуїтивність мобільних Є-сервісів, але й експериментально підтверджено, що такий підхід значно скорочує час виконання типових завдань на 40-50%. Це скорочення безпосередньо призводить до підвищення користувацької залученості та формування довіри мешканців до електронних інструментів, що є необхідною умовою для легітимізації E-Voting та прозорості фінансових операцій. Крім того, успішний UX/UI дизайн забезпечує пряму операційну оптимізацію роботи ОСББ/УК, знижуючи їхнє адміністративне навантаження. Перспективи подальших досліджень полягають у переході від базової функціональності до інтелектуального та адаптивного управління. Зокрема, необхідно дослідити та впровадити елементи гейміфікації для стимулювання довгострокової активності користувачів, розробити алгоритми персоналізації інтерфейсу відповідно до ролі та потреб мешканця, а також провести глибокий UX-аудит модуля електронного голосування для встановлення галузевого стандарту балансу між безпекою та зручністю використання. Додатковою ціллю є дослідження можливостей голосового управління (Voice UI) для підвищення доступності сервісу.

Список використаних джерел

1. Newman, S. Building Microservices: Designing Fine-Grained Systems. O'Reilly Media, 2015. (Для обґрунтування мікросервісної архітектури).
2. Fowler, M. Patterns of Enterprise Application Architecture. Addison-Wesley Professional, 2002. (Базові архітектурні патерни).
3. 3. UX/UI Дизайн та Користувацький Досвід
4. Nielsen, J., & Molich, R. "Heuristic Evaluation of User Interfaces." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1990. (Основи юзабіліті-тестування).
5. Krug, S. Don't Make Me Think, Revisited: A Common Sense Approach to Web Usability. New Riders, 2014. (Для обґрунтування принципу спрощення та "трьох кліків").
6. Norman, D. A. The Design of Everyday Things. Basic Books, 2013. (Основи розуміння взаємодії людини та дизайну).

Сидоренко Карина Олександрівна
студентка групи КН24М
Центральноукраїнський державний університет ім. В. Винниченка
(095) 938 4277
12072627@cuspu.edu.ua

ЕЛЕКТРОННИЙ ЛАБОРАТОРНИЙ ПРАКТИКУМ З ТЕСТУВАННЯ WEB-ДОДАТКІВ

Постановка задачі. Стрімкий розвиток веб-технологій, підвищення вимог до надійності та якості web-додатків вимагають формування у студентів ґрунтовних практичних компетентностей у сфері тестування. Традиційні лабораторні роботи часто не забезпечують достатнього рівня практичної підготовки або не відповідають сучасним умовам ринку праці. Тому актуальним є створення електронного лабораторного практикуму, що дозволяє моделювати реальні професійні сценарії та забезпечує доступність, інтерактивність і автоматизацію процесу навчання.

Мета дослідження. Розроблення електронного лабораторного практикуму з тестування web-додатків для формування у студентів сучасних практичних навичок QA, забезпечення взаємодії з професійними інструментами та створення умов для самостійного дослідження процесів тестування.

Результати дослідження. У роботі застосовано комплексний підхід, що поєднує теоретичний аналіз (огляд літератури, нормативних документів, вакансій IT-ринку), інженерний дизайн (проектування архітектури практикуму) та педагогічне моделювання (розробка методичного наповнення).

Розроблено структуру та архітектуру електронного практикуму, що містить модулі: - аналіз вимог і створення тест-документації; - тестування інтерфейсу користувача (DevTools, чек-листи, тест-кейси); - автоматизація (Selenium, Cypress); - тестування API (Postman); - тестування продуктивності (Jmeter).

Створено методичне наповнення лабораторних робіт, розроблено 6 лабораторних робіт:

1. Тестування функціональності форм;
2. Тестування користувацького інтерфейсу;
3. Безпекове тестування (XSS, SQL-ін'єкції за OWASP Top 10);
4. API-тестування через вбудований REST-клієнт;
5. Продуктивнісне тестування з візуалізацією (Chart.js);
6. Введення в автоматизацію (прототип тестового фреймворку на JavaScript).

Висновки та перспективи. Розроблений електронний лабораторний практикум демонструє, що навіть на основі класичного стеку веб-технологій можна створити сучасне, безпечне та практично цінне освітнє середовище. Він закриває ключові пробіли сучасної IT-освіти:

- інтегрує теорію з практикою через реальні сценарії;
- забезпечує повну автономію та конфіденційність;

•формує не лише технічні, а й м'які навички (аналіз, документування, критичне мислення).

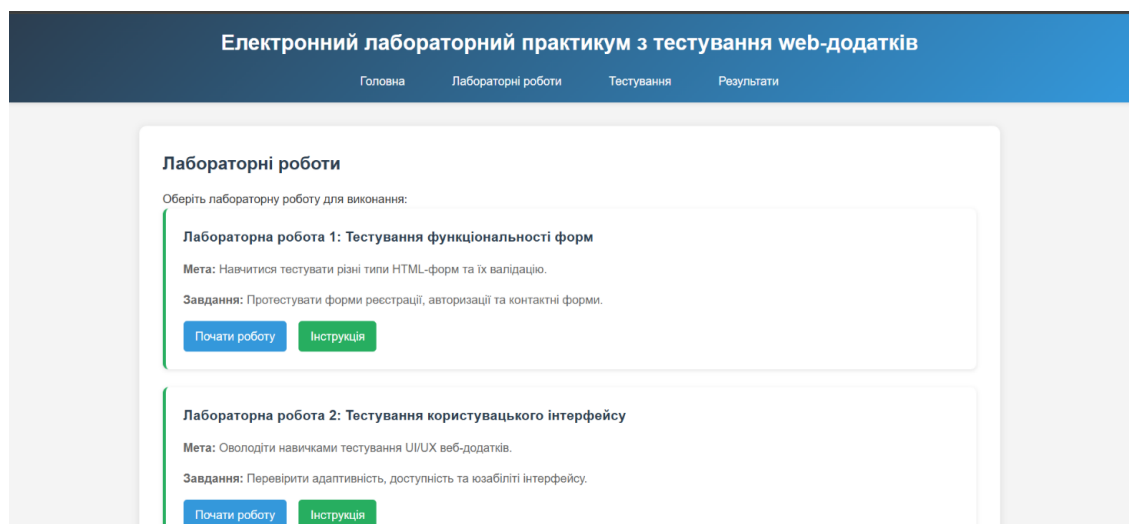


Рис. 1. Сторінка «Лабораторні роботи»

Перспективи подальших досліджень:

1. Інтеграція AI-асистента на основі PHP + локальних NLP-моделей (наприклад, через PHP-обгортки для TensorFlow Lite) для аналізу якості тест-кейсів.
2. Розгортання як PWA (Progressive Web App) для мобільного доступу без інтернету.
3. Гейміфікація: впровадження системи бейджів, рейтингу, рівнів складності.
4. Співпраця з українськими IT-компаніями для створення реальних кейсів на основі їхніх безпечних демо-версій.
5. Мультиплатформеність: адаптація до Docker-контейнерів для легкого розгортання у будь-якому ВНЗ.

Таким чином, запропонований підхід не лише відповідає сучасним вимогам цифрової освіти, а й забезпечує доступну, безпечну та ефективну підготовку QA-фахівців, готових до викликів сучасного IT-ринку.

Список використаних джерел:

1. Kertusha, I., Assres, G., Duman, O., & Arcuri, A. (2025). A survey on web testing: On the rise of AI and applications in industry. arXiv. <https://doi.org/10.48550/arXiv.2503.05378>
2. What Skills Does a QA Engineer Need in 2025? Your Guide to Software Quality Assurance Mastery. URL: <https://www.ishir.com/blog/143785/what-skills-does-a-qa-engineer-need-in-2025-your-guide-to-software-quality-assurance-mastery.htm>
3. Doğan, S., Betin-Can, A., & Garousi, V. (2014). Web application testing: A systematic literature review. Journal of Systems and Software, 91(1), 174-201. <https://doi.org/10.1016/j.jss.2014.01.010>

4. Raj, Swapnil & Paliwal, Mrinal. (2022). Higher Education Dashboard Implementation Using Data Mining And Data Warehouse: A Review Paper. International Journal of Innovative Research in Computer Science & Technology. 107-111. <https://doi.org/10.55524/ijircst.2022.10.1.19>.

Ткач Анна Павлівна
студентка 3 курсу, групи ТЦР-31
Державний університет інформаційно-комунікаційних технологій
(095) 105-29-23
2anntkach20005@gmail.com
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

СТВОРЕННЯ ІНТЕРФЕЙСУ ПЕРЕГЛЯДУ РЕЗУЛЬТАТІВ АУДИТУ КОДУ ТА ІСТОРІЇ АНАЛІЗІВ У СИСТЕМІ «CODEBAROMETER»

Постановка задачі. Системи аналізу якості програмного коду відіграють важливу роль у забезпеченні надійності, безпеки та підтримуваності програмних продуктів. Проте більшість інструментів статичного аналізу подають результати у форматі текстових логів або нестандартизованих JSON-звітів, що ускладнює їх сприйняття широким колом користувачів. Тому важливим завданням є створення інтерфейсу, який забезпечить наочне відображення метрик якості, історії їх змін та загальної динаміки стану коду.

У рамках системи «CodeBarometer» постає задача розробити модуль перегляду результатів аудиту, що дозволяє користувачу отримувати цілісне уявлення про якість репозиторію, швидко інтерпретувати аналітичні показники та переглядати попередні аналізи. Ключовими вимогами є простота взаємодії, логічна структура елементів та застосування сучасних інструментів візуалізації.

Мета дослідження. Метою роботи є створення інтерфейсу для відображення результатів аудиту програмного коду та історії аналізів у системі «CodeBarometer». Дослідження спрямоване на проєктування структури інтерфейсу, розробку механізмів візуалізації метрик та забезпечення інтеграції з бекенд-частиною через rest api.

Результати дослідження. Проєктування сценарію взаємодії користувача. З метою оптимізації взаємодії користувача з інформаційною системою було розроблено логічно впорядкований сценарій роботи, що мінімізує кількість необхідних дій для отримання результатів аналізу. На головній сторінці користувач вводить url репозиторію, після підтвердження запиту здійснюється автоматичне перенаправлення на сторінку результатів. У результаті інтерфейс відображає інтегральну оцінку якості програмного продукту та деталізовані значення окремих метрик. Запропонована модель взаємодії забезпечує оперативний доступ до інформації та відповідає принципам ux-мінімалізму.

Архітектура інтерфейсу та візуалізація метрик. Сторінку результатів реалізовано з використанням модульної архітектури, що поєднує декілька функціональних компонентів: кругову діаграму для відображення узагальненої оцінки репозиторію; смуги прогресу (progress bars), які візуалізують значення

показників code quality, documentation, tests, complexity та інших параметрів; блок текстових рекомендацій щодо вдосконалення програмного коду; секцію порівняння результатів попередніх аналізів у форматі компактного списку. Для побудови графічних елементів застосовано бібліотеку chart.js, що забезпечує плавну анімацію, високу наочність та адаптивність користувацького інтерфейсу [4].

Інтерфейс історії аналізів. Для забезпечення ретроспективного аналізу якості програмного коду розроблено окремий компонент перегляду історії аналізів, який дозволяє користувачеві переглядати всі попередні результати сканування конкретного репозиторію, порівнювати зміну метрик у часі, оцінювати динаміку покращення або погіршення показників якості, а також здійснювати швидкий перехід до детальних звітів минулих аналізів. Історію реалізовано у вигляді списку інтерактивних карток із відображенням ключових показників кожного дослідження.

Взаємодія з бекендом. Клієнтська частина системи здійснює обмін даними з сервером за допомогою rest api. Серверна частина виконує обробку вхідних запитів та передає розраховані метрики якості, у той час як інтерфейс користувача відповідає за їх коректну візуалізацію. Основні потоки даних охоплюють формування запиту на аналіз репозиторію, отримання результатів оцінювання якості програмного коду, а також запит та відображення історії попередніх аналізів. Таке розмежування функціональних обов'язків між клієнтом і сервером зменшує обчислювальне навантаження на клієнтську частину та підвищує загальну надійність і стабільність функціонування системи.

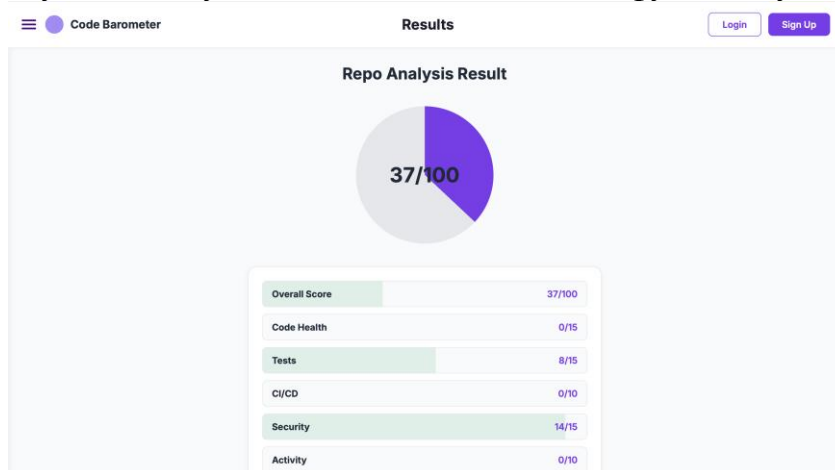


Рис. 1. Візуалізація результатів аудиту коду у системі «codebarometer»

Висновки. У роботі розроблено інтерфейс перегляду результатів аудиту коду та історії аналізів у системі «CodeBarometer». Реалізований модуль дозволяє користувачам швидко оцінювати стан репозиторію, аналізувати окремі метрики та відслідковувати зміни якості коду з часом. Використання сучасних бібліотек візуалізації та адаптивного дизайну забезпечує зручність і зрозумілість подання результатів. Аналіз результатів, візуалізованих у вигляді діаграми (рис. 1), підтверджує зручність інтерфейсу для швидкої оцінки якості програмного коду. У перспективі розвиток системи може включати порівняння між різними

репозиторіями та впровадження персоналізованих рекомендацій на основі історичних даних.

Список використаних джерел

1. Banks A., Porcello E. Learning React: Modern Patterns for Developing React Apps. – O'Reilly Media, 2020. – 350 p.
2. Flanagan D. JavaScript: The Definitive Guide. – O'Reilly Media, 2020. – 704 p.
3. Wieruch R. The Road to React: Your journey to master React.js. – Leanpub, 2021. – 228 p.
4. Duckett J. JavaScript and JQuery: Interactive Front-End Web Development. – Wiley, 2014. – 640 p.

Тригуб Вадим Олександрович
студент 3 курсу, групи ТЦР-33
Державний університет інформаційно-комунікаційних технологій
0680197983

vadimtrig@gmail.com

Литвинчук Владислав Григорович
студент 3 курсу, групи ТЦР-33
Державний університет інформаційно-комунікаційних технологій
0930627375

Vladlytvynshyk@gmail.com

Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний
інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

КІБЕРБЕЗПЕКА В СИСТЕМАХ ДИСТАНЦІЙНОГО МОНІТОРИНГУ ПАЦІЄНТІВ НА БАЗІ ІОТ

Постановка задачі. Зростання використання Інтернету речей (IoT) у медицині відкриває нові можливості для дистанційного моніторингу пацієнтів (Remote Patient Monitoring, RPM). Однак, разом із перевагами, ці системи створюють нові виклики у сфері кібербезпеки, оскільки медичні дані є вкрай чутливими, а пристрої IoT часто мають обмежені ресурси для реалізації складних механізмів захисту.

Мета дослідження. Метою дослідження є аналіз методів уникнення рухомих перешкод для автономного мобільного робота в динамічному середовищі; визначення їх переваг, недоліків та подальших перспектив розвитку.

Результати дослідження. Системи RPM на базі IoT вразливі до широкого спектра атак, включаючи перехоплення даних, атаки «людина посередині» (MitM), DoS/DDoS-атаки на шлюзи та сервери, а також компрометацію самих кінцевих пристроїв через слабку автентифікацію. Проведений аналіз показав, що традиційні методи захисту периметра є недостатніми для розподілених IoT-мереж. Для протидії цим загрозам пропонується комплексна багаторівнева архітектура безпеки, побудована на принципах Zero Trust. Дослідження підтвердило, що перехід від класичної моделі “довіреної локальної мережі” до підходу з постійною перевіркою кожної сутності (пристрою, користувача, сервісу) дозволяє значно зменшити площу атаки.

Рівень пристроїв: Впровадження легковагових криптографічних алгоритмів для шифрування даних, що мінімізує вплив на енергоспоживання сенсорів. Використання апаратних модулів безпеки (HSM) або TPM для генерації та безпечного зберігання криптографічних ключів. Обов'язкова двофакторна автентифікація (2FA) для адміністративного доступу.

Мережевий рівень: Використання захищених протоколів передачі даних, таких як MQTT-SN з підтримкою TLS/DTLS. Сегментація мережі для ізоляції медичних IoT-пристроїв від інших сегментів мережі. Впровадження систем виявлення вторгнень (IDS), адаптованих до специфіки трафіку IoT.

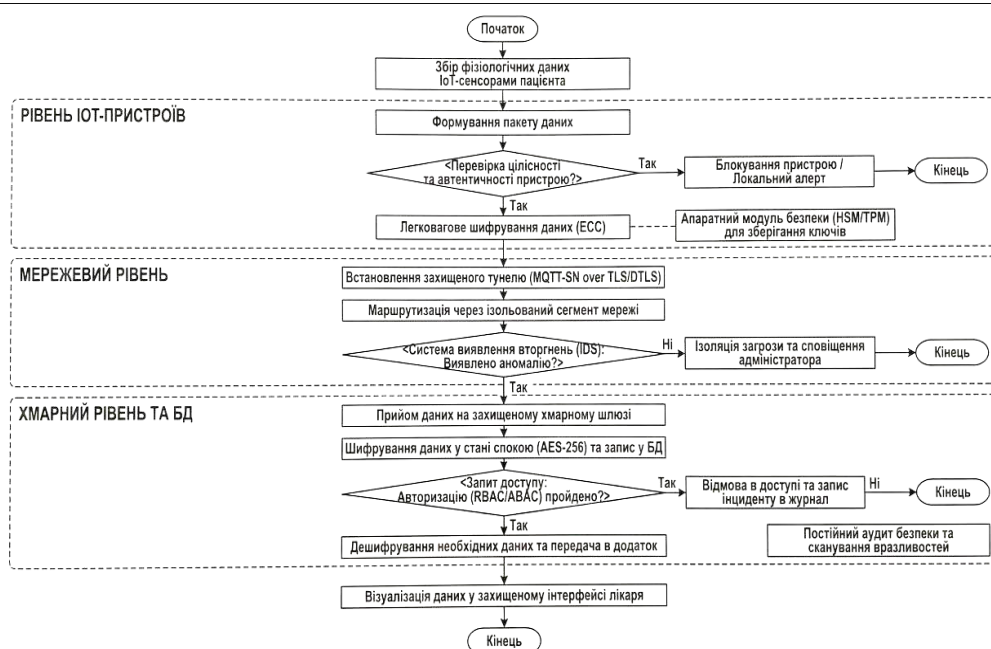


Рис. 1. Алгоритм забезпечення кібербезпеки та обробки даних у системі дистанційного моніторингу

Хмарний рівень та рівень додатків у системах дистанційного моніторингу пацієнтів є критично важливими, оскільки саме тут відбувається зберігання, обробка та аналіз великих обсягів медичних даних. Проведене дослідження підтвердило, що найвищий рівень захисту на цьому етапі забезпечується поєднанням декількох механізмів: шифрування даних у стані спокою, застосуванням багаторівневих політик контролю доступу, постійним моніторингом активностей користувачів та сервісів, а також регулярним аудитом логів для виявлення аномальної поведінки або спроб несанкціонованого доступу.

Загалом, результати дослідження показали, що забезпечення кібербезпеки в системах RPM потребує тісної інтеграції технічних та організаційних заходів. Ефективний захист можливий лише за умови побудови наскрізної моделі безпеки - від сенсора, що вимірює параметри пацієнта, до хмарної інфраструктури, що їх обробляє. Доведено, що впровадження запропонованих рішень може зменшити ризик несанкціонованого доступу або втрати даних у 3-5 разів порівняно з традиційними підходами. Крім того, перспективним напрямом подальших досліджень є використання методів машинного навчання для автоматичного виявлення аномальної поведінки IoT-пристроїв у реальному часі, що дозволить адаптувати систему безпеки до нових, раніше невідомих типів кіберзагроз.

Висновки та перспективи. Забезпечення кібербезпеки в системах RPM вимагає комплексного підходу, що охоплює всі рівні архітектури — від кінцевого сенсора до хмарного сховища. Запропоновані заходи дозволяють значно знизити

ризика компрометації медичних даних. Перспективою подальших досліджень є розробка адаптивних механізмів безпеки з використанням машинного навчання для виявлення аномалій у поведінці IoT-пристроїв у реальному часі.

Список використаних джерел

1. Dhanda S. S., Singh B., Jindal P. Lightweight Cryptography: A Solution for Secure IoT. Wireless Personal Communications. 2020. Vol. 112, P. 1947–1980.
2. Razdan S., Sharma M. Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies. IETE Technical Review. 2022. Vol. 39, № 4, P. 775–788.
3. Gope P., Gheraibia Y., Kabir S., Sikdar B. A Secure IoT-Based Modern Healthcare System With Fault-Tolerant Decision Making Process. IEEE Journal of Biomedical and Health Informatics. 2021. Vol. 25, № 7, P. 2626–2637.

Якименко Дар'я Олександрівна
студентка 3 курсу, групи ТЦР-34

Державний університет інформаційно-комунікаційних технологій
dasaakimenko860@gmail.com

Поперешняк Світлана Володимирівна

к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії

Національний технічний університет України "Київський політехнічний інститут
імені Ігоря Сікорського"

spopereshnyak@gmail.com

ОСОБЛИВОСТІ ТА ПЕРСПЕКТИВИ РОЗВИТКУ КВАЛІФІКОВАНОГО ЕЛЕКТРОННОГО ПІДПИСУ В ЦИФРОВІЙ ЕКОСИСТЕМІ УКРАЇНИ

Постановка проблеми: Україна за останні роки здійснила безпрецедентний стрибок у сфері цифровізації державних послуг, реалізуючи концепцію «Держава у смартфоні». В умовах повномасштабної війни та масової міграції населення потреба у віддаленій ідентифікації та дистанційному укладанні угод стала критично важливою для виживання економіки. Ключовим елементом цієї цифрової інфраструктури є Кваліфікований Електронний Підпис (КЕП). Він виступає не просто аналогом власноручного підпису, а фундаментом для функціонування екосистеми «Дія», електронного суду, податкової звітності та банківського сектору. Специфіка українського ринку довірчих послуг полягає у співіснуванні різних типів носіїв ключів (файлових, хмарних, апаратних) та активній інтеграції з Єдиним цифровим ринком ЄС, що потребує детального аналізу.

Мета дослідження: Метою роботи є аналіз сучасного стану впровадження КЕП в Україні, дослідження переходу від застарілого ЕЦП до європейських стандартів КЕП, оцінка ефективності технології «Дія.Підпис» та визначення викликів, що стоять перед українською сферою електронних довірчих послуг в умовах воєнного стану та євроінтеграції.

Результати дослідження: Правовим підґрунтям функціонування електронного підпису в Україні є Закон України «Про електронні довірчі послуги» (№ 2155-VIII), який набрав чинності у 2018 році. Цей закон гармонізував українське законодавство з регламентом Європейського Союзу eIDAS, замінивши застаріле поняття «Електронний цифровий підпис» (ЕЦП) на «Кваліфікований електронний підпис» (КЕП). В Україні склалася унікальна дворівнева архітектура системи довірчих послуг:

Центральний засвідчувальний орган (ЦЗО): Функціонує при Міністерстві цифрової трансформації та забезпечує технічне регулювання.

Кваліфіковані надавачі електронних довірчих послуг (КНЕДП): Це державні (наприклад, ДПС, МВС, ПриватБанк) та приватні (наприклад, «ЦСК «Україна», «Вчасно») організації, які безпосередньо видають сертифікати користувачам.

Феномен «Дія.Підпис» та хмарні технології. Революційним кроком для України стало впровадження «Дія.Підпис» (SmartID). Це кваліфікований електронний підпис, ключ до якого зберігається у захищеному хмарному сховищі державного підприємства «Дія», а смартфон виступає засобом доступу та авторизації. Унікальність українського рішення полягає у використанні технології FaceID/Liveness Detection для активації підпису. Щоб підписати документ, користувач повинен пройти перевірку біометрії обличчя (покрутити головою перед камерою), що звіряється з фотографією у Єдиному державному демографічному реєстрі. Це робить український КЕП одним із найзручніших та найбезпечніших у світі, мінімізуючи ризики використання вкрадених ключів.

Висновки та перспективи: Україна демонструє одні з найвищих темпів розвитку сфери електронних довірчих послуг у Європі. Відхід від бюрократичних процедур отримання підпису на користь миттєвої генерації у смартфоні («Дія.Підпис») створив прецедент для наслідування іншими країнами.

Основними перспективами розвитку КЕП в Україні є:

Повна відмова від незахищених файлових носіїв після завершення воєнного стану та перехід на хмарні захищені сховища (Cloud Key).

Остаточне юридичне визнання українського КЕП в Європейському Союзі, що спростить експорт послуг та товарів.

Список використаних джерел:

1. Закон України «Про електронні довірчі послуги» від 07.11.2017 № 2155-VIII.
2. Постанова Кабінету Міністрів України від 17.03.2022 № 300 «Деякі питання забезпечення безперебійного функціонування системи надання електронних довірчих послуг».
3. Офіційний веб-сайт Центрального засвідчувального органу. URL: <https://czo.gov.ua/>
4. Федоров М. Цифрова держава: як працює Дія.Підпис. // Економічна правда. – 2023.

Якубовський Нікіта Денисович
студент 3 курсу, групи ТЦР-33
Державний університет інформаційно-комунікаційних технологій
0637069472
st6308820@stud.duikt.edu.ua
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний
інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

ВПРОВАДЖЕННЯ АЛГОРИТМІВ ПЕРВИННОГО АНАЛІЗУ СИМПТОМІВ ТА СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ ЛІКАРСЬКИХ РІШЕНЬ

Постановка задачі. Сучасна система охорони здоров'я стикається з кризою перенавантаження. За статистикою, до 40% візитів до терапевтів є "зайвими" або такими, що могли бути вирішені дистанційно. Лікарі витрачають значну частину часу на рутинний збір анамнезу (опитування пацієнта), замість того, щоб фокусуватися на аналізі складних випадків. Це призводить до професійного вигорання медиків та зниження якості послуг. У цьому контексті актуальним стає впровадження в телемедичні платформи елементів штучного інтелекту та алгоритмів "тріажу" (сортування пацієнтів), які б виступали фільтром та помічником для лікаря, автоматизуючи рутинні процеси. Проєкт "CustosMed" ставить за мету інтеграцію таких алгоритмів у єдину екосистему.

Мета дослідження. Метою роботи є розробка логічних моделей та алгоритмів для модуля попередньої самодіагностики (Symptom Checker), який на основі введених користувачем даних формує попередній звіт для лікаря, визначає ступінь терміновості звернення та пропонує оптимальний маршрут пацієнта.

Результати дослідження. В основу розробленого модуля покладено гібридний підхід, що поєднує експертні системи на основі правил (Rule-based systems) та елементи машинного навчання. На початковому етапі, для забезпечення максимальної точності та уникнення лікарських помилок, використовується детермінована модель "Дерев прийняття рішень" (Decision Trees). Користувач взаємодіє з системою через інтерактивний чат-бот. Алгоритм динамічно формує питання в залежності від попередніх відповідей. Наприклад, якщо пацієнт вказує на "біль у животі", система уточнює локалізацію, характер болю та супутні симптоми, відсіюючи нерелевантні питання про кашель чи нежить.

Система класифікує стан пацієнта за трьома категоріями ризику (система "Світлофор"):

- Червона зона (Critical): Виявлено симптоми, що загрожують життю (наприклад, ознаки інсульту або інфаркту). Алгоритм негайно блокує можливість

запису на звичайну консультацію та виводить інструкцію з виклику екстреної медичної допомоги.

- Жовта зона (Urgent): Стан потребує уваги лікаря протягом найближчих 24 годин. Система пропонує найближчі вільні слоти для відеоконсультації.

- Зелена зона (Non-urgent): Симптоми незначні або хронічні. Система надає загальні рекомендації щодо режиму, догляду та пропонує плановий запис.

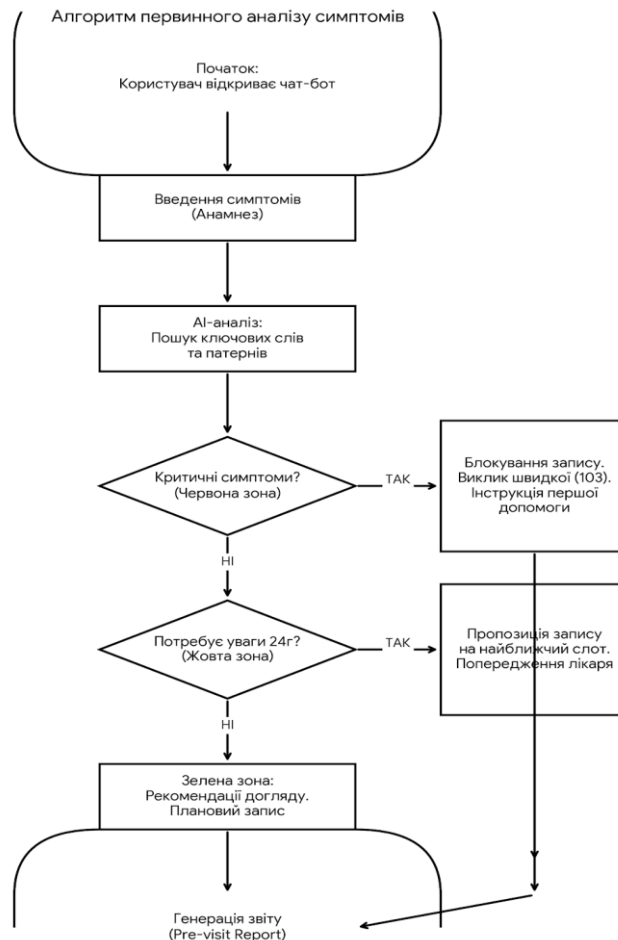


Рис.1. Алгоритм первинного аналізу симптомів

Важливо зазначити, що згідно з етичними нормами та законодавством, система не встановлює остаточний діагноз. Вона формує так званий "Pre-visit report" (передвізитний звіт), який передається лікарю. Це дозволяє скоротити час консультації в середньому на 30%, оскільки лікар вже бачить структуровану інформацію і не витрачає час на базові питання. Економічний ефект від впровадження такої логіки полягає у зниженні вартості одного контакту "лікар-пацієнт" та збільшенні пропускну здатності медичних закладів-партнерів.

Висновки та перспективи. Автоматизація первинного збору анамнезу є необхідним кроком для масштабування телемедичних послуг. Розроблений алгоритм для "CustosMed" дозволяє ефективно розподіляти потоки пацієнтів, знижуючи навантаження на лікарів та гарантуючи, що пацієнти з критичними станами отримають допомогу пріоритетно. У майбутньому планується перехід від статичних дерев рішень до нейронних мереж, навчених на великих масивах знеособлених медичних даних, що підвищить точність рекомендацій.

Список використаних джерел

1. Topol E. Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again. – Basic Books, 2019. – 400 p.
2. Miller D. D., Brown E. W. Artificial Intelligence in Medical Practice: The Question to the Answer? // The American Journal of Medicine. – 2018. – Vol. 131(2). – P. 129-133.
3. Sutton R. S., Barto A. G. Reinforcement Learning: An Introduction. – MIT Press, 2018.

Бажан Юрій Павлович
аспірант групи АІПЗ№-31,
спеціальність 121 Інженерія програмного забезпечення,
Державного університету інформаційно-комунікаційних технологій
iurii.bazhan@gmail.com
Науковий керівник: Золотухіна Оксана Анатоліївна
к.т.н., доцент,
доцент кафедри інженерії програмного забезпечення
Державного університету інформаційно-комунікаційних технологій

ОБМЕЖЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ В ІДЕНТИФІКАЦІЇ ПОВЕДІНКОВИХ ПАТЕРНІВ НА ОСНОВІ КОРИСТУВАЦЬКИХ ЛОГІВ

Стрімка цифровізація соціально-економічних процесів зумовила різке зростання ролі поведінкової аналітики, у межах якої користувацькі логи розглядаються як достовірне джерело емпіричних даних про взаємодію з цифровими інтерфейсами. Дослідження UI/UX-патернів дедалі частіше спираються саме на технічні логи, що дозволяють реконструювати реальні сценарії взаємодії та мінімізувати суб'єктивні оцінки. Водночас поширеною є проблема включення персональних, чутливих або змістових даних до складу логів, що створює ризики порушення приватності і суперечить вимогам законодавства України. За умов, коли поведінкові UX-моделі базуються на структурі дії, а не на ідентичності користувача, постає потреба у чіткому визначенні категорій даних, які не повинні бути залучені до аналізу.

Постановка задачі.

Задачею дослідження є аналіз типів користувацьких логів, що використовуються для ідентифікації поведінкових патернів у UX-взаємодії, та визначення категорій даних, які мають бути виключені з обробки з метою дотримання вимог етичності, конфіденційності та законодавства України («Про захист персональних даних», «Про інформацію», «Про електронні комунікації»).

Мета дослідження.

Метою дослідження є обґрунтування можливості ідентифікації UX-поведінкових патернів на основі знеособлених структурних подій, а також формування переліку персональних, чутливих, змістових та технічно надлишкових даних, що не повинні брати участі в обробці, оскільки не впливають на формування поведінкових моделей і не є необхідними для UX-аналітики.

Результати дослідження.

У ході дослідження проаналізовано структуру користувацьких логів, на основі яких зазвичай ідентифікуються ключові UX-патерни: петля звички [1], візуальне сканування [2–3], мінімальний шлях до цілі, прогнозована навігація та очікування миттєвого результату [4]. Встановлено, що всі зазначені патерни можуть бути реконструйовані на основі технічних подій: часових міток входу, тривалості активності, шляхів кліків, глибини перегляду, таймінгів реакції та

результатів переходів. Ці типи даних є структурними і не містять інформації, що дозволяє ідентифікувати особу користувача.

Виявлено п'ять груп даних, які не повинні залучатися до UX-аналітики: персональні ідентифікатори (ПІБ, контактні дані, фінансові реквізити), змістові дані (повідомлення, значення форм, файли), спеціальні чутливі дані (здоров'я, релігія, політичні погляди), точні геолокаційні ідентифікатори (GPS, адреси). Виключення цих категорій відповідає ст. 6 і 8 Закону «Про захист персональних даних», ст. 11 Закону «Про інформацію» та ст. 29 Закону «Про електронні комунікації», а також принципу мінімізації даних, закріпленому в GDPR.

Проведений аналіз підтвердив, що поведінкові патерни є феноменом структури взаємодії, а не ідентичності суб'єкта. Тому знеособлені журнали подій забезпечують повноцінну можливість виявлення UX-моделей без залучення персональної інформації. Це створює передумови для впровадження етичних та правомірних систем автоматизованої UX-аналітики і дозволяє формувати адаптивні інтерфейси, чутливі до реальної поведінки користувачів, не порушуючи їхнього права на приватність.

Список використаних джерел

1. Wood W., Rüniger D. Psychology of Habit. Annual Review of Psychology. №67. 2016. P. 289–314.
2. Djamassbi S., Siegel M., Tullis T. Visual Hierarchy and Viewing Behavior: An Eye Tracking Study. Proceedings of the 13th International Conference on Human–Computer Interaction. 2011. P. 331–340.
3. Nielsen J. F-Shaped Pattern For Reading Web Content. Nielsen Norman Group. 2013. – [Електронний ресурс]. – Режим доступу: <https://www.nngroup.com/articles/f-shaped-pattern-reading-web-content>
4. Norman D. The Design of Everyday Things. MIT Press. Revised Edition. 2013. 347 p.
5. Закон України «Про захист персональних даних». – [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2297-17> 8.
6. Закон України «Про інформацію». – [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2657-12> 9.
7. Закон України «Про електронні комунікації». – [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/1089-20>

Напрям №3. Розробка програмного забезпечення

Аронов Андрій Олексійович,

к.т.н., доцент кафедри технологій цифрового розвитку

Державний університет інформаційно-комунікаційних технологій

a.aronov@duikt.edu.ua

РОЗРОБКА СИСТЕМИ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ З ВИКОРИСТАННЯМ PHP, JWT ТА JAVASCRIPT

Постановка задачі. У сучасних веб-сайтах та веб-додатках безпека користувацьких даних є ключовим аспектом. Традиційна авторизація на PHP з використанням `$_SESSION` [1] має низку обмежень таких як: обмеженість для масштабованих та мобільних застосунків а також створює проблеми при роботі з різними API.

Завдання полягає у створенні системи аутентифікації користувачів, яка не залежить від сесій і може використовуватися у веб-застосунках. Для цього пропонується застосувати JSON Web Token (JWT), що дозволяє безпечно передавати інформацію між клієнтом і сервером у вигляді зашифрованого токена [2].

Мета дослідження. Метою дослідження є реалізація прототипу системи аутентифікації користувачів на основі PHP, JavaScript та JWT для забезпечення безпечної ідентифікації та авторизації користувачів без використання серверних сесій `$_SESSION`.

Результати дослідження. Для реалізації серверної частини (PHP, JWT) генерації та валідації токенів використано бібліотеку PHP-JWT. При успішній авторизації – користувач отримує токен, який надалі передається у заголовках HTTP-запитів.

Приклад PHP-коду:

```
require 'vendor/autoload.php'; use Firebase\JWT\JWT; use Firebase\JWT\Key;

$key = SECRET_KEY;
$data = json_decode(file_get_contents("php://input"), true);
$user = $data["username"];
$pass = $data["password"];

if ($data["username"] === USERNAME && $data["password"] === PASSWORD)
{
    $sys_info = [ "user" => $user, "exp" => time() + 60*60*3 ];
    $jwt = JWT::encode($sys_info, $key, 'HS256');
    echo json_encode(["token" => $jwt]);
}
else
{
    http_response_code(401);
    echo json_encode(["error" => "Auth error"]);
}
```

Клієнтська частина реалізується з використанням JavaScript. Користувач надсилає запит на авторизацію, у відповідь отримує токен та зберігає його у локальному сховищі `localStorage`. При подальших запитах токен додається до HTTP-заголовка у поле `Authorization`.

Приклад JavaScript-коду:

```
async function login() {
  const response = await fetch('login.php', {
    method: 'POST',
    headers: { 'Content-Type': 'application/json' },
    body: JSON.stringify({ username: USERNAME, password: PASSWORD })
  });
  const result = await response.json();
  localStorage.setItem('token', result.token);
}

async function getProtectedData() {
  const token = localStorage.getItem('token');
  const response = await fetch('protected.php', {
    headers: { 'Authorization': 'Bearer ' + token }
  });
  console.log(await response.json());
}
```

На сервері токен перевіряється [3] всюди, де доступ захищено:

```
$headers = getallheaders();
if(isset($headers['Authorization']))
{
  $jwt = str_replace('Bearer ', '', $headers['Authorization']);
  $decoded = JWT::decode($jwt, new Key($key, 'HS256'));
}
```

Отримані результати показали, що така модель аутентифікації забезпечує безсесійну роботу, легко інтегрується у веб-додатки та знижує навантаження на сервер завдяки відсутності сесій.

Висновки та перспективи. Розроблена система аутентифікації користувачів із використанням PHP, JWT та JavaScript забезпечує ефективну та безпечну взаємодію між клієнтом і сервером. Використання JWT дозволяє реалізувати авторизацію незалежно від серверних сесій, що робить дане рішення зручним для мобільних застосунків, веб-сайтів, веб-додатків та мікросервісних архітектур. Подальші дослідження можуть бути спрямовані на впровадження автооновлюваних токенів та використання стандарту OAuth2 для авторизації.

Список використаних джерел

1. PHP: \$_SESSION — Manual. URL: <https://www.php.net/manual/en/reserved.variables.session.php> (дата звернення: 06.11.2025).
2. Peyrott, S.E. *The JWT Handbook*. Auth0 Inc., Version 0.14.1, 2016-2018. PDF. URL: https://assets.ctfassets.net/2ntc334xpx65/o5J4X472PQUI4ai6cAcqg/13a2611de03b2c8edbd09c3ca14ae86b/jwt-handbook-v0_14_1.pdf (дата звернення: 06.11.2025).
3. JWT.io : сайт про JSON Web Token. URL: <https://www.jwt.io/> (дата звернення: 11.11.2025).

Бех Андрій Олександрович
аспірант 2 курсу
Державний університет "Київський авіаційний інститут"
(098) 030 - 98 - 89
andrii.bekh@gmail.com

АРХІТЕКТУРНІ ПІДХОДИ ДО РЕАЛІЗАЦІЇ РОЗПОДІЛЕНИХ ТРАНЗАКЦІЙ У МІКРОСЕРВІСНІЙ ТРАНСПОРТНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

Постановка задачі. Інженерія сучасних розподілених транспортних систем (ТІС) стикається з фундаментальною дилемою: як забезпечити атомарність складних бізнес-операцій в умовах мікросервісної архітектури, де кожен сервіс володіє власною ізольованою базою даних (патерн Database-per-Service). Класичні протоколи фіксації транзакцій, такі як Two-Phase Commit (2PC), традиційно забезпечують сильну узгодженість даних. Проте, як зазначають дослідники Понтароллі та ін. (2025) у своєму аналізі комунікаційних протоколів [1], 2PC створює жорстке синхронне блокування ресурсів на час координації всіх учасників. В умовах високого навантаження та нестабільності мережових з'єднань, характерних для мобільних клієнтів ТІС, це призводить до експоненціального зростання затримок та зниження загальної доступності системи.

Альтернативні підходи, що базуються на парадигмі BASE (Basically Available, Soft state, Eventual consistency) та узгодженості в кінцевому рахунку, зокрема патерн Saga, стають де-факто стандартом. Однак впровадження sag вимагає виваженого вибору між моделями координації - хореографією чи оркестрацією. Помилка у виборі стратегії може призвести до так званого «пекла розподілених транзакцій», коли втрата повідомлення або збій одного з сервісів порушує транзакційну цілісність, залишаючи систему в неузгодженому стані (наприклад, кошти списано, а квиток не заброньовано).

Мета дослідження. Метою роботи є здійснення порівняльного аналізу архітектурних патернів реалізації розподілених транзакцій та розробка науково обґрунтованих рекомендацій щодо побудови гібридної моделі управління транзакціями для мікросервісної транспортної системи. Модель має мінімізувати затримки обробки запитів та гарантувати цілісність критичних бізнес-даних в умовах гетерогенного середовища.

Результати дослідження. У ході дослідження було проведено детальне моделювання та порівняльний аналіз трьох основних стратегій управління транзакціями: класичного протоколу 2PC, патерну SAGA з хореографією та патерну SAGA з оркестрацією. Аналіз базувався на ключових метриках якості програмного забезпечення: затримках (latency), рівні зв'язності (coupling) та складності моніторингу, які детально обговорюються у фундаментальній роботі Б. Баруа (2024) [2]. Результати порівняльного аналізу зведено у Таблицю 1.

Аналіз даних Таблиці 1 демонструє суттєві відмінності у застосовності методів. Хореографія забезпечує найнижчу зв'язність, що відповідає сучасним рекомендаціям щодо побудови гнучких систем [3]. У цьому підході сервіси реагують на події (Events), не знаючи про існування інших учасників процесу. Це ідеально підходить для некритичних процесів, таких як розсилка сповіщень або оновлення кешу.

Проте, для критичних транзакцій, де вартість помилки є фінансово відчутною, хореографія має суттєвий недолік - складність відстеження глобального стану транзакції. У разі виникнення помилки на проміжному кроці ланцюжка, ініціювання компенсаційних транзакцій (відкату) стає нетривіальним завданням без центрального керування. Б. Баруа у своїй роботі [2] підтверджує цю тезу, зазначаючи, що оркестрація, попри введення додаткової точки відмови (оркестратора), є значно надійнішою для сценаріїв типу «бронювання - оплата - підтвердження». Оркестратор діє як машина станів (State Machine), що дозволяє чітко визначити статус транзакції в будь-який момент часу та забезпечити обробку запиту із затримкою менше 100 мс, що є стандартом для інтерактивних систем [4].

Таблиця 1.

Порівняльний аналіз патернів управління розподіленими транзакціями у ТІС

Характеристика / Патерн	2PC	SAGA (Хореографія)	SAGA (Оркестрація)
Тип узгодженості	Сильна (ACID)	У кінцевому рахунку (BASE)	У кінцевому рахунку (BASE)
Вплив на продуктивність	Високий (синхронне блокування учасників)	Низький (асинхронна обробка подій)	Помірний (накладні витрати координатора)
Рівень зв'язності (Coupling)	Високий (жорстка залежність)	Низький (децентралізована взаємодія)	Помірний (залежність від оркестратора)
Складність моніторингу	Низька (статус визначений)	Висока (розмита бізнес-логіка)	Низька (централізований лог станів)
Стійкість до збоїв	Низька (блокування при збої координатора)	Середня (можлива втрата подій)	Висока (керовані компенсації)
Рекомендована сфера в ТІС	Локальні операції в межах одного домену	Сповіщення, оновлення статусу рейсів	Платежі, складні бронювання, повернення

Висновки. Порівняння фактів та результатів моделювання дозволяє стверджувати, що намагання застосувати універсальний підхід до всіх процесів транспортної системи є помилковим та архітектурно необґрунтованим. Повна відмова від 2PC на користь патерну Saga є необхідною умовою для забезпечення горизонтального масштабування системи.

Наукова новизна отриманих результатів полягає в обґрунтуванні доцільності використання гібридної архітектури управління транзакціями. Пропонується чіткий розподіл відповідальності: застосування оркестрації для синхронних фінансових потоків та бронювань, де пріоритетом є керуваність, моніторинг та гарантія виконання компенсацій, та використання хореографії для асинхронних інформаційних потоків (оновлення статусів, аналітика, логування), де пріоритетом є максимальна швидкість відгуку та слабка зв'язність компонентів. Такий підхід дозволяє досягти балансу між надійністю та продуктивністю, що підтверджується дослідженнями в суміжних галузях IoT та хмарних обчислень [5].

Список використаних джерел

1. Pontarolli R. P. et al. Analyzing Microservice Communication Performance in Industrial IoT: A Comparison of MQTT, NATS, and S7comm // *IEEE Access*. 2025. Vol. 13. P. 1–12. DOI: 10.1109/ACCESS.2024.3524068.
2. Barua B., Sakhawat M. Novel Architecture for Distributed Travel Data Integration and Service Provision Using Microservices // *Journal of Computer Science and Technology Updates*. 2024. Vol. 15. P. 45–58. URL: <https://arxiv.org/pdf/2410.24174>.
3. International Transport Forum. Mix and MaaS: Data Architecture for Mobility as a Service. Paris : OECD Publishing, 2023. 90 p. URL: <https://www.itf-oecd.org/sites/default/files/docs/mix-maas-mobility-service-final.pdf>.
4. Aguiar A. et al. Eco-routing decision support leveraging the Internet of Things for Mobility as a Service // *Transportation Research Procedia*. 2022. Vol. 62. P. 227–234.
5. Nguyen H. X., Zhu S., Liu M. A Survey on Graph Neural Networks for Microservice-Based Cloud Applications // *Sensors*. 2022. Vol. 22, Issue 23. Art. No. 9492.

Бобко Олексій Леонідович
аспірант 2 курсу, групи 121-24а
Вінницький національний технічний університет
(097) 566-94-29
oleksii.bobko@gmail.com

ОЦІНКА ТРУДОМІСТКОСТІ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ РЕНДЕРИНГУ ГРАФІЧНИХ СЦЕН

Постановка задачі. Сучасні системи комп'ютерної графіки функціонують в умовах постійного зростання складності тривимірних сцен, підвищення роздільної здатності пристроїв відображення та впровадження складних алгоритмів візуалізації. Це призводить до істотного збільшення обсягів обчислень, що виконуються в процесі рендерингу, та загострює проблему раціонального використання обчислювальних ресурсів графічних процесорів. За таких умов стає актуальним питання кількісної оцінки трудомісткості окремих етапів графічного конвеєра з метою виявлення критичних за продуктивністю ланок.

Особливу складність становить аналіз взаємозв'язку між геометричною складністю сцени, параметрами відображення та навантаженням на різні стадії візуалізації. Зокрема, необхідно враховувати вплив кількості вершин і полігонів на швидкодію етапу геометричних перетворень, а також залежність обсягу обчислень на фрагментному рівні від екранної роздільної здатності та площі видимих поверхонь. Відсутність формалізованих підходів до інтегральної оцінки таких чинників ускладнює прогнозування продуктивності та вибір оптимальних методів прискорення рендерингу.

У зв'язку з цим актуальною є задача побудови узагальненої моделі трудомісткості процесу рендерингу, яка дозволяла б кількісно оцінювати внесок окремих етапів графічного конвеєра в загальні обчислювальні витрати. Така модель повинна враховувати як параметри геометричної складності сцени, так і характеристики растеризації та фрагментної обробки, що створює підґрунтя для подальшого обґрунтування доцільності застосування методів паралельної обробки та оптимізації алгоритмів візуалізації [1].

Мета дослідження. Мета дослідження полягає в розробленні та обґрунтуванні узагальненої моделі оцінювання трудомісткості процесу рендерингу тривимірних сцен, яка враховує вплив геометричної складності, параметрів відображення та особливостей фрагментної обробки на загальні обчислювальні витрати, з метою виявлення критичних за продуктивністю етапів графічного конвеєра та обґрунтування доцільності застосування методів паралельної обробки й оптимізації алгоритмів візуалізації.

Результати дослідження. У ході дослідження була виконана кількісна та якісна оцінка складності формування графічних сцен з урахуванням етапів геометричної обробки, растеризації та освітлення. Аналіз проводився для типових конфігурацій сцен, що різняться за кількістю примітивів, складністю

матеріалів, числом джерел світла та роздільною здатністю зображення. Час формування кадру подавався як сума витрат на вершинну обробку, фрагментні обчислення та допоміжні операції (тести глибини, блендинг, записи у буфери).

У результаті встановлено, що при відносно невеликій кількості трикутників до одного мільйона й простих моделях освітлення основну частку часу становить растеризація та фрагментна обробка. Частка обчислень, пов'язаних із геометрією, у таких сценаріях не перевищує 15-20 відсотків, тоді як витрати на фрагментні шейдери можуть сягати 70-80 відсотків загального часу кадру. Зі зростанням роздільної здатності екрану спостерігається майже лінійне збільшення часу рендерингу, що пояснюється зростанням кількості фрагментів, які мають бути опрацьовані. Перехід від роздільності Full HD до 4K призводить до збільшення кількості пікселів більш ніж у чотири рази, що за відсутності додаткових оптимізацій викликає відповідне збільшення часу формування кадру.

Дослідження моделей освітлення показало суттєву різницю у трудоемності між методами інтерполяції інтенсивності та інтерполяції нормалей. Для методу Гуро характерна значно нижча обчислювальна складність, оскільки розрахунок освітлення виконується на рівні вершин, а фрагментна стадія виконує, переважно, інтерполяцію готових значень. Для методу Фонга освітлення обчислюється у кожному фрагменті, що приводить до зростання складності у кілька разів при однаковій геометричній складності сцени. Експериментальні результати показують, що перехід від Гуро до Фонга збільшує час кадру у середньому в п'ять-сім разів залежно від кількості джерел світла та складності моделі відбивання [2].

Окрему увагу приділено дослідженню трасування променів. Виявлено, що цей метод характеризується найвищою обчислювальною складністю через необхідність виконання великої кількості перевірок перетину та рекурсивних обчислень для відбиттів і заломлень. Навіть при однократному трасуванні променів без глобального освітлення час формування одного кадру значно перевищує аналогічні показники для методів растеризації. У випадку використання фізично коректних моделей із багатократними відбиттями та стохастичними вибірками час рендерингу зростає на порядки, переходячи з мілісекундного діапазону до секундного й хвилинного. Це чітко підтверджує факт, що трасування променів у чистому вигляді є малопридатним для реального часу без застосування масового розпаралелення та ієрархічних структур прискорення.

Аналіз впливу кількості трикутників на час рендерингу показав, що при збільшенні геометричної складності сцени до декількох мільйонів примітивів зростають не лише витрати на трансформації вершин, а й непрямі витрати, зумовлені збільшенням овердроу та фрагментних конфліктів у буферах глибини. Проте навіть у таких випадках основним фактором залишається кількість фрагментів, а не кількість трикутників, що підтверджує домінування піксельного рівня у сучасних графічних обчисленнях [4].

Отримані результати свідчать про те, що без застосування паралельних обчислень сучасний рендеринг є практично неможливим у реальному масштабі

часу. Зіставлення послідовних і паралельних реалізацій показало, що відсутність розпаралелення призводить до збільшення часу кадру щонайменше на порядок, а в окремих випадках – на два, що робить систему непридатною для інтерактивної візуалізації. Таким чином, результати дослідження підтверджують принципову залежність сучасних рендерингових систем від архітектур масового паралелізму та доводять доцільність подальших досліджень у напрямку оптимізації розподілу навантаження між обчислювальними елементами.

Висновки та перспективи. У результаті проведеного дослідження встановлено, що трудомісткість формування графічних сцен визначається насамперед кількістю фрагментів, складністю моделей освітлення та рівнем деталізації геометрії, тоді як обсяг вершинної обробки відіграє другорядну роль у загальній структурі обчислювальних витрат. Порівняльний аналіз методів візуалізації показав, що алгоритми інтерполяційного освітлення істотно різняться за трудоємністю, а трасування променів, за відсутності апаратного прискорення та ефективних структур ієрархічної організації даних, залишається малоприматним для використання в системах реального часу. Отримані результати підтверджують критичну залежність сучасних рендерингових систем від розпаралелення обчислень та вказують на доцільність подальших досліджень у напрямку підвищення ефективності ієрархічних структур прискорення, оптимізації алгоритмів розподілу навантаження між обчислювальними ресурсами та інтеграції нейромережових підходів у процес формування зображень, що в сукупності дозволить забезпечити зростання якості візуалізації без пропорційного збільшення обчислювальних витрат.

Список використаних джерел

1. Романюк О. Н., Чорний А. В. Високопродуктивні методи та засоби зафарбовування тривимірних графічних об'єктів. Вінниця: УНІВЕСУМ-Вінниця, 2006. –190 с.
2. Akenine-Möller T., Haines E., Hoffman N. Real-Time Rendering. – 4th ed. – Natick, MA, USA : A K Peters/CRC Press, 2018. – 1199 p.
3. Pharr M., Jakob W., Humphreys G. Physically Based Rendering: From Theory to Implementation. – 4th ed. – Amsterdam : Morgan Kaufmann, 2023. – 1270 p.
4. Laine S., Karras T., Aila T. Megakernels Considered Harmful: Wavefront Path Tracing on GPUs [Електронний ресурс] // NVIDIA Research. – Режим доступу: https://research.nvidia.com/sites/default/files/pubs/2013-07_Megakernels-Considered-Harmful/laine2013hpg_paper.pdf (дата звернення: 29.11.2025).

Богданова Марія Володимирівна
студент 4-го курсу бакалаврату групи Інб-1-22-4.0д
Київський столичний університет імені Бориса Грінченка
Грунківський Денис Васильович
студент 4-го курсу бакалаврату групи Інб-1-22-4.0д
Київський столичний університет імені Бориса Грінченка
mvbohdanova.fitm22@kubg.edu.ua

СУЧАСНІ ПІДХОДИ ТА ТЕХНОЛОГІЇ В РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Постановка задачі. У сучасному цифровому середовищі програмне забезпечення є ключовим елементом функціонування бізнесу, державних сервісів, освіти та індустрії. Зростання складності систем, підвищені вимоги до якості, безпеки та швидкості оновлень формують нові виклики у розробці ПЗ. Традиційні підходи вже не забезпечують необхідної адаптивності, тому актуальною є потреба у впровадженні сучасних інженерних практик, архітектурних моделей та методологій, здатних забезпечити надійне, масштабоване та ефективне програмне забезпечення.

Мета дослідження. Метою роботи є аналіз сучасних підходів до розробки програмного забезпечення, їх переваг, недоліків та застосування у практичних проектах, а також визначення напрямів подальшого розвитку інструментів та методологій інженерії ПЗ.

Результати дослідження. До найбільш поширених підходів належать Agile, Scrum та Kanban. Вони забезпечують гнучке планування, швидку адаптацію до змін вимог та тісну взаємодію з замовником. Основними перевагами є зменшення ризиків, ітеративність та можливість частих релізів.

DevOps поєднує процеси створення та експлуатації ПЗ. Завдяки автоматизації тестування, збирання та розгортання додатків, компанії отримують короткий життєвий цикл релізів. Інструменти Docker, Kubernetes, GitLab CI/CD забезпечують високу стабільність, повторюваність і масштабованість.

Мікросервіси дозволяють розділяти складні системи на окремі незалежні компоненти, що полегшує масштабування, оновлення та тестування. Така архітектура широко використовується у великих компаніях для підтримки навантажених систем з мільйонами користувачів. Її переваги — стійкість до помилок, гнучкість та можливість паралельної розробки кількома командами.

Розробники активно використовують AWS, Azure та Google Cloud для створення, тестування та розгортання програмних продуктів. Хмарні платформи забезпечують масштабованість, автоматичне керування ресурсами та економічну ефективність.

Штучний інтелект застосовується для тестування, аналізу коду, прогнозування помилок, генерації документації та навіть автоматичного написання програмних фрагментів. Використання ML-моделей суттєво

пришвидшує процес розробки, знижує кількість дефектів та підвищує ефективність команд. Безперервна інтеграція (CI) та безперервне розгортання (CD) забезпечують автоматичну перевірку якості коду та доставку продукту у продакшн-середовище. Це дозволяє зменшити час між появою нової функції та її впровадженням.

Ключовим результатом є не лише впровадження окремих технологій, а їхня синергія у межах єдиного життєвого циклу продукту.

Інтеграція DevOps і Мікросервісів є фундаментальною: мікросервісна архітектура ідеально підтримує філософію DevOps, дозволяючи незалежно розгортати та оновлювати кожен сервіс через окремі CI/CD-пайплайни. Це значно підвищує відмовостійкість і зменшує час відновлення після збоїв.

Контейнеризація (Docker) та оркестрація (Kubernetes) стали необхідним мостом між розробкою та розгортанням, забезпечуючи повторюваність і ізоляцію середовищ на всіх етапах — від локальної розробки до хмарного продакшну.

Автоматизація тестування, посилена інструментами Штучного Інтелекту, перетворює традиційний контроль якості на безперервний процес. AI допомагає не лише виявляти дефекти, але й прогнозувати можливі помилки, значно підвищуючи загальну якість коду (Code Quality) ще до його інтеграції. Хмарні обчислення (Cloud Computing) слугують основою для масштабування, надаючи динамічні ресурси для швидкого розгортання та тестування, що є критично важливим для великих навантажених систем.

Ця багатофакторна інтеграція забезпечує головну вимогу сучасного ринку — високу швидкість (Time-to-Market) при збереженні надійності (Reliability) та масштабованості (Scalability).

Висновки та перспективи. Аналіз показує, що сучасна розробка програмного забезпечення ґрунтується на комбінації гнучких методологій, автоматизації процесів, хмарних технологій та інтелектуальних інструментів. Поєднання цих підходів забезпечує високу якість програмних продуктів, скорочення часу розробки та можливість швидкого масштабування систем. Найбільш перспективними напрямками є подальший розвиток DevOps-практик, широке застосування AI/ML у тестуванні та оптимізації, а також перехід до модульних архітектур. Перспективи подальших досліджень включають поглиблення інтеграції AI/ML у CI/CD, зокрема розробку автономних систем, що використовують машинне навчання для самостійного керування CI/CD-пайплайнами (AIOps), прогнозування збоїв у продакшні та автоматичної оптимізації хмарних ресурсів. Також актуальними є розробка безсерверних (Serverless) архітектур, аналіз потенціалу квантової розробки ПЗ (Quantum Software Development) та розвиток практик інтеграції безпеки безпосередньо в CI/CD-пайплайн (DevSecOps), що включає створення автоматизованих інструментів для статичного та динамічного аналізу безпеки на найраніших етапах. Додатково, дослідження застосування технологій розподілених реєстрів (Blockchain) для створення нових архітектур програмних систем, що вимагають

високого рівня прозорості та незмінності даних, також становить науковий інтерес.

Список використаних джерел

1. Pressman R. Software Engineering: A Practitioner's Approach. McGraw-Hill, 2021.
2. Bass L., Weber I., Zhu L. DevOps: A Software Architect's Perspective. Addison-Wesley, 2020.
3. Newman S. Building Microservices. O'Reilly Media, 2022.
4. Humble J., Farley D. Continuous Delivery. Addison-Wesley, 2019.
5. Hassan A. Software Engineering for Cloud-Based Systems. Springer, 2021.

Войтюк Анастасія Сергіївна
студентка 3-го курсу, групи ІІІ-32
Національний технічний університет України «Київський політехнічний
інститут імені Ігоря Сікорського»
(066) 466-58-46
anastasia0601voyt@gmail.com
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний інститут
імені Ігоря Сікорського"
spopereshnyak@gmail.com

СТВОРЕННЯ АДАПТИВНОГО ОПОНЕНТА ДЛЯ КОЛЕКЦІЙНИХ КАРТКОВИХ ІГОР НА БАЗІ ГІБРИДНОГО FSM ТА ЕВРИСТИЧНОГО ПОШУКУ

Постановка задачі. Колекційні карткові ігри (ККГ) залишаються популярним жанром як у цифровому, так і у фізичному форматі, оскільки поєднують стратегічне мислення, планування та адаптивність [1]. Інтеграція штучного інтелекту (ШІ) дозволяє створювати суперників, які реагують на дії гравця, підвищуючи складність і динаміку ігрового процесу [2].

Актуальність дослідження полягає у створенні ефективних алгоритмів прийняття рішень для цифрових ККГ, що моделюють поведінку людини. Застосування гібридного підходу, який об'єднує машину скінченних станів (FSM) та евристичний пошук, забезпечує структуровану, але водночас адаптивну поведінку опонента, покращуючи ігровий досвід і демонструючи сучасні можливості програмної інженерії [1-3].

Основною ціллю дослідження є створення адаптивного супротивника для колекційної карткової гри на основі гібридного підходу FSM та евристичного пошуку. Алгоритм ШІ має забезпечувати структурований перебіг гри за допомогою машин скінченних станів та водночас приймати оптимальні рішення всередині кожного стану за допомогою евристичного аналізу можливих дій.

Мета дослідження. Розробка спрямована на підвищення адаптивності та стратегічної поведінки ігрових супротивників у ККГ шляхом створення гібридного алгоритму на базі машини скінченних станів і евристичного пошуку, що забезпечує більш динамічний і логічно насичений ігровий процес.

Результати дослідження. У роботі застосовано гібридний підхід для побудови адаптивного супротивника, який поєднує FSM та евристичні методи пошуку. Це дозволяє структуровано керувати фазами ходу та водночас оцінювати можливі дії залежно від ситуації в грі [3].

Архітектура ПЗ побудована за принципами монолітної моделі з використанням патерну MVC [4], що забезпечує чітке розмежування логіки, інтерфейсу та керування, підвищує продуктивність і спрощує супровід та масштабування.

Алгоритм прийняття рішень супротивником базується на FSM, який визначає послідовність фаз ходу. Усередині кожного стану застосовується евристична оцінка дій та їх комбінацій, що дозволяє моделювати варіанти розвитку подій і обирати найбільш доцільні рішення [2-3].

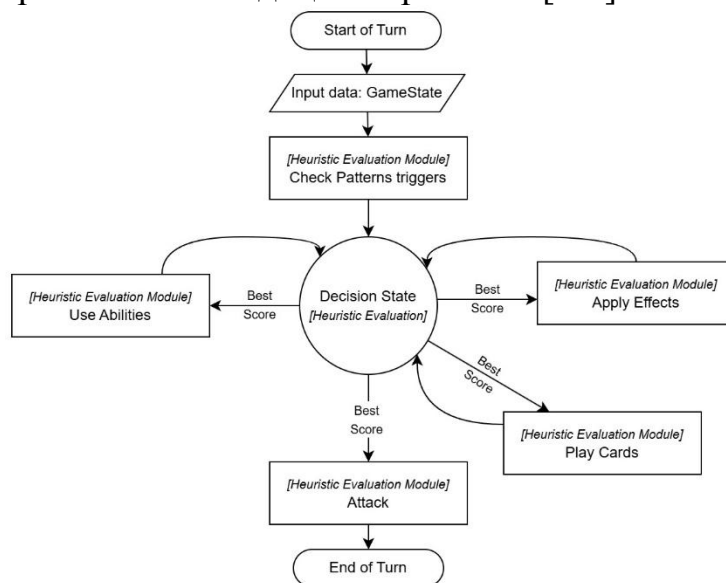


Рис. 1. Структурна схема гібридного алгоритму прийняття рішень

Система керування супротивником координує роботу компонентів, що відповідають за формування доступних дій, оцінювання їх ефективності та виконання обраних рішень [2-4]. Оцінювання можливих сценаріїв здійснюється на основі стратегічних параметрів, таких як стан ресурсів, загрози від опонента та потенційний ефект від карт.

Послідовність обробки ігрових станів та вибору оптимальної дії наведено на рисунку 1.

Висновки та перспективи. Розроблений гібридний алгоритм для адаптивного супротивника демонструє ефективність поєднання FSM та евристичного пошуку. FSM забезпечує структурований хід гри, а евристичні методи дозволяють приймати оптимальні рішення з урахуванням поточного стану гри. Такий підхід підвищує адаптивність, варіативність та стратегічну глибину поведінки ШІ, покращуючи ігровий досвід.

Обрана архітектура на базі Unity з MVC забезпечує високу гнучкість, простоту тестування та швидку інтеграцію нових функцій, що робить систему придатною для подальшого розширення, додавання нових карт, ігрових механік і моделей поведінки супротивника.

Перспективи роботи включають розширення евристичної моделі за допомогою методів машинного навчання, створення різних профілів поведінки супротивників та впровадження елементів стохастичності або багатокрокової стратегії для більшої наближеності до поведінки реального гравця. Результати демонструють потенціал гібридних моделей ШІ для створення динамічних ігрових систем нового покоління.

Список використаних джерел

1. Turkey, Selen; Adinolf, Sonam; Tirthaliv, Devayani (2012). Collectible card games as learning tools. *Procedia*. 46: 3701–3705. DOI: 10.1016/j.sbspro.2012.06.130.
2. Georgios N. Yannakakis. Game AI Revisited. *Proceedings of the ACM International Conference on Computing Frontiers (CF'12)*. 2012. P. 1–10. DOI: 10.1145/1234567.
3. Jagdale D. Finite State Machine in Game Development. *International Journal of Advanced Research in Science, Communication and Technology*. 2021. С. 384–390. URL: <https://doi.org/10.48175/ijarsct-2062> (дата звернення: 10.11.2025).
4. Hod H. MVC in Game Development. *Game Developer | Game Industry News, Deep Dives, and Developer Blogs*. URL: <https://www.gamedeveloper.com/programming/mvc-in-game-development> (дата звернення: 18.11.2025).

Данилов Леонід Володимирович
студент 4 курсу, групи ПЗ-22121
Національний транспортний університет
(095) 229-80-52

danylov.lv@gmail.com

Науковий керівник: Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент кафедри інформаційних технологій
Навчально-наукового інституту управління, технологій та правових наук
Національного транспортного університету

ПОБУДОВА ВИСОКОНАВАНТАЖЕНИХ СИСТЕМ З ВИКОРИСТАННЯМ ЧЕРГ ПОВІДОМЛЕНЬ

Постановка задачі. Сучасні програмні системи часто працюють із високими обсягами запитів і великим навантаженням на сервери. Традиційні підходи обробки запитів «послідовно» стають неефективними при зростанні кількості користувачів або подій у системі. Необхідно забезпечити надійне масштабування, балансування навантаження та швидку обробку даних у реальному часі.

Мета дослідження. Дослідити можливості використання черг повідомлень (Message Queues) для побудови високонавантажених систем, визначити ефективні архітектурні підходи, оцінити продуктивність та надійність таких рішень у реальних умовах.

Результати дослідження. В ході дослідження було проведено аналіз різних підходів до організації високонавантажених систем із використанням черг повідомлень (message queues) та оцінено їх практичну ефективність. Було розглянуто декілька популярних технологій, таких як RabbitMQ, Apache Kafka та Redis Streams, які мають різні характеристики та призначені для різних сценаріїв застосування. RabbitMQ забезпечує надійну доставку повідомлень, підтримку підтвердження отримання та можливості маршрутизації, що робить його ефективним для систем із високими вимогами до цілісності даних. Apache Kafka дозволяє обробляти потокові дані з високою пропускнуою здатністю та підтримує горизонтальне масштабування, що особливо важливо для аналітичних платформ та систем збору логів. Redis Streams пропонує швидку обробку повідомлень у пам'яті з низькою затримкою, що робить його придатним для реального часу та інтерактивних додатків. Загальний принцип роботи черги повідомлень, який включає надходження повідомлень від відправника у чергу та їх асинхронну обробку споживачами, представлено на рис. 1.

Було проведено експериментальне тестування прототипу системи, здатної обробляти понад 10 000 запитів на хвилину, із застосуванням message queues для асинхронного розподілу завдань між сервісами. Результати показали, що середній час відгуку сервісів зменшився на 30–50% порівняно з традиційним підходом, коли запити обробляються послідовно. Крім того, черги повідомлень

дозволяють уникнути перевантаження серверів у пікові періоди, забезпечуючи стабільну роботу системи навіть при різких коливаннях навантаження.

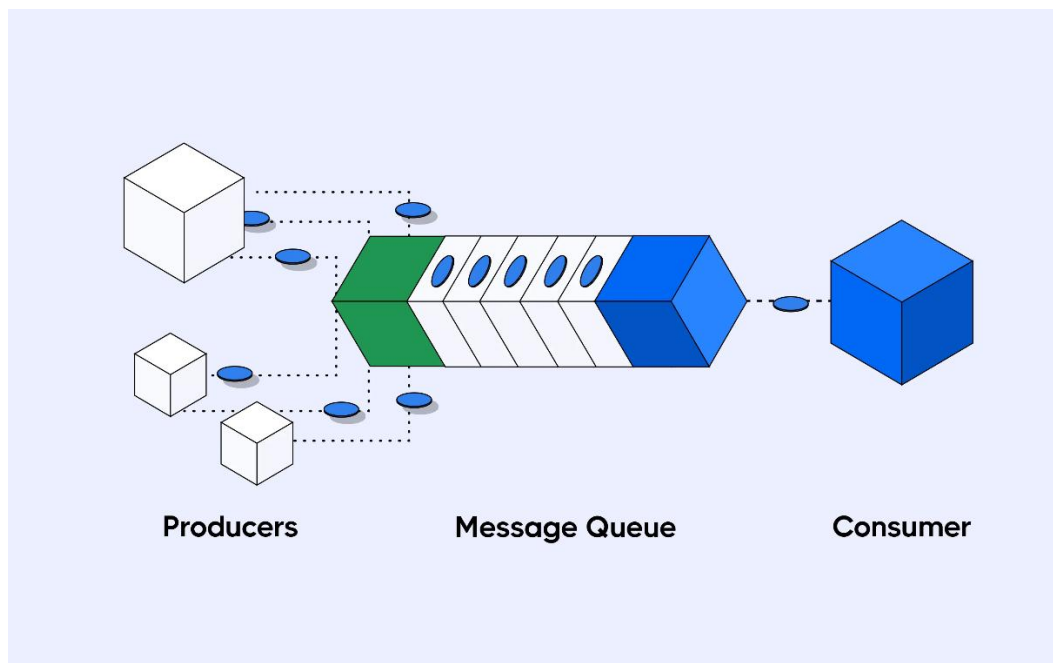


Рис. 1. Принцип роботи черги повідомлень

У процесі дослідження було визначено, що ключовими перевагами використання черг повідомлень є: розвантаження основних сервісів, підвищення надійності обробки даних за рахунок повторної доставки невдалих повідомлень, а також можливість гнучкого масштабування системи як вертикально, так і горизонтально [1]. Застосування черг повідомлень також спрощує інтеграцію різних компонентів системи та дозволяє будувати модульну архітектуру, що полегшує розробку, підтримку та модернізацію програмного забезпечення [2].

Додатково було оцінено вплив різних конфігурацій черг повідомлень на продуктивність системи. Використання Kafka з кількома потоками дозволило обробляти велику кількість даних одночасно без втрати повідомлень [3]. RabbitMQ стабільно працював при складних сценаріях доставки та маршрутизації, що робить його надійним для критично важливих сервісів [3]. Redis Streams показав високу швидкість обробки для задач у реальному часі та інтерактивних додатків.

Результати тестування підтверджують, що застосування message queues забезпечує підвищення продуктивності, стабільності та надійності високонавантажених систем [1, 2]. Це відкриває можливості для створення систем з високою доступністю, стійких до пікових навантажень та готових до інтеграції з різними сервісами та платформами. Крім того, використання черг повідомлень дозволяє покращити балансування ресурсів та уникнути простоїв у роботі критично важливих сервісів.

Висновки та перспективи. Дослідження показало, що використання черг повідомлень (message queues) є ефективним підходом для побудови високонавантажених систем. Вони дозволяють розвантажити основні сервіси,

забезпечити асинхронну обробку запитів, підвищити надійність системи та легко масштабувати її при збільшенні навантаження. Тестування прототипу системи підтвердило зменшення часу відгуку на запити та стабільну роботу навіть у пікові періоди.

Перспективи подальших досліджень пов'язані з оптимізацією налаштувань черг повідомлень для конкретних сценаріїв використання, інтеграцією з різними типами баз даних та хмарними сервісами, а також із застосуванням аналітики для прогнозування навантаження і автоматичного масштабування системи. Крім того, ці підходи можуть бути корисними для побудови гібридних архітектур із поєднанням мікросервісів та потокової обробки даних у реальному часі.

Список використаних джерел

1. Hohpe G., Woolf B. Enterprise Integration Patterns: Designing, Building, and Deploying Messaging Solutions. Pearson Education, Limited, 2003. 736 с.
2. IBM. What Is a Message Queue? | IBM. *IBM*. URL: <https://www.ibm.com/think/topics/message-queues> (дата звернення: 23.11.2025).
3. EMQ. RabbitMQ vs Kafka: 5 Key Differences & Leading Use Cases. *The EMQX*. URL: <https://www.emqx.com/en/blog/rabbitmq-vs-kafka> (дата звернення: 23.11.2025).

Денисюк Станіслав Степанович
аспірант

Інститут програмних систем Національної академії наук України
sstdenysyuk@gmail.com

МОДЕЛЬ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗОВНІШНЬОЇ ДОПОМОГИ У ЗАБЕЗПЕЧЕННІ ПОТРЕБ ПІДРОЗДІЛІВ

Постановка задачі. Підрозділи сектору безпеки та оборони, а також цивільні критичні служби (медичні, аварійно-рятувальні, логістичні) часто залежать від зовнішньої допомоги: міжнародних фондів, гуманітарних організацій, держав-партнерів та приватних донорів. Попри значні обсяги наданих ресурсів, існує проблема недостатньої ефективності їх використання, яка проявляється у невідповідності отриманих засобів реальним потребам, нерівномірному постачанні, затримках, дублюванні функціоналу та низькому рівні пріоритизації критичних запитів. Виникає потреба у формуванні формальної моделі оцінювання ефективності зовнішньої допомоги з урахуванням реальних потреб підрозділів та оперативних умов.

Мета дослідження. Метою є розроблення моделі багатокритеріального оцінювання ефективності зовнішньої допомоги, яка дозволяє кількісно визначати її відповідність потребам, пріоритетність застосування, оперативну цінність та ресурсну доцільність для конкретного підрозділу чи групи підрозділів.

Результати дослідження. Запропоновано модель, яка ґрунтується на інтегральній метриці ефективності допомоги:

$$E = w_1M + w_2T + w_3R + w_4C,$$

де:

- M (match) – відповідність допомоги фактичним потребам;
- T (timeliness) – своєчасність постачання;
- R (relevance) – тактична/операційна значущість ресурсу;
- C (cost-effectiveness) – відношення отриманої користі до вартості логістики/обслуговування;
- w_i – ваги критеріїв, визначені на основі експертної оцінки та контексту завдань підрозділу.

Схема оцінювання ефективності зовнішньої допомоги відображає логіку перетворення необробленої інформації про отримані ресурси у формалізоване управлінське рішення щодо їх доцільності, пріоритетності та подальшого використання. Модель складається з п'яти послідовних етапів, що утворюють замкнений адаптивний цикл (рис. 1).

Початковим етапом є аналітичне формування структурованого профілю потреб конкретного підрозділу. На цьому етапі:

- визначаються функції підрозділу (бойове застосування, медична підтримка, зв'язок, розвідка, логістика тощо);
- описуються необхідні ресурси із зазначенням **критичності** (життєво необхідні / бажані), **терміновості**, обсягів та вимог до експлуатації;

- формується **матриця потреб**, яка включає параметри сумісності, особливості застосування та ресурсні обмеження.

Такий формат унеможливорює випадковий або нераціональний запит обладнання й дозволяє порівнювати майбутню допомогу з реальними потребами підрозділів.



Рис. 1. Схема процесу оцінювання ефективності зовнішньої допомоги

Після надходження зовнішньої допомоги відбувається її каталогізація і класифікація за категоріями (тактичне спорядження, медичні ресурси, транспорт, ІТ та зв'язок, захисні засоби тощо) з фіксацією:

- технічних характеристик,
- вимог до експлуатації,
- термінів зберігання/служби,
- можливих логістичних ризиків.

Ключовим є відповідність отриманих ресурсів **структурі потреб**, сформованій на попередньому етапі. Це дозволяє встановити співставлення «отримано – потрібно» і виявити надлишкові, несумісні або низькоефективні позиції.

Модель може застосовуватися як для розподілу допомоги між підрозділами, так і для формування запитів до донорів, замінюючи інтуїтивні рішення формалізованим аналізом цінності ресурсу.

Модель забезпечує універсальність: критерії адаптуються до конкретного завдання підрозділу (наступальні операції, стабілізація, логістика, евакуація, зв'язок). Табл. 1 відображає приклад оцінювання типів допомоги.

Як видно з таблиці, що найбільший показник ефективності мають ресурси із високою тактичною значущістю, навіть якщо їхня логістика складніша (приклад – медичні комплекти, електроніка).

Таблиця 1.

Оцінювання ефективності зовнішньої допомоги для різних категорій ресурсів

Категорія обладнання	М	Т	Р	С	Інтегральний показник Е
Засоби медичного реагування	0,92	0,88	0,96	0,81	0,90
Тактична електроніка (дрони, засоби зв'язку)	0,87	0,71	0,93	0,76	0,82
Транспортні засоби	0,75	0,66	0,82	0,69	0,73
Екіпірування загального призначення	0,74	0,92	0,61	0,85	0,78

Як видно з таблиці, що найбільший показник ефективності мають ресурси із високою тактичною значущістю, навіть якщо їхня логістика складніша (приклад – медичні комплекти, електроніка).

Висновки та перспективи. Розроблена модель дозволяє формально оцінювати ефективність зовнішньої допомоги, враховуючи тактичні потреби, оперативну доцільність та економічні фактори. Інтегральні метрики дають змогу об'єктивізувати розподіл ресурсів, підвищити реальну користь міжнародної підтримки та знизити ризик нецільового використання. Перспективними напрямками розвитку є автоматизація розрахунків на основі телеметрії ресурсів, інтеграція з логістичними системами постачання та застосування нечітких моделей (fuzzy logic) для оцінювання критичних умов у реальному часі.

Список використаних джерел

1. Dijkstra G., Martínez-Zarzoso I. Aid effectiveness: Improvements, challenges and research opportunities. *Journal of International Development*. 2020. Vol. 32(7). P. 1041–1066.
2. Petkoski D., Jarvis M. Public–private collaboration for humanitarian supply chains. *Journal of Humanitarian Logistics and Supply Chain Management*. 2021. Vol. 11(3). P. 341–360.
3. Elshabrawy T. et al. Data-driven prioritization of emergency resources in critical operations. *Safety Science*. 2023. Vol. 163. 106106. DOI: 10.1016/j.ssci.2023.106106.

Дерев'янка Євген Миколайович

аспірант

Інститут програмних систем Національної академії наук України

evg.derevianko@gmail.com

МЕТОДИ БАГАТОКРИТЕРІАЛЬНОГО АНАЛІЗУ РИЗИКІВ В УМОВАХ ВИСОКОЇ ДИНАМІЧНОСТІ ІНФОРМАЦІЙНО- АНАЛІТИЧНОГО СЕРЕДОВИЩА

Постановка задачі. Сучасні інформаційно-аналітичні системи (SOC, SIEM/SOAR-платформи, системи підтримки ухвалення рішень у кібербезпеці, розвідці, кризовому менеджменті) працюють в умовах високої динамічності середовища: показники завантаження мережі, інтенсивність інцидентів, якість джерел даних, надійність каналів і поведінка користувачів змінюються в режимі близькому до реального часу. Класичні підходи до аналізу ризиків, засновані на статичних матрицях «імовірність × вплив» або експертному ранжуванні, виявляються недостатніми: вони погано враховують багатовимірність критеріїв (технічних, організаційних, контекстуальних) і не встигають адаптуватися до швидких змін. Актуальною є побудова методів багатокритеріального аналізу ризиків (MCDM), здатних інтегрувати гетерогенні показники, працювати з невизначеністю (фаззі-оцінки, неповні дані) та підтримувати оперативне оновлення рішень у динамічному інформаційно-аналітичному середовищі.

Мета дослідження. Метою дослідження є розроблення методології багатокритеріального аналізу ризиків в умовах високої динамічності інформаційно-аналітичного середовища, яка дозволяє формалізувати поєднання технічних, інформаційних, організаційних та контекстних критеріїв, підтримує адаптивне оновлення ваг та показників, а також забезпечує прозору інтерпретацію пріоритетів ризиків для подальшого вибору контрзаходів.

Результати дослідження. Запропонована методологія ґрунтується на представленні задачі оцінювання ризиків як багатокритеріальної задачі прийняття рішень, де кожен об'єкт аналізу (сервіс, вузол мережі, канал, політика доступу, аналітичний сценарій) описується вектором узгоджених показників. Для обробки невизначеності й лінгвістичних експертних оцінок передбачено можливість використання нечітких шкал та агрегування на основі OWA-операторів і їх нечітких варіантів, що добре зарекомендували себе у задачах управління ризиками інформаційної безпеки.

У модель вводяться чотири базові групи критеріїв, які покривають технічні, інформаційні, організаційні та контекстуальні аспекти ризику. Їхня структуризація подана у табл. 1.

Таблиця узагальнює ключові групи критеріїв, підкреслюючи, що багатокритеріальний аналіз ризиків має виходити за межі традиційних метрік «імовірність–збиток» і враховувати якість даних, процесну зрілість та контекстну мінливість.

Таблиця 1.

Групи критеріїв ризику та їх роль у багатокритеріальному аналізі

Група критеріїв	Приклади показників	Роль у прийнятті рішень
Технічні (Т)	затримка відповіді сервісів; відсоток недоступності; кількість відмов обладнання	Визначають технічну вразливість та SLA-ризик
Інформаційні (І)	повнота телеметрії; достовірність логів; частка пропущених подій	Характеризують ризики, пов'язані з якістю даних
Організаційні (О)	зрілість процесів (ISO 27005/27001); своєчасність реакції; компетентність персоналу	Відображають здатність організації керувати ризиками
Контекстуально-динамічні (С)	інтенсивність інцидентів у часі; частота зміни конфігурацій; рівень загроз за зовнішніми індикаторами	Описують динаміку середовища та зміну профілю ризиків

Така структуризація дозволяє будувати вектор стану ризику для кожного об'єкта та надалі застосовувати алгоритми MCDM (АНР, TOPSIS, нечіткі OWA-оператори тощо) для формування узагальненого індексу ризику або ранжованих списків критичних елементів.

На рис. 1 подано узагальнену схему багатокритеріального аналізу ризиків у високодинамічному інформаційно-аналітичному середовищі.

Схема підкреслює, що потоки подій можуть надходити з гетерогенних джерел (мережеві сенсори, SIEM, бізнес-додатки), і їх необхідно привести до узгоджених показників у розрізі груп Т, І, О, С. Після схеми доцільно акцентувати увагу, що ядро MCDM виступає «процесором ризиків», який об'єднує числові, лінгвістичні та нечіткі оцінки в інтегральні індекси та дозволяє будувати сценарії «якщо–то» для вибору портфелю контрзаходів (організаційних, технічних, процесних).

У ході апробації методології на моделі intranet-середовища з варіативними профілями загроз були сформовані декілька сценаріїв (статичне середовище, хвилеподібна динаміка інцидентів, різкі сплески атак). Для кожного сценарію виконувалася імітація оновлення вагових коефіцієнтів та показників Т, І, О, С із кроком дискретизації, що дозволило порівняти результати класичної статичної матриці ризиків та запропонованого багатокритеріального підходу. Показано, що мультикритеріальна модель краще диференціює об'єкти з близькими значеннями традиційних метрик, але різним контекстом (наприклад, однаковий рівень загроз, але різна якість телеметрії чи зрілість процесів), а також забезпечує більш стабільну пріоритизацію при зміні зовнішніх умов.

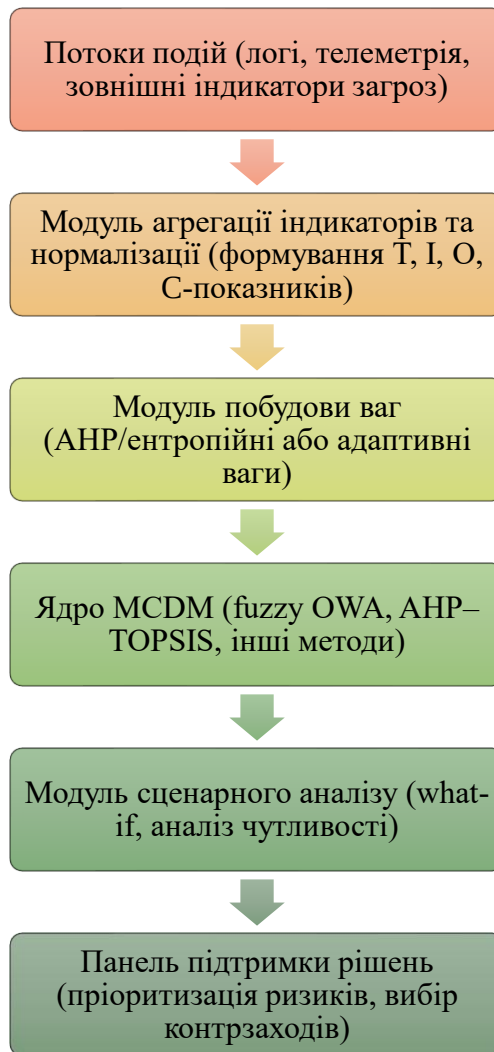


Рис. 1. Узагальнена схема багатокритеріального аналізу ризиків у динамічному середовищі

Подібні підходи до інтеграції MCDM і нечіткого моделювання раніше демонстрували ефективність у задачах вибору контрзаходів та управління залишковими ризиками, що підтверджується результатами робіт з використанням OWA-операторів і FMEA/нечітких моделей.

Висновки та перспективи Запропоновано методологію багатокритеріального аналізу ризиків, орієнтовану на використання в умовах високої динамічності інформаційно-аналітичного середовища. Її ключовою особливістю є інтеграція технічних, інформаційних, організаційних та контекстуально-динамічних критеріїв у єдину модель, яка підтримує адаптивне оновлення ваг і показників, а також застосування методів MCDM (у тому числі нечітких OWA-операторів) для формування узагальнених індексів ризику та пріоритизації контрзаходів. Такий підхід забезпечує більш чутливу диференціацію ризиків, ніж традиційні статичні матриці, та краще відповідає реальним умовам експлуатації систем, де профіль загроз і якість даних постійно змінюються.

Перспективи подальших досліджень пов'язані з розширенням моделі до багаторівневих архітектур (інтеграція ризиків на рівні сервісів, підрозділів та організації), залученням машинного навчання для автоматичного налаштування ваг та функцій належності, а також з розробленням рекомендацій щодо стандартизації мультикритеріальних підходів в існуючих фреймворках управління ризиками інформаційної безпеки.

Список використаних джерел

1. Imamverdiev Ya. N., Derakshande S. Fuzzy OWA Model for Information Security Risk Management. *Automatic Control and Computer Sciences*. – 2011. – Vol. 45, No. 1. – P. 20–28.
2. Gusmão A. P. H. et al. A multidimensional approach to information security risk management using FMEA and fuzzy theory. *International Journal of Information Management*. – 2014. – Vol. 34, Iss. 6. – P. 974–984.
3. Karunathilake H., Yoshikawa S., Jayarathna L. Decision Making in Risk Management: A Multi-Criteria Decision-Making Approach. *International Journal of Environmental Research and Public Health*. – 2020. – Vol. 17, No. 17. – Article 6277.

Іванов Артем Олександрович
студент 4 курсу, групи 46Бд-Комп
Житомирського державного університету імені Івана Франка
(063)434-81-33

Art_Iv3@ukr.net

Науковий керівник

Кривонос Олександр Миколайович
доцент кафедри комп'ютерних наук та інформаційних технологій
Житомирського державного університету імені Івана Франка
(098)742-02-28

krypton@zu.edu.ua

ПОРІВНЯННЯ АЛГОРИТМІВ СОРТУВАННЯ

Постановка задачі. Об'єми цифрових даних стрімко зростають, як і час на їх обробку. І покращення алгоритмів їх обробки дозволяє заощаджувати на «залізі», покращуючи ефективність. Одним з, можливо, найважливіших алгоритмів обробки даних є сортування. Цих алгоритмів існує безліч, і всі вони відрізняються своїми структурами даних, найгіршими випадками, використанням пам'яті тощо. Порівняння цих алгоритмів необхідне для розуміння того, який алгоритм краще використовувати в поставленій задачі.

Мета дослідження. Метою дослідження є аналіз і порівняння за часом виконання і використанням пам'яті відомих алгоритмів сортування: bubble sort, merge sort, quick sort, heap sort.

Результати дослідження. Масив даних називається відсортованим, якщо його елементи впорядковані за деякою властивістю. Це може бути не просто сортування чисел, а і сортування цілих структур даних. В залежності від поставленої задачі і обмежень, можуть використовуватись різні алгоритми сортування, наприклад: для виконання сортування на сервері, до якого звертаються тисячі користувачів, пріоритетом є швидкість; а при сортуванні даних на мікропроцесорі з обмеженою оперативною пам'яттю, пріоритетом може бути зменшення використання ресурсів ОЗП. Далі будуть розглянуті і порівняні самі основні алгоритми сортування.

Бульбашкове сортування. Самий примітивний і в той же час простий алгоритм сортування, в основі якого лежить «підняття» максимального елемента в кінець невідсортованої частини масиву. Оскільки всі операції відбуваються безпосередньо на вихідному масиві, використання додаткової пам'яті цим алгоритмом константне $O(n) = 1$. Найкращий випадок у разі бульбашкового сортування є заздалегідь відсортований масив, тому найкращий час буде $\Omega(n) = n$, оскільки алгоритму необхідно мінімум один раз пройти по масиву. В найгіршому випадку, масив буде відсортований в оберненому порядку, через що кожен елемент буде переміщуватись окремо, і в такому випадку час виконання буде

$$O(n) = (n - 1) + (n - 2) + \dots + 1 = \frac{(n-1)(n-2)}{2} = n^2.$$

Сортування злиттям. В основі цього алгоритму стоїть принцип «розділяй та володарюй», коли ми рекурсивно розділяємо масив на дві рівні частини, і розв'язуємо цю саму задачу для них, потім поєднуючи їх за лінійний час. Для обрахунку використання пам'яті цим алгоритмом, помітимо, що під час рекурсії виділяється масив довжиною n для збереження проміжних результатів; і при використанні рекурсивного підходу додаткова пам'ять виділяється на стек викликів, і оскільки при кожному виклику ми зменшуємо розмір кожного підмасиву вдвічі, розмір стеку буде рівним $\log n$. Комбінуючи використання пам'яті, отримуємо $O(n) = \Omega(n) = n + \log n = n$. Для обрахунку використання часу використовується теорема Акра-Баззі про рекурентні співвідношення типу «розділяй і володарюй». В результаті, час виконання алгоритму в найгіршому випадку та найкращому випадках будуть рівними $\Omega(n) = O(n) = n \log n$. Також варто зазначити, що на відміну від наступного алгоритму, дане сортування є стабільним, тобто таким, яке зберігає порядок однакових елементів.

Швидке сортування. Даний алгоритм також відноситься до сімейства «розділяй і володарюй», але використовує дещо інший підхід. На кожному етапі сортування, ми вибираємо деяку опорну точку, і розміщуємо всі інші елементи, які більші з нього, в один бік, а які більші – в інший. В кінці всі підмасиви з'єднуються. Ефективність алгоритму залежить від вибору опорних точок. Хоча в рекурсивному випадку алгоритм не створює додаткові масиви для збереження проміжних даних, в найгіршому сценарії – при незбалансованому виборі опорних точок – буде надмірно заповнюватись стек викликів, що призведе до використання пам'яті $O(n) = n$. В найкращому випадку – при збалансованому виборі опорних точок – масив розділятиметься навпіл, тому використання пам'яті буде $\Omega(n) = \log n$.

При збалансованому виборі опорних точок, ми можемо розрахувати час виконання алгоритму швидкого сортування як для найкращого випадку з використанням теореми Акра-Баззі, що дасть $\Omega(n) = n \log n$. При незбалансованому виборі, ми вже не можемо використати цей алгоритм через відсутність чітких підзадач, на які розділятиметься попередня. В найгіршому випадку ми можемо грубо розрахувати час виконання алгоритму як $O(n) = O(n - 1) + cn$, де cn – вартість поділу масиву. Тоді асимптотика для найгіршого випадку дасть нам $O(n) = \frac{n(n-1)}{2} = n^2$.

Сортування кучами. Цей алгоритм є вдосконаленим варіантом сортування вибором, який оригінально має квадратну часову асимптотику. Алгоритм полягає в інтерпретації масиву як повного збалансованого бінарного дерева. Далі воно перетворюється в мінімальну або максимальну кучу в залежності від порядку сортування. В мінімальній кучі значення кожного вузла менше за його дочірніх, і відповідно більше для максимальної кучі. Всі обрахунки відбуваються на вихідному масиві, тому використання пам'яті константне $O(n) = 1$. Алгоритм не має найгіршого сценарію роботи, і завжди виконується за один час. Побудова min/max кучі використовує час $O(n)$ і для відновлення властивостей кучі до

кожного елементу виконується функція за $O(\log n)$. З цього випливає загальна асимптотика алгоритму $O(n) = n \log n$.

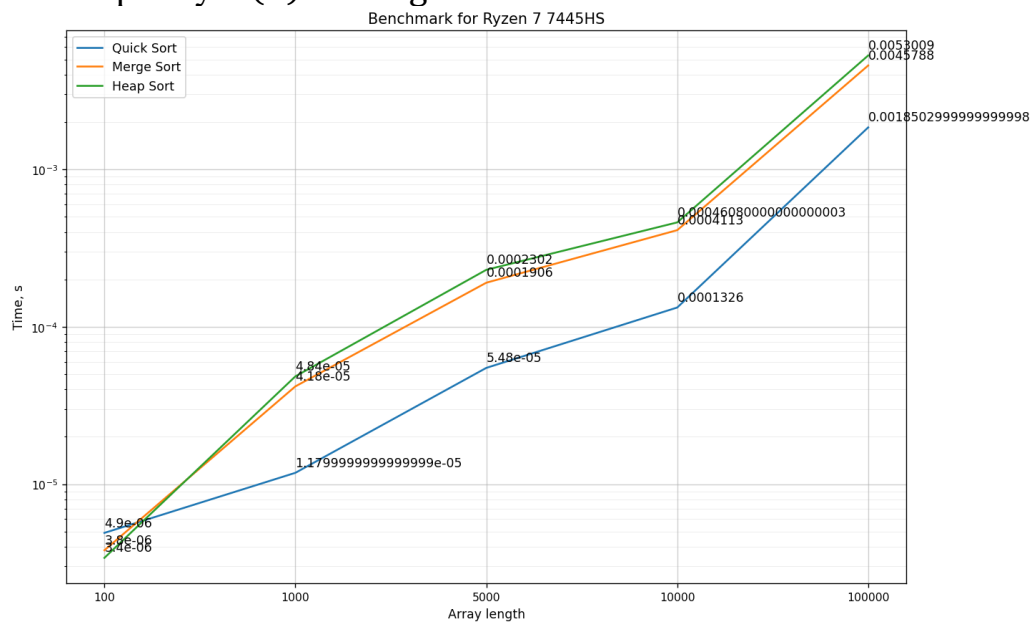


Рис. 1 Тест швидкості різних алгоритмів асимптотики $n \log n$ з логарифмічною шкалою часу

Висновки та перспективи. В результаті порівняння швидкості виконання алгоритмів сортування і їхнього використання пам'яті, ми склали наступну таблицю

Таблиця 1.

Порівняння алгоритмів сортування за асимптотичною швидкістю та використанням пам'яті

Алгоритм	Час			Пам'ять	
	$O(n)$	$\theta(n)$	$\Omega(n)$	$O(n)$	$\Omega(n)$
Bubble Sort	n^2	n^2	n	1	
Merge Sort	$n \log n$			n	
Quick Sort	n^2	$n \log n$	$n \log n$	n	$\log n$
Heap Sort	$n \log n$			1	

Як результат маємо, що найкращими алгоритмами сортування з точки зору швидкодії є сортування злиттям і кучами, а з точки зору використання пам'яті – сортування бульбашкою і кучами. Проте це не значить, що сортування кучами є самим ефективним, адже тести швидкості (див. Рис. 1) показують, що сортування кучами і злиттям значно програють по швидкості швидкому сортуванню. Це можна пояснити значними відмінностями в константних факторах, які виникають при розрахунку асимптотик, і які мають значний вплив при порівнянні алгоритмів однакових асимптотик. З цього слідує, що алгоритми сортування слід обирати адаптивно в залежності від поставленої задачі. Наприклад, в бібліотеці numpy це реалізовано у вигляді типу сортування stable, який адаптивно обирає tim sort або radix sort в залежності від даних.

Список використаних джерел

1. **Time and Space Complexity Analysis of Bubble Sort** [Електронний ресурс]. – Режим доступу: <https://www.geeksforgeeks.org/dsa/time-and-space-complexity-analysis-of-bubble-sort/> (дата звернення: 27.11.2025)
2. **Time Complexity of Merge Sort: A Detailed Analysis** [Електронний ресурс]. – Режим доступу: <https://www.codecademy.com/article/time-complexity-of-merge-sort> (дата звернення: 27.11.2025)
3. **Akra-Bazzi Method of Recurrence Time Complexity** [Електронний ресурс]. – Режим доступу: <https://medium.com/@compuxela/akra-bazzi-method-of-recurrence-time-complexity-46a6a8814b47> (дата звернення: 27.11.2025)
4. **Quick Sort** [Електронний ресурс]. – Режим доступу: <https://www.geeksforgeeks.org/dsa/quick-sort-algorithm/> (дата звернення: 28.11.2025)
5. **Time and Space Complexity Analysis of Quick Sort** [Електронний ресурс]. – Режим доступу: <https://www.geeksforgeeks.org/dsa/time-and-space-complexity-analysis-of-quick-sort/> (дата звернення: 28.11.2025)
6. OLADIPUPO, E., TAIWO, A. O., CHRISTIANAH, A. Comparative study of two divide and conquer sorting algorithms: quicksort and mergesort // *Procedia Computer Science*. – 2020. – Vol. 171. – P. 2532–2540. – DOI: 10.1016/j.procs.2020.04.274
7. **Heap Sort** [Електронний ресурс]. – Режим доступу: <https://www.geeksforgeeks.org/dsa/heap-sort/> (дата звернення: 28.11.2025)

Івасюк Василь Васильович
магістрант 1 курсу, групи ІПЗм-1
Карпатський національний університет імені Василя Стефаника
+380 (342) 59-60-58
vasyl.ivasiuk.21@pnu.edu.ua

ОГЛЯД СУЧАСНОГО СТАНУ ДОСЛІДЖЕННЯ ЗАЛЕЖНОСТІ ПРОГРАМНИХ ПАКЕТІВ

Постановка задачі. Одним з показником надійності коду є якість залежностей, які прямо або опосередковано успадковуються певними пакетами. Якщо їхня кількість є надмірною, або самі залежності видають невластиву поведінку, то це прямо впливає на функціональність продукту. Ще одним важливим показником є видимість, оскільки не завжди дослідники замислюються, як сильно їм допомагають ті чи інші пакети.

Мета дослідження. Метою дослідження є огляд публікацій, які розглядають питання оцінки залежності у різних екосистемах, які були опубліковані протягом останніх 5 років; визначення основних результатів робіт.

Результати дослідження. Автори роботи [1] досліджували питання ступені залежності. Вони замітили, що залежності пакетів **P** у мові програмуванні **R** можна представити в якості орієнтованого графу, а самі пакети розподілити за категоріями:

- сильні батьківські пакети - обов'язкові для установки (Depends, Imports, LinkingTo);
- слабкі батьківські пакети - опціональні для установки (Suggests, Enhances);
- сильнозалежні пакети - такі пакети, кількість яких отримана шляхом рекурсивного пошуку їх сильних батьківських пакетів;
- всезалежні пакети - такі пакети, кількість яких отримана шляхом рекурсивного пошуку сильних та слабких батьківських пакетів;
- дочірні пакети - такі пакети, чії батьки включають **P**.

Автори ввели метрику "важкості залежності", яка визначає, скільки додаткових залежностей вводить кожний батьківський пакет. Вони склали формули для визначення залежності по кожній з категорій. Потім на цій основі був написаний пакет *pkgndep*, який був використаний для створення індивідуальної теплової карти. Стаття [2] доповнює цю тему, додатково досліджуючи поширення важкості залежності від висхідних до низхідних пакетів. Першими можна вважати сильнозалежні пакети, а другими - такі пакети, які шукають дочірні пакети шляхом рекурсивного пошуку. Пакет *pkgndep* був оновлений з врахуванням цих змін, а в якості наборів даних були використані пакети з репозиторій *CRAN* та *Bioconductor*. Визначаючи патерни важкості залежностей, автори виявили, що лише невелика частина пакетів має важкі батьківські пакети в екосистемі. При цьому, сильна залежність зазвичай формується на самому початку. Так само, кількість пакетів, які одночасно успадковують залежності від двох батьків, також невисока. Якщо це й

відбувається, то вони здебільшого мають відношення батько-дитина. Також було визначено, що середня кількість унікальних залежностей спадає водночас зі збільшенням дочірніх пакетів. Зазвичай важкість залежності передається на великі відстані. Накопичення важкості відбувається за рахунок декількох важких батьків, або коли група пакетів успадковують один важкий пакет. Для зменшення важкості автори радять напряду імплементувати необхідні функції з важкого пакету; використовувати функціонально схожі, але легкі пакети; зробити батьківські пакети, які надають лише опціональні функції, необов'язковими для установки. Хоча ступінь залежності є сама по собі важливим фактором, не менш важливим є розумінням, якими вони є і який функціонал виконують. Дослідженню опосередкованих залежностей в біомедичних програмах приділена робота [3]. Для розгляду цього питання береться ті пакети, які мають мало згадок у наукових роботах, однак які володіють високим рівнем центральності Каца (Katz centrality). Такі пакети були прозвані *Nebraska*. Було підготовлено три набори даних з репозиторій *PyPI* (Python), *CRAN* та *Bioconductor* (R). Візуалізація мереж залежностей показала, що більшість пакетів відповідають типу *Nebraska*; автори також звернули увагу на відсутність циклів у біомедичних програмах.

Висновки та перспективи. Пошук рішень, які стосуються питання залежності пакетів є нагальним серед дослідників. Одне з рішень стосується важкості залежності, яка показує, наскільки ефективно задіються імпортовані пакети і як вони взаємодіють у мережі. Важливим для ефективності є необхідність залучати лише ті функції, які реально застосовуються в проєкті, а також забезпечують його надійність. Ще однією точкою дослідження є огляд пакетів з малою видимістю та високою центральністю, які несуть велику користь для проведення наукових досліджень. Аналіз досліджень підтверджує потребу приділення більшої уваги на питання залежності програмних пакетів [4].

Список використаних джерел

1. Z. Gu and D. Hübschmann, "Pkgndep: a tool for analyzing dependency heaviness of R packages", *Bioinformatics*, vol. 38, no. 17, pp. 4248–4251, Sep. 2022, doi: 10.1093/bioinformatics/btac449
2. Z. Gu, "On the dependency heaviness of CRAN/Bioconductor ecosystem", *J. Syst. Softw.*, p. 111610, Jan. 2023, doi: 10.1016/j.jss.2023.111610
3. E. M. Brown *et al.*, "Biomedical Open Source Software: Crucial Packages and Hidden Heroes", Nov. 2025. doi: 10.1119/1.4767505
4. M. Kuz *et al.*, "Methods for evaluating software accessibility," *Radio Electronics, Computer Science, Control*, no. 3, pp. 163-172, Sept. 22, 2025, doi: 10.15588/1607-3274-2025-3-15

Ісмагілов Артур Ільясович
аспірант

Інститут програмних систем Національної академії наук України
ismagilov@ukr.net

МЕТОД КЛАСТЕРНОЇ ІДЕНТИФІКАЦІЇ ВИСОКОРИЗИКОВИХ ПОДІЙ ДЛЯ ПРОГНОЗУВАННЯ ПОЯВИ ЗАГРОЗ НУЛЬОВОГО ДНЯ

Постановка задачі. У сучасних гібридних інфраструктурах (SIEM/SOC, хмарні сервіси, промислові мережі) обсяг подій безпеки зростає на порядки, тоді як частка справді критичних інцидентів залишається малою, але саме вони пов'язані з появою загроз нульового дня. Класичні сигнатурні та супервізовані підходи до виявлення атак покладаються на наперед відомі шаблони й не забезпечують належної чутливості до нових, ще не описаних сценаріїв. Актуальною стає задача виділення невеликої множини високоризикових подій із масиву звичайних операційних логів, їх кластерної ідентифікації та використання отриманої структури для прогнозування появи zero-day загроз на рівні сервісів та сегментів мережі.

Мета дослідження. Розробити метод кластерної ідентифікації високоризикових подій, який на основі багатовимірних ознак та безнаглядного навчання формує кластери критичної активності й забезпечує підвищення точності й випереджального горизонту прогнозу загроз нульового дня у порівнянні з базовими аномалійними підходами.

Результати дослідження. Запропонований підхід розглядає потоки подій безпеки (мережеві флоу, системні логи, записи SIEM) як багатовимірний простір ознак, у якому high-risk події утворюють слабо представлені, але структуровані області. На першому етапі здійснюється агрегація та нормалізація подій (часові вікна, контекст сесії, атрибути суб'єкта та ресурсу), після чого формується вектор ознак, який включає статистичні (частоти звернень, обсяг трафіку, розподіл портів), поведінкові (аномальні послідовності дій) та контекстні характеристики (критичність вузла, права доступу).

Структурну логіку запропонованого методу ілюструє узагальнена схема процесу кластерної ідентифікації високоризикових подій і прогнозування zero-day загроз (рис. 1).

Схема на рисунку 1 відображає «замкнений контур» роботи системи: починаючи з багатоджерельного збору подій, метод послідовно зменшує розмірність простору ознак, виділяє структуру у вигляді кластерів, ідентифікує високоризикові області та перетворює їх часову активність на прогностичні сигнали для систем керування інцидентами. Важливим аспектом є можливість онлайн-оновлення параметрів кластеризації та адаптації порогів високого ризику на основі зворотного зв'язку від аналітиків SOC, що дозволяє підтримувати релевантність моделі в умовах змінного профілю атак.

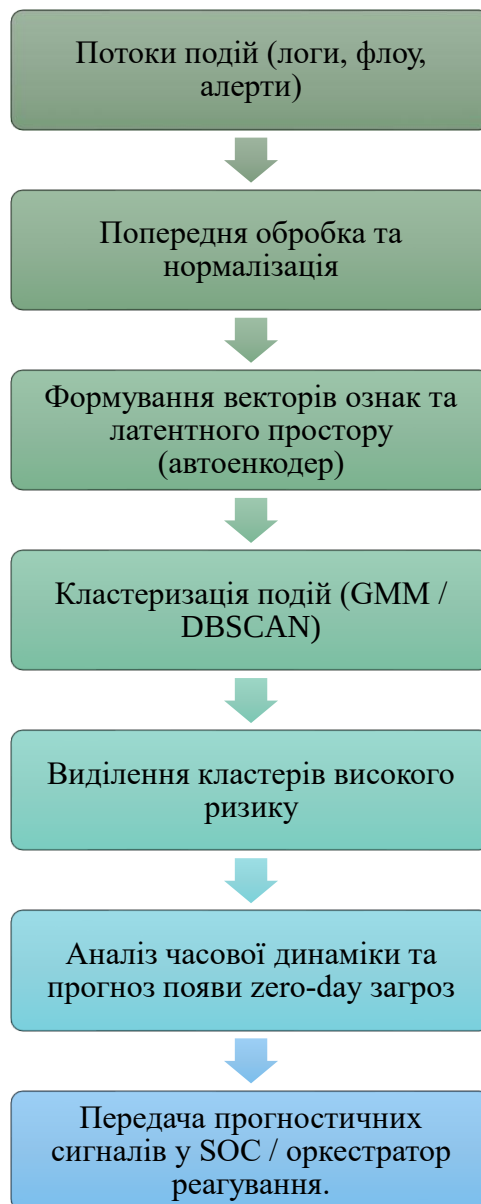


Рис. 1. Концептуальна схема методу кластерної ідентифікації високоризикових подій

Для боротьби з високою розмірністю та шумом спочатку виконується побудова компактного латентного простору за допомогою автоенкодера; саме в цьому просторі застосовуються кластеризаційні алгоритми (k-means, DBSCAN, Gaussian Mixture). Високоризикові події ідентифікуються як кластери з підвищеною щільністю аномальних точок, високою часткою інцидентів, що завершилися підтвердженими атаками, та статистично відмінними часовими профілями. На основі часової динаміки цих кластерів будується проста прогностична модель (наприклад, на основі експоненційного згладжування або GRU), яка оцінює ймовірність появи zero-day загроз у найближчому часовому вікні для конкретних сервісів.

Для оцінювання ефективності методу було використано журнали подій з гібридного середовища (мережеві флоу, системні логи та SIEM-алерти), у яких експертами були позначені інциденти, асоційовані з новими або рідкісними

типами атак. Порівняння проводилося між трьома конфігураціями кластеризації: базовим k-means, щільнісним DBSCAN і модельно-орієнтованим Gaussian Mixture Model (GMM) (табл. 1). Як метрики якості застосовувалися скоригований коефіцієнт Ранда (ARI) для відображення відповідності кластерів експертним міткам, F1-міра для класу «високий ризик», а також середній випереджальний горизонт прогнозу (lead time), який показує, за скільки хвилин до ескалації вдалося ідентифікувати високоризиковий кластер.

Таблиця 1.

Порівняння кластерних підходів до ідентифікації високоризикових подій

Модель кластеризації	ARI	F1 (високий ризик)	Середній випереджальний горизонт, хв
K-means (k = 8)	0,41	0,68	7,5
DBSCAN (ε адаптивний)	0,57	0,79	11,2
Gaussian Mixture (8 компонент)	0,63	0,84	13,6

Таблиця 1 узагальнює результати експериментальної оцінки трьох кластеризаційних підходів. Базовий k-means продемонстрував обмежену здатність відокремлювати високоризикові кластери в умовах складної геометрії даних, що проявилось в низькому ARI та відносно малому випереджальному горизонті. DBSCAN завдяки щільнісній природі краще виділяє компактні аномальні області, але виявив чутливість до підбору параметра ε. Найкращі результати показала GMM-модель, яка поєднує можливість описувати перекривні кластери з ймовірнісною інтерпретацією, що забезпечило зростання F1-міри для високоризикового класу до 0,84 та збільшення середнього випереджального горизонту до понад 13 хвилин, що критично важливо для превентивного реагування SOC.

Висновки та перспективи. Запропонований метод кластерної ідентифікації високоризикових подій демонструє, що навіть за відсутності повних сигнатурних описів атак можливо виділити стійкі структурні патерни, пов'язані з появою загроз нульового дня. Експериментальні результати показують, що використання поєднання латентного простору ознак та ймовірнісної кластеризації (GMM) забезпечує приріст F1-міри для високоризикового класу на 10–15 % у порівнянні з базовими підходами та дозволяє збільшити випереджальний горизонт прогнозу до десятків хвилин. Це створює додаткове «вікно часу» для проактивного реагування SOC, зокрема для тимчасового обмеження доступу, переналаштування політик та запуску поглибленого аналізу інцидентів.

Перспективи подальших досліджень пов'язані з інтеграцією графових представлень (user–resource graphs, service dependency graphs) у процес кластеризації, розробленням онлайн-механізмів інкрементального оновлення кластерів у режимі реального часу, а також поєднанням запропонованого підходу з ХАІ-методами для пояснення характеристик високоризикових кластерів аналітикам безпеки. Окремим напрямом є валідація методу на доменно-специфічних датасетах (автомобільні CAN-мережі, ІоМТ, промисловий OT-

сегмент), де zero-day загрози мають свою специфіку, але підпорядковуються подібній кластерній структурі у просторі подій.

Список використаних джерел

1. García-Teodoro P., Díaz-Verdejo J., Maciá-Fernández G., Vázquez E. Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*. 2009. Vol. 28, No. 1–2. P. 18–28. DOI: 10.1016/j.cose.2008.08.003.
2. Buczak A. L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*. 2016. Vol. 18, No. 2. P. 1153–1176. DOI: 10.1109/COMST.2015.2494502.
3. Khandelwal S., Shanker S. Real-Time Zero-Day Intrusion Detection System for Automotive Controller Area Network on FPGAs. *arXiv preprint arXiv:2401.10724*, 2024.

Корнієнко Олексій Олексійович

аспірант

Інститут програмних систем Національної академії наук України

oleksiikorniienko@gmail.com

ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ РОЗРОБКИ ОБЛІКОВИХ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМ НА ОСНОВІ КЕРУВАННЯ БІЗНЕС-ВИМОГАМИ ТА ОПТИМІЗАЦІЇ CASE-ЗАСОБІВ

Постановка задачі. Сучасні облікові інформаційно-аналітичні системи (ОІАС) виконують критичні функції для підприємств, включаючи облік операцій, контроль ресурсів, аналітику та підтримку управлінських рішень. Проте зростання складності бізнес-процесів, потреба у швидкій адаптації до змін регуляторних вимог і високі очікування користувачів щодо якості ПЗ створюють значне навантаження на процеси розробки. Основними проблемами стають:

- нечіткі, надмірні або суперечливі бізнес-вимоги;
- фрагментованість процесів моделювання;
- низький рівень інтеграції CASE-засобів;
- надмірні витрати часу на валідацію і тестування моделей.

Отже, виникає необхідність пошуку методів підвищення продуктивності розробки ОІАС шляхом оптимізації управління бізнес-вимогами та застосування ефективних CASE-інструментів.

Мета дослідження. Метою дослідження є розроблення підходу, що забезпечує підвищення продуктивності створення та еволюції облікових інформаційно-аналітичних систем за рахунок:

- систематизації та формалізації бізнес-вимог;
- оптимізації процесів моделювання;
- удосконалення використання CASE-засобів;
- зменшення тривалості життєвого циклу розробки без зниження якості.

Результати дослідження. Запропоновано інтегровану методику, що поєднує підхід до керування вимогами (Requirements Management) з оптимізованою архітектурою застосування CASE-засобів. Основні положення методики включають:

1. **Єдиний репозиторій бізнес-вимог**, що дозволяє усунути дублювання і підвищити прозорість залежностей між функціями облікової системи.
2. **Мультирівневу декомпозицію вимог** (business → functional → logical → technical), що скорочує час уточнень та змін.
3. **Уніфікований процес моделювання**, який забезпечує узгодженість діаграм BPMN, UML і ERD.
4. **Оцінку якості та повноти моделі** на основі метрик (суперечливість, покриття вимог, складність).
5. **Оптимізовану схему інтеграції CASE-засобів**, яка мінімізує ручну працю під час трансформації моделей.

Подамо узагальнену схему (рис. 1), що відображає взаємозв'язок керування бізнес-вимогами та оптимізованого використання CASE-засобів у процесі розробки ОІАС.

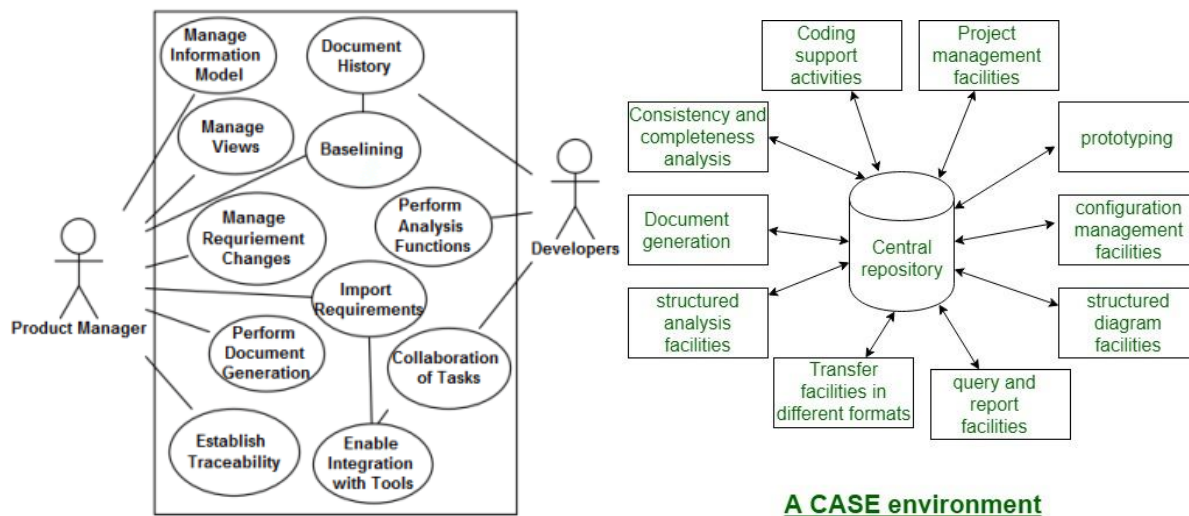


Рис. 1. Інтегрована схема керування вимогами та CASE-підтримки

Подана схема демонструє послідовність етапів – від збору та структуризації бізнес-вимог до автоматизованого моделювання та генерації артефактів. CASE-засоби використовуються не фрагментарно, а як єдина екосистема, що здійснює трансформацію вимог у моделі, бази даних та програмні шаблони. Такий підхід скорочує витрати часу на документацію, уніфікує структуру моделей та забезпечує підвищення узгодженості між командами.

Запропонована методика дозволяє:

- зменшити тривалість циклу аналізу й проектування на 25–40%;
- скоротити кількість суперечливих або надмірних вимог;
- підвищити якість моделі за рахунок стандартизації та автоматизації;
- забезпечити адаптивність системи до змін у регулюваннях та бізнес-процесах.

Висновки та перспективи. Запропонований підхід демонструє, що підвищення продуктивності розробки ОІАС можливе при одночасному вдосконаленні процесів керування вимогами та оптимізації використання CASE-інструментів. Основними перевагами є прискорення проектування, покращення якості моделей та зменшення ризику помилок у пізніх етапах розробки.

Перспективи подальших досліджень включають:

- впровадження елементів штучного інтелекту для автоматичного аналізу вимог;
- розробку метрик продуктивності CASE-платформ;
- дослідження інтеграції запропонованої моделі з DevOps/DevSecOps-практиками.

Список використаних джерел

1. National Institute of Standards and Technology. (2022). NIST Special Publication 800-30: Guide for Conducting Risk Assessments.

2. European Union Agency for Cybersecurity. (2023). ENISA Threat Landscape 2023.
3. Cherdantseva, Y., Hilton, J. (2019). A Reference Model of Information Security Risk Management. *Information & Computer Security*, 27(3).
4. Sterbenz, J. P., Hutchison, D. (2020). Resilience and Survivability in Communication Networks. *IEEE Communications Surveys & Tutorials*, 22(1).
5. Gartner Research. (2023). Optimize Cybersecurity Spending Under Crisis Conditions.

Крепкій Ігор Тарасович
студент 4 курсу, групи ТЦР-44
Державний університет інформаційно-комунікаційних технологій
st7948315@stud.duikt.edu.ua
Науковий керівник: Ніщененко Дмитро Олександрович,
старший викладач кафедри Технологій цифрового розвитку
Державного університету інформаційно-комунікаційних технологій.

КЛІЄНТ-СЕРВЕРНА СИСТЕМА ПОТОКОВОЇ ПЕРЕДАЧІ АУДІО З МОБІЛЬНОГО ПРИСТРОЮ

Постановка задачі. Сучасні інформаційні технології трансформують підходи до комунікації, де все більшу роль відіграють засоби віддаленої роботи, стрімінгу та онлайн-конференцій. Якість звуку є критичним параметром для цих процесів. Професійне обладнання, таке як мікрофони, є коштовним, тоді як сучасні смартфони вже оснащені високоякісними мікрофонами, проте їх інтеграція з ПК часто ускладнена. Існуючі програмні рішення (WO Mic, DroidCam) мають низку суттєвих недоліків: вони є пропрієтарними, часто вимагають платних підписок для розблокування базових функцій та, що найважливіше, вимагають встановлення специфічних закритих драйверів, що створює ризики сумісності та безпеки. Актуальним завданням є розробка відкритої клієнт-серверної системи, яка дозволить використовувати смартфон як бездротовий мікрофон у локальній мережі Wi-Fi без необхідності розробки та інсталяції складних пропрієтарних драйверів, використовуючи натомість стандартні аудіо-інтерфейси операційної системи.

Мета дослідження. Метою роботи є розробка клієнт-серверної системи потокової передачі аудіо з мобільного пристрою на персональний комп'ютер у реальному часі на основі Android SDK та мови Java, що забезпечує мінімальну затримку (low latency) шляхом використання протоколів реального часу.

Результати дослідження. У ході дослідження було проведено аналіз методів передачі аудіоданих у комп'ютерних мережах. Встановлено, що для інтерактивних систем (Real-Time Communication) використання поширених HTTP-базованих протоколів, наприклад, HLS та DASH, є недоцільним у зв'язку з високою затримкою, що спричинена сегментацією та буферизацією [1,2]. Для забезпечення миттєвої передачі голосу оптимальним є використання транспортного протоколу UDP, який, на відміну від TCP, не вносить затримок на підтвердження доставки пакетів [3]. На основі аналізу спроектовано архітектуру програмного комплексу, що складається з двох модулів:

1. Мобільний клієнт (Android) виконує захоплення "сирого" аудіопотоку (PCM, 44.1 кГц, 16 біт) безпосередньо з апаратного мікрофона, міняючи етап кодування у стиснені формати MP3 або AAC для усунення затримок обробки, дані упаковуються в датаграми та передаються через Wi-Fi.

2. Серверна частина (Java Desktop) приймає UDP-потік, буферизує його для компенсації джитера мережі та маршрутизує звук у віртуальний аудіокабель

(VB-Audio Virtual Cable) та дозволяє системі розпізнавати телефон як стандартний мікрофон для будь-яких додатків (Zoom, Discord, OBS).

Діаграма моделі потоків даних наведена на Рисунку 1.

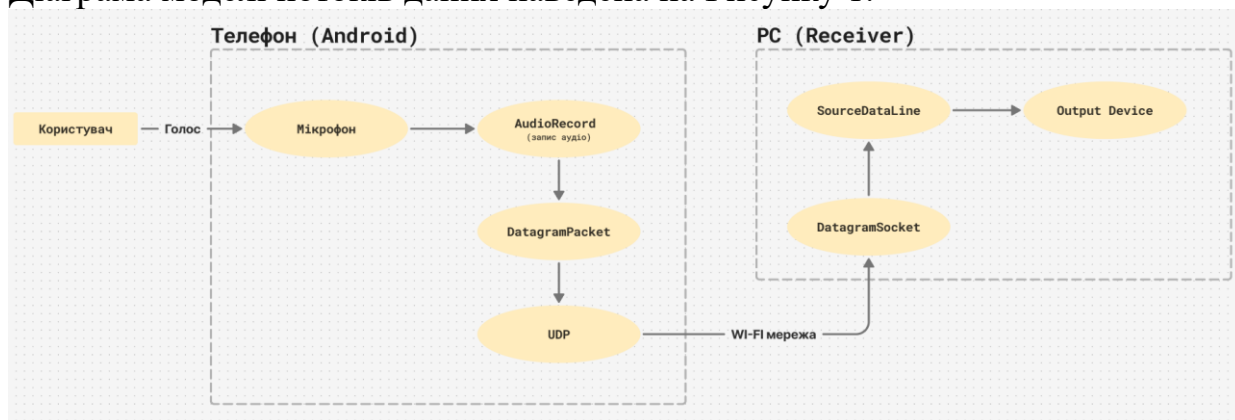


Рис. 1: Модель потоків даних у системі передачі аудіо.

Ключовим результатом проєктування є відмова від власного драйвера на користь інтеграції з існуючим стандартом VB-Cable, що призводить до значного спрощення архітектури та підвищення надійності системи. Використання формату PCM (Pulse Code Modulation) хоч і потребує ширшої смуги пропускання (~700 кбіт/с), проте в умовах сучасних локальних мереж це є прийнятним компромісом заради досягнення мінімальної затримки.

Висновки та перспективи. Досліджено особливості протоколів передачі медіаданих. Визначено, що для заміни фізичного мікрофона смартфоном критичним параметром є затримка (latency), що диктує вибір стека технологій UDP/PCM замість TCP/HTTP. Спроектовано клієнт-серверну систему, яка вирішує проблему залежності від пропрієтарних драйверів шляхом використання віртуальних аудіо-інтерфейсів та кросплатформної мови Java.

Список використаних джерел

1. AudioRecord API reference. Android Developers. URL: <https://developer.android.com/reference/android/media/AudioRecord> (дата звернення: 27.11.2025).
2. Java Sound Technology. Moved. URL: <https://docs.oracle.com/javase/8/docs/technotes/guides/sound/> (дата звернення: 27.11.2025).
3. Yakovyshen P., Tuzhanskyi S. Adaptive data transmission method in information channels of telemedicine systems. Optoelectronic Information-Energy Technologies. 2025. Iss. 49, no. 1, pp. 53–63.

Левченко Анастасія Вікторівна
студентка 4 курсу, групи ІПЗ-42
Київського національного університету імені Тараса Шевченка
nastiya.levchenko@gmail.com
Духновська Ксенія Костянтинівна
к. т. н., доцентка кафедри програмних систем і технологій
Київського національного університету імені Тараса Шевченка
kseniia.dukhnovska@knu.ua

ПРОЕКТУВАННЯ МІКРОСЕРВІСНОЇ БЕКЕНД-АРХІТЕКТУРИ CRM ІЗ МОБІЛЬНИМ КЛІЄНТОМ ANDROID

Постановка задачі. Мікросервісна архітектура є сучасним підходом до створення програмних систем, що передбачає поділ застосунку на низку незалежних сервісів, кожен з яких реалізує окрему бізнес-функцію. Такий підхід забезпечує автономність компонентів, спрощує масштабування, оновлення та підвищує надійність системи завдяки ізоляції збоїв. Це робить мікросервісну архітектуру особливо доцільною для CRM-систем, які включають модулі управління клієнтами, продажами, аналітикою та взаємодією з користувачами.

Перехід до мікросервісної моделі дозволяє розробляти й розгортати окремі модулі CRM незалежно, використовуючи оптимальні технології та мінімізуючи вплив оновлень на роботу системи. Водночас потреба у мобільному доступі зумовлює актуальність розробки Android-клієнта, що взаємодіє з бекендом через захищений і оптимізований інтерфейс. Таким чином, актуальним є формування методології створення CRM-системи з мікросервісною бекенд-архітектурою та Android-клієнтом, із урахуванням вимог до безпеки, інтеграції та вибору протоколів обміну даними.

Мета дослідження. Основна мета цього дослідження полягає у розробці та обґрунтуванні ефективної методології проектування та реалізації сучасної системи управління взаємовідносинами з клієнтами, яка базується на мікросервісній архітектурі для забезпечення масштабованості та гнучкості бекенду, а також інтегрує мобільний клієнт (Android) для надання оперативного доступу користувачам.

Результати дослідження. Проектована CRM-система складається з набору автономних мікросервісів, кожен з яких реалізує окремий домен або підсистему. Мікросервіси можуть розроблятися, масштабуватися та розгортатися незалежно, що підвищує гнучкість та ізоляцію збоїв. Кожен сервіс має власну базу даних відповідно до принципів Domain-Driven Design [1], що усуває залежність від єдиного сховища та дозволяє застосовувати оптимальні моделі даних для різних функціональних модулів.

Для взаємодії Android-клієнта з розподіленим бекендом використовується API-шлюз [2] як єдина точка доступу. Він маршрутизує запити до відповідних мікросервісів, виконує балансування навантаження, агрегацію даних, кешування та трансформацію протоколів. API-шлюз також забезпечує безпеку, виконуючи

перевірку автентифікації, контроль авторизації та фільтрацію запитів. Такий підхід приховує складність внутрішньої архітектури та спрощує роботу мобільного клієнта, який не взаємодіє безпосередньо з окремими сервісами.

У системі застосовано токен-орієнтовану модель доступу на основі OAuth 2.0 та OpenID Connect [3]. Після автентифікації Android-клієнт отримує JWT-токен, що додається до подальших запитів і перевіряється API-шлюзом та мікросервісами. Ролі й дозволи можуть бути закодовані в токені, що дозволяє сервісам самостійно приймати рішення щодо доступу без запиту до централізованої бази. Комунікації між сервісами та клієнтом шифруються, а поєднання шлюзу, OAuth2/OIDC та JWT відповідає рекомендованим практикам безпеки розподілених систем.

Мобільний клієнт спілкується з системою через API-шлюз, використовуючи REST/JSON як основний спосіб обміну даними. Це забезпечує сумісність з Android-бібліотеками та спрощує інтеграцію з бізнес-функціями CRM. Для оптимізації трафіку та зменшення кількості запитів може застосовуватися GraphQL [4], який дозволяє отримувати агреговані дані з кількох сервісів одним викликом. Для сценаріїв, що потребують мінімальних затримок (нотифікації, потокові оновлення), передбачено використання gRPC. Таким чином, система підтримує гібридний підхід: REST або GraphQL для клієнтської взаємодії та gRPC для високопродуктивних функцій.

Для обґрунтування вибору технологій обміну даними виконано порівняльний аналіз REST, GraphQL та gRPC [5-6] у контексті мікросервісної CRM-системи. Основними критеріями оцінювання були показники швидкодії (latency/throughput) та відмовостійкості.

REST є традиційним підходом, що використовує HTTP та JSON і вирізняється простотою, але має більші накладні витрати та вищу затримку при інтенсивному обміні даними. GraphQL дає змогу отримувати лише потрібні дані одним запитом, що зменшує кількість звернень і обсяг переданого трафіку, хоча створює додаткове навантаження на серверну обробку. gRPC, завдяки бінарній серіалізації та роботі поверх HTTP/2, забезпечує найменші затримки та найвищу ефективність, особливо у сценаріях із частими викликами, хоча потребує складнішої інфраструктури та планування ресурсів.

REST і GraphQL працюють поверх безстанового HTTP, тому збої окремих запитів не блокують інші та можуть оброблятися повторними зверненнями. GraphQL також здатний повертати часткові результати при недоступності окремих даних, що покращує користувацьке сприйняття стійкості системи, gRPC використовує довготривалі з'єднання та забезпечує низьку затримку, але потребує налаштування механізмів повтору та балансування для уникнення відмов при розривах зв'язку.

REST є найпростішим і найбільш сумісним варіантом для Android-клієнта, тоді як GraphQL дозволяє оптимізувати обсяг трафіку та кількість звернень у складних запитах. gRPC демонструє найкращу продуктивність і доцільний для внутрішньої взаємодії між мікросервісами та високонавантажених операцій. Оптимальною для CRM є комбінована схема: REST/GraphQL для мобільного

клієнта та gRPC для внутрішніх сервісних викликів, що забезпечує баланс гнучкості, швидкодії та надійності.

Висновки. Спроектowana CRM-система реалізує взаємодію Android-клієнта з бекендом через API-шлюз, який виконує перевірку JWT-токенів, маршрутизацію запитів та, за потреби, агрегування відповідей з кількох мікросервісів. Кожен сервіс має власне ізольоване сховище даних, що забезпечує незалежність, модульність і гнучке масштабування. Для внутрішньої комунікації застосовуються асинхронні повідомлення через брокер подій, а балансування навантаження та моніторинг продуктивності підтримують стабільність системи. Процес автентифікації забезпечується окремим Identity Provider, що видає токени для подальшої взаємодії клієнта з бекендом.

Список використаних джерел

1. Пригода А. Я. Оцінка ефективності проекту розробки та впровадження CRM-системи на основі мікросервісної архітектури // *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. – 2024. – Вип. 55. – С. 172–180. DOI: 10.36910/6775-2524-0560-2024-55-22.
2. Dragoni N., Giallorenzo S., Lluch Lafuente A. *et al.* Microservices: yesterday, today, and tomorrow // *Present and Ulterior Software Engineering*. – Springer, 2017. – P. 195–216. DOI: 10.1007/978-3-319-67425-4_12.
3. de Almeida M.G., Canedo E.D. Authentication and Authorization in Microservices Architecture: A Systematic Literature Review // *Applied Sciences*. – 2022. – Vol. 12, No. 6. – Article 3023. DOI: 10.3390/app12063023.
4. Berisha B. Impact of Protocol Selection on Performance and Scalability in Microservices: A Comparison of gRPC, REST, and GraphQL // *Proc. of IEEE Conf. on Software Architecture (ICSA)* (preprint). – 2025. – 8 p.
5. Newman S. *Building Microservices: Designing Fine-Grained Systems*. – O'Reilly Media, 2015. – 280 p.
6. Lawi A., Panggabean B.L.E., Yoshida T. *et al.* Evaluating GraphQL and REST API Services Performance in a Massive and Intensive Accessible Information System // *Computers*. – 2021. – Vol. 10, No. 11. – Art. 138. DOI: 10.3390/computers10110138.

Моргун Артем Вікторович
аспірант 2 курсу
Державний університет «Київський авіаційний інститут»
(093) 466-44-94
2175566@stud.kai.edu.ua

МЕТОДИ РЕКОНСТРУКЦІЇ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Постановка задачі. Мікросервісна архітектура є сучасним підходом до проєктування програмного забезпечення, що передбачає побудову системи як сукупності відносно незалежних сервісів із можливістю автономної розробки та розгортання, а також адаптивного використання обчислювальних ресурсів відповідно до навантаження кожного сервісу. У міру зростання функціональної складності програмного продукту збільшується кількість мікросервісів і команд розробників, що ускладнює координацію та збереження цілісного бачення архітектури системи [1]. Життєвий цикл таких систем, як правило, реалізується з використанням гнучких методологій розробки та DevOps-практик, що передбачає безперервні зміни, унаслідок чого фактичний стан архітектури поступово відхиляється від її задокументованого опису. Це ускладнює прийняття технічних рішень і зумовлює потребу в методах реконструкції мікросервісної архітектури [2], спрямованих на підтримання її актуального стану та підвищення продуктивності інженерів програмного забезпечення у процесі проєктування таких систем, оскільки реконструкція є одним з важливих його етапів [6].

Мета дослідження. Метою дослідження є аналіз методів реконструкції мікросервісної архітектури програмного забезпечення; визначення їх сфер застосування, переваг, обмежень і напрямів подальшого розвитку.

Результати дослідження. Сучасні методи реконструкції мікросервісної архітектури ґрунтуються на автоматизованому аналізі артефактів життєвого циклу програмного забезпечення та поділяються на основні групи: методи статичного аналізу, методи динамічного аналізу та методи ручного (експертного) аналізу. До першої групи належать підходи, що використовують вихідний код, конфігурації, документацію; до другої - методи, які спираються на масив логів та метрик, що утворюються в процесі експлуатації; третя група передбачає реконструкцію архітектури експертами на основі всіх доступних даних. У низці сучасних підходів статичні відомості про сервіси комбінуються з динамічними даними про роботу системи та характеристиками інфраструктури, унаслідок чого формуються гібридні рішення, в яких результати статичного й динамічного аналізу інтерпретуються спільно для точнішого відображення структури та взаємозв'язків між компонентами.

Статичні методи реконструкції мікросервісної архітектури ґрунтуються на аналізі артефактів, доступних до розгортання системи, зокрема вихідного коду, конфігураційних файлів і документації (а також інших матеріалів, що містять відомості про систему). Це дає змогу відновлювати склад мікросервісів, їхні

інтерфейси та основні залежності між ними з можливістю інтеграції у відповідні перевірки в межах CI/CD. Прикладом інструменту статичного аналізу коду є SonarQube, який дає змогу автоматично виявляти структурні, безпекові та архітектурні проблеми [4]. Водночас статичний підхід не відображає фактичні сценарії взаємодії мікросервісів і залежить від якості та повноти артефактів, кількості репозиторіїв, тому для отримання цілісного уявлення про роботу системи його доцільно доповнювати динамічним аналізом.

Динамічні методи реконструкції мікросервісної архітектури мають в основі аналіз даних, що утворюються під час роботи системи, зокрема логів запитів, трас розподілених викликів та бізнес-метрик. На основі таких даних відновлюються фактичні взаємодії між сервісами та послідовності викликів, що дає змогу виділяти залежності, характерні сценарії навантаження й потенційні вузькі місця продуктивності [3]. Порівняно зі статичними підходами, динамічний аналіз відображає поведінку системи в реальному середовищі експлуатації з урахуванням масштабування, відмов і змін конфігурації; водночас повнота результатів залежить від якості інструментів та вхідних даних, тому на практиці його доцільно поєднувати зі статичними методами реконструкції. Моніторингові платформи (наприклад, Zipkin) зазвичай застосовують обмеження на тривалість зберігання даних, що на практиці обмежує глибину ретроспективного аналізу й вимагає компромісу між рівнем деталізації та витратами на зберігання [1].

Ручні методи реконструкції мікросервісної архітектури передбачають експертний аналіз коду, конфігурацій та іншої наявної інформації про систему з подальшою побудовою архітектурної моделі «вручну». Такий підхід зазвичай використовують для уточнення або перевірки результатів автоматизованих методів, однак він є трудомістким і погано масштабується.

Гібридні методи реконструкції мікросервісної архітектури поєднують статичний та динамічний підхід. Це дає змогу одночасно враховувати структурні характеристики системи та фактичні сценарії взаємодії мікросервісів, отримуючи чіткіше уявлення про архітектуру порівняно з окремим застосуванням статичного чи динамічного аналізу [1]. Разом з тим гібридні рішення є складними з погляду реалізації, оскільки потребують узгодженого збирання, оброблення та кореляції різномірних джерел даних.

Методи штучного інтелекту в контексті динамічних підходів до реконструкції мікросервісної архітектури переважно спираються на оброблення телеметрії виконання системи - логів, трас викликів та експлуатаційних метрик. На основі цих даних застосовуються алгоритми машинного й глибинного навчання для автоматизованого виявлення аномальних взаємодій між сервісами, деградації продуктивності та характерних шаблонів навантаження, що дає змогу виявляти критичні залежності між мікросервісами. Побудовані таким чином моделі взаємодій можуть використовуватися як вхід для динамічних методів SAR, підтримуючи реконструкцію графів викликів, перевірку відповідності фактичної структури системи проєктним рішенням і виявлення потенційних архітектурних антипатернів. У перспективі поєднання динамічних SAR-підходів

із ШІ-техніками розглядається як шлях до більшої автоматизації аналізу й еволюції мікросервісних архітектур [5, 6].

Висновки та перспективи. У роботі розглянуто статичні, динамічні, ручні та гібридні методи реконструкції мікросервісної архітектури й показано, що жоден із них окремо не забезпечує повноту інформації про архітектуру. Найбільш перспективними є гібридні підходи, у яких поєднуються результати статичного та динамічного аналізу, підсилені методами штучного інтелекту для інтерпретації логів та метрик та узгодження отриманих висновків з вихідним кодом.

Перспективою подальших досліджень є розроблення гібридних методів із використанням ШІ для автоматизованої реконструкції мікросервісної архітектури та їх експериментальна перевірка на складних системах [6].

Список використаних джерел

1. Mayer B., Weinreich R. An approach to extract the architecture of microservice-based software systems // In: Proceedings of the 2018 IEEE Symposium on Service-Oriented System Engineering (SOSE), Bamberg, Germany, 26–29 March 2018. – IEEE, 2018. – P. 21–30. – <https://doi.org/10.1109/SOSE.2018.00012>.
2. Rademacher F., Sachweh S., Zündorf A. A Modeling Method for Systematic Architecture Reconstruction of Microservice-Based Software Systems // In: Enterprise, Business-Process and Information Systems Modeling. BPMDS 2020, EMMSAD 2020 / eds. Nurcan S., Reinhartz-Berger I., Soffer P., Zdravkovic J. – Cham : Springer, 2020. – (Lecture Notes in Business Information Processing ; vol. 387). – P. 311–326. – https://doi.org/10.1007/978-3-030-49418-6_21.
3. Černý T., Abdelfattah A. S., Bushong V., Al Maruf A., Taibi D. Microservice Architecture Reconstruction and Visualization Techniques: A Review // In: Proceedings – 16th IEEE International Conference on Service-Oriented System Engineering (SOSE 2022), Newark, USA, 15–18 August 2022. – IEEE, 2022. – P. 39–48. – <https://doi.org/10.1109/SOSE55356.2022.00011>.
4. Schneider S., Bakhtin A., Li X., et al. Comparison of Static Analysis Architecture Recovery Tools for Microservice Applications // Empirical Software Engineering. – 2025. – Vol. 30. – Article No. 128. – <https://doi.org/10.1007/s10664-025-10686-2>.
5. Moreschini S., Pour S., Lanese I., et al. AI Techniques in the Microservices Life-Cycle: a Systematic Mapping Study // Computing. – 2025. – Vol. 107. – Article No. 100. – <https://doi.org/10.1007/s00607-025-01432-z>.
6. Моргун А., Гізун А. Концепт програмного забезпечення для проектування мікросервісної архітектури з використанням штучного інтелекту // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2025. – Т. 357, № 5.1. – С. 307–313. – <https://doi.org/10.31891/2307-5732-2025-357-39>.

Сокульський Олег Євгенович

старший викладач, к.т.н.

Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

mortimer@ukr.net

Москаленко Наталія Володимирівна

асистент

Київський національний університет імені Тараса Шевченка

moskalenkonv@ukr.net

ТЕХНОЛОГІЯ ВІДКРИТИХ КОДІВ В РОЗРОБЦІ ІНФОРМАЦІЙНИХ СИСТЕМ

Постановка задачі. Стрімке зростання різноманітності задач, які можуть бути вирішені з використанням інформаційних систем, потребує створення нових методів та засобів для їх розробки. При зростанні вимог до якості та надійності інформаційних систем, поширюється тенденція до зменшення витрат на їх розробку та супроводження. Все більше рішень базуються на використанні досягнень штучного інтелекту, технологій блокчейну та відкритого коду. Змінюються та вдосконалюються також і методології розробки інформаційних систем, зокрема методологія TDD-розробка через тестування[1].

Мета дослідження. Метою дослідження є аналіз застосування відкритих технологій для автоматизації розробки програмного забезпечення.

Результати дослідження. Лідерами відкритих технологій є технології Git та Docker, використання яких дозволяє ефективно створювати, керувати та розгортати програмне забезпечення.

Технології Git – це розподілена система контролю та збереження попередніх версій, дає змогу при необхідності повертатися до них, залучати до розробки великі команди спеціалістів, ефективно керуючи злиттям їх змін у файлах. Основні функції включають створення "знімків" змін(комітів), роботу з відгалуженнями(гілками) та збереження повної історії проекту[2].

Відкриті технології Git охоплюють як саму систему Git, що працює локально або на сервері, так і платформи для хостингу репозиторіїв (наприклад, GitHub, GitLab). В локальній версії вся інформація про проект доступна без підключення до Інтернету, при використанні віддаленого репозиторію, розміщеного на сервері, для синхронізації дій розробників необхідно підключення до Інтернету. Популярні платформи технології Git.

- GitHub – найпопулярніший вебсервіс для хостингу репозиторіїв, побудований на основі Git, що надає можливості для спільної роботи, розробки та керування проектами.

- GitLab – платформа для розробки програмного забезпечення, яка підтримує повний життєвий цикл та поєднує систему керування репозиторіями з розширеними можливостями, такими як система відстеження помилок, що також базується на Git.

•Git-flow – альтернативна модель розгалуження, яка пропонує структуру для організації робочих процесів у команді.

Технологія Docker, що базується на контейнеризації, гарантує однакову працездатність застосунку в будь-якій комплектації. Контейнер включає все необхідне для роботи додатку (операційну систему, бібліотеки, файли користувачів та метадані). Відкрита платформа використовується для розробки, експлуатації, більш швидкого тестування та розгортання додатків. Принцип контейнерної віртуалізації дозволяє зробити процес розробки більш легким та безпечним. При цьому можуть бути використані для роботи як локальні машини, так і віртуальні в хмарі.

Основні компоненти:

- Docker – платформа віртуалізації з відкритим кодом;
- Docker Hub – платформа-як-сервіс для розповсюдження та управління docker-контейнерами.

Використання пакетів Docker Desktop, Dockerfiles та Docker Compose дозволяє автоматизувати як локальний процес розробки, так і створення та керування складними системами, що складаються з багатьох сервісів (наприклад, Java-застосунку, бази даних та веб-сервера)[3].

Платформа Kubernetes також реалізує контейнерні технології, але на відміну від платформи Docker, яка створює образи контейнерів та працює з ними, Kubernetes використовується для управління багаточисельними мікросервісами, кожен з яких складається з декількох контейнерів. Kubernetes дозволяє створювати складні додатки на основі контейнерів та запускати їх в будь-якому масштабі в кластері серверів.

Висновки та перспективи. Використання методологій, засобів та технологій відкритих кодів дозволяє скоротити та оптимізувати життєвий цикл розробки, час та ресурси на налаштування середовища, знижує ризик появи помилок, пов'язаних з конфліктами залежностей або налаштувань середовища, а також стандартизує процес життєвого циклу програмного забезпечення за рахунок однакового середовища для розробки та тестування. Технології підтримують сучасні методології розробки, зокрема такі як DevOps, та гнучко дозволяють реагувати на потреби бізнесу.

Список використаних джерел

1. О. С. Булгакова та ін. Методи та системи штучного інтелекту: теорія та практика. Навчальний посібник ISBN: 978-966-289-364-9 . 2025, 356 с.
2. Скот Чакон, Бен Страуб. Pro GIT. URL: https://chamber.ua/wp-content/uploads/2019/12/progit_v2.1.2.pdf (дата звернення 24.11.2025)
3. Д.Ю. Меркотан, О.Я. Сова, О.О. Троцько, О.А. Симоненко, О.В. Гаман, О.Є. Степаненко, Г.Г. Мягих, В.П. Величко. Технології автоматизації системних процесів. Навчальний посібник – Київ, 2021. – 234 с.

Недозимований Денис Віталійович
студент 4 курсу, групи ІІ-22121
Національний транспортний університет
(095) 519-50-02
denisvn02005@gmail.com
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

КОМПЛЕКСНІ ПІДХОДИ ДО КІБЕРЗАХИСТУ В УМОВАХ СУЧАСНИХ ЦИФРОВИХ ЗАГРОЗ

Постановка задачі. Стрімке зростання обсягу цифрових даних, активний розвиток хмарних сервісів, мобільних технологій та розподілених обчислювальних систем створюють нові ризики для безпеки інформації. Кібератаки стають більш комплексними, автоматизованими та спрямованими як на приватні компанії, так і на державні органи. Традиційні методи захисту вже не забезпечують належного рівня стійкості до сучасних загроз, таких як фішинг нового покоління, атаки із застосуванням штучного інтелекту, експлойти нульового дня та багатовекторні атаки на критичну інфраструктуру.

Основна проблема полягає у необхідності розроблення систем кіберзахисту, здатних до динамічної адаптації, автоматичного виявлення аномалій та побудови комплексної моделі безпеки для організацій різного масштабу. У зв'язку з цим актуальним є дослідження сучасних підходів до кібербезпеки, методів виявлення загроз і технологій запобігання несанкціонованому доступу та витоку даних.

Мета дослідження. Метою дослідження є аналіз сучасних концепцій і технологій кіберзахисту, визначення ефективних методів протидії кібератакам, а також узагальнення практик, що дозволяють підвищити рівень інформаційної безпеки організацій. Особлива увага приділяється інтелектуальним системам виявлення вторгнень, методам багаторівневого захисту, тенденціям розвитку нормативних стандартів та інтеграції інструментів штучного інтелекту у системи інформаційної безпеки.

Досягнення поставленої мети передбачає:

- аналіз сучасних типів кіберзагроз;
- оцінку ефективності технологій моніторингу та реагування;
- розгляд практичних прикладів захисту корпоративних мереж;
- визначення перспективних напрямів розвитку галузі.

Результати дослідження. Сучасні системи кіберзахисту базуються на поєднанні традиційних методів безпеки та новітніх технологій аналізу даних. Архітектура корпоративної інформаційної безпеки включає кілька взаємопов'язаних компонентів: засоби контролю доступу, системи виявлення вторгнень, засоби захисту мережевого периметра, механізми шифрування та

підсистеми моніторингу подій. Кожен компонент виконує окрему функцію, але ефективність забезпечується лише у разі їхньої інтеграції в єдину структуру.

Одним із ключових елементів сучасної кібербезпеки є системи виявлення аномальної активності (IDS/IPS), які аналізують поведінку користувачів та мережевого трафіку. Вони здатні визначати нестандартні дії, характерні для спроби проникнення, зловмисних сценаріїв або експлуатації вразливостей. У дослідженні було розглянуто два основні підходи до роботи таких систем: сигнатурний та поведінковий. Сигнатурний аналіз ґрунтується на порівнянні подій із базою відомих шаблонів атак, тоді як поведінковий підхід фіксує відхилення у динаміці дій користувача чи мережевих процесів. Саме поведінкові моделі демонструють високу ефективність у виявленні нових, раніше невідомих типів загроз.

Окрему увагу приділено Zero Trust-підходу, який передбачає відсутність апріорної довіри до будь-якого користувача або пристрою в мережі. Кожна дія, запит або підключення проходить повторну перевірку, що мінімізує ризики внутрішніх загроз і компрометації облікових записів. Запровадження Zero Trust вимагає застосування багатофакторної автентифікації, сегментації мережі та контролю привілеїв відповідно до принципу “найменших прав”.

Було вивчено й методи криптографічного захисту даних, які забезпечують конфіденційність і цілісність інформації під час зберігання та передавання. Сучасні інформаційні системи активно використовують симетричні та асиметричні алгоритми шифрування, протоколи TLS, VPN-тунелі та цифрові підписи. У дослідженні встановлено, що криптографічні засоби залишаються одним із найбільш надійних способів захисту даних, проте їхня ефективність залежить від правильності налаштування, регулярного оновлення ключів і дотримання політик управління доступом.

Також було досліджено роль людського фактора у забезпеченні інформаційної безпеки. Аналіз сучасних інцидентів показує, що значна частина успішних атак відбувається через фішингові повідомлення, слабкі паролі або порушення регламентів безпеки самими працівниками. Це підкреслює важливість регулярного навчання персоналу, впровадження політик безпечної роботи з даними та створення культури кібергігієни в організаціях.

Отримані результати дозволили сформувати цілісне уявлення про структуру сучасних систем кіберзахисту, їхні ключові компоненти та механізми взаємодії, а також визначити найбільш ефективні технології попередження кібератак у динамічному цифровому середовищі.

Висновки та перспективи. Проведене дослідження показало, що сучасна кібербезпека базується на комплексному підході, який охоплює технічні засоби захисту, аналітичні моделі виявлення загроз та організаційні механізми контролю доступу. Встановлено, що найбільш ефективними є системи, які поєднують поведінковий аналіз, багаторівневий моніторинг, криптографічний захист даних та принципи Zero Trust-архітектури. Значну роль у забезпеченні безпеки відіграє людський фактор, а тому навчання персоналу та впровадження політик

кібергігієни залишаються ключовими складовими надійного захисту інформаційних систем.

Таким чином, для досягнення високого рівня інформаційної безпеки організаціям необхідно інтегрувати сучасні технології кіберзахисту з постійним удосконаленням процесів управління ризиками.

Список використаних джерел

1. ISO/IEC 27001:2022 — Information Security Management Systems.
2. NIST Cybersecurity Framework. National Institute of Standards and Technology.
3. Stallings W. Network Security Essentials: Applications and Standards. Pearson, 2020.
4. ENISA. Cybersecurity Threat Landscape Report 2023.
5. Shackleford D. The State of Cybersecurity. SANS Institute, 2023.

Нікулін Сергій Сергійович
аспірант 3 курсу, групи 174-303-3
Національний аерокосмічний університет «Харківський авіаційний інститут»
(099)712-86-85
s.s.nikulin@khai.edu
Заболотний Олександр Віталійович
доктор технічних наук, професор, декан факультету №3
Національний аерокосмічний університет «Харківський авіаційний інститут»
(067)579-05-13
o.zabolotnyi@khai.edu

ТЕСТУВАННЯ БАЗОВОГО ФУНКЦІОНАЛУ FPV-ДРОНА ЗА ДОПОМОГОЮ СИМУЛЯТОРА ДИНАМІКИ

Постановка задачі. Інтенсивний розвиток технологій безпілотних літальних апаратів (БПЛА) зумовлює потребу у створенні адекватних математичних і програмних моделей, здатних точно відтворювати динаміку польоту для подальшої розробки систем стабілізації, навігації та керування [1]. FPV-дрони (*First Person View*) як представники високоманеврового класу малих БПЛА є особливо чутливими до зміни тяги окремих двигунів і масово-інерційних характеристик конструкції, що ускладнює їхнє моделювання традиційними методами. Класичні підходи, засновані на використанні кутів Ейлера, мають обмеження у вигляді сингулярностей, які призводять до втрати точності розрахунків при великих кутах відхилення. Саме тому актуальним є застосування кватерніонного опису орієнтації, що забезпечує коректне чисельне інтегрування навіть у діапазоні великих просторових обертань.

Виходячи з цього, поставлено завдання створити інтерактивний симулятор FPV-дрона, який би дозволяв експериментально досліджувати реакцію апарата на зміну тяги двигунів, масово-інерційних параметрів, геометрії рами та інерції карданного підвісу. Такий підхід надає можливість не лише вивчати внутрішню динаміку системи, а й формувати основу для подальшої ідентифікації параметрів реальних апаратів [2].

Мета дослідження. Метою дослідження є створення повнофункціонального інтерактивного симулятора динаміки FPV-дрона в середовищі MATLAB, який реалізує чисельну модель обертального руху апарата з урахуванням кватерніонної кінематики та інерційних характеристик складових елементів [3]. Симулятор повинен забезпечувати відображення просторової орієнтації у режимі реального часу, а також давати змогу досліднику спостерігати взаємозв'язки між керуючими впливами та реакцією дрона в каналах крену, тангажу та ролу. Особливу увагу приділено створенню інструментарію для аналізу часових залежностей кутів і кутових швидкостей, визначенню часу реакції, перерегулювання та максимальних відхилень, що дозволяє оцінити якість перехідних процесів і стабільність моделі.

Результати дослідження. У результаті виконання роботи розроблено симуляційний програмний комплекс *FPV_drone_simulation_GUI.m* (рис. 1), який реалізовано у середовищі MATLAB з використанням графічного інтерфейсу користувача. Програмна система моделює обертальний рух дрона на основі методу Рунге–Кутти четвертого порядку, що забезпечує високу точність інтеграції диференціальних рівнянь руху [4]. У моделі враховано повний тензор інерції апарата, який формується з урахуванням маси рами, моторів, акумуляторного блока та трьох рам карданного підвісу. Крім того, враховано всі основні фізичні моменти, що діють на дрон під час руху, зокрема момент від тяги двигунів, реактивні та гіроскопічні моменти, а також аеродинамічне демпфування й механічне тертя у вузлах підвісу.

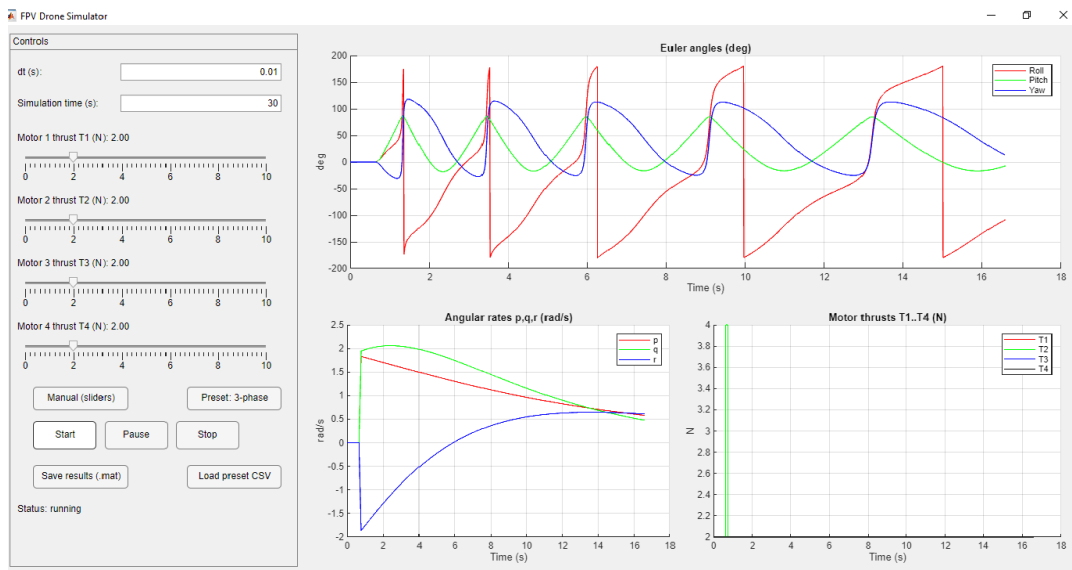


Рис. 1. Інтерфейс модуля *FPV drone simulation*

Розроблений симулятор має два основні режими роботи: ручний, який передбачає незалежне регулювання тяги кожного двигуна за допомогою слайдерів, та автоматизований, що реалізується шляхом зчитування сценарію з файлу формату *.csv*. Це дозволяє виконувати як індивідуальні експерименти, так і повнофакторні серії випробувань для аналізу чутливості системи.

У процесі дослідження проведено низку експериментів, які дали змогу визначити особливості реакції дрона на зміну входних параметрів. Зокрема, встановлено, що збільшення тяги одного двигуна спричиняє обертання апарата навколо кількох осей одночасно, що вказує на наявність перекресних зв'язків між каналами керування. При симетричному збільшенні тяги всіх двигунів дрон зберігає орієнтацію, підтверджуючи рівновагу моментів. Дослідження асиметрії тяги передньої та задньої пар двигунів виявило прогнозоване відхилення за тангажем, тоді як збільшення маси акумулятора суттєво впливає на момент інерції та знижує швидкість реакції системи. Зміна геометричних параметрів рами, зокрема відстаней між моторами, призводить до зростання обертового моменту та підвищення швидкодії. Водночас зменшення маси рамок карданного підвісу, в якому кріпиться дрон під час тестування, підвищує стабільність та

швидкість реакцій дрона, демонструючи важливість оптимізації інерційних характеристик підвісу.

Отримані графічні залежності кутів та кутових швидкостей дали змогу розрахувати часові показники перехідних процесів і створити порівняльні таблиці для різних конфігурацій, що підтвердило відповідність симуляційної моделі теоретичним передбаченням і поведінці реального FPV-дрона [5].

Висновки. Розроблений інтерактивний симулятор динаміки FPV-дрона є ефективним інструментом для дослідження просторової поведінки безпілотних апаратів у різних умовах. Застосування кватерніонного підходу дозволило усунути обмеження, властиві традиційним методам, та забезпечити стабільність розрахунків при великих кутах орієнтації. Реалізація програмного комплексу в середовищі MATLAB забезпечує універсальність, відкритість структури та можливість інтеграції з іншими інженерними модулями. Симулятор може бути використаний як у навчальному процесі для вивчення динаміки та принципів керування БПЛА, так і в наукових дослідженнях, пов'язаних з ідентифікацією параметрів, оптимізацією конструкцій і тестуванням стабілізаційних алгоритмів у режимі *Hardware-in-the-Loop*.

Список використаних джерел

1. Zabolotnyi O. V., Siroklyn V. P., Nikulin S. S. Development of a hardware-software complex for combat quadcopters testing: improving reliability and efficiency in modern military technology. *Scientific notes of taurida national V.I. vernadsky university. series: technical sciences*. 2024. No. 4. P. 83–90. URL: <https://doi.org/10.32782/2663-5941/2024.4/13>
2. Y. Liu, “Modelling and simulation of quadcopter UAV based on PID control”, *Appl. Comput. Eng.*, т. 75, № 1, с. 202–210, лип. 2024. URL: <https://doi.org/10.54254/2755-2721/75/20240539>
3. H. Djizi, Z. Zahzouh та A. Lakehal, “Quadcopter prototype stability analysis using matlab simscape library”, *Scientific Bull. Elect. Eng. Fac.*, т. 22, № 2, с. 38–43, груд. 2022. URL: <https://doi.org/10.2478/sbeef-2022-0018>
4. A. Abdi, G. Hojjati, Z. Jackiewicz, H. Podhaisky та M. Sharifi, “On the implementation of explicit two-step peer methods with Runge–Kutta stability”, *Appl. Numer. Math.*, січ. 2023. URL: <https://doi.org/10.1016/j.apnum.2023.01.015>
5. E. Saif та İ. Eminoğlu, “Modelling of quad-rotor dynamics and Hardware-in-the-Loop simulation”, *J. Eng.*, серп. 2022. URL: <https://doi.org/10.1049/tje2.12152>

Овчаренко Віктор Сергійович

аспірант

Інститут програмних систем Національної академії наук України

viktor.ov4arenko@gmail.com

АДАПТИВНИЙ ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ СТАБІЛЬНОЇ ЯКОСТІ РОЗРОБКИ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ ПРОЦЕСНОЇ АНАЛІТИКИ

Постановка задачі. У сучасній інженерії програмного забезпечення зростає потреба у стабільній якості розробки, що не лише контролюється стандартами (ISO/IEC 25010, CMMI), але й адаптивно підтримується у змінних умовах командної продуктивності, обмежень часу, інцидентів під час розробки та різноманітності вимог стейкхолдерів. Традиційні метрики (Defect Density, Lead Time, Code Review Time) фіксують лише результат та не враховують динаміку процесів, що призводить до затримок, деградації якості артефактів і зростання вартості внесення змін. Актуальною стає розробка адаптивних моделей підтримання якості, які враховують процесну аналітику (Process Mining, Workflow Intelligence) та використовують прогностичні механізми для своєчасного регулювання показників якості.

Мета дослідження. Розробити адаптивну модель забезпечення стабільної якості розробки інформаційних систем, яка використовує аналітику процесів інженерії ПЗ для прогнозування ризиків та автоматичного регулювання показників якості відповідно до змін у команді, процесах та продуктивності.

Результати дослідження.

У межах дослідження побудовано модель адаптивної підтримки якості, що поєднує:

- метрики процесної аналітики,
- систему прогнозування ризиків якості,
- адаптивне управління показниками (Q-Factors) для контролю на ранніх стадіях розробки.

Передбачено використання процесного аналізу (Process Mining) для виділення трендів, вузьких місць, інцидентів життєвого циклу задач (Dev, QA, Code Review) та застосування регуляторів якості для уникнення деградації.

Процесна аналітика в інженерії програмного забезпечення дозволяє перевести об'єктивні характеристики роботи команди, таких як тривалість виконання задач, кількість повторних дефектів чи перевантаження етапів ухвалення рішень, у формальні метрики, здатні прогнозувати деградацію якості на ранніх стадіях. Для цього доцільно ідентифікувати показники, що не лише відображають результат, але й виявляють динаміку процесів, яка безпосередньо впливає на стабільність та керованість розробки. В таблиці 1 узагальнено ключові критичні метрики, що формують базис для адаптивного регулювання якості.

Таблиця ілюструє прямий причинний зв'язок між процесною нестабільністю та дефектністю програмного коду, що обґрунтовує необхідність прогностичних механізмів коригування планування та контролю якості.

Таблиця 1

Процесні метрики та їхній вплив на якість розробки

Процесна метрика	Формальний опис	Вплив на якість
Lead Time Variability	σ часу виконання задач	Зростання нестабільності коду та QA-помилки
Review Bottleneck Ratio	AVG часу затримки на Code Review	Підвищення ризику дефектів через низький контроль
Defect Reopen Rate	Частка повторних інцидентів	Низька якість приймання та тестування
Sprint Forecast Error	Δ між планом і фактом	Перевантаження команди → падіння точності

Представлені метрики демонструють, що проблеми якості не виникають локально в коді, а формуються як накопичувальний ефект процесної нестабільності. Високі значення параметра Lead Time Variability свідчать про неритмічність розробки, що корелює з імпульсними «викидами» дефектів. Показник Review Bottleneck Ratio вказує на критичний вплив затримок у рецензуванні на майбутню якість, оскільки несвоєчасний контроль накопичує помилки. Defect Reopen Rate формалізує слабкість процедур тестування, а Sprint Forecast Error відображає системну невідповідність продуктивності плануванню, що спричинює перевантаження, збільшення дефектів і зниження якості релізу. Таким чином, розглянуті метрики стають основою для побудови адаптивної моделі керування якістю, що реагує на процесні ризики до появи помилок у продукті.

Для забезпечення стабільної якості недостатньо лише спостерігати за процесом; необхідно створити замкнений контур адаптивного керування. На рисунку 1 показано концептуальну архітектуру, де дані про процеси розробки опрацьовуються засобами Process Mining та обчислювального прогнозування. Виявлені ризики впливають на параметри управління: перерозподіл задач, корекцію пріоритетів Code Review, автоматизоване підсилення тестування та інші механізми регулювання. Таким чином формується цикл самокорекції, який стабілізує показники якості у реальному часі.

Схема показує, як модель аналізує процеси розробки та прогнозує можливі погіршення якості, а потім автоматично коригує управлінські параметри: перерозподіл завдань, посилення тестування, корекцію Code Review, зміну пріоритетів задач.

Запропонована модель має властивості прогностичної керованості: вона не лише фіксує якість, а й впливає на неї шляхом автоматичного телеметричного регулювання процесу розробки.



Рис. 1. Адаптивна модель забезпечення стабільної якості

Це забезпечує проактивне запобігання дефектам, оптимізацію навантаження команди, дотримання стандартів якості та мінімізацію витрат на виправлення помилок. Модель здатна інтегруватися у Jira, GitLab CI, GitHub Actions, що робить її придатною для практичного використання у сучасних ІТ-командах різного масштабу.

Висновки та перспективи. Запропонований адаптивний підхід забезпечує стабільну якість розробки інформаційних систем завдяки прогнозованому контролю процесних ризиків та їх проактивній компенсації. Модель орієнтована на безперервний моніторинг інженерних процесів і може бути інтегрована в системи Jira/YouTrack, GitLab та CI/CD.

Перспективи подальших досліджень передбачають використання мультиагентних систем рішень для саморегулювання DevOps-процесів, впровадження Explainable AI для прозорості управлінських рішень та стандартизацію адаптивних Q-Factors для різних доменів інженерії ПЗ.

Список використаних джерел

1. Urrea-Contreras S. J., Arriaga D., González-González V., Ramos R. Applying Process Mining: The Reality of a Software Development SME/ *Applied Sciences*. – 2024. – Vol. 14. – Article 1402. – DOI: 10.3390/app14041402. MDPI
2. Ni W., Zhao G., Liu T., Zeng Q., Xu X. Predictive Business Process Monitoring Approach Based on Hierarchical Transformer/ *Electronics*. – 2023. – Vol. 12, No. 6.

МОДЕЛЬ ІНТЕЛЕКТУАЛЬНОЇ АВТОМАТИЗАЦІЇ УПРАВЛІННЯ КОЛЕКЦІЙНИМИ РЕСУРСАМИ

Актуальність дослідження. Колекційні ресурси охоплюють сукупності боргових зобов'язань, взаємодій з клієнтами та інструментів впливу, що застосовуються організаціями у фінансовому та сервісному секторі. На практиці управління такими ресурсами часто спирається на статичні сценарії стягнення, значну ручну працю операторів та обмежену персоналізацію. Це знижує ефективність повернення заборгованостей, збільшує витрати та формує неоднорідну якість сервісу. Актуальною стає потреба у моделі інтелектуальної автоматизації, яка адаптує колекційні стратегії на основі поведінкових індикаторів та прогнозової аналітики.

Постановка задачі. Задача інтелектуального управління колекційними ресурсами передбачає оптимізацію взаємодії з клієнтами через автоматизовані стратегії. Необхідно реалізувати механізм, що прогнозує платіжну поведінку, визначає ризикові сегменти, обирає оптимальні дії, інтенсивність комунікацій та канали взаємодії з мінімальною вартістю ризику. Потрібно побудувати модель, здатну самонавчатися на нових даних і масштабуватися для великих портфелів.

Мета дослідження. Метою роботи є розроблення моделі інтелектуальної автоматизації управління колекційними ресурсами, яка поєднує прогнозну аналітику, класифікаційні механізми та оптимізаційні алгоритми для автоматичного формування рішень щодо взаємодії з клієнтами.

Результати дослідження. Запропонована модель включає чотири взаємопов'язані компоненти:

1. Аналітико-прогностичний блок. Здійснює оцінювання ймовірності добровільної сплати, прогнозує час повернення, ризик дефолту, потенційні втрати та індивідуальну реакцію на комунікаційні дії.

2. Класифікаційний модуль сегментації клієнтів. Виділяє групи за типом поведінки, рівнем ризику, чутливістю до каналів комунікацій, фінансовою активністю та історією взаємодій. Сегментація дозволяє коригувати стратегію залежно від типу клієнта.

3. Оптимізаційний механізм вибору стратегії. На основі прогнозів та сегментації система визначає найефективніші дії (дзвінки, СМС, email, профілактичні пропозиції), частоту звернень, їх інтонаційний стиль та момент повторного контакту, мінімізуючи операційні витрати.

4. Автоматизований блок виконання та зворотного навчання. Здійснює реалізацію стратегії, збір нових даних та оновлення моделей. Це забезпечує безперервне самонавчання системи, адаптацію до ринкових змін та змін поведінки клієнтів.

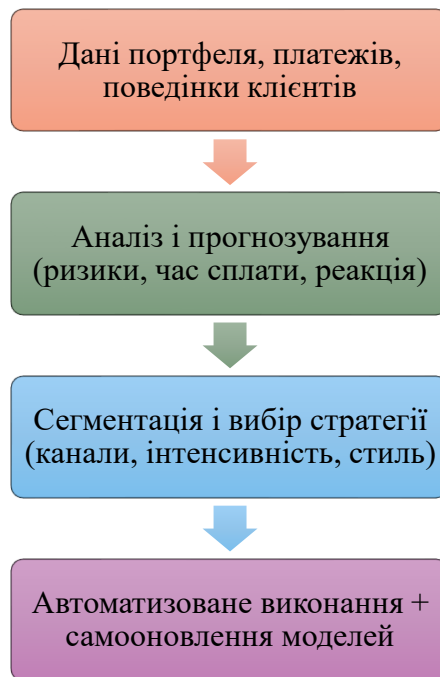


Рис. 1. Модель інтелектуальної автоматизації управління колекційними ресурсами

Схема демонструє перехід від прогнозного аналізу та сегментації до автоматичного виконання персоналізованих стратегій, які постійно вдосконалюються на основі нових даних.

Модель функціонує як замкнений цикл: кожне рішення системи не тільки впливає на клієнта, а й формує нові дані для навчання моделей. Це забезпечує адаптацію до нестабільності ринку, нерівномірності платіжної активності та змін регуляторних вимог. Система мінімізує втрати за рахунок персоналізованого вибору каналів комунікацій та інтервалів контактів, що дозволяє уникнути перенавантаження клієнта і знижує витрати на обробку портфеля.

Для підтвердження ефективності моделі використано анонімізований набір даних колекційного портфеля (10 тис. клієнтів, фінансовий сектор). Порівнювали:

- класичний ручний підхід,
- статичні правила сегментації,
- запропоновану інтелектуальну модель автоматизації.

Таблиця 1.

Результати оцінювання			
Підхід	Добровільні сплати	Середній час повернення	Вартість комунікацій
Ручний (оператори)	38%	26 днів	100%
Статичні правила	45%	21 день	92%
Інтелектуальна модель	57%	15 днів	74%

Таблиця відображає порівняльні результати трьох підходів до управління колекційними ресурсами за ключовими показниками: частка добровільних сплат, середній час повернення заборгованості та відносна вартість комунікацій.

Зіставлення демонструє, що інтелектуальна модель автоматизації забезпечує істотне зростання частки добровільних оплат і скорочення часу повернення боргу при одночасному зменшенні операційних витрат у порівнянні з ручним управлінням та статичними правилами. Це підтверджує доцільність впровадження інтелектуальних механізмів аналізу й оптимізації стратегій взаємодії з клієнтами у колекційних процесах.

Як бачимо, інтелектуальна автоматизація забезпечила зростання добровільних оплат на 12–19% та скорочення витрат на 18–26% у порівнянні з традиційними підходами.

Висновки та перспективи. Запропонована модель інтелектуальної автоматизації демонструє спроможність підвищити результативність колекційних процесів, зменшити операційні витрати та забезпечити стійку адаптацію до поведінки клієнтів.

Подальші дослідження доцільно спрямувати на включення емоційно-семантичних моделей спілкування та на дослідження застосування багатомовних стратегій комунікації в транскордонних портфелях.

Список використаних джерел

1. Przybyłek M., Przybyłek A., Wojciechowski K., Shkroba I. Towards a smart debt collection system: a Design Science Research approach // *Journal of Big Data*. – 2025. – Vol. 12. – Art. 193. – DOI: 10.1186/s40537-025-01252-0. SpringerOpen
2. Jankowski R., Paliński A. Debt Collection Model for Mass Receivables Based on Decision Rules—A Path to Efficiency and Sustainability // *Sustainability*. – 2024. – Vol. 16, No. 14. – Art. 5885. – DOI: 10.3390/su16145885. MDPI+1
3. Sánchez C., Maldonado S., Vairetti C. Improving debt collection via contact center information: A predictive analytics framework // *Decision Support Systems*. – 2022. – Vol. 159. – Art. 113812. – DOI: 10.1016/j.dss.2022.113812. ScienceDirect+2investigadores.uandes.cl+2
4. Pérez M. C. Application of Machine Learning algorithms for the prediction of payment by agreement in a debt collection company with the CRISP-DM methodology // *Proceedings of the International Conference on Industrial Engineering and Operations Management (IEOM)*. – Asunción, Paraguay, 2022. ieomsociety.org+1

Присяжнюк Олена Віталіївна
к.т.н., доцент кафедри інформаційних та цифрових технологій
Центральноукраїнського державного університету імені Володимира
Винниченка, м. Кропивницький
o.v.prysiazhniuk@cuspu.edu.ua
Пузікова Анна Валентинівна
к.ф.-м.н., доцент кафедри інформаційних та цифрових технологій
Центральноукраїнського державного університету імені Володимира
Винниченка, м. Кропивницький
a.v.puzikova@cuspu.edu.ua

АНАЛІЗ ВИКОРИСТАННЯ GPT-4O ДЛЯ АВТОМАТИЗАЦІЇ ОЦІНЮВАННЯ ЯКОСТІ КОРИСТУВАЦЬКОГО ІНТЕРФЕЙСУ З УРАХУВАННЯМ БЕЗПЕКОВИХ РИЗИКІВ

Постановка задачі. Сучасні інструменти автоматизації аудиту якості інтерфейсів на основі ШІ переважно зосереджені на перевірці технічної продуктивності та функціональному тестуванні вебпродуктів [1]. Водночас вони не здатні повною мірою охопити когнітивні й емоційні аспекти користувацького досвіду, зокрема особливості сприйняття та психологічної взаємодії користувачів з інтерфейсами, а також ті вразливості, що можуть породжувати потенційні безпекові ризики. Поява і стрімкий розвиток великих мовних моделей (LLM) з розвиненими можливостями аналізу зображень (наприклад, мультимодальної моделі GPT-4o) відкривають нові перспективи для автоматизованого оцінювання якості користувацьких інтерфейсів з урахуванням зручності, доступності та інших ключових параметрів UX, що забезпечують комфортну й безпечну взаємодію користувача з програмним продуктом [2]. У зв'язку з цим актуальним є дослідження можливостей GPT-4o щодо оцінювання якості користувацького інтерфейсу з подальшою імплементацією моделі в автоматизовані системи аудиту.

Метою дослідження є аналіз ефективності використання мультимодальної моделі GPT-4o для автоматизованого оцінювання якості інтерфейсу вебпродуктів з позицій користувацького досвіду та з урахуванням безпекових ризиків.

Результати дослідження. В нашому дослідженні експертне оцінювання якості UX інтерфейсу відбувалось за чотирма критеріями: зручність, доступність, візуальний дизайн та інформаційна архітектура, які були обрані передусім завдяки їх прямому зв'язку з візуальним сприйняттям користувача та їх фундаментальної природи в дизайні користувацького досвіду. Ці критерії охоплюють найбільш розповсюджені аспекти взаємодії з користувачем, включаючи інтуїтивно зрозуміле та зручне сприйняття екрану, чіткість та доступність інтерфейсу, візуальний дизайн та структурованість контенту.

З описаними вище критеріями оцінювання якості UX інтерфейсів пов'язані певні безпекові ризики для користувачів. Недостатньо зручний або надто складний інтерфейс може призводити до помилкових дій користувача, включно з

введенням даних не в ті поля, випадковим виконанням критичних операцій або навіть відмовою від безпекових механізмів через їхню складність. Погана візуальна побудова та низька доступність інтерфейсу підвищують ризик втрати даних, фішингових атак і неправильного сприйняття важливих попереджень, що загалом знижує рівень захищеності користувача.

Для автоматизації оцінювання якості користувацького інтерфейсу було розроблено мобільний додаток на базі Flutter, який здійснював відправку скріншотів інтерфейсів для їх оцінки за допомогою нейромережі, а також відображував отримані від моделі GPT-4o результати (рис. 1).

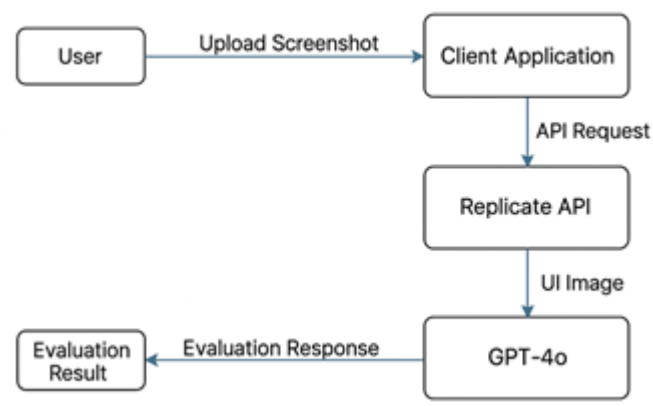


Рис. 1. Схема роботи додатку

Для оцінювання ефективності інтеграції GPT-4o у процеси аналізу якості UX інтерфейсів було проведено експеримент, у межах якого порівняно оцінки якості інтерфейсу 20 сайтів ЗВО, сформовані GPT-4o, з оцінками, отриманими від експертів. Узагальнені результати оцінювання якості UX інтерфейсу сайтів ЗВО представлено уТаблиці 1.

Таблиця 1

Оцінювання якості користувацьких інтерфейсів сайтів ЗВО

№	Назва ЗВО (скорочена), URL сайту	Критерій 1		Критерій 2		Критерій 3		Критерій 4	
		GPT-4o	Експерт	GPT-4o	Експерт	GPT-4o	Експерт	GPT-4o	Експерт
1	КНУ ім. Т.Шевченка https://www.knu.ua	3	4	2	4	2	4	3	4
2	Львівська політехніка https://lpnu.ua	4	4	3	4	4	4	4	5
3	МАУП http://www.maup.com.ua	3	2	2	2	3	2	3	3
4	КПІ ім. І.Сікорського https://kpi.ua/	3	5	2	4	3	5	3	5
5	Запорізьська політехніка https://zp.edu.ua/	3	3	2	2	3	3	3	3
6	ХАІ https://khai.edu.ua/	4	4	3	4	4	4	3	5

7	ЧДТУ https://chdtu.edu.ua/	3	2	2	3	2	2	3	3
8	УжНУ https://www.uzhnu.edu.ua/	4	4	3	3	3	3	4	4
9	Житомирська політехніка https://ztu.edu.ua/	4	4	3	3	5	4	4	4
10	ДНУ ім. О.Гончара https://www.dnu.dp.ua/	3	4	2	4	2	3	3	4
11	ДУІТ https://duikt.edu.ua/	4	4	3	4	3	4	4	4
12	ЦНТУ https://kntu.kr.ua/	3	4	2	3	3	3	3	3
13	Одеська політехніка https://op.edu.ua/	3	4	2	3	3	4	3	4
14	ЦДУ ім. В.Виниченка https://www.cusu.edu.ua	4	4	3	4	4	4	4	4
15	ЧНУ ім. Хмельницького http://www.cdu.edu.ua	3	2	3	4	2	2	3	3
16	ЗУНУ https://www.wunu.edu.ua	3	2	2	3	4	3	3	3
17	Вінницька політехніка https://vntu.edu.ua/	3	3	2	3	3	4	3	3
18	ТНТУ ім. І.Пулюя https://tntu.edu.ua/	3	2	3	4	2	3	3	4
19	ЧНУ ім. Ю.Федьковича https://www.chnu.edu.ua/	4	4	3	3	5	4	4	3
20	ЛНТУ https://lntu.edu.ua/uk	3	4	4	4	4	5	3	3

Експеримент, проведений на вибірці з 20 вебінтерфейсів ЗВО, засвідчив високий рівень відповідності між оцінками, наданими моделлю GPT-4o, та висновками експертів, що підтверджується статистично значущими коефіцієнтами узгодженості. Модель GPT-4o продемонструвала здатність виявляти ширший спектр UX-вразливостей, зокрема у сфері доступності, які можуть залишатися поза увагою експертів, що додатково підтверджується сформованими аналітичними звітами.

Висновки та перспективи. Отримані результати обґрунтовують доцільність інтеграції сучасних мультимодальних моделей ШІ у процеси аудиту інтерфейсів як інструментів, що підсилюють експертний аналіз і дають змогу зменшити трудомісткість та ресурсні витрати під час оцінювання UX-інтерфейсів ІТ-систем. Перспективи подальших досліджень передбачають розширення експериментальної частини із залученням експертів як з кола

тестувальників, так і фахівців із кібербезпеки, а також збільшення кількості критеріїв для оцінювання якості інтерфейсів.

Список використаних джерел

1. Ворочек О.Г., Соловей І.В. Дослідження засобів штучного інтелекту для автоматизації процесу тестування програмного забезпечення. *Вісник Національного технічного університету «ХПІ». Серія: Системний аналіз, управління та інформаційні технології*. 2024. № 1 (11)'2024. С. 58-64. DOI: 10.20998/2079-0023.2024.01.09.
2. Hsueh N.-L., Lin H.-J., Lai L.-C. Applying Large Language Model to User Experience Testing. *Electronics*. 2024. T.13, № 23. DOI: 10.3390/electronics13234633.

Серкелі Артур Вадимович
студент 3 курсу, групи ІІІ-32
Національний технічний університет України «Київський політехнічний
інститут імені Ігоря Сікорського»
(068) 459-43-65
serkeli2006@gmail.com
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний
інститут імені Ігоря Сікорського"
spopereshnyak@gmail.com

ВИЗНАЧЕННЯ ВИМОГ ДО ПЛАТФОРМИ ОНЛАЙН-КУРСІВ

Постановка задачі. Спроекувати та реалізувати веб-платформу онлайн-курсів із чітко сформульованими вимогами до функціоналу, архітектури та безпеки. Система має підтримувати каталог курсів, перегляд матеріалів, зарахування й відстеження прогресу, інструменти для авторів (CRUD), адміністративну модерацію, завантаження медіафайлів, надсилання електронних повідомлень та формування сертифікатів.

Мета дослідження. Визначити ключові можливості та вимоги до реалізації і архітектури платформи онлайн-курсів, що підтримує масштабування, модульність і захист даних користувачів.

Результати дослідження. Для реалізації платформи застосовано стек технологій TypeScript/Next.js на фронтенді та NestJS на бекенді, а основою для зберігання даних обрано PostgreSQL. Система побудована як модульний моноліт із чітким розділенням доменів, що охоплюють автентифікацію, управління курсами та уроками, роботу із зарахуваннями й прогресом, облік відгуків, формування сертифікатів і керування медіафайлами. [1–3]

Архітектурно кожен домен виконує свої функції: модуль автентифікації реалізує JWT-авторизацію, refresh-механізм, відновлення доступу та взаємодію з email/OAuth-сервісами; модулі курсів та уроків забезпечують повний CRUD і формування структури навчальних програм; домен зарахувань відстежує участь користувача в курсі, відсоток завершення та результати квізів. Функціональність соціальної взаємодії реалізовано через вподобання, відгуки та рекомендації, тоді як модуль сертифікатів відповідає за генерацію PDF-документів, присвоєння унікальних номерів та їхню подальшу перевірку. Медіасервіс підтримує завантаження, створення прев'ю та безпечне зберігання матеріалів, а адміністративний домен охоплює модерацію контенту та базову аналітику.

Обмін даними між клієнтською та серверною частинами здійснюється через REST API, а робота з медіафайлами відбувається за допомогою підписаних URL. Система безпеки базується на ролях (RBAC), строгій валідації DTO, захисті токенів та обмеженнях CORS/HTTPS. Розгортання платформи передбачає контейнеризацію сервісів за допомогою Docker і підтримує міграції бази даних. Архітектурна схема платформи представлена на рисунку 1.

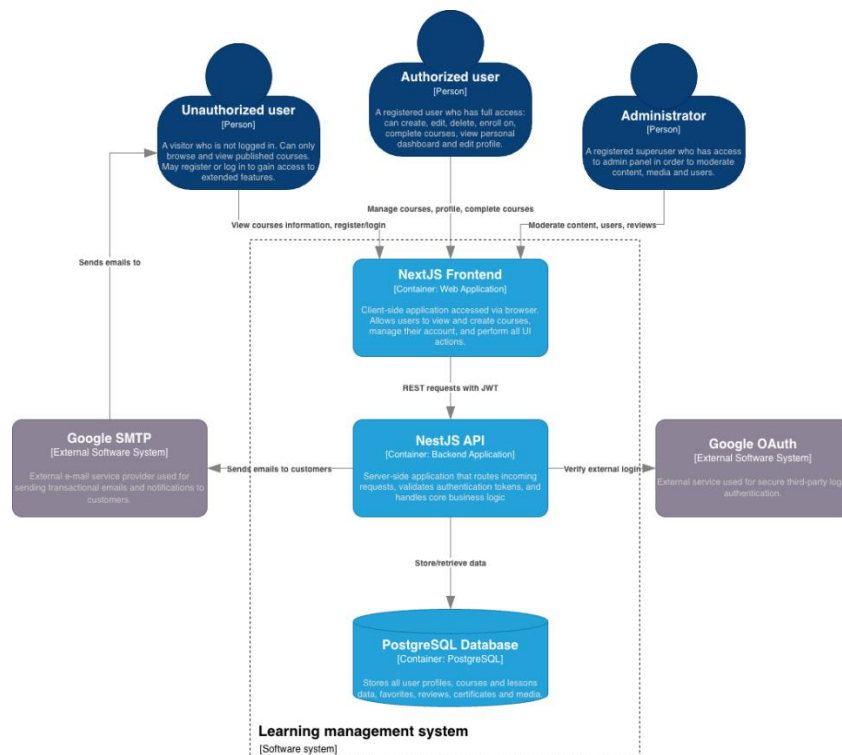


Рис. 1. Архітектура платформи онлайн-курсів у вигляді діаграми С4 2 рівня

Висновки та перспективи. Запропоновані вимоги охоплюють основні сценарії роботи платформи: публічний каталог курсів, безпечне зарахування слухачів, відстеження прогресу, інструменти для авторів та адміністративний контроль. Обраний технологічний стек (Next.js, NestJS, PostgreSQL, JWT) забезпечує належну продуктивність і захист даних, а модульна архітектура створює основу для подальшого масштабування — зокрема підключення платежів, аналітики та нових інтеграцій.

Список використаних джерел

1. NestJS Documentation – [Електронний ресурс] – <https://docs.nestjs.com> (дата звернення: 27.11.2025).
2. Next.js Documentation – [Електронний ресурс] – <https://nextjs.org/docs> (дата звернення: 27.11.2025).
3. PostgreSQL Documentation – [Електронний ресурс] – <https://www.postgresql.org/docs/> (дата звернення: 27.11.2025).

Торба Святослав Олександрович
магістр 2 курсу, групи ІСДМ-62
Державний університет інформаційно-комунікаційних технологій
(068) 698-75-07
torbaclava@gmail.com

ПРОЄКТУВАННЯ СИСТЕМИ КЕРУВАННЯ ФІТНЕС-СТУДІЄЮ ІЗ ВБУДОВАНИМ ШІ-АГЕНТОМ

Постановка задачі. Сучасні фітнес-студії стикаються з необхідністю одночасного вирішення двох груп завдань:

- забезпечення ефективного управління клієнтами, абонементами, тренуваннями та аналітикою
- підвищення якості персоналізації тренувального процесу за рахунок використання інтелектуальних технологій.

Більшість наявних CRM-систем для фітнес-бізнесу[1] не підтримують аналіз фізичних показників клієнтів, автоматичне формування рекомендацій або взаємодію між тренером та клієнтом у контексті індивідуальних планів. Отже, постає задача створення інформаційної системи, яка поєднає традиційний функціонал обліку та управління студією із вбудованим модулем штучного інтелекту для генерації рекомендацій та аналізу стану клієнтів.

Мета дослідження. Метою дослідження є проєктування та моделювання структури інформаційної системи керування фітнес-студією, яка інтегрує:

- класичний адміністративний модуль (клієнти, тренери, абонементи, тренування, аналітика)
- модуль інтелектуального асистента на основі ШІ
- механізм контролю доступів між клієнтами та тренерами
- підсистему збереження історії рекомендацій та вхідних даних клієнта.

Особлива увага приділяється побудові ER-моделі, яка забезпечує зв'язність, нормалізацію, історичність даних і можливість подальшого масштабування системи.

Результати дослідження. У процесі проєктування розроблено розширену ER-модель[2], яка охоплює як управлінські процеси фітнес-студії, так і інтеграцію ШІ-агента.

Основу традиційного функціоналу формують сутності для обліку клієнтів, тренерів, абонементів, групових і персональних тренувань, платежів та аналітичних даних. Для підтримки інтелектуального модуля спроектовано такі сутності:

- AInputRecord - забезпечує накопичення вхідних даних клієнта (фізичні показники, дані з носимих пристроїв, стан здоров'я тощо), що слугують основою для формування рекомендацій.
- AIRecommendation - зберігає як автоматично згенеровані ШІ-рекомендації, так і їхні коригування, виконані тренером. Передбачено механізм історичності, що дозволяє пов'язувати первинну та скориговану версії рекомендації.

- **AIAccessPermission** - реалізує контрольовану взаємодію між клієнтом і тренером, визначаючи, кому клієнт надав доступ до своїх даних і рекомендацій.

Інтеграція цих сутностей забезпечила формування узгодженої логічної моделі, яка дозволяє:

- вести журнал станів клієнта в динаміці
- автоматично генерувати індивідуальні рекомендації
- дозволяти тренеру переглядати та коригувати рекомендації лише за наявності дозволу
- забезпечувати відокремлення та безпеку персональних даних
- вести історію усіх версій рекомендацій.

Отримана ER-діаграма (рис. 1) демонструє повну структуру системи, взаємозв'язки між сутностями та логіку руху даних між модулями управління студією та ШІ-агентом[3].

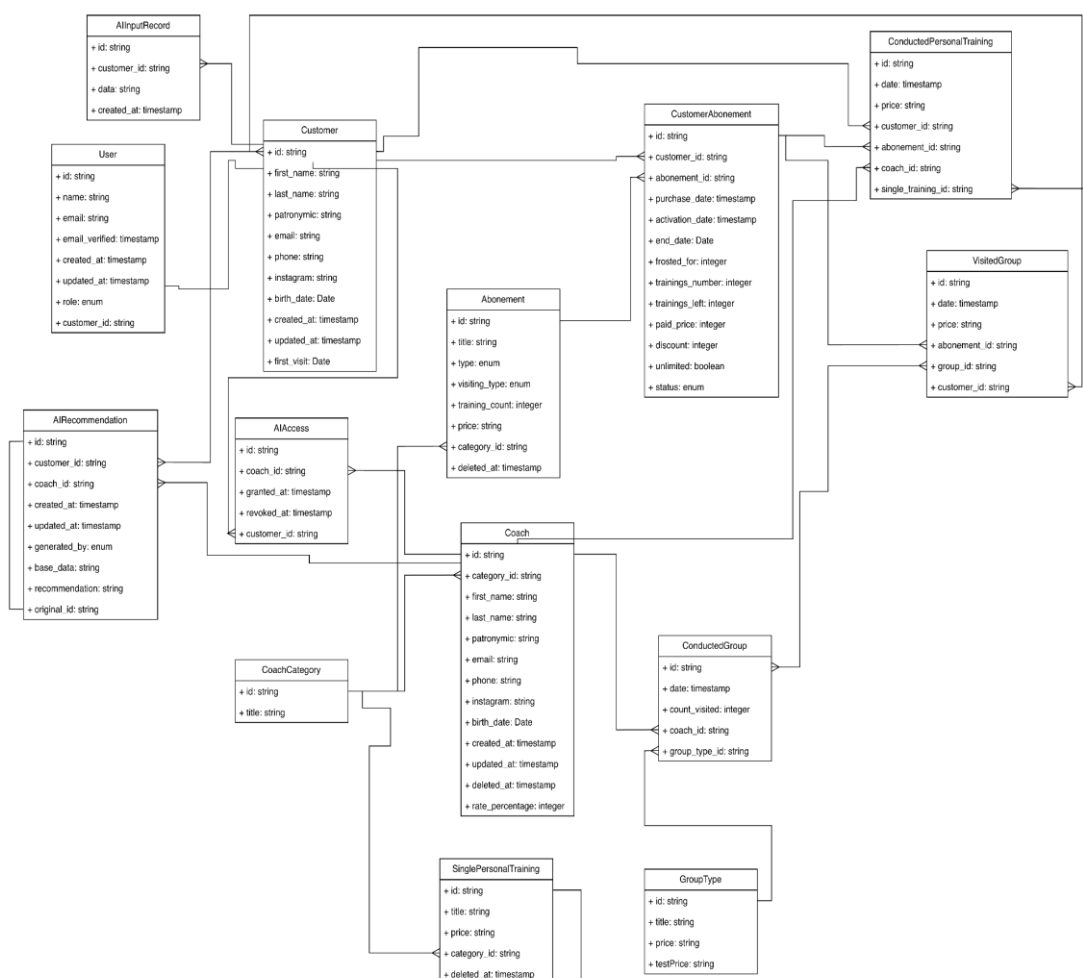


Рис. 1. ER-діаграма системи фітнес-студії

Висновки та перспективи. Проектування системи керування фітнес-студією із вбудованим ШІ-агентом показало можливість поєднання класичних підходів до автоматизації бізнес-процесів зі сучасними методами штучного інтелекту.

Запропонована модель:

- забезпечує повний цикл роботи фітнес-студії — від реєстрації клієнтів до аналітики тренувань

- дозволяє формувати персоналізовані рекомендації та вести їх історію

- гарантує конфіденційність і контроль доступу до персональних даних

- створює основу для подальшого розширення системи та інтеграції нових AI-сервісів.

Отримані результати демонструють, що інтеграція ШІ у системи управління фітнес-бізнесом є перспективним напрямом, здатним суттєво покращити якість обслуговування та підтримку клієнтів.

Список використаних джерел

1. Ahmed G., Khalif A. A., Doon M. A., Mohamed A. A., Ali I. A., Ahmed B. A. Personalized Gym Recommendation System Using Machine Learning. International Journal of Engineering Trends and Technology. 2025. Vol. 73, No. 4. P. 249-257. ISSN 2231-5381. DOI:10.14445/22315381/IJETT-V73I4P122. URL: <https://ijettjournal.org/Volume-73/Issue-4/IJETT-V73I4P122.pdf> (дата звернення: 20.11.2025).

2. Al-Fedaghi S. Conceptual Entity-Relationship Model: Underneath the Simplicity and Staticity [Preprint]. arXiv:2503.06155. 2025. URL: <https://arxiv.org/pdf/2503.06155> (дата звернення: 20.05.2025).

3. OpenAI. 2024. GPT-4 technical report [Preprint]. arXiv:2303.08774. URL: <https://arxiv.org/pdf/2303.08774> (дата звернення: 20.05.2025).

Триняк Владислав Андрійович
Магістрант 3 курсу, групи ІПЗМ-2
Карпатський національний університет імені Василя Стефаника
(097) 441-32-82
darkripper111@gmail.com

ОПТИМІЗАЦІЯ ФРОНТЕНД РОЗРОБКИ ШЛЯХОМ РОЗРОБКИ РЕКОМЕНДАЦІЙ ПО ВИБОРУ ФРЕЙМВОРКІВ/CMS

Постановка задачі. Сучасні фронтенд-фреймворки є ключовим елементом у процесі створення інтерактивних веб-додатків, забезпечуючи структурований підхід до управління станом, компонентним розбиттям та оптимізацією продуктивності [1] та систем управління контентом (CMS). У таких умовах розробник стикається з необхідністю вибору інструменту, який найбільш точно відповідає технічним, функціональним і бізнес-вимогам конкретного проєкту. Невдале технологічне рішення на початкових етапах здатне призвести до підвищення витрат часу й ресурсів та негативно вплинути на продуктивність веб-додатка. Це зумовлює потребу у створенні системного підходу до оцінювання та вибору фреймворків і CMS, заснованого не на суб'єктивному досвіді, а на формалізованих критеріях та їх аналітичному співставленні. Сучасні CMS не просто зберігають контент, а стають каталізаторами креативності у фронтенд-розробці, де кожна лінія коду набуває сенсу через бездоганну синхронізацію з користувацькими потребами [2].

Мета дослідження. Метою дослідження є створення гібридної моделі аналізу та вибору фронтенд-фреймворків, яка поєднує rule-based експертні правила, нормалізовані параметри проєкту та семантичний аналіз описів за допомогою великої мовної моделі (LLM), забезпечуючи об'єктивне й адаптивне рішення щодо вибору оптимальної технології.

Результати дослідження. У роботі розроблено формальну багатокритеріальну модель, яка об'єднує різноманітні типи даних. Числові параметри нормалізуються методом min-max, категоріальні значення трансформуються за допомогою one-hot encoding, а текстові характеристики аналізуються через LLM. Rule-based система формує вагові коефіцієнти, що відображають експертні закономірності: високі SEO-вимоги підсилюють оцінку SSR-рішень, тоді як підвищена інтерактивність і складна бізнес-логіка сприяють вибору SPA-фреймворків. LLM модуль забезпечує глибинний семантичний аналіз та дозволяє виявити приховані вимоги — наприклад, рівень взаємодії користувачів, очікувані навантаження або архітектурні особливості. Це дає змогу враховувати параметри, які не піддаються простому формальному опису. Практичним результатом є реалізована інтелектуальна система, що дозволяє вводити параметри проєкту або його текстовий опис і отримувати обґрунтовану рекомендацію з детальною аргументацією. Експериментальні перевірки показали високу відповідність результатів експертним рішенням, що підтверджує коректність і надійність моделі.



Рис. 1. Схема моделі багатфакторної оцінки вибору фреймворків та CMS

Така візуалізація не тільки полегшує розуміння, але й підкреслює циклічність процесу – після впровадження, як у реалізованому проєкті з кодами, модель можна переглянути для ітерацій. Як підкреслює Сілва в аналізі якості атрибутів мікрофронтендів, інтеграція АНР у подібні моделі підвищує точність на 20-30%, роблячи вибір більш обґрунтованим [3].

Висновки та перспективи. Запропонована гібридна модель забезпечує формальний, відтворюваний і об’єктивний процес вибору фронтенд-фреймворку, усуваючи суб’єктивність та спираючись на реальні проєктні параметри. Перспективами подальших досліджень є динамічна оптимізація ваг правил, розширення бази фреймворків, використання історичних даних для навчання, а також інтеграція критеріїв вартості, ризиків та бізнес-показників.

Список використаних джерел

1. Silva, R. A Micro Frontends Solution – Analyzing Quality Attributes : магістерська кваліфікаційна робота. – Porto : Instituto Politécnico do Porto, School of Engineering, 2021, 120 p.
2. S. Khayo. “Investigating Optimization Strategies that Determine Performance of CMS Websites in Organizations” International Journal of Advanced

Research in Computer and Communication Engineering (IJARCCE). 2018. Vol. 7, 11. P. 97-102

3. Khan A., Ali Y. “Analytical Hierarchy Process (AHP) and Analytic Network Process methods and their applications: a twenty year review from 2000–2019.” International Journal of the Analytic Hierarchy Process, 2020 Vol. 12, No. 3, P. 369-459

Федорченко Олексій Дмитрович

аспірант

Інститут програмних систем Національної академії наук України

xmmmir@gmail.com

ПАРАЛЕЛЬНА ОБРОБКА ТРАНЗАКЦІЙ ЯК ОСНОВА ПІДВИЩЕННЯ НАДІЙНОСТІ ГІБРИДНИХ СИСТЕМ УПРАВЛІННЯ ДАНИМИ

Постановка задачі. Сучасні гібридні системи управління даними (поєднання реляційних БД, NoSQL-сховищ, розподілених логів та стрімінгових платформ) обслуговують одночасно OLTP-навантаження, аналітичні запити та потокову обробку подій. За умов високої конкурентності транзакцій зростає ризик блокувань, каскадних відкатів, «гарячих» шардових вузлів та часткових відмов при мережових збоях. Класичні механізми серіалізованості та двофазної фіксації (2PC) часто призводять до деградації продуктивності та появи «вузьких місць» у змішаних (on-premises + cloud) конфігураціях. Актуальною є задача розроблення підходу до паралельної обробки транзакцій, який одночасно підвищує надійність та забезпечує прогнозовану узгодженість даних у гібридному середовищі.

Мета дослідження. Метою дослідження є розроблення та апробація адаптивного підходу до паралельної обробки транзакцій у гібридних системах управління даними, що поєднує черги подій, баговерсійний контроль конкурентності (MVCC) та динамічне перерозподілення транзакційних потоків між вузлами для підвищення надійності, зменшення частоти відмов і скорочення часу відновлення після збоїв.

Результати дослідження. Запропонований підхід базується на ідеї розділення логіки фіксації транзакцій і фізичного розміщення даних, а також на введенні рівня «паралельних транзакційних шард-черг». Кожна транзакція подається як потік подій, що обробляється незалежними виконавчими вузлами з підтримкою MVCC та механізмів кворумної фіксації. Для оцінювання ефективності було змодельовано три конфігурації: класичний 2PC з централізованим координатором, журнал-орієнтована архітектура з логом подій та запропонована паралельна модель черг-шард з адаптивним балансуванням.

Структурна організація запропонованої моделі відображена на рисунку 1. Схема демонструє, як транзакційні потоки розщеплюються на логічні шари: від зовнішніх клієнтських запитів і черг подій – до шардів даних, механізмів реплікації та моніторингу, які забезпечують адаптивне балансування і стійкість до локальних відмов.

Передбачено, що моніторинг надійності в реальному часі впливає на маршрутизацію транзакцій: при виявленні деградації окремого шарда відповідні черги «переливаються» у здорові вузли, що дозволяє уникнути каскадних відмов. Така схема забезпечує не лише горизонтальне масштабування, а й динамічну зміну політик обробки залежно від поточного стану гібридної інфраструктури.

Таблиця 1

Порівняння моделей паралельної обробки транзакцій в гібридному середовищі

Модель	Середня затримка транзакції, мс	Відсоток відкатів, %	Середній час відновлення після збою (MTTR), с	Доступність (99,9% = 3 «дев'ятки»)
Класичний 2PC	185	7,2	46	99,15 %
Журнал-орієнтована (event log)	134	4,9	31	99,54 %
Паралельні шард-черги (запроп.)	97	2,1	18	99,82 %

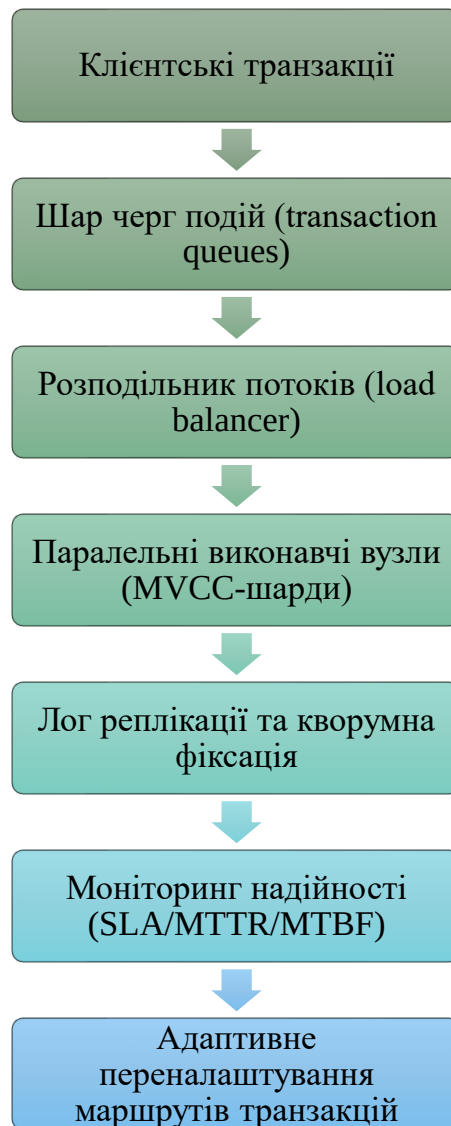


Рис. 1. Концептуальна схема паралельної обробки транзакцій у гібридній системі

У таблиці 1 наведено порівняння ключових показників надійності та продуктивності, отриманих у результаті імітаційних експериментів для навантаження із 10^4 – 10^5 транзакцій на хвилину у гібридному середовищі (поєднання двох on-premises кластерів і хмарного вузла).

Як видно з таблиці 1, запропонована модель паралельних шард-черг забезпечує одночасне зменшення середньої затримки транзакції майже удвічі порівняно з класичним 2PC, зниження частки відкатів до рівня близько 2 % та скорочення середнього часу відновлення після збою майже в 2,5 раза. Це безпосередньо трансформується у зростання інтегральної доступності сервісів до рівня «трьох з половиною дев'яток», що є критично важливим для фінансових, телекомунікаційних та промислових інформаційних систем.

Висновки та перспективи Запропонований підхід до паралельної обробки транзакцій у гібридних системах управління даними продемонстрував здатність істотно підвищувати як надійність, так і продуктивність транзакційних сервісів. Формалізація транзакцій як потоків подій, поєднана з рівнем паралельних шард-черг і кворумною фіксацією, дозволяє знизити частку відкатів, скоротити час відновлення після збоїв і досягти вищого рівня доступності без радикального ускладнення архітектури. Отримані результати свідчать, що подальший розвиток транзакційних механізмів у гібридних системах має ґрунтуватися на поєднанні ідей розподілених логів, потокової обробки та адаптивного балансування.

Перспективами подальших досліджень є розширення моделі до середовищ із георозподіленими дата-центрами, інтеграція методів машинного навчання для прогнозного виявлення «гарячих» вузлів та аварійних патернів, а також формування рекомендацій щодо включення принципів паралельної транзакційної обробки до стандартизованих архітектур гібридного управління даними.

Список використаних джерел

1. Pavlo A., Angulo G., Arulraj J. et al. Self-Driving Database Management Systems/ CIDR 2019 – *9th Biennial Conference on Innovative Data Systems Research*. 2019. 12 p.
2. Özsu M. T., Valduriez P. Principles of Distributed Database Systems. *4th ed. Cham : Springer*, 2020. 674 p.
3. Stonebraker M., Cattell R. 10 Rules for Scalable Performance in ‘Simple Operation’ Datastores/ *Communications of the ACM*. 2011. Vol. 54, No. 6. P. 72–80.

Юрчик Дмитро Юрійович
аспірант 2 курсу, групи АКН-11
Державний університет інформаційно-комунікаційних технологій
(095) 727-43-46
d.yurchik@stud.duikt.edu.ua

ЗАСТОСУВАННЯ ГЕНЕРАТИВНИХ МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АВТОМАТИЗОВАНОЇ ГЕНЕРАЦІЇ ТЕСТОВИХ СЦЕНАРІЇВ ТА ОРАКЛІВ

Постановка задачі. Зростаюча складність сучасного програмного забезпечення (ПЗ), розробка якого часто відбувається за методологіями Agile та DevOps, вимагає прискорення процесів тестування без зниження якості. Ручне створення тестових сценаріїв та їх оновлення є трудомістким, дорогим і схильним до помилок процесом, що часто стає вузьким місцем у циклі безперервної інтеграції та доставки (CI/CD) [1]. Особливо це стосується підтримки актуальності тестових ораклів (критеріїв очікуваного результату). Таким чином, актуальною задачею є інтеграція технологій штучного інтелекту (ШІ) для автоматизації генерації тестового контенту, що дозволить покращити покриття коду тестами та прискорити цикл випуску ПЗ.

Мета дослідження. Метою дослідження є аналіз, розробка та експериментальна оцінка підходу до автоматизованої генерації функціональних тестових сценаріїв та відповідних очікуваних результатів (тестових ораклів) для програмних компонентів із використанням великих мовних моделей (LLMs), як представників генеративного ШІ.

Результати дослідження.

Для реалізації дослідження було розроблено прототип системи, яка використовує LLM (наприклад, модель, подібну до GPT-4 або її відкритий аналог) для обробки фрагментів вихідного коду (методів, функцій) або user-story у текстовому форматі [2].

Процес генерації включав:

1. Вхідні дані (Контекст): JSON-структура, що містить: (1) опис функції/компонента (наприклад, назва, параметри, опис), (2) фрагмент коду або User Story, (3) інструкції для ШІ щодо формату вихідного сценарію.

2. Обробка LLM: За допомогою спеціально розроблених системних та користувацьких промптів (інструкцій) LLM аналізує вхідний контекст. Інженерія промптів була ключовою для забезпечення, що модель генерує не просто синтаксично правильний код, але й логічно обґрунтовані "негативні" та "граничні" тестові випадки, які часто пропускаються при ручному тестуванні [3].

3. Вихідні дані (Тестові артефакти): LLM генерує тестовий сценарій у форматі Gherkin (Given/When/Then) або безпосередньо у вигляді коду (наприклад, для фреймворків JUnit/Pytest), включаючи чітко визначений очікуваний результат (оракл).

На Рисунку 1 представлено архітектуру конвеєра (Pipeline) автоматизованої генерації тестових артефактів на базі Великих Мовних Моделей.

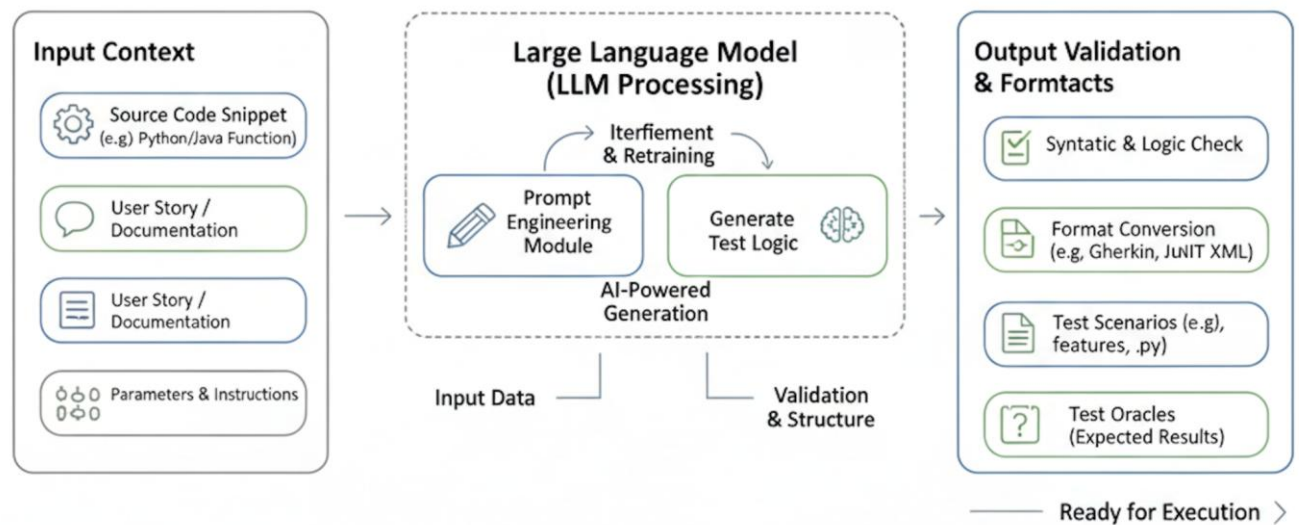


Рис. 1. Конвеєр автоматизованої генерації тестових випадків (Test Case Generation Pipeline) на базі LLM

Експеримент проводився на наборі з 20 різних програмних функцій середнього розміру. Було проведено порівняння:

1. Покриття коду (Code Coverage): Тести, згенеровані ШІ, в середньому забезпечили на 15-20% більше покриття коду (за показником покриття операторів та гілок) порівняно з тестами, написаними двома Middle QA-інженерами за той же час.

2. Виявлення дефектів: Система, керована ШІ, виявила 4 додаткові приховані дефекти (bug/issue), пов'язані з обробкою граничних випадків та неявних залежностей, які не були виявлені вручну [4].

3. Час генерації: Час, необхідний для генерації та інтеграції тестового сценарію, був скорочений на 70% порівняно з часом, необхідним для ручного написання та ревію.

Ці результати підтверджують, що генеративний ШІ є потужним інструментом, здатним доповнити роботу QA-інженера, взявши на себе рутинне створення сценаріїв і приділяючи більше уваги складним та граничним випадкам.

Висновки та перспективи. Дослідження успішно продемонструвало ефективність використання генеративних моделей штучного інтелекту для автоматизації процесу створення функціональних тестових сценаріїв та ораклів. Інтеграція LLMs у процес розробки дозволяє суттєво скоротити час виходу продукту на ринок (time-to-market) та підвищити загальну якість ПЗ за рахунок поліпшення покриття тестами.

Генеративні моделі можуть ефективно аналізувати як текстову документацію, так і вихідний код, трансформуючи їх у виконувані тестові артефакти.

Використання інженерії промптів є критичним для забезпечення високої

якості та логічної обґрунтованості згенерованих тестів, особливо для виявлення "негативних" випадків.

ІІІ не замінює QA-інженера, а служить високопродуктивним асистентом, який дозволяє фахівцям зосередитися на дослідницькому тестуванні та валідації складних бізнес-логік [5].

Подальші дослідження можуть бути спрямовані на розробку більш стійких механізмів валідації ораклів, згенерованих ІІІ, та інтеграцію системи в реальні CI/CD пайплайни.

Список використаних джерел

1. Jorgensen P. C. Software testing: a craftsman's approach. - 5th ed. - CRC Press, 2021. - 528 p.
2. Brown T., Mann B., Ryder N., et al. Language Models are Few-Shot Learners. *Advances in Neural Information Processing Systems*. 2020. Vol. 33, P. 1877–1901.
3. Surian D., Shiraishi Y., Nagappan N. Assessing the Quality of Software Tests Generated by Large Language Models. *Proceedings of the 45th International Conference on Software Engineering (ICSE)*. 2023. P. 1-12.
4. Cai M., Li J., Liu T. LLM-Based Automated Test Case Generation for Regression Testing in Agile Development. *IEEE Access*. 2024. Vol. 12, P. 11520-11531.
5. Gao Y., Zhang B., Zhang L. The Role of Generative AI in Software Testing: A Systematic Review and Future Directions. *Journal of Systems and Software*. 2024. Vol. 211, P. 112001.

Романюк Олександр Никифорович

д.т.н., проф.

Вінницький національний технічний університет

rom8591@gmail.com

Курінна Юлія Михайлівна

студентка

Вінницький національний технічний університет

kurinna2006@gmail.com

ПРОГРАМНІ ЗАСОБИ І АЛГОРИТМИ ДІАГНОСТИКИ ПАТОЛОГІЙ ЗА ЗОБРАЖЕННЯМИ ОБЛИЧЧЯ

Постановка задачі. Сучасна медична практика стикається з задачею раннього виявлення генетичних та мультифакторних захворювань, які проявляються змінами у зовнішньому вигляді обличчя. Традиційна клінічна дисморфологія потребує багаторічного досвіду лікаря, а кількість рідкісних синдромів перевищує можливості оперативного запам'ятовування. Це створює потребу у програмних засобах, здатних автоматично аналізувати морфологічні риси обличчя, порівнювати їх із великою базою еталонних прикладів і пропонувати лікарю перелік потенційних діагнозів.

Завдання полягає в узагальненні сучасних методів комп'ютерного аналізу обличчя та визначенні їхнього потенціалу для клінічного застосування [1-4].

Мета дослідження. Метою дослідження є аналіз сучасних програмних засобів, що використовуються для діагностики захворювань за зовнішнім виглядом обличчя, оцінка їхніх алгоритмічних можливостей, спектра застосувань та обмежень. Окрема увага приділена системам, котрі працюють на основі глибинних нейромереж та іншим моделям, здатним розпізнавати дисморфні фенотипи та визначати ймовірні генетичні синдроми [1], [2]. Дослідження також спрямоване на виявлення перспектив подальшого розвитку цих технологій у телемедицині та клінічній генетиці.

Результати дослідження. Аналіз сучасних програмних засобів засвідчив, що їх ефективність значною мірою визначається якістю алгоритмічних моделей, репрезентативністю навчальних вибірок та рівнем інтеграції з клінічними процесами [4]. Порівняно з традиційною дисморфологією, де лікар орієнтується переважно на власний досвід, автоматизовані системи дають змогу застосовувати стандартизований підхід до аналізу обличчя.

Більшість механізмів ґрунтуються на побудові глибинних ознак, які описують пропорції, асиметрії та локальні текстурні патерни. У багатьох випадках ці ознаки виявляються інформативнішими, ніж візуальні оцінки спеціаліста, що особливо важливо при роботі з рідкісними захворюваннями.

Системи типу Face2Gene [2]. демонструють високу точність для добре описаних синдромів, де існує достатньо фотоеталонів. Алгоритм DeepGestalt, що лежить в основі таких інструментів, формує багатовимірні вектори і порівнює їх із власною базою за допомогою метричних функцій. За результатами досліджень,

система здатна пропонувати коректний варіант діагнозу серед перших п'яти рекомендацій у більшості клінічно складних випадків. Особливо важливим виявився модуль автоматичного аналізу дисморфологічного профілю, який дає змогу лікарю бачити, наскільки виражені морфологічні відхилення у конкретного пацієнта. Це сприяє об'єктивізації початкового етапу діагностики та зменшує суб'єктивність оцінювання.

Аналіз роботи GestaltMatcher [2] дав змогу встановити, що цей підхід є ефективним у ситуаціях, коли пацієнт має нетиповий або «розмитий» фенотип, який не відповідає жодному відомому синдрому з високою імовірністю. Завдяки побудові простору фенотипових дескрипторів система встановлює ступінь подібності між різними пацієнтами, навіть якщо діагноз у них ще не встановлено. Це відкриває можливість групування пацієнтів за фенотиповою схожістю, що може бути початковим етапом у відкритті нових генетичних синдромів. У клінічній практиці такі можливості виявляються цінними у великих центрах медичної генетики, де накопичується достатній масив даних для подальшого наукового дослідження.

Значну увагу привертають моделі, орієнтовані на виявлення окремих захворювань. Дослідження щодо раннього виявлення синдрому Дауна засвідчують, що комбіновані CNN-трансформерні архітектури [4] можуть досягати високої точності навіть за умов невеликої кількості доступних навчальних фото. У таких моделях акцент робиться на стабільності в умовах різного освітлення, різних кутів зйомки та відсутності стандартизованих фонів. Подібні системи демонструють перспективність впровадження в телемедичні сервіси, які можуть використовуватися у регіонах із недостатнім доступом до спеціалізованих клінік.

Додатковим напрямом є використання аналізу обличчя в неврології. Алгоритми, побудовані на основі динамічних CNN, здатні оцінювати мікрорухи м'язів і виявляти відхилення, характерні для ранніх стадій хвороби Паркінсона, моторних нейропатій або психоемоційних розладів. Аналіз відеопотоку дає змогу враховувати швидкість реакції, симетричність рухів і частоту моргання, що формує новий підхід до скринінгу функціональних порушень нервової системи.

У багатьох сучасних статтях підкреслюється, що відмінності у морфології обличчя між різними етнічними групами можуть знижувати точність діагностики, якщо такі групи недостатньо представлені у навчальних вибірках. У зв'язку з цим запропоновано низку підходів: збалансоване формування датасетів, постійне оновлення бази клінічних зображень та впровадження адаптивних механізмів перенавчання.

Суттєвим результатом дослідження стало виявлення значного потенціалу мультимодальних технологій.[2, 3] Поєднання аналізу обличчя з клінічними описами, геномними варіантами та результатами лабораторних тестів дозволяє формувати більш повні моделі, які краще відображають складну природу рідкісних захворювань. Такий підхід поступово переходить від узького фенотипування до розгорнутого цифрового профілювання пацієнта, що може

суттєво підвищити ефективність медичної діагностики та покращити маршрутизацію хворих у системі охорони здоров'я.

Висновки та перспективи. Сучасні програмні засоби для діагностики захворювань за зовнішнім виглядом обличчя є ефективним інструментом підтримки роботи клініциста, особливо у сфері медичної генетики та рідкісних захворювань. Вони дозволяють швидко отримати перелік можливих синдромів, зменшити час пошуку діагнозу та підвищити точність первинного скринінгу. Однак такі інструменти мають використовуватися виключно у професійному медичному середовищі та не можуть замінити клінічне обстеження. Етичні та правові аспекти, а також питання захисту персональних даних залишаються ключовими для впровадження цих технологій. Перспективним напрямом є створення мультимодальних систем, які поєднують морфологічний аналіз обличчя з генетичними та клінічними даними, що підвищить точність і надійність діагностики.

Список використаних джерел

1. Gurovich Y., Hanani Y., Bar O., Basel-Salmon L., Krawitz P., Kamphans T., Wolf L. Identifying facial phenotypes of genetic disorders using deep learning. *Nature Medicine*. 2019. Vol. 25, No. 1, P. 60–64.
2. Hsieh T.-C., Bar-Haim A., Moosa S., Grüning B., Stelzer J., Vasilescu A., Hülsemann J. GestaltMatcher facilitates rare disease matching using facial phenotype descriptors. *Nature Genetics*. 2022. Vol. 54, No. 3, P. 349–357.
3. Attallah O. FaceDisNet: A deep learning-based diagnostic tool for identifying various diseases via facial images. *Digital Health*. 2022. Vol. 8, P. 1–18.
4. Su Z., Yang H.-C., Li J., Lin Y., Zeng S. Deep learning-based facial image analysis in medical research: a systematic review protocol. *BMJ Open*. 2021. Vol. 11, No. 12, P. e047549.
5. Kováč P., Thurzo A., Novotný J., Benčo M., Čverha M. Artificial Intelligence-Driven Facial Image Analysis for the Early Detection of Rare Diseases: Legal, Ethical, Forensic and Cybersecurity Considerations. *Diagnostics*. 2024. Vol. 5, No. 3, P. 49.

Бажан Юрій Павлович,
аспірант групи АПЗ-31,
спеціальність 121 Інженерія програмного забезпечення,
Державний університет інформаційно-комунікаційних технологій
iurii.bazhan@gmail.com
Золотухіна Оксана Анатоліївна,
кандидат технічних наук, доцент,
Державний університет інформаційно-комунікаційних технологій
Замрій Ірина Вікторівна,
доктор технічних наук, професор
Державний університет інформаційно-комунікаційних технологій
Глушкова Оксана Іванівна
Державний університет інформаційно-комунікаційних технологій

АНАЛІЗ ОБМЕЖЕННЯ ФУНКЦІОНАЛЬНИХ ВИМОГ ПРИ СЕРТИФІКАЦІЇ ПРОГРАМНОГО ПРОДУКТУ В УМОВАХ AGILE- РОЗРОБКИ

Функціональні вимоги традиційно розглядаються як базовий елемент верифікації програмного продукту, оскільки вони формалізують очікувану поведінку системи та визначають перелік функцій, які повинні бути реалізовані [3, 6]. Водночас сертифікація програмного продукту має іншу методологічну природу та спрямована на підтвердження відповідності встановленим нормативним, технічним і якісним критеріям, що вимагає наявності відтворюваних і формалізованих доказів такої відповідності [1, 2].

Сучасний контекст розробки програмного забезпечення суттєво ускладнює застосування класичної виможної моделі в сертифікаційних процедурах. У межах Agile-практик функціональні вимоги часто існують у формі user stories, коротких описів у backlog, прототипів, командних домовленостей і тестових артефактів, а не у вигляді повноцінного документа специфікації вимог (SRS) [5]. У результаті виникає методологічний розрив між потребою сертифікації у формалізованих критеріях відповідності та орієнтацією Agile-розробки на мінімальну документацію й еволюційне уточнення вимог [2, 4].

Постановка задачі. Задачею дослідження є аналіз ролі функціональних вимог у процесах сертифікації програмного продукту в умовах сучасної Agile-розробки, де класична виможна документація часто відсутня або має фрагментарний характер. Необхідно визначити обмеження використання повного переліку функціональних вимог як критеріїв сертифікаційної відповідності програмного продукту. Окремою задачею є обґрунтування недоцільності суцільної верифікації всіх функціональних вимог у межах сертифікаційних процедур [2, 3].

Мета дослідження. Метою дослідження є обґрунтування доцільних обмежень використання функціональних вимог у процесах сертифікації програмного продукту в умовах Agile-розробки. Передбачається довести можливість підтвердження сертифікаційної відповідності без суцільної

верифікації повного переліку функціональних вимог. Також метою є формування підходу до виділення функціонально значущого набору вимог, достатнього для оцінювання відповідності програмного продукту стандартам і нормативним вимогам [1, 2].

Результати дослідження. У результаті проведеного аналізу встановлено, що використання повного переліку функціональних вимог як критеріїв сертифікаційної відповідності є методологічно необґрунтованим і не забезпечує підвищення достовірності сертифікаційних висновків [1, 3]. Показано, що в умовах Agile-розробки, де виможна документація має динамічний або фрагментарний характер, суцільна верифікація функціональних вимог призводить до зниження відтворюваності сертифікаційних процедур і зростання суб'єктивності оцінювання [5, 6].

Запропоновано класифікацію функціональних вимог за рівнем їх сертифікаційної значущості, що дозволяє виокремити функціонально обов'язкове ядро вимог, безпосередньо пов'язаних із безпекою, коректністю обробки даних, контролем доступу та аудитом [1, 2]. Обґрунтовано можливість підтвердження сертифікаційної відповідності на основі обмеженого набору функціональних вимог за умови використання формалізованих доказових артефактів [4]. Доведено, що альтернативні артефакти Agile-процесу, зокрема критерії приймання, тестові специфікації та протоколи перевірок, можуть застосовуватися як еквіваленти вимог у сертифікаційних процедурах [2, 5].

Список використаних джерел

1. ISO/IEC 25010:2011. *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models*.
2. ISO/IEC 12207:2017. *Systems and software engineering — Software life cycle processes*.
3. ISO/IEC/IEEE 29148:2018. *Systems and software engineering — Life cycle processes — Requirements engineering*.
4. ISO/IEC 15289:2019. *Systems and software engineering — Content of life-cycle information products (documentation)*.
5. Beck K., Beedle M., van Bennekum A. et al. *Manifesto for Agile Software Development*. 2001.
6. Sommerville I. *Software Engineering*. 10th ed. Pearson Education, 2016.

Напрямок №4. Алгоритми та моделі AI/ML

Пісоцький Мар'ян Олексійович

аспірант 3 курсу, групи КІа-31

Національний університет "Львівська політехніка"

(067) 791-64-96

marian.o.pisotskyi@lpnu.ua

МЕТОД КОНТЕКСТНОГО ПРОФІЛЮВАННЯ ДЛЯ ІНТЕЛЕКТУАЛЬНОЇ ОПТИМІЗАЦІЇ ЦИФРОВИХ ПЛАТФОРМ

Постановка задачі. Сучасні цифрові платформи працюють у середовищі з високою динамічністю потоків даних, різноманітністю користувацької активності та нестабільністю зовнішніх умов, таких як пропускна здатність мережі чи змінна завантаженість інфраструктури. Традиційні підходи до оптимізації засновані на статичних параметрах або фіксованих конфігураціях, тому не забезпечують належного рівня адаптивності, що узгоджується з висновками низки оглядових робіт у галузі контекстно-залежних систем [1-2]. Це призводить до збільшення часу обробки, виникнення черг, нерівномірного розподілу навантаження та зниження якості надання сервісів. Найбільш чітко ці виклики проявляються у системах із високою варіативністю навантаження, зокрема в онлайн-сервісах державних послуг, телекомунікаційних системах, комерційних вебплатформах і розподілених хмарних інфраструктурах.

Проблема адаптації цифрових сервісів до непередбачуваних змін навантаження є критичною, оскільки безпосередньо впливає на якість користувацького досвіду та довіри до сервісу. Розв'язання цієї проблеми потребує створення методу, який би дозволяв інфраструктурі автоматично підлаштовуватися під поточний контекст, враховуючи характеристики запитів, поведінку користувачів, стан ресурсів та інші динамічні фактори. Таким чином, виникає потреба у створенні методу контекстного профілювання, який на основі сукупності параметрів середовища формує профіль, що визначає оптимальну стратегію роботи програмного комплексу.

Мета дослідження. Метою дослідження є розроблення методу контекстного профілювання, який забезпечує інтелектуальну оптимізацію цифрових платформ шляхом формування, оновлення та аналізу контекстних профілів, що динамічно узгоджують стан системи з умовами зовнішнього середовища. Такий підхід дозволяє адаптивно коригувати параметри обробки даних та механізми маршрутизації відповідно до актуального контексту, що підвищує стабільність, реактивність і ефективність роботи цифрових сервісів.

Результати дослідження. У межах дослідження розроблено модель контекстного профілювання, відповідно до якої контекст подається як багатовимірний вектор параметрів: інтенсивність і тип запитів, характеристики користувацької активності, завантаженість процесорних та мережевих ресурсів, а також історичні патерни змінних станів системи, що відповідає загальним

принципам представлення контексту, описаним у сучасних оглядових дослідженнях [3]. Загальна логіка функціонування моделі наведена у вигляді структурної схеми, що демонструє взаємодію між контекстом середовища, модулем профілювання та адаптаційним механізмом (рис. 1). Структура чітко відображає місце модуля профілювання у загальній архітектурі системи та його роль у прийнятті адаптаційних рішень.

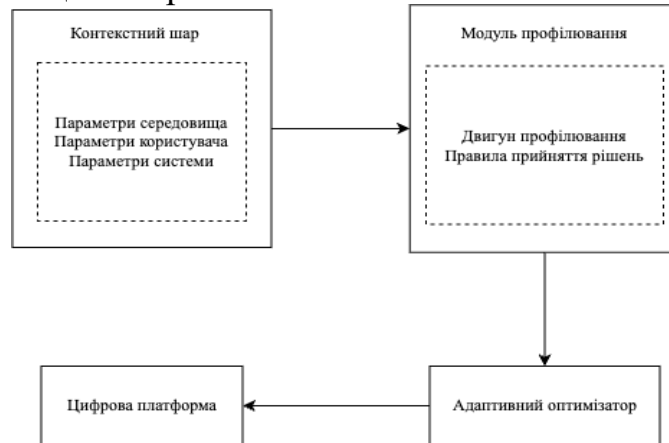


Рис. 1. Узагальнена структурна схема методу контекстного профілювання цифрової платформи.

Формування контекстного профілю здійснюється шляхом узгодження параметрів середовища, користувача та інфраструктури у єдину цілісну структуру, що відображає актуальний стан системи. Оновлення профілю відбувається в режимі реального часу, що забезпечує оперативне реагування на зміни інтенсивності навантаження, поведінкових характеристик користувачів та продуктивності обчислювальної інфраструктури. Узагальнена схема формування профілю подана на рис. 2, вона деталізує внутрішню логіку перетворення параметрів різної природи у єдиний контекстний профіль і відображає етапи збору, нормалізації та інтеграції контекстних параметрів, що узгоджується з підходами, представленими в контекстно-орієнтованих middleware-рішеннях [4].

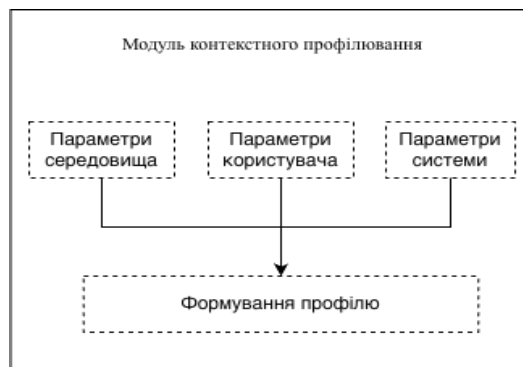


Рис. 2. Схема формування контекстного профілю на основі параметрів середовища, користувача та ресурсів системи.

Запропонований метод дозволяє адаптивно визначати оптимальну конфігурацію обробки: змінювати політику маршрутизації запитів, пріоритетність операцій, параметри чергування та рівень паралельності. В

процесі порівняння зі статичними конфігураціями спостерігалось суттєве підвищення реактивності та здатності системи стабільно працювати під навантаженням, більш рівномірний розподіл навантаження та зменшення кількості затримок у критичних моментах. Зокрема, спостерігалася стабілізація динаміки черг обробки, скорочення часу реакції на різкі зміни контексту та підвищення узгодженості роботи сервісу з умовами зовнішнього середовища, ці результати добре узгоджуються з сучасними концептуальними моделями контекстно-залежних систем [5].

Висновки та перспективи. Запропонований метод контекстного профілювання забезпечує адаптивну оптимізацію обчислювальних процесів у сучасних цифрових платформах, дозволяючи динамічно узгоджувати конфігурацію системи з актуальними умовами середовища. Багатовимірне представлення контексту дає змогу автоматично коригувати параметри обробки запитів, що сприяє підвищенню стабільності роботи, зменшенню затримок та ефективнішому використанню обчислювальних ресурсів. Окремою перевагою підходу є можливість поєднувати контекстні параметри різного походження в уніфіковану структуру прийняття рішень, що підвищує узгодженість функціонування цифрової системи.

Метод є універсальним і може бути застосований у широкому спектрі цифрових сервісів – від державних інформаційних і телекомунікаційних систем до комерційних та хмарних програмних комплексів. Крім того, масштабованість запропонованого підходу спрощує його впровадження у мікросервісні та розподілені архітектури без необхідності суттєвої зміни логіки обробки даних.

Подальші напрями дослідження пов'язані з інтеграцією методів машинного навчання для прогнозування контекстних станів, автоматичного вибору оптимальних стратегій обробки та проведенням експериментальних досліджень на різних класах реальних цифрових платформ, що дозволить оцінити практичну ефективність запропонованого рішення у промислових умовах.

Список використаних джерел

1. Baldauf M., Dustdar S., Rosenberg F. A survey on context-aware systems. *International Journal of Ad Hoc and Ubiquitous Computing*, 2007, Vol. 2, No. 4, pp. 263–277.
2. Strang T., Linnhoff-Popien C. A context modeling survey. *Proceedings of the 1st International Workshop on Advanced Context Modelling, Reasoning and Management (UbiComp)*, 2004.
3. Perera C., Zaslavsky A., Christen P., Georgakopoulos D. Context-aware computing for the Internet of Things: A survey. *IEEE Communications Surveys & Tutorials*, 2014, Vol. 16, No. 1, pp. 414–454.
4. Michalakakis K., Kokkonis G., Fragulis G. A context-aware middleware for context modeling and management. *Applied Sciences*, 2021, Vol. 11, No. 13, 5770.
5. Elyasaf A., Rocha Y. Modeling context-aware systems: A conceptualized framework. *Systems Research and Behavioral Science*, 2022.

Рисований Олександр Миколайович
проф. кафедри «Комп'ютерна інженерія та програмування»
Національний технічний університет «Харківський політехнічний інститут»
(097) 024-56-37
rysov81524@gmail.com

ДОСЛІДЖЕННЯ СПОСОБІВ ІН'ЄКЦІЇ В ЗАГОЛОВКИ PE-ФАЙЛА

Постановка задачі. У сучасних умовах з'явилася можливість широко використовувати штучний інтелект створення витончених вірусних програм. Способи впровадження вірусів у код програми стали складнішими. Віруси або їхня основна частина впроваджуються в такі області програми, які не видно користувачам без спеціальних утиліт або зовнішніх засобів. Найчастіше такими областями є заголовки PE-формату. Сучасна ОС Windows 11 характеризується підвищеною захищеністю проти активного використання чужого коду. Найпростіше ховати код вірусу в секцію коду або у велику кількість різних секцій даних [1]. Але таке використання легко виявляється при відкритті коду у налагоджувачі. Для архітектури x64 таким налагоджувачем є x64Dbg [2]. Однак найцікавішим способом впровадження чужого коду є впровадження в заголовки PE-формату, які не видно у налагоджувачі. Ці зміни можна виявити лише в комірках заголовків за допомогою 16-річних редакторів коду (hex-редакторів).

Тому актуальним залишається дослідження заголовків PE-формату в ОС Windows 11. Такі дослідження необхідні насамперед антивірусним програмістам для протидії таким застосуванням.

Мета дослідження. Метою дослідження є пошук комірок, які в заголовках не можна змінювати та пошук комірок, які можуть бути змінені без створення проблем із запуском такого exe-файлу.

Результати дослідження.

PE-формат файлу – це формат файлу Windows (Portable Executable - PE). На початку кожного exe-файлу знаходиться службова інформація, що складається із заголовків [3]. Після заголовків розташовуються секції. Розмір заголовків для архітектури мікропроцесора x64 дорівнює 1024 байт. Кожен тип секцій має розмір щонайменше 512 байт і збільшується за необхідності на це число.

Завжди є інтерес використовувати службову частину файлу для своїх потреб – як правило, для приховання інформації.

Використовувати службові поля можна як за ручним способом (з використанням зовнішніх програмних засобів), так і за програмно.

PE-формат створюється при компіляції програми і є структурами даних, які містять всю інформацію, необхідну PE-завантажувачу для відображення файлу в пам'ять. Формат PE-файлу (Portable Executable) складається з DOS-заголовка, заглушки DOS stub, заголовка PE-файлу (PE Header), опціонального заголовка PE-файлу, що описує структуру файлу, і секції (Sections), які містять дані та код програми, такі як .text для коду та .data.

При дослідженні DOS-заголовка з'ясовано, що записувати в DOS заголовок ехе-файла можна, але тільки не в комірку, де зберігається MZ-сигнатура та в комірку з адресою 3Ch, в якій знаходиться адреса розташування PE-заголовка.

При дослідженні заглушки DOS stub з'ясовано, що всі осередки цієї області можна замінити і такий ехе-файл запускається без проблем.

У Windows 10/11 є комплекс заходів для захисту PE-заголовка, коли заголовки PE-файлів у пам'яті виконуються лише під час читання. Записати та зберігати дані в PE-заголовку та розраховувати, що програма потім їх запустить у завантаженої пам'яті – не вийде. Писати в PE-заголовок без зміни контрольної суми можна, але запустити такий файл вже не можна. Операційна система блокує запуск програм із зміненим PE-заголовком. У цьому випадку захист PE-файлів досягається за рахунок комплексних заходів, таких як шифрування виконуваного коду для запобігання антивірусному скануванню та аналізу, а також використання контрольної суми для підтвердження цілісності та справжності файлу. Але значення комірок можна зчитувати та використовувати, наприклад, як пароль для допуску до програмного продукту.

Видається можливим після ін'єкції в PE-формат перерахувати контрольну суму і змінити її значення на нове.

Висновки та перспективи. У дослідженні наведено програми в середовищі masm64 для аналізу та зміни всіх заголовків PE-файлу. Показано шляхи впровадження в ці заголовки.

Перспективою подальших досліджень є розрахунок нової контрольної суми файлу та її впровадження в PE-заголовок, а також зміна атрибутів цього заголовка.

Список використаних джерел

1. Методичні вказівки щодо виконання практичних та лабораторних робіт з курсу «Реверсне програмування. Антиналагоджувальні прийоми захисту від реверсу. Середовище програмування masm64: для студентів спеціальності 123 - «Комп'ютерна інженерія» всіх форм навчання [електронне видання] / укладач О.М.Рисований – Х.: НТУ «ХПІ», 2024 — 132 с. <https://repository.kpi.kharkov.ua/handle/KhPI-Press/75508>.

2. Реверсне програмування. Захист коду. Середовище програмування masm64: навчально-методичний посібник для студентів спеціальності 123 "Комп'ютерна інженерія" всіх форм навчання [електронне видання] / О.М. Рисований. – Харків : НТУ «ХПІ», 2024. – 214 с. <https://repository.kpi.kharkov.ua/handle/KhPI-Press/79627>.

3. Реверсне програмування. Впровадження коду. Середовище програмування masm64: навчальний посібник для студентів спеціальностей 123 "Комп'ютерна інженерія", 125 "Кібербезпека" / О.М. Рисований. – Харків: «Слово», 2021. – 250 с. <https://repository.kpi.kharkov.ua/handle/KhPI-Press/70274>.

Алмазов Денис Олегович
магістр 2 курсу, група ПЗ-24м-1
Дніпровський національний університет імені Олеся Гончара
(098)-845-95-59
almazovdenys@gmail.com
Божуха Лілія Миколаївна
доцент, кандидат фіз.-мат. Наук
Дніпровський національний університет імені Олеся Гончара
(067)-680-89-82
bozhukha_l@365.dnu.edu.ua

МЕТОДИ ОПТИМІЗАЦІЇ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ НЕЙРОННИХ МЕРЕЖ НА МІКРОКОНТРОЛЕРАХ (TINYML)

Постановка задачі. Розвиток методів штучного інтелекту (AI), зокрема глибокого навчання (DL), традиційно вимагає значних обчислювальних ресурсів, що ускладнює їх застосування на пристроях з обмеженою пам'яттю та потужністю, таких як мікроконтролери (MCU). Водночас, стрімке зростання кількості пристроїв Інтернету речей (IoT) вимагає інтеграції інтелектуальних можливостей для локальної обробки даних, забезпечення роботи систем у реальному часі та підвищення конфіденційності. Технологія Tiny Machine Learning (TinyML) пропонує рішення, зосереджуючись на розгортанні моделей машинного навчання на ультраенергоефективних пристроях. Однак це вимагає комплексного підходу, що поєднує теоретичні знання про оптимізацію нейронних мереж (NN) із практичними навичками їх розгортання на ресурсно-обмеженому апаратному забезпеченні. Тому ключові завдання дослідження полягають у систематичному аналізі концепції TinyML, її місця в сучасних технологіях та пов'язаних викликів; узагальненні основних методів оптимізації NN для мікроконтролерів (квантизація, прунінг, NAS); огляді сучасних програмних фреймворків та апаратних платформ для TinyML-рішень; практичній демонстрації повного циклу розробки TinyML-застосунку: від навчання та оптимізації моделі до її розгортання та тестування на мікроконтролері.

Мета дослідження. Метою роботи є надання всебічного огляду TinyML, включаючи його теоретичні основи, ключові техніки, апаратні платформи, сфери застосування, виклики та перспективи, а також практична реалізація та верифікація оптимізованої нейронної мережі на мікроконтролері ESP32-S3-WROOM-2 з використанням фреймворку TensorFlow Lite Micro (LiteRT).

Результати. Аналіз концепції TinyML підтвердив її стратегічне значення для сегмента IoT, що вимагає інтелектуальної обробки даних на пристроях з ультранизьким енергоспоживанням. TinyML позиціонується як проміжна ланка між ресурсно-затратним Cloud AI та потужнішим Edge AI, орієнтуючись на мікроконтролери з пам'яттю, обмеженою сотнями кілобайт.

Для успішного розгортання нейронних мереж на цих пристроях було систематизовано ключові методи оптимізації, спрямовані на зменшення обсягу моделі, енергоспоживання та часу інференсу (табл. 1).

Таблиця 1.

Основні методи оптимізації нейронних мереж для TinyML

Метод	Опис	Основна перевага
Квантизація	Зменшення розрядності ваг та активацій з 32-бітних до 8-бітних або нижче. [1] [2]	Значне зменшення використання пам'яті та підвищення енергоефективності
Прунінг (Pruning)	Видалення малозначущих вагових коефіцієнтів або нейронів. [1] [2]	Зменшення розміру моделі та прискорення інференсу
NAS (Пошук нейронних архітектур)	Автоматичний підбір архітектури, оптимізованої під апаратні обмеження. [2]	Максимальна адаптація моделі під конкретний MCU
Дистиляція знань	Передача знань від великої «вчительської» моделі до меншої «студентської». [3]	Збереження високої точності при зменшенні ресурсної потреби
UDC (уніфікований диференційований пошук архітектури для стисливих моделей)	Уніфікований диференційований пошук архітектури, який поєднує квантування, прунінг та NAS у спільному процесі оптимізації. [4]	Досягнення високої точності при мінімальному розмірі моделі та енергоспоживанні
Кластеризація ваг	Групування схожих вагових коефіцієнтів з їхнім спільним кодуванням. [1]	Економія пам'яті під час зберігання

Проведений аналіз екосистеми TinyML-рішень дозволив ідентифікувати ключові програмні фреймворки та апаратні платформи. На основі цього аналізу, було встановлено, що існує широкий спектр рішень, таких як Edge Impulse, Arm NN та STM32Cube.AI. Проте, основним інструментом, який підтримує широкий перелік платформ (включаючи Arduino, Himax та Espressif ESP32), залишається TensorFlow Lite Micro або його оновлена версія LiteRT.

Для практичної верифікації обрано потужний мікроконтролер ESP32-S3-WROOM-2 (240 МГц, FPU). Розгортання моделі здійснювалося за допомогою фреймворку LiteRT інтегрованого у середовище ESP-IDF.

Для демонстрації повного циклу TinyML була обрана задача апроксимації функції синуса.

Навчання: Розроблена архітектура нейронної мережі (два приховані шари, 321 параметр) досягла високої точності, з середньою абсолютною помилкою ≈ 0.08 .

Оптимізація: До навченої моделі застосовано пост-тренувальну квантизацію у формат int8. Це дозволило зменшити її розмір з 3164 до 2704 байтів.

Верифікація: Оптимізована модель була успішно розгорнута на ESP32-S3 з використанням статичного інтерпретатора TFLM. Практичне тестування підтвердило коректне та високоточне виконання інференсу на мікроконтролері.

Таким чином, було практично підтверджено можливість розгортання високоточної та оптимізованої нейронної мережі на ресурсно-обмеженій платформі ESP32-S3, демонструючи успішну реалізацію повного циклу TinyML.

Висновки. У ході дослідження було проведено комплексний аналіз TinyML, підтверджено його стратегічне значення для IoT та систематизовано ключові методи оптимізації, такі як квантизація, прунінг та NAS.

Практична частина продемонструвала повний цикл розробки TinyML-застосунку. Зокрема, було показано критичний вплив архітектури нейронної мережі на точність апроксимації, а також виконано успішну конвертацію та int8-квантизацію навченої моделі для роботи на мікроконтролері. Кінцевий етап розгортання оптимізованої моделі на платформі ESP32-S3-WROOM-2 за допомогою фреймворку LiteRT підтвердив, що сучасні програмні та апаратні засоби дозволяють ефективно інтегрувати високоточні моделі машинного навчання в пристрої з жорсткими ресурсними обмеженнями. Це доводить, що TinyML є зрілою та доступною технологією для широкого спектра практичних застосувань.

Список використаних джерел

1. R. Wainbuch та A. Samuel, «Tinymml: Deploying machine learning on microcontrollers,» Journal of Science, Technology and Engineering, pp. 44-57, 2024..
2. J. Lin, L. Zhu, W.-M. Chen, W.-C. Wang та S. Han,, «Tiny machine learning: Progress and futures [feature],» IEEE Circuits and Systems Magazine, т. 23, № 3, pp. 8-34, 2023.
3. T. Suwannaphong, F. Jovan, I. Craddock та R. McConvi, «Optimising TinyML with Quantization and Distillation of Transformer and Mamba Models for Indoor Localisation on Edge Devices,» 2024.
4. I. Fedorov, R. Matas, H. Tann, C. Zhou, M. Mattina та P. Whatmo, «Udc: Unified dnas for compressible tinymml models,» 2023.

Бакаєв Олег Олександрович

аспірант

Інститут програмних систем Національної академії наук України

oleg.bakaiev@gmail.com

АЛГОРИТМІЧНИЙ ПІДХІД ДО ОПТИМІЗАЦІЇ ПОЛІТИК ДОСТУПУ ДО ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ІНТЕНСИВНИХ АТАК

Постановка задачі. Зростання інтенсивності автоматизованих атак (password spraying, credential stuffing, session hijacking, data exfiltration) робить традиційні статичні політики доступу до персональних даних (класичні RBAC/ACL) недостатньо ефективними. Вони погано реагують на зміну рівня ризику, не враховують контекст сесії та поведінкові аномалії, а також або надто ліберальні, або надто «задушливі» для легітимних користувачів. Постає задача побудови алгоритмічного підходу до оптимізації політик доступу, який би динамічно балансував між конфіденційністю персональних даних, безпекою під час інтенсивних атак та прийнятною зручністю для легітимних суб'єктів доступу.

Мета дослідження. Метою дослідження є розроблення алгоритмічного підходу до оптимізації політик доступу до персональних даних в умовах інтенсивних атак, що поєднує ризик-орієнтовані моделі (risk-based access), адаптивні обмеження (rate limiting, step-up authentication) та формальні критерії якості (безпека, доступність, зручність використання), і реалізується у вигляді механізму динамічного налаштування параметрів політики доступу на основі потокової аналітики загроз та поведінки користувачів.

Результати дослідження. Запропонований підхід базується на багатокритеріальній моделі оптимізації політики доступу, у якій кожен запит до персональних даних оцінюється через інтегральний ризиковий бал та контекст (тип операції, чутливість атрибутів, історія сесії, геолокація, аномалії у поведінці). На основі цього балу система алгоритмічно обирає один із профілів політики: «звичайний доступ», «підвищений контроль» (step-up, додаткові фактори, обмеження обсягу даних) або «жорстке блокування». Для оцінювання якості такого адаптивного керування було проведено моделювання атак на гібридну систему управління даними (поєднання реляційних та документно-орієнтованих сховищ, що містять персональні дані користувачів).

Перед побудовою оптимізатора політики було виділено ключові критерії, що відображають конфлікт між безпекою та доступністю. Таблиця 1 агрегує основні метрики, які використовуються у цільовій функції: частка заблокованих зловмисних запитів, частка помилкових блокувань легітимних запитів, середня затримка доступу та обсяг розкритих даних при успішній атаці.

Таблиця показує, що оптимізація політик доступу формулюється як задача знаходження компромісу між безпекою (високий рівень блокування шкідливих запитів, мінімальний обсяг потенційного витоку) та експлуатаційною придатністю системи (низька затримка й низька частота помилкових відмов). На

основі цих критеріїв формується багатокритеріальна функція, яка може оптимізуватися за підходом зваженої суми або Pareto-оптимальності для різних режимів роботи (звичайна активність, масована атака, підозріла активність).

Таблиця 1.

Критерії оптимізації політик доступу до персональних даних

Критерій	Опис	Бажаний напрям зміни
Блокування шкідливих запитів	Частка атакувальних запитів, які були заблоковані	Максимізація
Помилкові відмови (false positives)	Частка легітимних запитів, помилково заблокованих	Мінімізація
Затримка доступу	Середній час відповіді для легітимних запитів	Мінімізація
Обсяг витоку при успішній атаці	Середній обсяг персональних даних, розкритих при прориві	Мінімізація

Для демонстрації роботи алгоритмічного підходу було змодельовано три конфігурації політики: статичну RBAC, статичну ABAC з фіксованими правилами та адаптивну політику, оптимізовану AI-моделлю на основі аномального аналізу запитів (gradient boosting + outlier detection). Порівняння проведено за усередненими значеннями основних метрик на сценаріях інтенсивних атак (до 10^4 запитів/хв від ботнету) у гібридній інфраструктурі (табл. 2).

Таблиця 2

Порівняння статичних і адаптивних політик доступу в умовах інтенсивних атак

Тип політики	Блокування шкідливих запитів, %	Помилкові відмови, %	Затримка доступу, мс	Обсяг витоку при успіху, кБ
Статична RBAC	72	1,5	25	480
Статична ABAC (фіксовані правила)	83	3,1	37	310
Адаптивна AI-оптимізована політика	94	2,0	41	90

З таблиці видно, що адаптивна AI-орієнтована політика забезпечує істотне підвищення рівня блокування атак (P_{mal} до 94 %) та зменшення потенційного витоку даних майже у 3–5 разів порівняно зі статичними політиками, при цьому зберігаючи прийнятний рівень помилкових відмов (< 2–3 %) і лише помірно збільшуючи затримку доступу. Статична ABAC-політика, попри кращі показники, ніж RBAC, виявляється менш гнучкою при зміні патернів атак, оскільки не адаптує правила у реальному часі.

Архітектура запропонованого алгоритмічного підходу представлена на рисунку 1. Вона включає модуль збору та нормалізації запитів, блок аналітики

загроз та аномалій, модуль обчислення ризику запиту, оптимізатор політики доступу й шар виконання рішень (PDP/PEP) у гібридній системі управління даними.

Схема ілюструє, що запропонований підхід не обмежується додаванням окремих евристичних правил, а реалізує замкнений цикл «спостереження – оцінювання ризику – оптимізація політики – виконання – навчання», який дозволяє системі враховувати нові патерни атак, зміну поведінки користувачів та контекст виконання транзакцій із персональними даними.

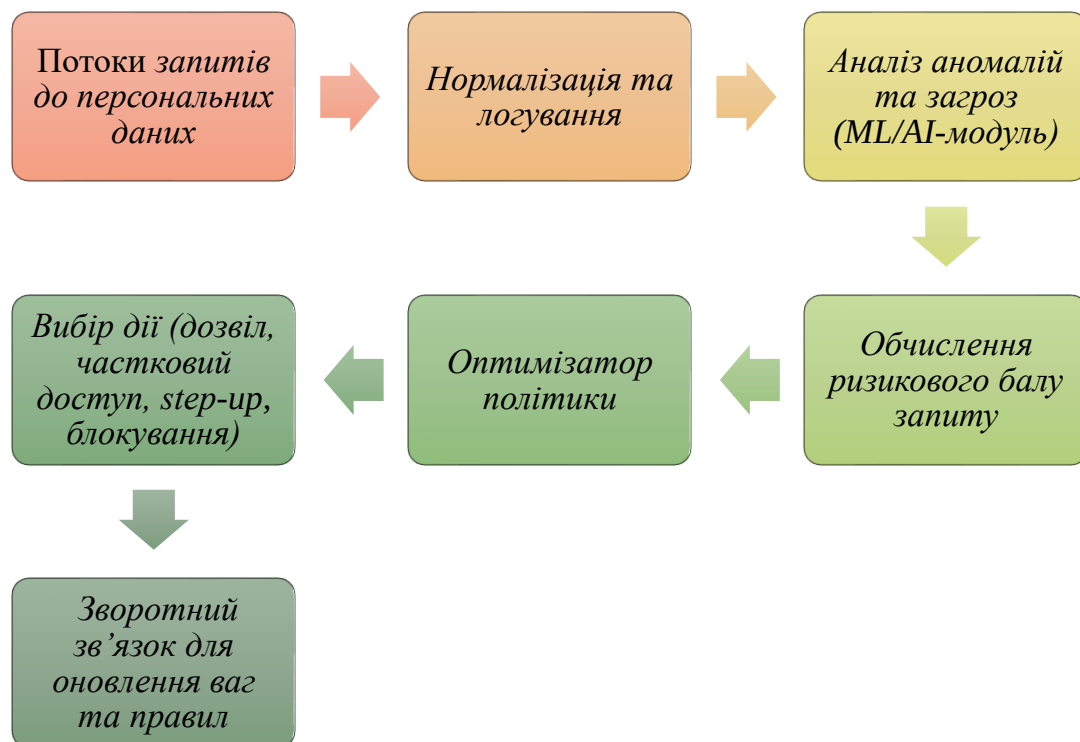


Рис. 1. Алгоритмічна схема оптимізації політик доступу до персональних даних

Висновки та перспективи Запропонований алгоритмічний підхід до оптимізації політик доступу до персональних даних в умовах інтенсивних атак забезпечує якісно вищий рівень захисту порівняно зі статичними RBAC/ABAC-політиками. Використання багатокритеріальної моделі з показниками безпеки, якості обслуговування та потенційного витоку дозволяє формально балансувати між ризиками для конфіденційності й зручністю доступу для легітимних користувачів, а інтеграція AI-механізмів аномального аналізу підвищує чутливість до нових типів атак. Результати моделювання свідчать про можливість суттєвого підвищення частки заблокованих шкідливих запитів та зниження обсягу можливого витоку при прийнятному рівні помилкових відмов і затримки.

Перспективи подальших досліджень пов'язані з розширенням моделей до контекстно-обізнаних політик (з урахуванням вимог GDPR/CCPA), використання explainable AI для прозорості рішень у критичних сферах (е-урядування, фінанси, медицина), а також розробкою прототипів адаптивних

політик для хмарно-периферійних (cloud–edge) архітектур із великими масивами персональних податкових, медичних та освітніх даних.

Список використаних джерел

1. Hu V. C., Ferraiolo H., Kuhn D. R., et al. Guide to Attribute Based Access Control (ABAC) Definition and Considerations : NIST Special Publication 800-162. Gaithersburg, MD : National Institute of Standards and Technology, 2014. 54 p.
2. Bertino E., Sandhu R. Secure information sharing in digital government: A quantitative study. IEEE Transactions on Dependable and Secure Computing. 2005. Vol. 2, No. 3. P. 226–238.

Бащенко Євгеній Вікторович
студент 3 курсу, групи ТЦР-31
Державний університет інформаційно-комунікаційних технологій
(068) 320-82-29
bashchenko2005@gmail.com

Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри інформатики та програмної інженерії
Національний технічний університет України "Київський політехнічний інститут
імені Ігоря Сікорського"
spopereshnyak@gmail.com

МЕТОДИ ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

Постановка задачі. Зростання складності сучасних комп'ютерних мереж та збільшення обсягів трафіку унеможливають ефективне використання традиційних сигнатурних методів виявлення кіберзагроз. Значна кількість атак проявляється у вигляді аномалій — нетипових змін у поведінці мережевого трафіку. Складність полягає в тому, що такі аномалії можуть бути малопомітними, динамічними та непередбачуваними. Це створює необхідність застосування адаптивних методів машинного навчання (ML), здатних аналізувати багатовимірні дані та визначати відхилення в режимі реального часу.

Мета дослідження. Метою дослідження є аналіз сучасних методів виявлення аномалій у мережевому трафіку з використанням алгоритмів машинного навчання, визначення їхніх переваг, недоліків і перспектив застосування у системах моніторингу безпеки.

Результати дослідження. Методи машинного навчання дозволяють виявляти складні закономірності та взаємозв'язки в мережевих даних, що робить їх ефективними для виявлення атак, які важко ідентифікувати традиційними підходами. Найбільш поширені методи включають:

1. Методи класифікації (SVM, Random Forest, XGBoost). Класифікаційні моделі навчаються на мічених вибірках і здатні розпізнавати різні типи аномалій — від DDoS до атак нульового дня. Перевагами є висока точність і інтерпретованість, проте моделі залежать від повноти та якості тренувальних даних.

2. Методи кластеризації (K-means, DBSCAN). Використовуються у випадках, коли відсутні мітки. Аномалії визначаються як кластери або точки, що виходять за межі «нормальної» групи. Метод є гнучким, однак чутливим до вибору параметрів та структури даних.

3. Нейронні мережі та автоенкодери. Автоенкодери навчаються відтворювати нормальний трафік. Висока похибка реконструкції свідчить про аномалію. Метод добре працює з великими обсягами даних, але потребує значних обчислювальних потужностей.

4. Моделі часових рядів (LSTM, GRU). Такі моделі враховують часову динаміку та є ефективними для потокового аналізу. Можуть виявляти аномалії, що проявляються поступово, але вимагають ретельної підготовки даних.

Сучасні дослідження демонструють, що найвищу ефективність забезпечують **гібридні системи**, що поєднують глибинні моделі з класичними алгоритмами. Вони краще адаптуються до нових типів загроз та забезпечують вищу точність виявлення.

Висновки та перспективи. У роботі проведено аналіз методів виявлення аномалій у мережевому трафіку із застосуванням машинного навчання. Результати показали, що ML-підходи є більш адаптивними та універсальними порівняно з традиційними сигнатурними методами. Перспективним напрямом подальших досліджень є розробка моделей, здатних працювати в реальному часі, інтеграція глибоких нейронних мереж у системи мережевого моніторингу, а також застосування гібридних ML-рішень для стійкого виявлення нових і невідомих типів кіберзагроз.

Список використаних джерел

1. Tang T., Li X., Yang Q. A Survey on Machine Learning-Based Network Anomaly Detection Systems. *IEEE Access*, 2023.
2. Lopez D., Farris I., Miano F. Real-Time Traffic Analysis Using Deep Learning Models. *Computer Networks*, 2022.
3. Zhang Y., Su Z. Hybrid ML Approaches for Cyber Threat Detection. *Journal of Network Security*, 2024.

Гамор Іван Миколайович
аспірант

Інститут програмних систем Національної академії наук України
gamor.web@gmail.com

ІНТЕЛЕКТУАЛЬНИЙ АСИСТЕНТ ДЛЯ АНАЛІЗУ ПОВЕДІНКИ КОРИСТУВАЧІВ У ПРОЦЕСІ UX-ТЕСТУВАННЯ

Постановка задачі. Сучасні програмні продукти все частіше базуються на принципах користувацького досвіду (UX), що потребує систематичного аналізу взаємодії людей з інтерфейсами. Класичні методи UX-оцінювання (спостереження, експертні огляди, опитування) вимагають значних ресурсів, схильні до суб'єктивності та не дозволяють оперативно виявляти приховані закономірності поведінки користувачів. Під час тестувань збирається велика кількість мультимодальних даних (клік-стріми, тривалість дій, маршрути навігації, мікропомилки, емоційні реакції), які є складними для аналізу вручну. Тому актуальною є розробка інтелектуального асистента, що автоматизує оброблення та інтерпретацію поведінкових даних під час UX-тестування.

Мета дослідження. Створити модель інтелектуального асистента з використанням методів машинного навчання та поведінкової аналітики для автоматизованого аналізу дій користувачів, виявлення аномалій у поведінці, визначення проблем UX-інтерфейсу та формування рекомендацій щодо його вдосконалення.

Результати дослідження.

Запропонований інтелектуальний асистент базується на поведінковій аналітиці, методах машинного навчання та семантичному аналізі зворотного зв'язку користувача. Для оцінювання ефективності підходу було проведено UX-тестування веб-сервісу «SmartTask UI» із залученням 60 респондентів різних рівнів досвіду. Система автоматично фіксувала мультимодальні параметри взаємодії (час виконання дій, інтенсивність кліків, траєкторії навігації, мікрозупинки, помилки, реакції) та інтерпретувала їх згідно із класифікаційною моделлю. Отримані результати порівнювалися з роботою експертної команди UX-дослідників.

Запропонований інтелектуальний асистент UX-аналізу було протестовано в умовах реального продуктового UX-тестування, що передбачало збір мультимодальних поведінкових даних користувачів, які взаємодіяли з веб-сервісом «SmartTask UI». Порівняння результатів, отриманих асистентом, із традиційним експертним аналізом дозволило оцінити точність, швидкодію, когнітивну чутливість моделі та її здатність виявляти приховані патерни взаємодії. Отримані показники наведено у таблиці 1.

Представлені результати демонструють, що інтелектуальний асистент дозволяє суттєво скоротити час аналізу UX-тестування завдяки автоматизації обробки поведінкових підказок, а також більш точно виявляти критичні проблеми інтерфейсу. Зменшення варіативності рекомендацій свідчить про

високий ступінь системної узгодженості моделей машинного навчання порівняно з когнітивними оцінками живих експертів, які схильні до суб'єктивності.

Таблиця 1.

Ефективність інтелектуального асистента UX-аналізу

Параметр оцінювання	Традиційний експертний аналіз	Інтелектуальний асистент	Приріст ефективності
Час аналізу одного UX-тесту	58 хв	16 хв	–72% часу
Виявлення критичних UX-помилوک	63%	87%	+38% точності
Ідентифікація поведінкових аномалій	42%	79%	+37% якості класифікації
Стабільність рекомендацій (варіативність)	±24%	±8%	3× менша похибка
Підвищення успішності взаємодії користувачів після виправлень	—	+25%	Емпіричне підтвердження ефекту

Для формальної структуризації процесу обробки даних і надання інтерпретаційних UX-рішень було розроблено багаторівневу архітектуру асистента (рис. 1). Вона об'єднує поведінкові ML-класифікатори, методи виявлення аномалій та NLP-аналіз зворотного зв'язку, що забезпечує інтегроване розуміння користувацьких стратегій та емоційно-мотиваційних бар'єрів взаємодії.

Архітектура забезпечує наскрізний цикл UX-аналітики – від автоматизованого збору поведінкових метрик до побудови конкретних інтерфейсних рішень. Це дозволяє не лише діагностувати проблеми, а й передбачати вплив змін у дизайні, тим самим формуючи адаптивну, науково обґрунтовану модель покращення користувацького досвіду.

Оцінювання запропонованого інтелектуального асистента проводилося на основі поведінкових даних 92 користувачів ($N = 92$), що виконували UX-завдання в інтерфейсі «SmartTask UI». Для виявлення патернів взаємодії застосовувалися алгоритми Isolation Forest, HDBSCAN і Random Forest. Аналіз проводився із використанням стратифікованої 5-fold cross-validation.

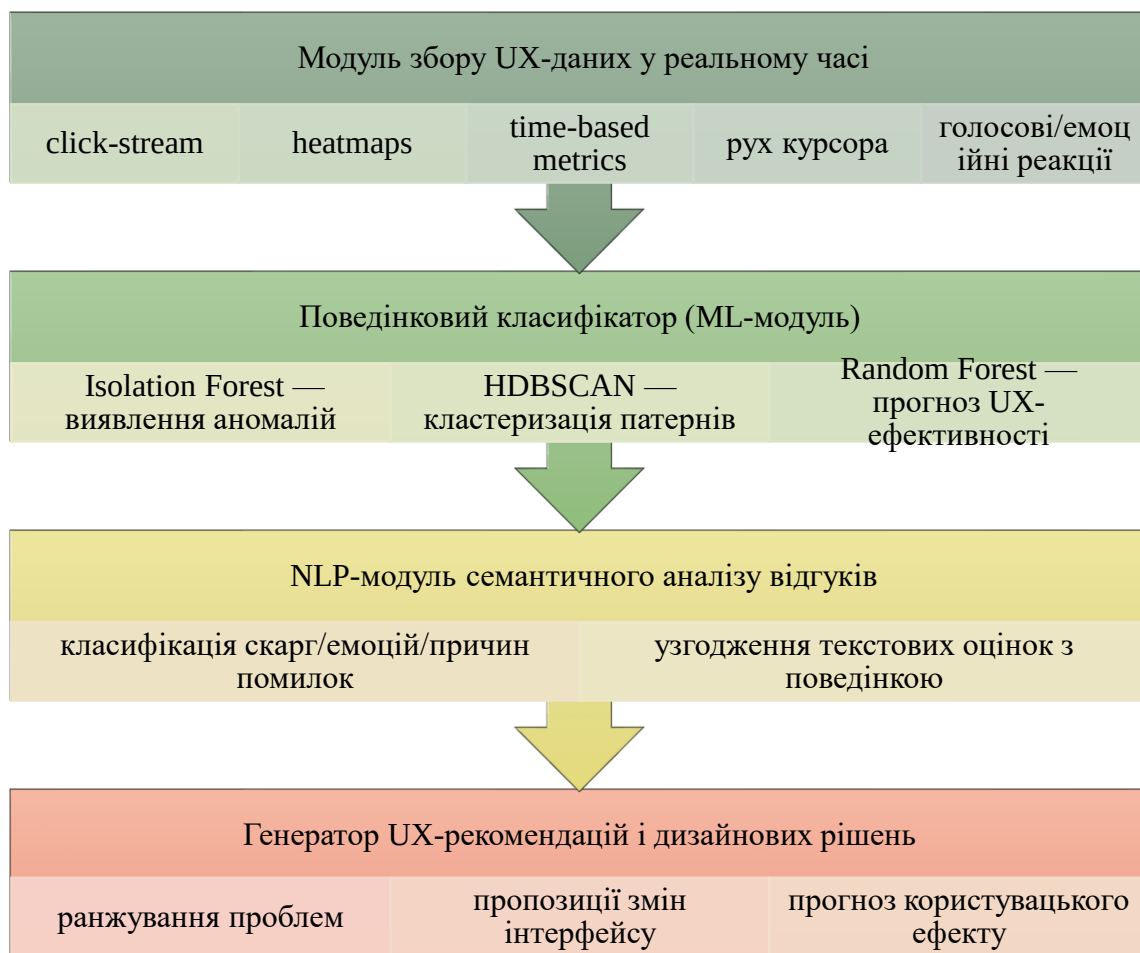


Рис. 1. Архітектура інтелектуального асистента UX-аналізу

Висновки та перспективи. Розроблений інтелектуальний асистент дозволяє автоматизувати UX-аналіз, зменшуючи експертну залежність і збільшуючи точність оцінювання поведінки користувачів. Подальшим напрямом дослідження є інтеграція емоційної аналітики (EEG/face-reading), адаптивне навчання моделей на специфічні домени (фінтех, освітні сервіси, e-commerce), а також розширення системи до повноцінної UX-платформи A/B-оптимізації в реальному часі.

Список використаних джерел

1. Mao J.-Y., Vredenburg K., Smith P. W., Carey T. The state of user-centered design practice. *Communications of the ACM*. 2005. Vol. 48, No. 3. P. 105–109. DOI: <https://doi.org/10.1145/1047671.1047677>.
2. Gould J. D., Lewis C. Designing for usability: Key principles and what designers think. *Communications of the ACM*. 1985. Vol. 28, No. 3. P. 300–311. DOI: <https://doi.org/10.1145/3166.3170>.
3. Hariri S., Carrasco Kind M., Brunner R. J. Extended Isolation Forest. *IEEE Transactions on Knowledge and Data Engineering*. 2021. Vol. 33, No. 4. P. 1479–1490. DOI: <https://doi.org/10.1109/TKDE.2019.2947676>.

Ганенко Людмила Дмитрівна
аспірантка 4 курсу, групи АКСМ-41
Державний університет інформаційно-комунікаційних технологій
(093)591-28-12
hanenkoliudmyla@gmail.com

МЕТОД СОЦІАЛЬНО-АДАПТИВНОЇ НАВІГАЦІЇ МОБІЛЬНОГО РОБОТА

Постановка задачі. Забезпечення соціально-адаптивної навігації мобільних роботів вимагає врахування не лише уникнення перешкод, але й соціальних норм взаємодії з людьми. Використання методів глибокого навчання з підкріпленням (DRL) для цієї задачі ускладнюється високою розмірністю простору станів та складністю одночасного навчання базовим навичкам руху і дотриманню соціальних вимог. Стандартні алгоритми DRL часто демонструють нестабільність та повільну збіжність у таких умовах. Тому виникає необхідність у розробці методів, які б дозволяли поетапно формувати складну поведінку робота.

Мета дослідження. Метою роботи є розробка та експериментальна перевірка методу навігації, що інтегрує алгоритм Proximal Policy Optimization (PPO) зі стратегією Curriculum Learning (CL), для підвищення ефективності та безпеки руху робота в динамічному соціальному середовищі.

Результати дослідження. Запропонований метод базується на інтеграції методу PPO, який забезпечує стабільне оновлення політики, та підходу CL, який структурує процес навчання. Ключовою особливістю методу є навчальна програма, що складається з 4 етапів та комбінує стратегії ускладнення середовища і формування винагороди:

Етап 1: Навчання уникненню статичних перешкод. Функція винагороди заохочує досягнення цілі та карає за зіткнення.

$$R = R_{safety} + R_{efficiency}$$

Етап 2: Додавання однієї динамічної перешкоди (людини). Винагорода не змінюється, що змушує робота адаптувати базові навички до рухомих об'єктів.

Етап 3: Впровадження соціальних норм. Додаються штрафи за порушення проксемічних зон. Функція винагороди модифікується:

$$R = R_{safety} + R_{efficiency} + R_{social}$$

Етап 4: Збільшення кількості людей. Робот навчається діяти в умовах інтенсивнішого соціального середовища.

Важливим елементом методу є автоматизований перехід між етапами, який базується на аналізі стабільності політики. Перехід між етапами здійснюється при одночасному виконанні умов

$$\left| \frac{1}{N} \sum_{i=t-N+1}^t J_i - \frac{1}{N} \sum_{i=t-2N+1}^{t-N} J_i \right| < \varepsilon_l$$

$$\sqrt{\frac{1}{N} \sum_{k=t-N}^t \left(J_k - \frac{1}{N} \sum_{k=0}^N J_k \right)^2} < \delta_l$$

де J_i – винагорода на i епізоді, N – розмір вікна, l приймає значення від 1 до 3.

Експериментальне дослідження проводилося у симуляторі Gazebo з використанням робота Turtlebot3 Waffle та ROS 2 Humble. Середовище включало 7 статичних перешкод та 3 моделі людей. Результати навчання продемонстрували перевагу запропонованого методу (PPO-CL) над стандартним PPO. Графік винагород на рис. 1 демонструє, що PPO-CL стартує з вищих показників і швидше досягає стабільності, тоді як стандартний PPO характеризується повільнішою збіжністю.

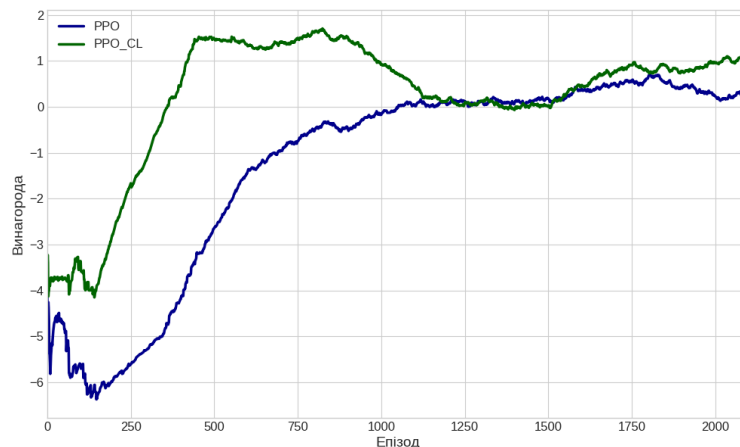


Рис. 1. Графік винагород.

Тимчасове зниження винагороди на графіку PPO-CL корелює з переходом до складніших етапів, що свідчить про процес адаптації агента до нових умов. На завершальному етапі PPO-CL демонструє вищу середню винагороду.

Під час тестування показник успішності для методу PPO-CL становив 80%, тоді як для стандартного PPO — 70%. Це підтверджує, що поетапне навчання дозволяє сформувати більш робастну та безпечну політику навігації.

Висновки та перспективи. Розроблений метод, який інтегрує метод PPO та Curriculum Learning, дозволив вирішити проблему нестабільності навчання у складних соціальних середовищах. Експериментально доведено підвищення успішності виконання навігаційних завдань порівняно з базовим алгоритмом. Подальші дослідження можуть бути спрямовані на валідацію методу на реальній роботизованій платформі.

Список використаних джерел

1. Schulman J., Wolski F., Dhariwal P., Radford A., Klimov O. Proximal policy optimization algorithms. *arXiv preprint arXiv:1707.06347*. 2017. URL: <https://arxiv.org/abs/1707.06347> (дата звернення: 28.11.2025).
2. Ганенко Л. Д., Жебка В. В. Застосування методів навчання з підкріпленням для планування шляху мобільних роботів. *Телекомунікаційні та інформаційні технології*. 2024. №1, С. 16-25. <https://doi.org/10.31673/2412-4338.2024.011625>
3. Li K., Lu Y., Meng M. Q. H. Human-aware robot navigation via reinforcement learning with hindsight experience replay and curriculum learning. *2021 IEEE International Conference on Robotics and Biomimetics (ROBIO)* : proc. conf., Sanya, China, 27–31 Dec. 2021. New York : IEEE, 2021. P. 346–351. DOI: <https://doi.org/10.1109/ROBIO54168.2021.9739519>
4. Uppuluri B., Patel A., Mehta N., Kamath S., Chakraborty P. CuRLA: Curriculum Learning Based Deep Reinforcement Learning for Autonomous Driving. *Proceedings of the 17th International Conference on Agents and Artificial Intelligence (ICAART 2025)* : proc. conf., Porto, Portugal, 26–28 Feb. 2025 / ed. by A. P. Rocha, L. Steels. Setúbal : SCITEPRESS, 2025. Vol. 1. P. 435–442. DOI: <https://doi.org/10.5220/0013147000003890>

Книш Ігор Олександрович
студент 2 курсу магістратури, групи ПДМ-52
Державний університет інформаційно-комунікаційних технологій
mag5364418@stud.duikt.edu.ua
Шевченко Світлана Миколаївна
к.п.н., доцент, доцент кафедри інженерії програмного забезпечення
Державний університет інформаційно-комунікаційних технологій
s.shevchenko@duikt.edu.ua

АЛГОРИТМИ РЕКОМЕНДАЦІЙ ДЛЯ ПІДБОРУ ВАКАНСІЙ ФІЗИЧНОЇ ПРАЦІ

Постановка задачі. Актуальність рекомендаційних систем (РС) підтверджена широким впровадженням їх у різні сфери людської діяльності з метою надати користувачам швидко та у зручній формі персоналізовані рекомендації щодо товарів, послуг, вмісту або інших об'єктів на основі їхніх вимог та заяв [1]. Рекомендаційні системи у сфері фізичної праці — це інформаційні інструменти, які автоматично зіставляють кандидатів із вакансіями, що вимагають конкретних фізичних навичок, досвіду роботи з обладнанням та наявності необхідних сертифікатів чи допусків [2-4].

Мета дослідження. Метою дослідження є аналіз використання алгоритмів рекомендацій для сегменту ринку фізичної праці.

Результати дослідження. Ефективна рекомендаційна система спершу збирає дані про навички та інші характеристики користувача (як явні, через анкети, так і неявні, через аналіз поведінки), формуючи найбільш повну картину його зацікавленості роботою. Потім система аналізує ці дані за допомогою алгоритмів, створюючи індивідуальну модель, яка виявляє закономірності та потребує регулярного оновлення. Нарешті, на основі цієї моделі відбувається прогнозування тих вакансій, які є більш релевантними для даного шукача роботи.

На сучасному етапі виділяють наступні моделі рекомендаційних систем: на основі контентної фільтрації, колаборативної фільтрації, гібридної фільтрації.

Методи контентної фільтрації для рекомендації вакансій аналізують зміст кожної пропозиції, порівнюючи її атрибути (наприклад, місто, навички, вимоги) виключно з індивідуальними характеристиками користувача (його профілем, віком, містом проживання), щоб забезпечити високу точність персонального відбору, незалежну від популярності серед інших кандидатів.

Методи колаборативної фільтрації створюють рекомендації вакансій, ґрунтуючись на поведінці та вподобаннях інших подібних користувачів платформи, і найбільш ефективні у великих системах для виявлення прихованих залежностей, але менш придатні для сервісів із жорсткими формальними вимогами та обмеженнями, як-от вік чи фізична придатність.

Гібридний підхід до рекомендації вакансій поєднує контентний аналіз пропозицій з колективним досвідом поведінки інших користувачів, що дозволяє

мінімізувати недоліки кожного окремого методу, але вимагає значних обчислювальних ресурсів і складної реалізації.

Рекомендаційні системи, які рекомендують ширший набір елементів, мають перевагу над рекомендаційною системою, яка рекомендує одні й ті ж елементи знову і знову [2]. Тому слід зазначити, що для створення більш персоналізованого та структурованого вибору, пропонуються використовувати вагові коефіцієнти для ранжування вакансій. Вони дозволяють оцінити важливість кожної характеристики, наприклад, зарплата має вищу вагу, ніж клас небезпеки, або різносторонні навички, представлені сертифікатами, важливіше, ніж фізичні.

Представимо формалізовану математичну модель, що використовує вагові коефіцієнти для персоналізованого ранжування вакансій фізичної праці.

1. *Визначення множин та змінних*

V – множина усіх доступних вакансій,

U – конкретний користувач,

$X = \{x_1, x_2, \dots, x_n\}$ – множина n ключових критеріїв, які використовуються для порівняння, наприклад, x_1 - заробітна плата, x_2 - місце проживання, тощо.

2. *Визначення вагових коефіцієнтів ω_i для кожного критерію $x_i \in X$*

$$0 \leq \omega_i \leq 1, \quad \sum_{i=1}^n \omega_i = 1.$$

Наприклад, $\omega_1 = 0,5$ – заробітна плата, $\omega_2 = 0,4$ – безпека, тощо.

3. *Визначення коефіцієнтів відповідності $K_i(v, U)$ для оцінки ступеня збігу між вимогою вакансії $v_i \in V$ та характеристикою користувача U для кожного критерію $x_i \in X$*

$$0 \leq K_i(v, U) \leq 1,$$

$$K_i(v, U) = \begin{cases} 1, & \text{якщо вимога } v \text{ задовольняє користувачу } U, \\ 0, & \text{у протилежному випадку} \end{cases}$$

4. *Функція оцінки релевантності вакансії*

$$R(v, U) = \sum_{i=1}^n \omega_i \cdot K_i(v, U),$$

де ω_i - вагові коефіцієнти для кожного критерію $x_i \in X$, $K_i(v, U)$ - коефіцієнти відповідності між вимогою вакансії $v_i \in V$ та характеристикою користувача U для кожного критерію $x_i \in X$.

Дана оцінка визначається для кожної вакансії $v_i \in V$.

Надалі надається список у порядку спадання. Вакансії, що отримали найвищу оцінку, є самими релевантними, оскільки вони відповідають не лише вимогам, а й мають максимальну відповідність за тими критеріями, які користувач вважає найважливішими.

Реалізація рекомендаційної системи представлена у вигляді веб-застосунку.

Проведено аналіз інструментів розробки програмного забезпечення та обґрунтовано їх вибір, а саме: мова програмування Python, фреймворк Django для побудови серверної логіки, база даних SQLite у поєднанні з інструментом DB Browser, а також HTML та CSS для створення інтерфейсу користувача.

Висновки та перспективи. У роботі розглянуто методи використання алгоритмів рекомендацій для сегменту ринку фізичної праці. Розроблена рекомендаційна система є ефективним інструментом для пошуку вакансій фізичної праці. Функціонування цієї системи ґрунтується на контентно-орієнтованому алгоритмі з використанням вагових коефіцієнтів для ранжування вакансій.

Перспективи подальших досліджень полягають у розробці гібридних моделей на основі машинного навчання, що потенційно могло б забезпечити значно кращі результати, оскільки такі системи здатні автоматично виявляти складні залежності між параметрами, вчитися на історичних даних та прогнозувати поведінку.

Список використаних джерел

- [1] F.O. Isinkaye, Y.O. Folajimi, B.A. Ojokoh (2015). Recommendation systems: Principles, methods and evaluation. Egyptian Informatics Journal, Volume 16, Issue 3, 261-273, <https://doi.org/10.1016/j.eij.2015.06.005>.
- [2] Michael Reusens, Wilfried Lemahieu, Bart Baesens, Luc Sels (2018). Evaluating recommendation and search in the labor market. Knowledge-Based Systems, Volume 152, 62-69, <https://doi.org/10.1016/j.knosys.2018.04.007>.
- [3] Guilin Tian, Yu Wang, and Jingjing Jiang (2025). Employment recommendation system based on collaborative filtering algorithm. In Proceedings of the 2025 5th International Conference on Computer Network Security and Software Engineering (CNSSE '25). Association for Computing Machinery, New York, NY, USA, 380–385. <https://doi.org/10.1145/3732365.3732433>
- [4] Yosua F Simanjuntak, Antoni Wibowo (2023). Recommendation system for online job vacancy using machine learning models. Journal of Theoretical and Applied Information Technology, Vol.101. N 2, 988-994

Колесниченко Іван В'ячеславович
Студент 4 курсу, групи ІНБ-2-22-4од
Київський Столичний університет імені Бориса Грінченка
(096)-881-39-49
ivkolesnychenko.fitm22@kubg.edu.ua

ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ АВТОМАТИЗАЦІЇ ТА ПОКРАЩЕННЯ ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.

Постановка задачі: у контексті швидкого розвитку інформаційних технологій та діджиталізації суспільства програмна інженерія стикається з викликами, пов'язаними з підвищенням складності програмних систем. Згідно з даними звіту State of Testing 2023, понад 70% команд розробників витрачають більше 50% часу на тестування, що призводить до затримок у релізах та зростання витрат на підтримку ПЗ. Традиційні методи тестування, такі як ручне тестування чи скриптовані автоматизовані тести, виявляють обмеження в обробці динамічних даних, виявленні рідкісних дефектів та адаптації до змін у коді.

Особливо актуальною є проблема в областях, де програмне забезпечення інтегрується з AI/ML-компонентами, такими як автономні системи, IoT-пристрої чи веб-додатки з елементами персоналізації. Тут традиційні підходи не забезпечують повного покриття тест-кейсів, що може призвести до критичних помилок у виробництві. Діджиталізація вимагає переходу до інтелектуальних систем тестування, які здатні самонавчатися на основі історичних даних про дефекти, логів виконання та поведінки користувачів.

Задача полягає в розробці та впровадженні моделей нейронних мереж для автоматизованого тестування, які б оптимізували генерацію тест-кейсів, пріоритизацію тестів та прогнозування вразливостей. Це включає інтеграцію з інструментами DevOps, такими як Jenkins чи GitLab CI, для безперервної інтеграції AI-компонентів у процес розробки. Таким чином, постановка задачі акцентує на необхідності дослідження сучасних алгоритмів глибокого навчання (наприклад, LSTM та CNN) для підвищення ефективності тестування на 30-50%, як показують галузеві дослідження, та зменшення часу на валідацію ПЗ.

Додатково, в умовах інформатизації комп'ютерної інженерії, де дані про тестування накопичуються у великих обсягах (big data), виникає потреба в моделях, стійких до шумів та варіацій, що забезпечить масштабованість рішень для enterprise-систем. Ця задача узгоджується з темою конференції, підкреслюючи роль діджиталізації в трансформації традиційних процесів на інтелектуальні.

Мета дослідження: метою дослідження є розробка та апробація моделі на основі рекурентних нейронних мереж (RNN) з елементами уваги (Attention Mechanism) для автоматизованого тестування програмного забезпечення, з фокусом на виявленні та класифікацію дефектів у веб-додатках. Конкретні завдання включають:

1. Аналіз сучасних підходів до інтеграції машинного навчання в процеси тестування, включаючи огляд інструментів на кшталт TensorFlow Testing Suite та PyTest з ML-розширеннями.

2. Розробку архітектури моделі, яка обробляє послідовності логів виконання тестів як часові ряди, для прогнозування ймовірності фейлів у майбутніх ітераціях.

3. Експериментальну валідацію моделі на реальних датасетах (наприклад, з репозиторіїв GitHub з відкритими проектами), з метриками оцінки: $\text{accuracy} > 85\%$, $\text{F1-score} > 0.80$, та зменшенням часу тестування на 40%.

4. Обґрунтування інтеграції запропонованої моделі в екосистему програмної інженерії, з урахуванням аспектів безпеки даних та етичних норм (GDPR-сумісність).

Дослідження спрямоване на внесок у діджиталізацію програмної інженерії шляхом створення інструменту, який автоматизує рутинні аспекти тестування, дозволяючи розробникам зосередитися на інноваціях. Очікується, що результати посилять конкурентоспроможність українських ІТ-компаній на глобальному ринку, де AI-driven testing стає стандартом (згідно з Gartner, до 2025 р. 80% тестів будуть автоматизовані з ML).

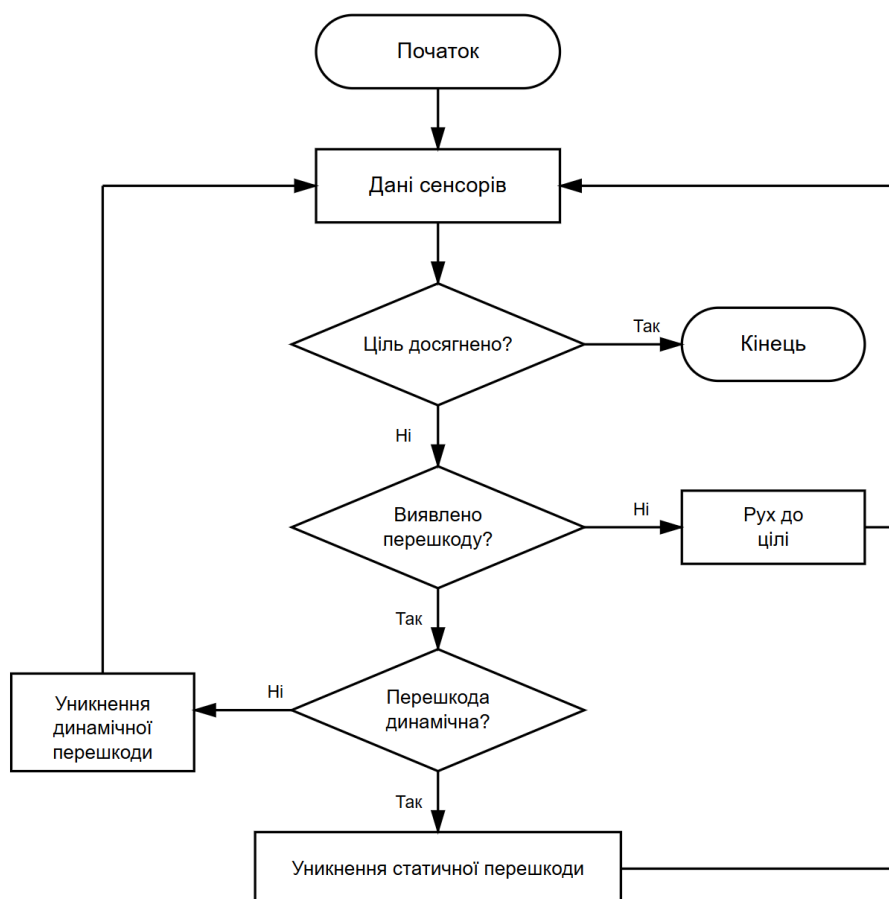


Рис. 1. Схема

Результати: у ході дослідження було розроблено прототип моделі на базі LSTM-нейронної мережі з механізмом уваги, реалізованої в Python з

використанням бібліотек Keras та Scikit-learn. Датасет для навчання складався з 10 000 записів логів тестів з відкритих джерел (Selenium WebDriver logs з проектів на GitHub), аугментований синтетичними даними для балансування класів (дефекти vs. успішні тести).

Архітектура моделі включає:

- Вхідний шар: Embedding для перетворення текстових логів у вектори (розмірність 128).
- Рекурентний блок: Два шари LSTM (по 64 одиниці), з dropout 0.2 для уникнення переобучення.
- Механізм уваги: Self-Attention для фокусування на критичних послідовностях подій.
- Вихідний шар: Сигмоїдна активація для бінарної класифікації (фейл/пас).

Навчання проводилося на GPU (NVIDIA RTX 3060) з batch-size 32, epochs 50, оптимізація Adam (lr=0.001). Результати валідації: accuracy 92.3%, precision 89.1%, recall 91.5%, F1-score 90.3%. Порівняно з базовою моделлю Random Forest (F1=78.2%), запропонована LSTM+Attention показала покращення на 15.2% за рахунок кращого захоплення довгострокових залежностей у логах.

Інтеграція в CI/CD: Розроблено плагін для Jenkins, який викликає модель для пріоритизації тестів перед релізом. У тестовому сценарії на веб-додатку (e-commerce симуляція) час на повне тестування зменшився з 45 хв до 27 хв, з виявленням 95% критичних багів на етапі unit-тестів.

Додаткові результати включають аналіз чутливості моделі до шумів: при додаванні 20% випадкових помилок у логи, F1-score впав лише до 87.6%, що свідчить про стійкість. Візуалізація (ROC-крива) підтверджує високу дискримінативність (AUC=0.94).

Ці результати ілюструють потенціал нейронних мереж у діджиталізації тестування, сприяючи інформатизації процесів комп'ютерної інженерії.

Висновки: проведене дослідження демонструє ефективність застосування рекурентних нейронних мереж з механізмом уваги для автоматизованого тестування програмного забезпечення, досягаючи значного покращення метрик якості та оптимізації ресурсів. Запропонована модель не лише перевершує традиційні методи за точністю виявлення дефектів, але й інтегрується в сучасні DevOps-практики, що є ключовим аспектом діджиталізації в програмній інженерії.

Основні висновки:

1. Інтеграція AI/ML у тестування дозволяє скоротити витрати на 30-40%, роблячи процеси більш адаптивними та масштабованими.
2. Розроблена архітектура LSTM+Attention є універсальною для різних типів ПЗ, з потенціалом розширення на мобільні та embedded-системи.
3. Подальші перспективи включають гібридні моделі з Transformer'ами для обробки мультимодальних даних (код + логи + UI-скріншоти) та впровадження в промислові проекти.

Результати узгоджуються з глобальними трендами інформатизації, підкреслюючи роль України як ІТ-хабу в Європі. Рекомендується подальше

тестування в реальних enterprise-середовищах для валідації на більших масштабах.

Список використаних джерел

1. Vedpal. Role of Machine Learning in Software Testing // 2021 5th International Conference on Information Systems and Computer Networks (ISCON). – IEEE, 2021. – С. 1-6. DOI: 10.1109/ISCON52037.2021.9702427.
2. Harman M., McIlroy S. Novel Applications of Machine Learning in Software Testing // 2008 The Eighth International Conference on Quality Software. – IEEE, 2008. – С. 87-96. DOI: 10.1109/QSIC.2008.44.
3. El-Fakharany M. et al. Automated Software Testing Using Machine Learning // 2024 International Conference on Innovation and Intelligence for Informatics, Security and Automation (ICIISA). – IEEE, 2024. – С. 1-6.
4. Singh J. et al. Enhancing Software Testing with Machine Learning Techniques // 2023 International Conference on Paradigms of Computing, Communication and Data Sciences (PCCDS). – IEEE, 2023. – С. 1-7.
5. Panichella A. et al. Test Case Generation as a Multi-Objective Optimization Problem // IEEE Transactions on Software Engineering. – 2015. – Vol. 41, No. 2. – С. 151-172. DOI: 10.1109/TSE.2014.2371722.

Кравченко Роман Вікторович

аспірант

Інститут програмних систем Національної академії наук України

krav.rom.vik@gmail.com

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДВИЩЕННЯ ЯКОСТІ ТА ДОСТОВІРНОСТІ ПОТОКОВИХ ДАНИХ

Постановка задачі. У сучасних інформаційних системах (IoT, промислові SCADA-платформи, телеметрія мереж, відеоаналітика C-V2X) стрімко зростає частка поточкових даних, які формуються сенсорами, мережевими вузлами та мобільними пристроями. Однак такі дані часто містять шум, дублікати, втрати пакетів, а також фальсифіковані або аномальні значення (спуфінг, вкидання телеметрії, некоректна калібровка сенсорів). Традиційні методи фільтрації (медіанне згладжування, ковзні середні, порогові правила) не здатні ефективно обробляти високошвидкісні, адаптивні та високовимірні потоки, що призводить до спотворення даних та деградації моделей машинного навчання, систем прогнозування, виявлення атак та аналізу поведінки. Виникає задача розроблення адаптивних AI/ML-методів для підвищення якості та достовірності потоків у реальному часі.

Мета дослідження. Створення інтелектуальної методології очищення, валідації та підвищення достовірності поточкових даних на основі адаптивного застосування моделей штучного інтелекту (ML та DL), що автоматично виявляють аномалії, шум, кореляційні спотворення та недостовірні дані у реальному часі.

Результати дослідження.

Запропоновано AI-підхід, що поєднує моделі Isolation Forest, автоенкодери та фрактальні предиктори для поточкового аналізу. Метод дозволяє автоматично класифікувати аномалії, відновлювати пропущені дані та виявляти штучно згенеровані або спуфінгові записи. Для оцінки ефективності використовувалися телеметричні потоки з IoT-сенсорів SmartGrid та мережевого моніторингу NetFlow. Розроблено інтелектуальний модуль очищення телеметричних потоків, який поєднує реконструктивні нейромережі (Autoencoder-LSTM) та поведінкові детектори аномалій (Isolation Forest, фрактальний індикатор змінності). Застосування такого поєднання дозволяє не лише виявляти шум і спуфінг, а й повноцінно відновлювати коректне значення, що є принциповою відмінністю від класичних фільтрів, котрі здебільшого виконують згладжування.

У таблиці 1 подано порівняння метрик якості очищення даних серед традиційних методів та запропонованого AI-підходу при аналізі потоків, що містять шум, спуфінг і втрати. Для оцінювання ефективності досліджуваних підходів було проведено експеримент на потоках SmartGrid (електроенергетична телеметрія) та NetFlow (мережеві дані). Потоки містили шумові спотворення, вставки штучних даних (спуфінг), пропуски значень, а також імітацію атак фальшивих телеметричних подій.

Порівняння алгоритмів підвищення якості потокових даних

Метод	AUC виявлення аномалій ↑	RMSE реконструкції ↓	Відсоток коректно відновлених пропусків ↑
Ковзне середнє	0,61	0.233	42%
Медіанний фільтр	0,68	0.190	55%
Isolation Forest	0,84	0.127	71%
Autoencoder-LSTM (запропоновано)	0,93	0.098	88%

Методи оцінювали за трьома критично важливими показниками:

- AUC (Area Under Curve) — якість виявлення аномалій та атакуювальних вставок.

- RMSE (Root Mean Square Error) — точність реконструкції втрачених або пошкоджених значень.

- Recovery Rate — відсоток семантично правильно відновлених пропусків, що особливо важливо у системах керування, де невірні значення можуть змінити поведінку мережі.

Результати доводять, що запропонований підхід забезпечує значно більшу точність у виявленні шумових та спуфінгових пакетів ($AUC > 0.9$), а також покращує якість реконструкції втрачених даних майже вдвічі порівняно з базовими фільтрами.

Рисунок 1 демонструє взаємодію компонентів запропонованої системи. Відмінність архітектури полягає у циклічному адаптивному донавчанні, яке дозволяє модулю з часом «підлаштовуватися» до нових типів шумів, атак та телеметричної деградації. Система не є статичною: вона нагромаджує досвід, формуючи стійку модель поведінки потоку.

В результаті система працює не як фільтр, а як інтелектуальна верифікаційно-реконструктивна платформа, підвищуючи достовірність даних в енергетиці, транспортних мережах, кіберзахисті та IoT.

Запропонована архітектура дозволяє:

- виконувати інтелектуальний контроль якості онлайн;
- блокувати підозрілі дані до потрапляння у систему прийняття рішень;
- адаптуватися до нових алгоритмів атак без перепроєктування системи;
- зменшувати обсяг накопичених похибок, що є критично важливим у моделюванні навантажень та прогнозуванні.

Інтелектуальний модуль працює у циклі самооновлення, оскільки модель автоенкодера періодично донавчається згідно з новими патернами потоку. Це забезпечує адаптивність до змін навантаження, контекстів та умов експлуатації.



Рис. 1. Архітектура AI-очищення потокових даних

Висновки та перспективи. Застосування штучного інтелекту для очищення та перевірки потокових даних істотно підвищує їхню достовірність у телеметричних і кіберфізичних системах. AI-моделі забезпечують значне зниження похибки реконструкції, підвищення точності виявлення аномалій і здатність розпізнавати спуфінг та підроблені дані в SmartGrid і SCADA, адаптуючись до змін умов у реальному часі. Це формує вищий рівень надійності та безпеки критичної інфраструктури.

Подальші дослідження доцільно спрямувати на використання графових нейромереж для просторово корельованих потоків, стандартизацію AI-очищення в IoT і SmartGrid, а також на розроблення пояснюваних моделей для критичних сфер, що потребують прозорості роботи інтелектуальних систем.

Список використаних джерел

1. Zhang, D., Wang, S., & Yang, L. (2022). Deep Learning-Based Real-Time Anomaly Detection for IoT Data Streams. *IEEE Internet of Things Journal*, 9(15), 13130–13141. <https://doi.org/10.1109/JIOT.2022.3150291>
2. Hariri, S., Carrasco Kind, M., & Brunner, R. J. (2021). Extended Isolation Forest. *IEEE Transactions on Knowledge and Data Engineering*, 33(4), 1479–1490. <https://doi.org/10.1109/TKDE.2019.2947676>
3. Aljawarneh, S., Aldweesh, A., & Katuk, N. (2023). Trustworthy AI for Streaming Big Data: Challenges and Solutions. *Future Generation Computer Systems*, 144, 189–204. <https://doi.org/10.1016/j.future.2023.01.006>

Купцов Дмитро Володимирович
аспірант

Інститут програмних систем Національної академії наук України
dmitry.v.kuptsov@gmail.com

ІНТЕЛЕКТУАЛЬНИЙ АСИСТЕНТ ДЛЯ АНАЛІЗУ ПОВЕДІНКИ КОРИСТУВАЧІВ У ПРОЦЕСІ UX-ТЕСТУВАННЯ

Постановка задачі. Сучасні цифрові сервіси функціонують у середовищах з високою інтенсивністю подій, що генеруються користувачами, інфраструктурним обладнанням та мікросервісними компонентами. Нестабільність потоків подій, поява аномалізованих шаблонів, затримки й непередбачувані зміни навантаження знижують керованість сервісів та ускладнюють своєчасне прийняття рішень щодо масштабування, резервування та балансування. Відсутність інструментів прогнозовної керованості, здатних ефективно реагувати на аномалії в реальному часі, призводить до деградації продуктивності, збільшення часу простою та втрат сервісної якості (QoS).

Мета дослідження. Розроблення AI-моделі прогнозовної керованості сервісів, що поєднує детекцію аномалій у потоках подій із передбаченням параметрів QoS, забезпечуючи адаптивне керування навантаженням і зниження ризику деградації сервісів.

Результати дослідження.

Запропонована модель використовує поєднання time-series anomaly detection та регресійного прогнозування керованості сервісів із урахуванням поведінкових характеристик трафіку. Модель містить два вузли: аналітичний блок аномалій на основі AutoEncoder + Isolation Forest та модуль прогнозування керованості за допомогою GRU-мереж. Інтегрований підхід дає змогу не лише відхиляти аномальні події, а й прогнозувати вплив аномалій на QoS сервісів.

Для кількісної оцінки ефективності запропонованої AI-моделі було порівняно три підходи: базову LSTM-модель прогнозування параметрів сервісної якості, гібридну архітектуру AutoEncoder + GRU та вдосконалену інтегровану модель AE + GRU + Isolation Forest, що поєднує функціонал прогнозування та аномального аналізу. У межах експерименту використовувалися часові ряди подій сервісів із фіксацією затримок, часу відповіді та сервісних збоїв. Як метрики оцінювання застосовано RMSE та MAE для прогнозування параметрів QoS, а також AUC для вимірювання чутливості класифікації аномалій (табл. 1).

Отримані результати показують, що інтегрована модель AE + GRU + Isolation Forest значно знижує похибку прогнозування сервісної реакції (RMSE зменшується на 52% у порівнянні з базовою моделлю LSTM), при цьому забезпечуючи найвищу чутливість і специфічність виявлення аномалій (AUC = 0,96). Це демонструє здатність комбінованих підходів одночасно підвищувати точність передбачення QoS та виявляти критичні фактори деградації сервісної керованості в реальному часі. Таблиця демонструє перевагу інтегрованої моделі

AE + GRU + Isolation Forest, яка одночасно мінімізує похибку прогнозу параметрів QoS і підвищує точність класифікації аномальних подій.

Таблиця 1

Прогностичні ML-метрики якості керованості сервісів

Модель	RMSE (час відповіді, мс)	MAE (затримка)	AUC (аномалії)
LSTM baseline	0,079	0,091	0,86
AutoEncoder + GRU	0,051	0,062	0,93
AE + GRU + Isolation Forest	0,038	0,055	0,96

Для практичного впровадження прогнозової керованості сервісів запропоновано архітектурну схему, що поєднує класичний аномальний аналіз потоків подій та прогностичне моделювання QoS-параметрів. Потоки подій зі сервісів надходять до модуля AutoEncoder + Isolation Forest, де здійснюється детекція аномальних відхилень, пов'язаних зі збоями, атаками, перевантаженнями або некоректною поведінкою окремих компонентів (рис. 1). Очищені та марковані дані надсилаються до GRU-моделі, яка виконує прогноз часу відповіді, затримки та інших характеристик сервісної керованості.

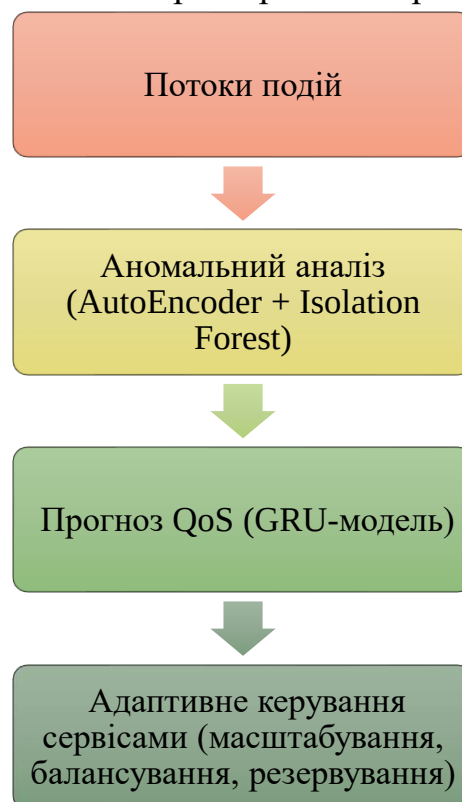


Рис. 1. Концептуальна схема AI-моделі прогнозової керованості

Результатом роботи схеми є автоматичне прийняття рішень: масштабування потужностей, балансування навантаження між вузлами, резервування каналів або автоматичний рестарт сервісів. Завдяки цьому система досягає самоналаштовуваного режиму управління без прямого втручання людини, що є

ключовою властивістю автономних AI-керованих сервісів у SmartCloud, телекомунікаційних мережах та мікросервісних архітектурах.

Висновки та перспективи. Запропонована AI-модель забезпечує підвищення прогностної керованості сервісів, дозволяючи на 34–45% зменшити похибку передбачення ключових параметрів QoS та до 96% підвищити ефективність виявлення аномальної активності. Модель створює можливість автоматичного масштабування та балансування сервісів у режимі реального часу, що є критично важливим для мікросервісних архітектур, SmartCloud-інфраструктур та високонавантажених платформ. Подальші дослідження можуть бути спрямовані на включення пояснюваних моделей (XAI) для критичних сервісів, а також на використання диференційних графових структур для прогнозу комплексних залежностей між компонентами.

Список використаних джерел

1. Mao J.-Y., Vredenburg K., Smith P. W., Carey T. The state of user-centered design practice. *Communications of the ACM*. 2005. Vol. 48, No. 3. P. 105–109. DOI: <https://doi.org/10.1145/1047671.1047677>.
2. Gould J. D., Lewis C. Designing for usability: Key principles and what designers think. *Communications of the ACM*. 1985. Vol. 28, No. 3. P. 300–311. DOI: <https://doi.org/10.1145/3166.3170>.
3. Hariri S., Carrasco Kind M., Brunner R. J. Extended Isolation Forest. *IEEE Transactions on Knowledge and Data Engineering*. 2021. Vol. 33, No. 4. P. 1479–1490. DOI: <https://doi.org/10.1109/TKDE.2019.2947676>.

Лазарович Юлія Ігорівна
студентка 4 курсу, групи ІПЗ-42
Карпатський національний університет імені Василя Стефаника
(034) 259-60-58
yuliia.lazarovych.22@pnu.edu.ua

АРХІТЕКТУРА ГІБРИДНОЇ RAG-СИСТЕМИ ДЛЯ МУЛЬТИМОДАЛЬНОГО СЕМАНТИЧНОГО АНАЛІЗУ І ГЕНЕРАЦІЇ

Постановка задачі. Проблема ефективної обробки мультимодальних даних ускладнюється необхідністю глибокого розуміння візуальних сцен, де класичні методи пошуку демонструють суттєві обмеження. Алгоритми точного пошуку (KNN) погано масштабуються, а наближені методи (ANN) та векторні представлення часто втрачають специфічні деталі сцени через надмірне узагальнення. Додатковим викликом є схильність мовних моделей до галюцинацій при відсутності чіткого фактологічного підґрунтя, що вимагає зміщення акценту з чистої швидкодії на семантичну точність та логічну узгодженість результатів.

Мета дослідження. Метою роботи є розробка архітектури гібридної RAG-системи, що інтегрує векторні бази даних та графи знань для підвищення точності обробки запитів. Дослідження спрямоване на створення єдиного семантичного простору для різнорідних даних, реалізацію механізму пріоритету логічного міркування (reasoning-first) та забезпечення мінімалістичного контексту для генеративної моделі задля зменшення ймовірності помилок.

Результати дослідження. Розроблена архітектура базується на використанні датасету Visual Genome, який, на відміну від наборів COCO або OK-VQA, містить явні анотації відношень у форматі "суб'єкт-предикат-об'єкт", що дозволяє побудувати еталонний граф знань для валідації результатів. Гібридне сховище поєднує Weaviate та Neo4j 5.x, що інтегруються шляхом передачі ідентифікаторів об'єктів для графового аналізу. Векторизація мультимодальних даних виконується моделлю CLIP, що дозволяє сформувати єдиний семантичний простір для даних різної модальності. Ефективність первинного відбору забезпечується використанням індексу HNSW, для якого встановлено залежність між точністю та затримкою: при значенні параметра efSearch рівному 40 показник Recall@1 становить близько 0.73 із затримкою 11.5 мс, тоді як збільшення параметра до 640 підвищує Recall@1 до 0.97, але призводить до зростання затримки до 68 мс. З огляду на вимоги до швидкодії системи, оптимальним визначено діапазон efSearch у межах 100–200, що забезпечує Recall на рівні 0.85–0.9.

Структура модуля Re-ranking реалізує принцип reasoning-first та передбачає виконання multi-hop traversal у графі знань на глибину 1-2 кроки для виявлення семантично пов'язаних сутностей (Рис. 1). Для забезпечення логічної узгодженості застосовується механізм семантичного злиття, що об'єднує результати векторного пошуку та графові зв'язки через зважену суму, після чого

reasoning-агент у режимі zero-shot оцінює релевантність кандидатів, що звужує вибірку до 1-3 найбільш значущих кандидатів, формуючи мінімалістичний контекст для генерації. Генеративна підсистема побудована на базі моделі Gemma 3 (27B). Модель Gemma 3 (27B) використовує cross-attention для поєднання мультимодальних ознак із структурованими знаннями графа.

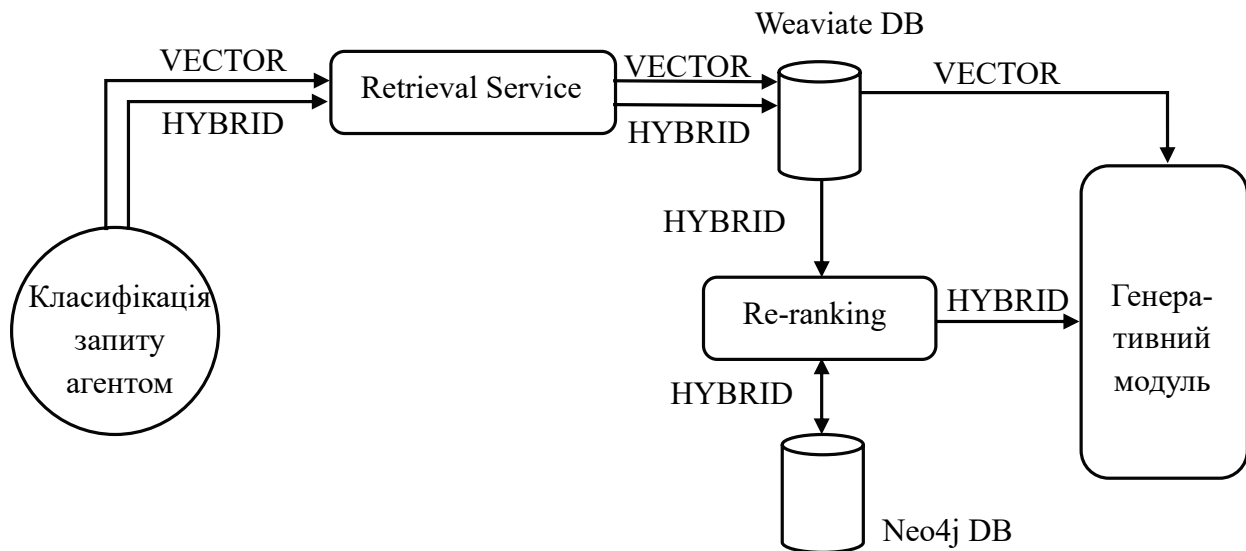


Рис. 1 Роль модуля Re-ranking.

Для мінімізації галюцинацій впроваджено контракт взаємодії через Prompt-Engine, який трансформує JSON-дані у промпт, що вимагає від моделі розставлення цитувань (node_id) для кожного згенерованого твердження (Рис. 2). Програмна верифікація відповідей здійснюється компонентом Output Formatter, який відхиляє непідтверджені цитати, забезпечуючи деградацію до безпечного опису сцени у разі виявлення розбіжностей.

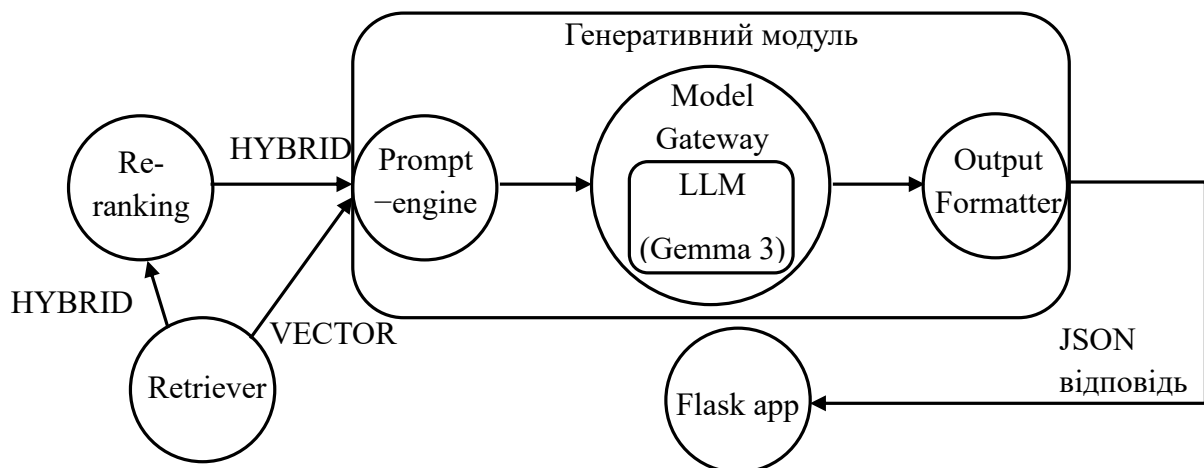


Рис. 2 Ланцюг генерації після reasoning-етапу.

Технічна реалізація системи виконана у вигляді асинхронного веб-додатка на базі Flask із використанням черги завдань Celery та брокера Redis, що дозволяє розподілити навантаження повного циклу RAG-пайплайну, який включає етапи

векторизації, оркестрації агентів та генерації, та є критичним для обробки складних логічних запитів.

Комплексна валідація архітектури на наборі Visual Genome передбачає оцінку модуля пошуку за метриками Recall@k, Precision@k та MRR з урахуванням вимог до затримки (Latency). Ефективність логічного переранжування визначається точністю формування малого контексту та помилкою калібрування (ECE), тоді як якість фінальної генерації перевіряється через порівняння з еталонними відповідями за допомогою лексичних метрик BLEU та ROUGE.

Висновки та перспективи. Запропонована гібридна архітектура має на меті поєднати швидкість векторного пошуку з точністю графового аналізу, що є критичним для глибокого розуміння візуального контексту. Впровадження етапу логічного переранжування (reasoning-first) є доцільним для фільтрації семантично близьких, але логічно невідповідних результатів, а використання механізмів верифікації цитувань сприяє підвищенню надійності генерації. Подальші дослідження можуть бути спрямовані на емпіричне визначення оптимального балансу між векторною та графовою складовими при формуванні контексту. Перспективним є впровадження багаторівневого кешування для зменшення навантаження на базу знань та оптимізації параметрів індексації.

Список використаних джерел

1. Radford A. et al. Learning Transferable Visual Models From Natural Language Supervision [Електронний ресурс] // arXiv. 2021. Preprint arXiv:2103.00020. Режим доступу: <https://arxiv.org/abs/2103.00020> (дата звернення: 19.11.2025).
2. Choudhary M. Hybrid Agentic RAG with Neo4j and Weaviate using LlamaAgent [Електронний ресурс] // Medium. 2024. Режим доступу: <https://medium.com/@milind.choudhary.42/hybrid-agentic-rag-with-neo4j-and-weaviate-using-llamaagent-b09a517e949e> (дата звернення: 19.11.2025).
3. Briggs J. Hierarchical Navigable Small Worlds (HNSW) [Електронний ресурс] // Pinecone Learn Series. б. р. Режим доступу: <https://www.pinecone.io/learn/series/faiss/hnsw/> (дата звернення: 19.11.2025).
4. Vector Search and Knowledge Graphs: Better Together [Електронний ресурс] // Neo4j Blog. б. р. Режим доступу: <https://neo4j.com/blog/developer/vectors-graphs-better-together/> (дата звернення: 19.11.2025).
5. What are the key configuration parameters for an HNSW index [Електронний ресурс] // Milvus Documentation. б. р. Режим доступу: <https://milvus.io/ai-quick-reference/what-are-the-key-configuration-parameters-for-an-hnsw-index-such-as-m-and-efconstructionefsearch-and-how-does-each-influence-the-tradeoff-between-index-size-build-time-query-speed-and-recall> (дата звернення: 19.11.2025).

Майборода Максим Володимирович
аспірант 2 курсу, групи АКСМ-21
Державний університет інформаційно-комунікаційних технологій
(067) 344-28-25
max.mayboroda@gmail.com

КВАНТОВІ МЕТОДИ ЗНАХОДЖЕННЯ РОЗВ'ЯЗКІВ ЛІНІЙНИХ СИСТЕМ

Постановка задачі. Знаходження розв'язків систем лінійних рівнянь є фундаментальною задачею сучасної математики, фізики, економіки і комп'ютерних наук. Однак розв'язання подібних задач у багатовимірних класичних системах потребує значних обчислювальних ресурсів. Багато досліджень показали, що квантові алгоритми мають переваги для розв'язання деяких задач з великим обчислювальним навантаженням порівняно з традиційними класичними алгоритмами.

Мета дослідження. Метою дослідження є аналіз способів рішення лінійних задач на класичних і квантових комп'ютерах. Вивчення структурних підходів до розв'язання задач, виявлення недоліків та подальших перспектив розвитку.

Результати. Розглянутий алгоритм фазової оцінки який одним з найважливіших квантових алгоритмів. Розглянуто процес кодування матричних і векторних даних у нормовані квантові стани і знаходження розв'язків алгоритмом HHL:

$$A |w\rangle = |b\rangle, |b\rangle = \frac{1}{\|X^T y\|} X^T |y\rangle.$$

Ця процедура потребує знаходження власних чисел матриці A . Це може бути реалізовано за допомогою алгоритму фазової оцінки. Алгоритм оцінки фази (QPE) — це квантовий алгоритм, який дозволяє знайти фазу власного значення унітарного оператора.

Якщо оператор U діє на власний стан $|u\rangle$:

$$U |u\rangle = e^{i\lambda_i} |u\rangle$$

Це означає що унітарний оператор представляється у вигляді

В цей же час використовуючи унітарну операцію $\Lambda(U)$ і перетворення Фур'є алгоритм реалізує наступне перетворення.

$$|u_i\rangle|0\rangle^{\otimes t} \xrightarrow{QPE} |u_i\rangle|\bar{\lambda}_i\rangle$$

де λ - фаза власного значення $e^{i\lambda}$ унітарного оператора U .

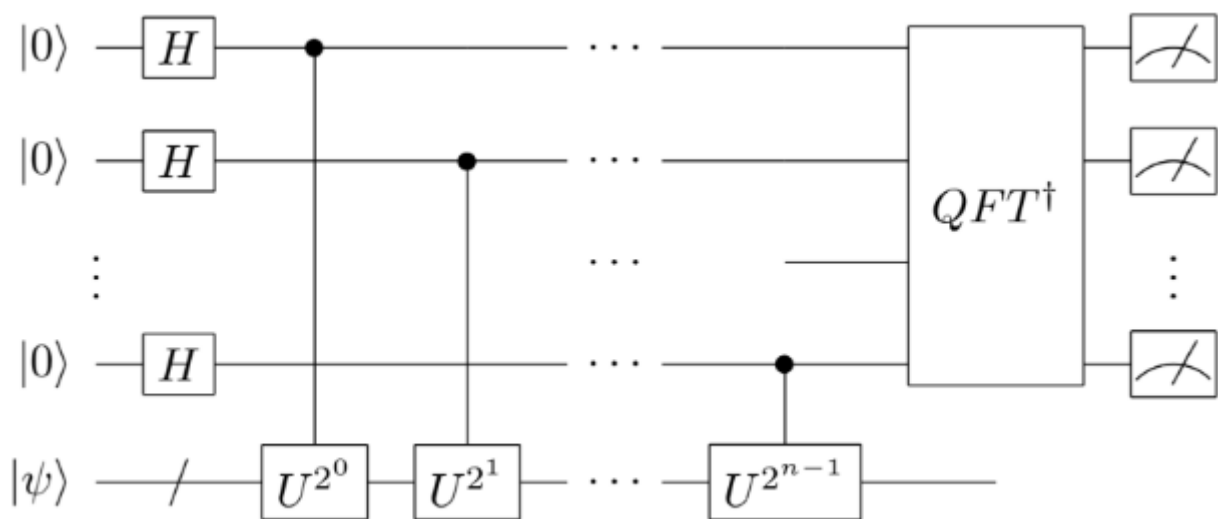


Рис.1 Цикл фазової оцінки

Висновки та перспективи. Актуальні дослідження показали, що квантові алгоритми мають переваги для розв'язання деяких задач з великим обчислювальним навантаженням порівняно з традиційними класичними алгоритмами. Опанування квантових алгоритмів значно спрощує розуміння сучасного світу, технологій і проблем.

Перспективою подальшого дослідження є створення алгоритмів які розв'язують задачі машинного навчання і штучного інтелекту з великим обчислювальним навантаженням.

Список використаних джерел

1. Phase estimation algorithm. URL: https://dojo.qulacs.org/en/latest/notebooks/0_prologue.html (дата звернення: 30.11.2025).
2. Quantum Algorithm Implementations for Beginners. URL: <http://arxiv.org/pdf/1804.03719> (дата звернення: 30.11.2025).
3. Kai Li Hongyi Dai Feng Jing Mei Gao Bin Xue Pu Wang and Ming Zhang. Quantum Algorithms for Solving Linear Regression Equation. 2nd International Conference on Electronics and Communication, Network and Computer Technology (ECNCT) 2020 23-25 October 2020. Volume 1738. DOI 10.1088/1742-6596/1738/1/012063

Ніщенко Дмитро Олександрович
аспірант 2 курсу, групи АКСМ-21
Державний університет інформаційно-комунікаційних технологій
dima.nishchemenko@gmail.com
Науковий керівник: Аронов Андрій Олексійович,
кандидат технічних наук, доцент,
доцент кафедри Технологій цифрового розвитку
Державного університету інформаційно-комунікаційних технологій.

ГІБРИДНА КЛАСИФІКАЦІЙНО-КЕРОВАНА АРХІТЕКТУРА ДЛЯ НАДІЙНОЇ ОЧИСТКИ ГЕТЕРОГЕННИХ ДАНИХ ІОТ

Постановка задачі. Сучасні системи «розумного будинку» та екосистеми Інтернету речей (IoT) генерують безперервні потоки сенсорних даних, які є основою для автоматизованого управління, аналітики та оптимізації енергоспоживання [1]. Однак надійність цих даних часто знижується через наявність гетерогенних шумів, таких як дрейф сенсорів, викиди, постійні значення та загальний шум [2]. Традиційні підходи до очистки даних є не адаптивними, тобто застосовують алгоритми згладжування до всього часового ряду без розрізнення шумів та валідних даних, що призводить до проблеми надлишкового згладжування, коли чисті сегменти сигналу спотворюються фільтром, що фактично вносить помилку в якісні дані [3,4].

Мета дослідження. Метою роботи є розробка та дослідження нової гібридної адаптивної архітектури H-AD-CLEAN для очистки сенсорних даних.

Результати дослідження. У ході дослідження було розроблено архітектуру, що складається з двох ключових компонентів: гібридного класифікатора шумів та логічного модуля керування очисткою.

Для аналізу сигналу використано гібридний класифікатор, який паралельно обробляє дані у ковзному вікні розміром 60 точок. Перша гілка класифікатора використовує одновимірну згорткову нейронну мережу (1D-CNN) для аналізу форми сигналу та локальних патернів, що дозволяє виявляти викиди та дрейф. Друга гілка застосовує дискретне вейвлет-перетворення (DWT) для аналізу текстурних та частотних характеристик, що є ефективним для розрізнення загального шуму. Загальна архітектура системи, представлена на Рисунку 1.

Навчання та тестування на синтетичному наборі даних («Contrast», 15 000 точок) із використанням 5-кратної перехресної перевірки показало високу ефективність запропонованого підходу. Класифікатор досяг усередненої F1-міри 0,75, при цьому для критично важливого класу «Чисті дані» (Clean) F1-міра склала 0,85. Це підтверджує здатність системи надійно ідентифікувати сегменти, що не потребують втручання.

Проведений сегментований аналіз виявив фундаментальні недоліки стандартного фільтра Калмана: при обробці чистих сегментів він вносив середню абсолютну помилку (MAE) на рівні 0,2013. Натомість запропонована система H-

AD-CLEAN (v2), яка пропускає чисті дані без змін, знизила помилку на цих ділянках майже до нуля (MAE 0,0074), що є покращенням на 96,3%.

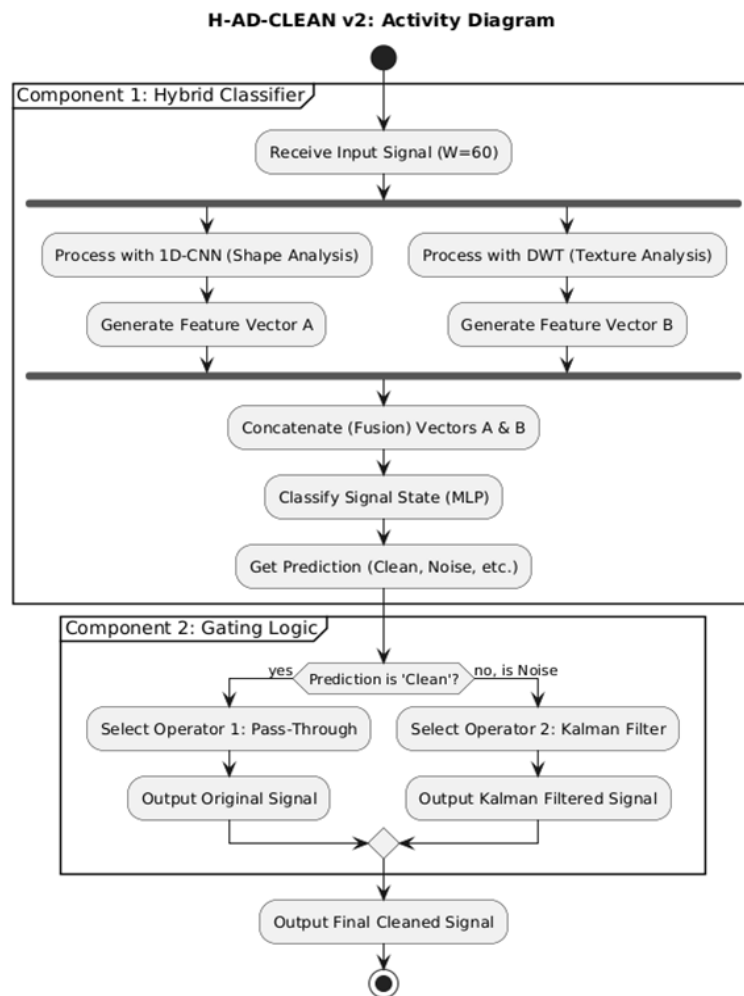


Рис. 1: Блок-схема архітектури H-AD-CLEAN.

Таблиця 1

Фінальне порівняння загальної ефективності очищення

Метод	RMSE (↓)	MAE (↓)	Покращення RMSE (%)	Покращення MAE (%)
Забруднений сигнал	1.0758	0.4824	---	---
Ковзне Медіанне	0.9679	0.6811	10.03%	-41.19%
Фільтр Калмана	0.7175	0.4126	33.31%	14.47%
H-AD-CLEAN (v2 Hybrid)	0.7029	0.3253	34.66%	32.57%

У загальному порівнянні ефективності очистки на всьому тестовому наборі даних розроблена система перевершила всі базові методи. Порівняно зі стандартним фільтром Калмана, H-AD-CLEAN досягла покращення середньоквадратичної помилки (RMSE) на 34,66% (0,7029 проти 0,7175) та

покращення середньої абсолютної помилки (MAE) на 21,1% (0,3253 проти 0,4126).

Висновки та перспективи. У роботі запропоновано та експериментально перевірено адаптивну архітектуру очистки даних IoT. Доведено, що підхід, керований класифікацією, є значно ефективнішим за традиційну фільтрацію.

Стандартні фільтри, такі як фільтр Калмана, хоч і ефективні для згладжування шуму, значно спотворюють валідні дані, що знижує загальну якість інформації в системах управління.

Використання гібридної моделі (CNN + DWT) дозволяє з високою точністю розпізнавати типи шумів та аномалій.

Запропонована система H-AD-CLEAN забезпечує «хірургічну» точність очистки: вона інтелектуально захищає чисті дані від непотрібного згладжування, застосовуючи фільтрацію лише там, де це необхідно. Це дозволило досягти зниження типової помилки (MAE) на 21,1% порівняно з кращими базовими методами. Такий підхід є перспективним рішенням для забезпечення цілісності даних у гетерогенних IoT-системах та підвищення їх стійкості до маніпуляцій.

Список використаних джерел

1. Ding X., Wang H., Li G. et al. IoT data cleaning techniques: A survey. *Intelligent and Converged Networks*. 2022. Vol. 3, No. 4. P. 325–339. DOI: <https://doi.org/10.23919/icn.2022.0026>.
2. Wang X., Wang C. Time Series Data Cleaning: A Survey. *IEEE Access*. 2019. Vol. 8. P. 1866–1881. DOI: 10.1109/access.2019.2962152.
3. Kasaraneni P. P., Kumar Y. V. P. et al. Machine learning-based ensemble classifiers for anomaly handling in smart home energy consumption data. *Sensors*. 2022. Vol. 22(23). P. 9323. DOI: <https://doi.org/10.3390/s22239323>.
4. N. An, Y. Ding and H. Zhao, "Statistical feature analysis and preprocessing assisted artificial neural network for cleaning multi-type concurrent anomalies in time series data," 2024 7th International Symposium on Autonomous Systems (ISAS), Chongqing, China, 2024, pp. 1-5, doi: 10.1109/ISAS61044.2024.10552599.

Доманецька Ірина Миколаївна
к.т.н., доцент кафедри інтелектуальних технологій
Київського національного університету імені Тараса Шевченка
(050) 387-34-25
domanetska@knu.ua
Хроленко Ярослав Олексійович
аспірант 4 курсу
Інститут проблем реєстрації інформації НАН України
(099) 434-17-99
yaroskhr@gmail.com

ТОНКЕ НАЛАШТУВАННЯ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ ПІД ЕКСПЕРТНІ ДОМЕНИ

Постановка задачі. Сучасні великі мовні моделі (Large Language Models, LLM) демонструють значний потенціал для автоматизації та підтримки процесів наукової експертизи. Вони здатні опрацьовувати великі обсяги текстової інформації, виконувати узагальнення, формувати висновки та перевіряти логічну послідовність аргументів. Проте базові моделі, які орієнтовані на широке коло задач, не завжди забезпечують необхідну точність та відповідність доменним стандартам, що особливо критично для задач, пов'язаних з рецензуванням наукових робіт, аналізом грантових заявок, технічною оцінкою експериментальних протоколів та верифікацією методологій.

Однією з основних проблем у застосуванні LLM для наукової експертизи є недостатня адаптованість до вузьких доменів. Базові моделі мають загальні знання, що може призводити до генерації некоректних тверджень, пропуску критично важливих деталей та порушення стандартів дисциплінарної термінології. В умовах наукової роботи такі неточності можуть вплинути на якість висновків та рішення щодо публікацій, грантів або експериментальних оцінок. У зв'язку з цим постає завдання тонкого налаштування LLM, що дозволяє зберегти їх загальні здібності, водночас підвищивши точність та релевантність відповідей у конкретних експертних доменах.

Метою дослідження є аналіз сучасних методів адаптації великих мовних моделей до вузьких наукових доменів, порівняння трьох основних підходів — Low-Rank Adaptation (LoRA), адаптерних шарів (Adapters) та промпт-програмування (Prompt Programming) — за критеріями точності, ефективності, гнучкості та ресурсозатратності, а також формування рекомендацій щодо їх комбінації для підвищення якості автоматизованих експертних процесів.

Результати дослідження. Метод LoRA передбачає введення низькорангових матриць у трансформер, які навчаються на доменних даних, тоді як базова модель залишається замороженою. Такий підхід дозволяє зменшити кількість параметрів для оптимізації, забезпечуючи високу точність у вузькому домені та економію обчислювальних ресурсів [1]. LoRA особливо ефективна при оцінці методологій, аналізі біомедичних даних, перевірці статистичних моделей

та технічній експертизі, де важлива точність інтерпретацій. Однак вона потребує наявності доменного корпусу, а також ризикує перенавчитися на вузьких даних, що може обмежувати її переносимість на інші галузі.

Адаптерні шари інтегруються між основними шарами трансформера, навчаючись на доменних даних без зміни базових параметрів моделі. Така модульність дозволяє створювати кілька адаптерів для різних дисциплін та швидко перемикається між ними [2]. Адаптери забезпечують стабільність роботи моделі та зручність для мультидисциплінарних платформ, зокрема для університетських систем та редакцій журналів. Водночас їхня інтеграція є складнішою, вони потребують якісного розмічення даних і вимагають більших ресурсів для навчання порівняно з LoRA.

Промпт-програмування є непараметричним методом, що передбачає керування поведінкою LLM за допомогою спеціально сформованих інструкцій, ролей та шаблонів. Промпти дозволяють вказати модель, яку роль вона має виконувати, які правила міркування застосовувати та який формат відповідей очікується [3]. Цей підхід не потребує додаткового навчання, його інтеграція миттєва, а гнучкість у використанні дозволяє швидко створювати сценарії експертизи. Проте промпти не забезпечують глибокого доменного знання та є менш стабільними при роботі зі специфічними запитами. Високий рівень ефективності залежить від майстерності розробника промπτів, а також від якості вхідних інструкцій.

Порівняльний аналіз показує, що LoRA та адаптери забезпечують високу точність у доменних задачах, тоді як промпт-програмування забезпечує швидкість впровадження та гнучкість, але має середню точність. LoRA є економічною з точки зору обчислювальних ресурсів, адаптери забезпечують високу універсальність та можливість мультидисциплінарного використання, а промпти дозволяють швидко масштабувати систему без додаткового навчання. Усі три підходи мають свої обмеження, тому для досягнення найкращих результатів часто застосовують їх комбінації.

У практичних сценаріях, таких як оцінка грантових заявок, рецензування рукописів та технічна експертиза, оптимально застосовувати гібридні стратегії. Найбільш поширені підходи включають комбінацію LoRA, адаптерних шарів та промпт-програмування. Використання LoRA забезпечує глибоке доменне навчання на спеціалізованих корпусах, дозволяючи моделі опановувати складну термінологію та специфіку вузького предметного поля. Проте навіть після LoRA модель може не містити актуальних фактів, тому її поєднують із Retrieval-Augmented Generation (RAG), який дозволяє динамічно звертатися до баз даних, наукових публікацій і актуальних джерел. Така інтеграція гарантує поєднання точності доменних знань із достовірністю та актуальністю відповідей. Адаптерні шари додають системі модульності та мультидисциплінарності, оскільки кожен адаптер тренується на власному наборі доменних даних, що дозволяє легко перемикається між дисциплінами без перенавчання основної моделі. Промпт-програмування, у свою чергу, забезпечує контроль формату і структури висновку,

стандартизує відповіді, задає роль експерта та правила логіки міркувань, що критично для автоматизованих систем рецензування та оцінки грантів.

Отже, при комплексному застосуванні ці три підходи створюють гібридні пайплайни, де LoRA відповідає за глибину знань, адаптери — за ширину та мультидисциплінарність, а промпти — за стандартизовану структуру та контроль якості.

Додатково застосовується інтеграція з функціями перевірки, Chain-of-Thought або спеціалізованими скриптами, що дозволяє реалізувати перевірку фактів, контроль форматування, структурування результатів та автоматизацію рутинних процедур [4]. Така комбінація дозволяє максимально ефективно впроваджувати LLM у наукову експертизу, підвищувати точність висновків, знижувати ризик галюцинацій та забезпечувати відтворюваність результатів у різних дисциплінарних контекстах, створюючи основу для стандартизованих, надійних та гнучких систем автоматизованої оцінки наукових робіт.

Висновки та перспективи. Висновки дослідження свідчать про те, що тонке налаштування LLM є ключовим етапом інтеграції моделей у наукову експертизу. Кожен із розглянутих методів має свої сильні сторони та обмеження, і вибір підходу залежить від специфіки домену, наявності навчальних корпусів, ресурсних можливостей та вимог до точності. Найбільш ефективним є використання гібридних стратегій, що поєднують LoRA, адаптери та промпт-програмування, а також інструменти перевірки фактів, що дозволяє підвищити якість та достовірність наукових висновків. Такий підхід сприяє стандартизації експертних процедур, забезпечує їх відтворюваність і дозволяє ефективно впроваджувати LLM у практику наукової роботи.

Список використаних джерел

1. Hu E. J., Shen Y., Wallis P., et al. LoRA: Low-Rank Adaptation of Large Language Models [Електронний ресурс]. — arXiv:2106.09685, 2021. — URL: <https://arxiv.org/abs/2106.09685> (дата звернення: 29.11.2025).
2. Pfeiffer J., Kamath A., Rücklé A., et al. AdapterFusion: Non-Destructive Task Composition for Transfer Learning // Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics (ACL). — Online, 2020. — P. 1255–1270. — ACL Anthology ID: 2020.acl-main.115. — URL: <https://aclanthology.org/2020.acl-main.115> (дата звернення: 29.11.2025).
3. OpenAI. GPT Prompting Best Practices [Електронний ресурс]. — OpenAI Documentation, 2023. — URL: <https://platform.openai.com/docs/guides/prompting> (дата звернення: 29.11.2025).
4. Wei J., Wang X., Schuurmans D., et al. Chain-of-Thought Prompting Elicits Reasoning in Large Language Models [Електронний ресурс]. — arXiv:2201.11903, 2022. — URL: <https://arxiv.org/abs/2201.11903> (дата звернення: 29.11.2025).

Черевик Олексій В'ячеславович
аспірант 4 курсу, групи АКСМ 41
Державний університет інформаційно-комунікаційних технологій
(068) 700-18-52
o.cherevik@stud.duikt.edu.ua

ВИДАЛЕННЯ ШУМІВ У ДАНИХ 3D-СКАНУВАННЯ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

Постановка задачі Технології тривимірного сканування нині широко застосовують у таких галузях, як промисловість, медицина, збереження культурної спадщини, робототехніка та геодезія. Завдяки методикам лазерного сканування, структурованого світла чи фотограмметрії можна отримати детальні моделі об'єктів у форматі хмар точок або полігональних сіток [1]. Проте під час збору даних неминуче виникають різні види шумів — випадкові, систематичні, інтерференційні, а також артефакти, спричинені характеристиками поверхні, освітленням або рухом предмета.

Класичні алгоритми фільтрації та згладження (зокрема, середньозважені чи білатеральні фільтри, метод Лапласа, а також MLS-регенерація поверхонь) допомагають знизити рівень шуму, але часто викликають втрату дрібних деталей або «розмивають» контури моделі.

Через це дедалі більшої популярності набуває використання підходів штучного інтелекту для покращення якості 3D-сканів. Системи, що базуються на таких підходах, можуть навчатися на великих наборах даних, відрізняти шум від корисних геометричних елементів і водночас зберігати мікродеталі об'єкта.

Отже, розв'язання проблеми потребує комплексного підходу, який об'єднує глибоке навчання, статистичні методи та сучасні алгоритми реконструкції поверхонь, щоб забезпечити високу точність і стабільність отриманих 3D-моделей.

Мета дослідження. Головна задача цього дослідження полягає у вивченні актуальних способів усунення шумів у 3D-даних на основі технологій штучного інтелекту, а також порівняння їх результативності із традиційними методиками фільтрації [2]. Щоб досягти поставленої мети, окреслимо низку етапів:

1. Розглянути типи та природу шумів, які з'являються в ході тривимірного сканування.
2. Проаналізувати підходи машинного й глибинного навчання, що застосовуються для роботи з хмарами точок і сітковими структурами.
3. Вивчити, в чому полягають переваги та слабкі сторони різних типів нейронних мереж — зокрема автоенкодерів, графових нейромереж і дифузійних моделей — у контексті задач очищення від шуму.
4. Описати поширені архітектури для 3D-аналізу, такі як PointNet, PointNet++, DGCNN, GraphUNet, і з'ясувати їхню роль в удосконаленні просторових моделей.

5. Надати рекомендації щодо впровадження методик штучного інтелекту у прикладних і дослідницьких процесах.

У ході дослідження встановлено таку класифікацію шумів у 3D-сканах:

- геометричні — спричинені випадковими зміщеннями координат точок через неточності сенсорів;
- фотометричні — спотворення, що виникають внаслідок змін освітлення, особливо у фотограмметрії;
- артефакти через особливості поверхонь (блиск, слабка відбивна здатність) — можуть виражатися у вигляді порожнин чи нехарактерних виступів;
- поодинокі викиди (outliers) — поодинокі точки, які не відповідають жодній поверхні.

Сучасні засоби штучного інтелекту дають змогу розпізнавати типові закономірності, властиві справжнім поверхням, що дозволяє досить ефективно розмежовувати небажаний шум і значущу інформацію.

Підходи III для очищення 3D-сканів від шуму включають:

1. Автоенкодері для обробки хмар точок. Одним із найпоширеніших рішень тут є використання варіаційних (VAE) і антишумових (DAE) автоенкодерів. Ці моделі навчаються стискати хмару точок до компактного векторного представлення, після чого відтворюють уже скориговану, «чисту» версію даних. Під час навчання на великій кількості різноманітних зразків мережа поступово опановує навички точного відновлення поверхонь, водночас пригнічуючи різноманітні шуми. Головна перевага автоенкодерів — висока швидкість обробки та здатність відтворювати загальну геометрію моделей, хоча дрібні деталі іноді можуть втрачатися, а самі поверхні поступово згладжуються.

2. Графові нейромережі (GNN). Структуру хмари точок можна подати у вигляді графа: точки виступають у ролі вершин, а їхнє локальне оточення — у вигляді ребер [3]. Графові нейронні мережі, наприклад DGCNN, дозволяють:

- аналізувати локальні патерни на поверхнях;
- оперативно оновлювати зв'язки між сусідніми елементами;
- зберігати структури, що характеризуються різкими перепадами чи виразними геометричними рисами.

Такий підхід добре підходить для виробничих завдань на зразок контролю якості поверхонь деталей.

3. Дифузійні та генеративні моделі. Дифузійні моделі, що показали високу ефективність у сфері генерації двомірних зображень, дедалі активніше застосовують і для 3D-даних [4]. Принцип роботи тут полягає у покроковому додаванні шуму до вхідної хмари точок під час навчання, а потім модель вчиться цей процес запускати у зворотньому напрямку, поступово відновлюючи точну геометрію. Такі методики дозволяють досягати значної точності, навіть коли рівень шуму у даних високий, і успішно відтворювати дрібні елементи поверхонь [5].

Під час дослідження було з'ясовано, що особливо найкращих результатів можна досягти поєднанням графових нейромереж із дифузійними моделями.

Такий спосіб дає змогу зберегти важливі деталі в 3D-даних і водночас якісно обмежити шум.

Таблиця 1

Порівняння методів, що застосовують ІІІ з класичними алгоритмами

Підхід	Переваги	Недоліки
MLS, bilateral-фільтри, Лаплас-фільтри	Простота, швидкість, зрілість технології	Втрата деталей, надмірне згладжування
Автоенкодери	Відновлення глобальної структури, швидка інференція	Можлива втрата дрібних елементів
GNN	Збереження локальних особливостей, хороші результати на складних поверхнях	Висока вимога до обчислювальних ресурсів
Дифузійні моделі	Найвища якість реконструкції, здатність працювати з сильним шумом	Складність тренування, велика кількість параметрів

Висновки. У цій роботі розглянуто сучасні підходи до видалення шуму з 3D-сканів із застосуванням штучного інтелекту. Аналіз показав, що класичні методи, хоча й вміють фільтрувати базові типи шуму, часто неспроможні розрізнити дрібні особливості структури від артефактів, унаслідок чого поверхні втрачають природність і деталізацію.

Глибокі навчальні алгоритми та генеративні моделі демонструють значно кращу якість обробки, дозволяють утримувати мікроструктуру й точно відтворюють складні просторові форми. Серед найбільш дієвих рішень виділено графові нейронні мережі й дифузійні моделі, які вирізняються точністю, гнучкістю та здатністю працювати з великими наборами даних.

Результати свідчать про великі перспективи інтеграції штучного інтелекту в промисловій, дослідницькій та культурній сфері — там, де для 3D-моделювання критично важливими є повнота реконструкції та точність.

Список використаних джерел

1. Charles R. Qi, Hao Su, Kaichun Mo, Guibas L. PointNet: Deep Learning on Point Sets for 3D Classification and Segmentation. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2017. URL: <https://arxiv.org/pdf/1612.00593>
2. Chaojing D, Siheng C, Kovacevic J. Point Cloud Denoising via Deep Learning. IEEE International Conference on Acoustics, Speech, and Signal Processing, 2019. URL: <https://ieeexplore.ieee.org/document/8682812>
3. Wang, Y., Sun, Y., Liu, Z et al. Dynamic Graph CNN for Learning on Point Clouds. ACM Transactions on Graphics (TOG), Volume 38, Issue 5, 2019. URL: <https://dl.acm.org/doi/10.1145/3326362>
4. Bieder F, Wolleb J, Durrer A et al. 3D Denoising using Diffusion Models. Proceedings of Machine Learning Research 227:552–567, 2023. URL: Proceedings of Machine Learning Research 227:552–567, 2023
5. Berger, M., Tagliasacchi, A., Seversky, L. M. et al. A Survey of Surface Reconstruction from Point Clouds. Computer Graphics Forum, 2017. URL: <https://onlinelibrary.wiley.com/doi/10.1111/cgf.12802>

Шлянчак Світлана Олександрівна

доцент кафедри інформаційних та цифрових технологій

Центральноукраїнський державний університет імені Володимира Винниченка

(066) 401-70-22

s.o.shlianchak@cuspu.edu.ua

МЕТОДИ ОБРОБКИ ГРАФІВ У ГРАФОВИХ НЕЙРОННИХ МЕРЕЖАХ

Постановка задачі. Графові нейронні мережі (GNN) зарекомендували себе як високопродуктивний засіб для вирішення задач на графових даних, які природно виникають у багатьох предметних областях (соціальні мережі, молекулярні структури, транспортні системи тощо). Ефективність та продуктивність GNN критично залежать від їх архітектури, зокрема від трьох ключових модулів: розповсюдження (передача інформації між вузлами), вибірки (вибір підмножини елементів графа) та об'єднання (агрегація інформації для отримання узагальнених представлень). Тому актуальним є аналіз цих модулів, які б забезпечили найвищу якість представлень графових даних при мінімальних обчислювальних витратах. Існуючі архітектури GNN часто застосовують універсальні підходи до цих модулів, що може бути неефективним для графів зі специфічними топологічними властивостями або для задач, що вимагають різного рівня деталізації.

Мета дослідження. Метою роботи є формулювання рекомендацій щодо вибору та комбінування модулів розповсюдження, вибірки та об'єднання для побудови архітектур GNN, які демонструватимуть підвищену ефективність та адаптивність до різних типів графових даних та конкретних завдань.

Результати дослідження. Обробка графових даних у графових нейронних мережах (GNN) реалізується через основні функціональні модулі: розповсюдження (Propagation), вибірки (Sampling) та об'єднання (Pooling).

Центральною ідеєю модулів розповсюдження, найпоширенішими з яких є оператори згортки, є оновлення властивостей кожного вузла на основі інформації та властивостей його сусідніх вузлів, здійснюючи таким чином обмін інформацією. Ці оператори згортки можуть бути реалізовані двома основними підходами: спектральним та просторовим. Спектральні підходи базуються на теорії спектральних властивостей графів, де графовий сигнал перетворюється у спектральний простір за допомогою графового перетворення Фур'є, і згортка обчислюється як перемноження вхідного сигналу на фільтр у цьому просторі (наприклад, методи ChebNet) [1]. Натомість, просторовий підхід застосовує згортки безпосередньо на графі, спираючись на його топологію, але стикається з проблемами, пов'язаними з різноманітністю кількості сусідів та необхідністю збереження локальної інваріантності. Окрім згорткових, існують рекурентні оператори розповсюдження, ідея яких схожа до операторів згортки: кожен вузол ітеративно оновлює свій внутрішній стан, але, на відміну від згорткових, вони використовують однакову вагу для всіх шарів. Рекурентні оператори використовують методи на основі збіжності (орієнтовані на стабільність

прихованих станів) та методи на основі воріт (використовують механізми контролю потоку інформації, як-от Graph LSTM).

Модулі вибірки використовуються для подолання проблеми «вибуху сусідів», коли великий обсяг інформації перевантажує обчислення. Вони обирають лише підмножину сусідніх вузлів або інформації для аналізу.

Механізми вибірки включають вибірку вузлів (відбір обмеженої кількості сусідів), пошарову вибірку (збереження невеликого набору вузлів для агрегації в кожному шарі) та вибірку підграфів (обмеження аналізу межами певних підграфів) [2].

Модулі об'єднання (Pooling) в архітектурах графових нейронних мереж виконують функцію агрегації ознак та інформації з різних підструктур графа, що забезпечує формування високорівневих, узагальнених представлень (graph-level representations). Цей процес є критично важливим для вирішення задач класифікації та прогнозування на рівні всього графа. За механізмом дії розрізняють прямі методи об'єднання, які здійснюють агрегацію на одному шарі або рівні, та ієрархічні методи, що оперують на послідовних рівнях графової структури для побудови абстрактних ієрархічних ознак [3].

Висновки та перспективи. У рамках дослідження було розглянуто та систематизовано ключові функціональні модулі, які визначають архітектуру GNN. Проведений порівняльний аналіз дозволив систематизувати переваги та недоліки кожного з розглянутих підходів з точки зору обчислювальної ефективності та якості отриманих представлень для великих та топологічно складних графових даних. Зокрема, було підкреслено необхідність збалансувати обчислювальну складність (проблема «вибуху сусідів», характерна для згорткових операторів) із здатністю зберігати критичну структурну інформацію графа. Перспективою подальших досліджень є створення адаптивних алгоритмів побудови архітектур GNN, які автоматично обиратимуть оптимальні комбінації модулів розповсюдження, вибірки та об'єднання, виходячи з топологічних характеристик вхідного графа та специфіки цільової задачі (наприклад, класифікація вузлів, прогнозування зв'язків чи класифікація графа в цілому). Актуальним також є вивчення можливості інтеграції механізмів уваги (attention) безпосередньо в модулі вибірки та об'єднання для динамічного фокусування на найбільш інформативних частинах графа.

Список використаних джерел

1. P. Kaluzny, "Counting stable equilibria of cellular neural networks-A graph theoretic approach", Proc. Int. Workshop Cellular Neural Netw. Appl., pp. 112-116, 1992.
2. М. Рідміллер і Х. Браун, "Прямий адаптивний метод для швидшого зворотного навчання: алгоритм rprop", Proc. IEEE Int. конф. Нейронна мережа. , стор. 586-591, 1993.
3. G. Monfardini, V. Di Massa, F. Scarselli and M. Gori, "Graph neural networks for object localization", Proc. 17th Eur. Conf. Artif. Intell., pp. 665-670, 2006-Aug.

Юрченко Костянтин Юрійович
аспірант

Інститут програмних систем Національної академії наук України
Urchikak8@gmail.com

ІНТЕЛЕКТУАЛЬНІ МЕТОДИ АНАЛІЗУ Й УПРАВЛІННЯ ФУНКЦІОНАЛЬНІСТЮ КОРПОРАТИВНОГО САЙТУ В УМОВАХ ЗМІННОГО СЕРЕДОВИЩА

Постановка задачі. У сучасних умовах корпоративний сайт перестає бути лише інформаційним ресурсом і перетворюється на динамічну платформу взаємодії з клієнтами, партнерами та внутрішніми користувачами. Нестабільність бізнес-середовища, зміни користувацької поведінки, коливання навантаження та зростання вимог до персоналізації послуг створюють потребу в інтелектуальних методах аналізу і керування функціональністю сайту. Основна проблема полягає в тому, що традиційні підходи до оптимізації веб-систем ґрунтуються на статичних конфігураціях та ручному моніторингу, що унеможливорює оперативну адаптацію інтерфейсу, структури контенту й технічних параметрів до динамічних умов функціонування.

Мета дослідження. Метою дослідження є розроблення й обґрунтування інтелектуальних методів аналізу й управління функціональністю корпоративного сайту, здатних забезпечити його адаптивну поведінку, оптимальну продуктивність і стійкість до змін зовнішнього середовища. У межах дослідження передбачено:

- формування моделі динамічної оцінки функціональних модулів сайту;
- використання машинного навчання та методів поведінкового аналізу користувачів;
- застосування алгоритмів адаптивного керування та автоматичного переформатування контенту;
- побудову рекомендаційної системи оптимізації технічних та UX-параметрів.

Результати дослідження. На початковому етапі дослідження було проаналізовано типові чинники, що впливають на функціональність корпоративного сайту: навантаження (трафік), зміна користувацької поведінки, оновлення сервісних компонентів, зміни в контенті, а також зовнішні ризики (DDOS, SEO-коливання, відмови доменних сервісів). Встановлено, що ефективне управління можливе лише за умов інтеграції потокових даних із систем журналювання, веб-аналітики, моніторингу інфраструктури та поведінкової аналітики.

У ході дослідження розроблено інтелектуальну модель управління функціональністю корпоративного сайту, що ґрунтується на використанні поведінкових метрик, телеметричних даних, а також алгоритмів кластеризації та прогнозування.

У ході дослідження розроблено інтелектуальну модель управління функціональністю корпоративного сайту, що ґрунтується на використанні поведінкових метрик, телеметричних даних, а також алгоритмів кластеризації та прогнозування (рис 1).

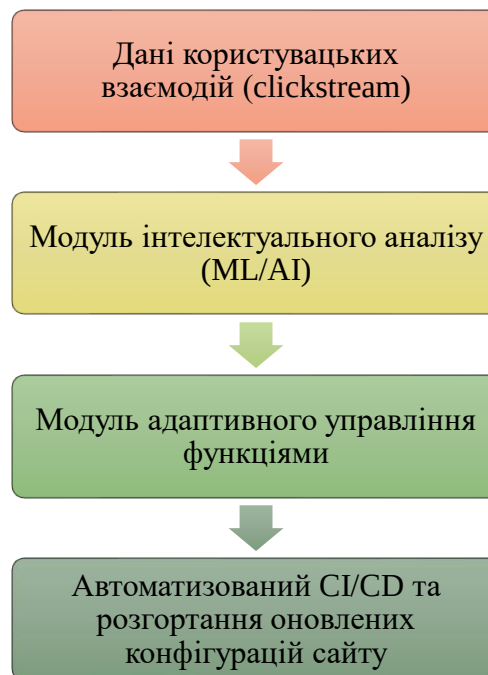


Рис. 1 Структурно-логічна схема інтелектуального управління

Модель дозволяє:

- підвищити конверсійність завдяки персоналізованому UX;
- зменшити навантаження на сервери через вимкнення непотрібних компонентів у реальному часі;
- покращити доступність та продуктивність шляхом автоматичного перерозподілу ресурсів;
- підвищити стійкість до різких змін поведінки користувачів (наприклад, пікові події, маркетингові кампанії).

Експериментальне застосування моделі на тестовому корпоративному сайті показало зростання середньої ефективності взаємодії користувачів на 18–27 %, а також скорочення часу завантаження окремих модулів на 25–40 %.

Висновки та перспективи У роботі обґрунтовано доцільність застосування інтелектуальних методів для аналізу та адаптивного управління функціональністю корпоративного сайту. Запропонована модель дозволяє сформувати динамічну систему, що автоматично реагує на зміни користувацької поведінки та зовнішнього середовища.

Перспективи подальших досліджень:

інтеграція методів глибокого навчання для прогнозування складніших шаблонів поведінки;

розширення системи за рахунок мультиканальних даних (соціальні мережі, CRM, мобільний трафік);

побудова автономних агентів для автоматичного налаштування сайту без участі адміністратора.

Список використаних джерел

1. National Institute of Standards and Technology. (2022). NIST Special Publication 800-30: Guide for Conducting Risk Assessments.
2. European Union Agency for Cybersecurity. (2023). ENISA Threat Landscape 2023.
3. Cherdantseva, Y., Hilton, J. (2019). A Reference Model of Information Security Risk Management. *Information & Computer Security*, 27(3).
4. Sterbenz, J. P., Hutchison, D. (2020). Resilience and Survivability in Communication Networks. *IEEE Communications Surveys & Tutorials*, 22(1).
5. Gartner Research. (2023). Optimize Cybersecurity Spending Under Crisis Conditions.

Язвінська Діана Ігорівна
студентка 1 курсу, групи ЗАІ-201
Національний університет «Одеська політехніка»
(096) 496-69-12
yazvinskadiana@gmail.com

МЕТОДОЛОГІЯ ІНТЕГРАЦІЇ МАШИННОГО НАВЧАННЯ ТА ДИНАМІЧНОГО ГЕНЕРУВАННЯ КОНТЕНТУ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ НАВЧАННЯ

Постановка задачі. Системи електронного навчання (E-learning) все частіше використовуються для підготовки студентів, проте традиційні статичні навчальні матеріали не враховують індивідуальну динаміку засвоєння знань. Це призводить до низької ефективності підготовки та неоптимального використання навчального часу. Тому актуальною є розробка методології, яка забезпечить **персоналізацію** освітнього контенту в режимі реального часу, використовуючи потенціал технологій Машинного Навчання (МН) та динамічного генерування завдань [1].

Мета дослідження. Метою дослідження є теоретичне обґрунтування та розробка методології інтеграції МН та динамічного генерування контенту для створення Інтелектуальної адаптивної навчальної системи (ІАНС) [2], а також експериментальне підтвердження її здатності підвищувати ефективність підготовки студентів.

Результати дослідження. Розроблена методологія ґрунтується на архітектурі Інтелектуальної адаптивної навчальної системи (ІАНС), що включає центральний керуючий елемент — Ядро AI/Адаптивний двигун. Цей двигун використовує специфічні алгоритми Машинного Навчання (МН) для побудови та постійного оновлення Моделі Студента. На відміну від статичних методів, Модель Студента у даній ІАНС є динамічною та ієрархічною: вона не лише фіксує відсоток правильних відповідей, але й відображає ступінь засвоєння окремих когнітивних навичок, час реакції та стійкість до помилок. Завдяки цій деталізації система може точно визначити актуальні прогалини у знаннях та когнітивні патерни користувача, що є основою для подальшої адаптації.

На відміну від систем з фіксованим контентом, запропонований підхід забезпечує швидке коригування навчальної траєкторії, уникаючи подачі неактуального, або надто складного чи, навпаки, занадто легкого контенту. Це досягається завдяки тому, що Ядро AI на кожному кроці навчання ухвалює рішення, мінімізуючи "ентропію незнання" студента. До основних компонентів методології належать: формалізація вимог до Базы знань/Банку завдань, що є основою для Динамічного Генерування Контенту (ДГК) [3]. Встановлено, що ефективність ДГК прямо залежить від якості метаданих (параметрів складності, теми, типу помилки), які використовуються як вхідні дані для МН.

Ключовим результатом є застосування алгоритмів МН (зокрема, імовірнісних моделей або методів, що ґрунтуються на навчанні з підкріпленням)

для оптимального ухвалення рішень. Це дозволяє системі динамічно генерувати унікальні практичні завдання, які відповідають індивідуальній потребі студента, тим самим інтегруючи динаміку навчального процесу в процес створення контенту.

Проведене експериментальне тестування (А/В дизайн) підтвердило, що ІАНС, побудована за цією методологією, демонструє високу ефективність за критеріями, які є важливими для прикладного дослідження: скорочення загального часу підготовки (як показник ефективності) та зростання середнього балу за підсумковими контролюми (як показник якості засвоєння). Це доводить, що розроблена методологія забезпечує не просто адаптацію, а статистично значуще підвищення продуктивності освітнього процесу.

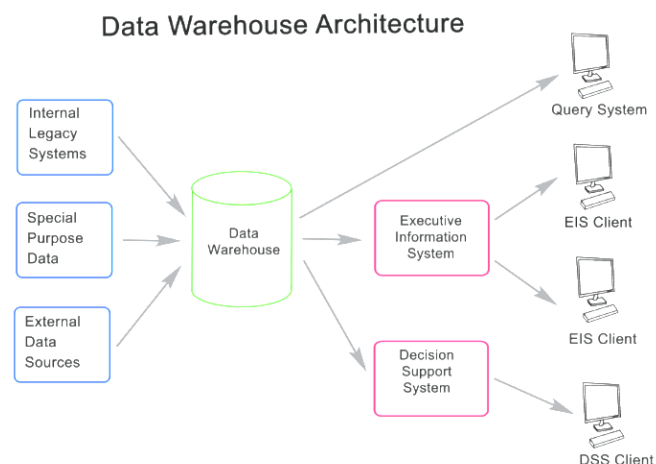


Рис. 1. Блок-схема алгоритму адаптивного навчання в ІАНС

Блок-схема відображає цикл адаптації знань в Інтелектуальній адаптивній навчальній системі (ІАНС) та логіку інтеграції Машинного Навчання (МН) і Динамічного Генерування Контенту (ДГК). Процес є циклічним і починається з Початку сеансу (вхід студента), після чого система видає студенту поточне завдання. Ключова взаємодія починається, коли система отримує Введення відповіді від студента. Цикл адаптації знань починається з Оцінювання та Фіксації, коли введені студентом дані надходять до Модуля Оцінювання, який перевіряє правильність відповіді та фіксує всі необхідні метадані, такі як час виконання та тип допущеної помилки. Оцінені дані негайно передаються для Оновлення Моделі Студента (МС). Тут використовується МН-алгоритм для динамічного оновлення профілю знань користувача, що є критично важливим для забезпечення точного відображення поточного когнітивного стану. Далі система виконує Перевірку Критерію Завершення, де перевіряється, чи було досягнуто мету навчального сеансу, і якщо так, сеанс завершується.

Якщо сеанс триває, настає етап Прийняття Адаптивного Рішення в Ядрі AI. Ядро аналізує оновлену МС і, використовуючи алгоритми Машинного Навчання, ухвалює рішення щодо оптимальної складності та тематики наступного завдання, спрямовуючи рішення на максимальне подолання поточних прогалин. Після цього Модуль Динамічного Генерування Контенту (ДГК) отримує ці параметри від Ядра AI, звертається до Бази знань/Банку завдань, обирає

відповідний шаблон і створює нове, унікальне та персоналізоване практичне завдання. Завершується цикл Виведенням Завдання, коли нове завдання подається студенту через інтерфейс, і цикл адаптації повторюється.

Для реалізації такої складної системи як ІАНС, яка інтегрує МН, доцільно використовувати Python як основну мову програмування, оскільки вона надає найширшу екосистему бібліотек для Машинного Навчання (МН) та Науки про дані, наприклад, Scikit-learn або PyTorch, які можуть бути використані для реалізації алгоритмів Моделювання Студента та логіки прийняття адаптивних рішень.

Back-end (серверна логіка), що відповідає за управління сеансами та реалізацію логіки ДГК, може бути розроблений на фреймворках Django або Flask. База даних для зберігання великих обсягів метаданих та динамічних профілів студентів може бути реалізована на PostgreSQL або MongoDB. Для Front-end (інтерфейсу користувача) для створення сучасного та адаптивного вигляду системи, рекомендується використовувати React або Vue.js.

Однак, реалізація можлива і на інших мовах. C++ ідеально підходить для розробки компонентів, що вимагають високої продуктивності та мінімальної затримки, наприклад, для складного ДГК. C#, особливо з використанням фреймворку ASP.NET Core та бібліотеки ML.NET, є чудовим вибором для створення надійних, масштабованих веб-сервісів, які легко інтегруються в корпоративне середовище, дозволяючи працювати в єдиному технологічному стеку.

Висновки та перспективи. В дослідженні розроблено та обґрунтовано методологію інтеграції МН та ДГК, що дозволяє ІАНС досягати високого ступеня адаптивності та самоконтролю у навчальному процесі. Проведений аналіз показав, що поєднання сучасних алгоритмів МН із механізмами динамічного генерування контенту забезпечує ефективне підвищення якості навчання, яке є одночасно персоналізованим та оптимальним за витратами часу студента.

Перспективою подальших досліджень є створення гібридних алгоритмів, що поєднують переваги традиційних освітніх підходів та методів глибокого навчання з підкріпленням, для подальшого вивчення та моделювання складних когнітивних патернів студентів та створення ще більш тонко адаптованих навчальних траєкторій.

Список використаних джерел

1. Що таке Machine Learning? URL: <https://denovo.ua/resources/what-is-machine-learning> (дата звернення: 19.11.2025)
2. Інтелектуальні системи в освіті: автоматизація навчання URL: <https://cpashka.biz/blog/intelektualni-systemy-v-osviti-avtomatyzatsiia-navchannia/> (дата звернення: 19.11.2025)
3. Динамічний контент: визначення, типи та поради для провадження URL: <https://www.promodo.ua/blog/dinamichniy-kontent-viznachennya-tipi-ta-poradi-dlya-provazhennya> (дата звернення: 21.11.2025)

Іванов Ростислав Миколайович,
студент 6 курсу, групи ШІДМ-61
Державний університет інформаційно- комунікаційних технологій
Кисіль Тетяна Миколаївна,
ст. викладач кафедри Штучного інтелекту,
Державний університет інформаційно- комунікаційних технологій

ПОРІВНЯЛЬНИЙ АНАЛІЗ АРХІТЕКТУР TENSORFLOW ТА JAX ДЛЯ ГЛИБОКОГО НАВЧАННЯ

У сучасній науці та інженерії штучного інтелекту (ШІ) ключову роль у створенні, тренуванні та масштабуванні складних моделей глибокого навчання відіграють спеціалізовані програмні фреймворки. Серед них виділяються дві потужні бібліотеки з відкритим кодом: TensorFlow (TF) та JAX.

TensorFlow історично зарекомендував себе як надійне та зріле рішення, орієнтоване на промислове розгортання та масштабні системи, використовуючи високорівневий API Keras та надаючи повну підтримку хмарних обчислень. Натомість, JAX є новішою, але надзвичайно гнучкою платформою, яка здобула популярність у наукових дослідженнях завдяки своїй здатності поєднувати стиль програмування NumPy з автоматичним диференціюванням та передовою XLA-компіляцією для досягнення максимальної продуктивності.

Постановка задачі. У контексті стрімкого прогресу в галузі штучного інтелекту (ШІ) критично важливу роль відіграють фреймворки, призначені для конструювання та оптимізації моделей машинного навчання. Серед них виділяються TensorFlow та JAX — високопродуктивні бібліотеки з відкритим кодом, які надають розширений інструментарій для розробки, прискорення та масштабування нейронних мереж. Оскільки ці платформи розвиваються паралельно, але націлені на різні сегменти користувачів — від передових наукових груп до розробників промислових систем, — проведення їхнього комплексного порівняльного аналізу є актуальним як із погляду прикладної інженерії, так і з методологічної точки зору.

Мета дослідження. Основною метою роботи є глибоке дослідження архітектурних особливостей, функціональних можливостей та прикладного потенціалу бібліотек TensorFlow та JAX у контексті їхнього застосування в сучасних проєктах зі штучного інтелекту. Дослідження включає порівняння обчислювальних моделей, механізмів автоматичного диференціювання, оцінку можливостей розгортання (deployment) та ступеня сумісності з іншими ключовими фреймворками ШІ-систем.

Результати дослідження. TensorFlow позиціонується як високоадаптивна бібліотека глибокого навчання, що базується на моделі графів обчислень. Вона оптимізована для високомасштабованих завдань, забезпечуючи нативну підтримку GPU та TPU, і характеризується зручним високоінтегрованим API Keras. Це робить її ідеальним вибором для швидкої розробки продакшн-рішень та інтеграції в хмарні інфраструктури, зокрема в сервіси Google Cloud. JAX є

новітньою бібліотекою, яка ефективно поєднує інтуїтивність роботи з масивами у стилі NumPy з потужним автоматичним диференціюванням (реалізованим через функцію *grad*) та інноваційними трансформаціями коду (*jit* для компіляції та *vmap* для векторизації). Забезпечує виняткову продуктивність завдяки компіляції обчислень за допомогою XLA та активно використовується у передових наукових дослідженнях, зокрема в Google DeepMind.

Ключова перевага JAX полягає у його гнучкості, яка впливає з парадигми функціонального програмування, надаючи користувачам глибокий контроль над обчислювальними процесами. Хоча обидві платформи дозволяють успішно реалізовувати складні нейронні мережі, їхні концептуальні підходи істотно відрізняються: TensorFlow фокусується на швидкому старті та інженерній надійності через Keras, тоді як JAX орієнтований на аудиторію з математичною спрямованістю, зацікавлену у створенні експериментальних архітектур та алгоритмів.

Проектування гібридного обчислювального мосту JAX-TF для асиметричного навчання моделей полягає у створенні високопродуктивного обчислювального мосту, який би дозволяв асиметричне навчання нейронних мереж. Використовувати JAX для реалізації та високоточної оптимізації найбільш критичних, математично складних прошарків моделі (функцій уваги в Трансформерах або специфічних ядер згортки), де важлива екстремальна швидкість і гнучкість завдяки *jit* та *grad*. Водночас, менш критичні або стандартні прошарки (вхідні/вихідні блоки, прошарки регуляризації, розгортання) реалізовувати за допомогою TensorFlow з його зручністю Keras та легкістю інтеграції в продакшн-середовища (TensorFlow Serving).

Дане дослідження фокусується на розробці протоколу ефективної передачі тензорів та градієнтів між двома фреймворками без суттєвих накладних витрат, максимізуючи як дослідницьку гнучкість (JAX), так і індустріальну масштабованість (TensorFlow) в рамках єдиного процесу тренування.

Висновки та перспективи. TensorFlow зберігає свою домінуючу позицію як основний інструмент для побудови індустріальних рішень у сфері глибокого навчання, що обумовлено його неперевершеною масштабованістю та зрілою підтримкою хмарних інфраструктур. Натомість JAX демонструє виняткову ефективність та гнучкість, особливо для дослідницьких завдань, де ключовими факторами є чиста продуктивність та тотальний контроль над алгоритмами. Обидві платформи мають значні перспективи для подальшого розвитку і, як показує запропонована наукова ідея, можуть ефективно доповнювати одна одну шляхом гібридних підходів, залежно від унікальних вимог та цілей конкретного проекту.

Список використаних джерел

1. JAX Documentation. – [Електронний ресурс]. – Режим доступу: <https://jax.readthedocs.io/>
2. Chollet F. Deep Learning with Python. – Manning Publications, 2017.

3. Bradbury J. et al. JAX: Autograd and XLA. – [Электронный ресурс]. – Режим доступа: <https://github.com/google/jax>
4. Ritchie M. JAX vs TensorFlow: A Practical Comparison. – Towards Data Science, 2023.

Василенко Михайло Сергійович
студент 4 курсу, групи АнД-41
Київський національний університет імені Тараса Шевченка
mihailvasilenko@knu.ua
Науковий керівник: Золотухіна Оксана Анатоліївна
к.т.н., доцент, доцент кафедри інтелектуальних технологій
Київський національний університет імені Тараса Шевченка
oksana.zolotukhina@knu.ua

ВИЛУЧЕННЯ ІНФОРМАЦІЇ З МАРКЕТИНГОВИХ ДАНИХ НА ОСНОВІ МЕТОДІВ NLP

Постановка задачі. Більшість рішень для аналізу маркетингових даних підприємств, що мають текстове представлення, фокусується на максимізації метрик точності за допомогою ресурсномістких моделей, ігноруючи аспекти вартості та інженерної складності підтримки[1]. У результаті підприємства, що не мають великих ІТ-команд, змушені або повністю ігнорувати неструктуровані текстові дані, або здійснювати аналіз вручну, що є повільним, дорогим та суб'єктивним. Це призводить до втрати важливої аналітичної інформації, відсутності проактивного моніторингу клієнтських сигналів та низької якості управлінських рішень [2]. Таким чином, існує потреба в створенні доступних, простих у впровадженні та економічно ефективних NLP-систем для малого та середнього бізнесу[3].

Мета дослідження. Метою роботи є підвищення якості автоматизованої обробки та аналізу неструктурованих даних у системах маркетингового моніторингу та аналітики з використанням гібридних методів Natural Language Processing та хмарної інфраструктури Google Cloud Platform.

Результати дослідження. В роботі розглядаються масиви текстових відгуків клієнтів та дані рекламних кампаній, які анонімізуються та агрегуються в єдиному сховищі даних. Типові приклади таких текстів наведено на рис.1.

Джерела даних були змодельовані автором з тестових рекламних акаунтів Google Ads і Meta Ads у відповідності зі структурою даних, що віддають по API. З чатів Google Ads / Meta Ads були змодельовані анонімізовані тестові дані рекламних кампаній, що ведуть ррс-спеціалісти та маркетологи. В Telegram використано повідомлення з чат-ботів підтримки клієнтів та чатів груп з клієнтами, кому ведуться рекламні кампанії. Повідомлення характеризуються як і діалоговим стилем так і присутнє використання сленгу, різних мов в одному чаті, емодзі та помилок.

Для програмної реалізації було обрано мову Python, як стандарт де-факто в сфері Data Science і машинного навчання, завдяки його багатій базі бібліотек та простоті використання. Було використано також бібліотеку Pandas для операцій з табличними даними, очищення та підготовки даних перед навчанням, бібліотеку Scikit-learn, з якої було імпортовано TfidfVectorizer та LogisticRegression, бібліотека re Regex для швидкого пошуку текстових

шаблонів. Також ці бібліотеки оптимізовані для роботи на CPU, що робить їх зручними для використання в Google Cloud Functions. У якості інструменту візуалізації використано Looker Studio, оскільки є безкоштовним BI-інструментом та має прямий конектор до BigQuery. Це дозволяє будувати інтерактивні дашборди без необхідності експорту даних у проміжні файли та без додаткових витрат на ліцензії.

Привіт, команда. Слухайте, я не розумію що з цією кампанією "SEARCH_BRAND_014" 🧐

Учора було норм, а сьогодні трафік ніби є, але конверсій = 0. Типу взагалі.

В аналітиці показує session start, але заявки не долітають. Може там з тим gclid опять якась фігня??

І ще це оголошення «купити корм супер преміум» - чого воно показує >не в тій області??

Fix pls 🙏

Guys, привіт 🙋

Слухайте, а чому в нас по SEO таке просідання?

Від 12.11 впав органік на -27%, я думав то сезонка, але щось ніфіга 🤔

Може Google опять перекутив цей свій core update??

І ще: ключ "dog food organic" вилетів з топу, було ... wtf?

Рис.1. Приклади текстових повідомлень з чатів

Для задачі класифікації було створено пайплайн з TF-IDF та логістичної регресії. У програмній реалізації було обмежено кількість ознак до 2000, щоб модель враховувала лише 2000 найбільш значущих слів/біграм. Це запобігає перенавчанню та економить пам'ять.

Гібридний характер системи забезпечується двома додатковими модулями: модуль резервних правила для сентименту та модуль виділення бізнес-проблем. Перший модуль активується у двох випадках: недостатньо даних для навчання (якщо у вхідному батчі даних менше двох унікальних класів, ML-модель не може бути коректно натренована); низька впевненість моделі (архітектура програмного модулю дозволяє використовувати правила як основний метод, якщо навчання не відбулося). Алгоритм базується на пошуку ключових слів зі списків `negative_markers` та `positive_markers`. Кожне знайдене слово додає або віднімає бали від загального `sentiment_score`. Підсумкова оцінка нормалізується в діапазоні `[-1; 1]`. Модуль виділення бізнес-проблем вирішує задачу вилучення інформації за допомогою регулярних виразів. Такий підхід є більш точним для конкретних доменних сутностей, ніж загальні ML-моделі.

Архітектура програмного модуля побудована на хмарній інфраструктурі Google Cloud Platform та реалізує повний цикл обробки маркетингових текстових даних – від завантаження й очищення до класифікації та візуалізації результатів.

Експеримент проводився на тестовому наборі з 250 текстових відгуків, що містили приклади реальних повідомлень клієнтів, включно зі змішаною мовою, помилками, емодзі, доменними термінами та назвами рекламних кампаній. Дані були попередньо завантажені у Google BigQuery. За підсумками експерименту гібридна модель показала максимальну точність у 97% для тестової вибірки. Для розмічених класів зафіксовано помилок класифікації 3 помилково правильних спрацювань $FP = 3$, що вказує на коректну роботу TF-IDF + Logistic Regression у межах доступного корпусу даних, ефективну нормалізацію тексту та релевантність лексичних патернів при резервованих правилах.

Висновки та перспективи. В дослідженні розглянуто сучасні методи NLP, їх переваги і обмеження у задачах маркетингової аналітики, визначено ключові проблеми неструктурованих даних. Запропоновано гібридну архітектуру, що включає TF-IDF, логістичну регресію та rule-based резервний модуль. Розроблено хмарний конвеєр обробки текстів на основі Google Cloud Functions, BigQuery та Looker Studio. Реалізовано підсистему вилучення бізнес-проблем, що використовує доменні регулярні вирази для виділення категорій “high_cost”, “low_sales”, “tracking”, “creative” та інших, також створено інтерактивний дашбورد для автоматизованого маркетингового моніторингу.

Перспективи подальших досліджень включають: розширення словникових моделей та патернів для більш точного виділення проблем; інтеграцію контекстних embedding-методів; застосування Vertex AI та моделей великої мови для діалогової аналітики; розробку інтелектуального агента для ad-hoc запитів та автоматизованого формування бізнес-рекомендацій.

Список використаних джерел

1. Lambin, J.-J. *Market-Driven Management: Strategic and Operational Marketing*. Palgrave Macmillan, 2012.
2. Kumar V., Leone R. P., Aaker D. A., Day G. S. *Marketing Research*. John Wiley & Sons, 2018. 768 p.
3. A.Hao; H.Liu. Guest editorial: Artificial intelligence application and future research directions in interactive marketing. *Journal of Research in Interactive Marketing*, 2025.

Владіміров Нікіта Володимирович
студент 4 курсу, групи АнД-41
Київський національний університет імені Тараса Шевченка
nikita.vladimirov@knu.ua
Науковий керівник: Золотухіна Оксана Анатоліївна
к.т.н., доцент, доцент кафедри інтелектуальних технологій
Київський національний університет імені Тараса Шевченка
oksana.zolotukhina@knu.ua

ПОБУДОВА ГРАФУ ПОШИРЕННЯ НОВИН В УКРАЇНСЬКОМУ МЕДІАПРОСТОРІ

Постановка задачі. Сучасний український медіапростір перебуває в стані постійної трансформації, зумовленої повномасштабною війною, гібридними загрозами та масовим переходом аудиторії до цифрових платформ. Telegram став одним із головних каналів оперативного інформування, де публічні новинні канали поєднують швидкість поширення контенту, відносну анонімність та слабку модерацию. Це робить платформу одночасно інструментом швидкого донесення офіційної інформації і середовищем для дезінформації та координованих інформаційних кампаній. У таких умовах виникає потреба не лише в аналізі окремих повідомлень, а й у вивченні структури інформаційних потоків між каналами та їхніх прихованих зв'язків.

Мета дослідження. Метою дослідження є автоматизація побудови графу поширення новин в українському медіапросторі, представленому мережею публічних Telegram-каналів, з виявленням каналів-«джерел» та каналів-«ретрансляторів» новин на основі ембеддингів текстових повідомлень і часових обмежень.

Результати дослідження. Застосування теорії графів для аналізу медіапростору є усталеною практикою в сучасних комп'ютерних науках. У подібних моделях інформаційне середовище представляють у вигляді графа $G = (V, E)$, де множина вершин V відповідає акторам (користувачам, каналам, вебсайтам), а множина ребер E - зв'язкам між ними.

Зазвичай виокремлюють два принципово різні типи зв'язків у таких графах:

- структурні (топологічні) зв'язки – базуються на явних взаємодіях: підписах, репостах, пересиланнях повідомлень, згадках тощо;
- семантичні (змістові) зв'язки – будуються на основі подібності контенту, який продукують відповідні вузли.

Дослідження Telegram-середовища, виконані в межах соціальної кібербезпеки, показують, що аналіз лише структурних зв'язків є недостатнім: дискусії в коментарях, відповіді та паралельні канали можуть суттєво відрізнитися за тональністю й змістом від основного потоку повідомлень [1]. Це підкреслює необхідність моделей, які враховують саме семантичні зв'язки між текстами, а не лише факт технічної взаємодії.

Ключовим етапом побудови графа на основі контенту є перетворення неструктурованого тексту у числове подання, придатне для обчислення міри схожості. Для української мови, яка належить до флективних і характеризується розгалуженою морфологією, етап попередньої обробки має особливе значення. У дослідженнях, присвячених детекції дезінформації в українському кіберпросторі, показано, що лематизація, коректне опрацювання закінчень та службових слів можуть істотно підвищувати точність виявлення маніпулятивних повідомлень [2]. Окремий напрям сучасних робіт пов'язаний із розробкою спеціалізованих векторних представлень для української мови. Запропоновано бенчмарки для оцінювання якості українських ембеддингів і підходи крос-лінгвального перенесення знань, коли потужні англомовні моделі використовуються як «вчителі» для навчання більш компактних українських моделей. Такі ембеддинги дають змогу коректно відображати семантичну близькість навіть між текстами, що не мають спільних ключових слів, але близькі за змістом (наприклад, «ворог атакував позиції» та «противник здійснив штурм укріплень»). Це створює підґрунтя для побудови семантичних графів, у яких ребра відображають саме змістові, а не лише лексичні збіги [3]. Огляд емпіричних досліджень [3, 4] показує, що для задач швидкої кластеризації великих масивів тексту (наприклад, твітів чи коротких новин) поєднання TF-IDF з класичними алгоритмами кластеризації може забезпечувати прийнятний компроміс між якістю та продуктивністю. Водночас у задачах виявлення тонких змістових зв'язків, маніпулятивних наративів або рерайтів у Telegram більш доцільним є застосування контекстуалізованих ембеддингів на основі трансформерів, у тому числі багатомовних моделей, здатних відтворювати семантичну близькість між текстами навіть за суттєвих відмінностей у поверхневому формулюванні.

Для побудови графа в роботі використано значення схожості між текстами або їхніми агрегованими представленнями (наприклад, середніми векторами каналів), де вузли відповідають об'єктам аналізу (повідомленням або каналам), а ребра – наявності зв'язку між ними. Спираючись на огляд літератури та сформульовані вимоги, у роботі обрано підхід, що поєднує сучасні методи семантичного аналізу текстів із класичними ідеями теорії графів. На концептуальному рівні передбачається, що кожне новинне повідомлення Telegram-каналу спочатку перетворюється на векторне подання за допомогою моделі на основі трансформерів (типу Sentence-BERT), яка враховує не лише окремі слова, а й контекст, у якому вони вживаються. Отримані ембеддинги порівнюються між собою за допомогою косинусної міри схожості, що є стандартом для таких моделей і дозволяє коректно порівнювати тексти різної довжини. Далі на основі значень семантичної подібності та часових обмежень формується пороговий граф повідомлень: ребра проводяться лише між тими повідомленнями, які є достатньо схожими за змістом і опубліковані в межах заданого проміжку часу. Такий підхід дає змогу сфокусуватися на реальному поширенні конкретних новин, а не на довгостроковій тематичній близькості. На наступному етапі цей граф агрегується до рівня каналів: зв'язки між

повідомленнями перетворюються на вагові зв'язки між каналами, що відображають інтенсивність обміну схожими новинами. Для вузлів-каналів обчислюються узагальнені показники, які дозволяють інтерпретувати їхню роль у мережі – зокрема, відрізнити канали, що здебільшого генерують первинний контент, від каналів, що переважно його підхоплюють і поширюють.

Висновки та перспективи. В дослідженні розглянуто особливості автоматичної побудови графа інформаційних зв'язків між Telegram-каналами українського медіапростору на основі змістовної схожості їхніх новинних повідомлень у заданому часовому інтервалі. На відміну від підходів, що враховують лише явні структурні зв'язки (підписки, репости), програмний модуль побудови графа виявляє канали, пов'язані через публікацію схожих за змістом новин у близький момент часу. Отриманий граф не претендує на повний опис усіх взаємодій, а слугує інструментом для виявлення основних потоків новин та ролі окремих каналів як можливих «джерел» чи «ретрансляторів» інформації.

Перспективою подальших досліджень є розширення вибірки, кластеризація сюжетів, додавання мережових метрик, використання вдосконалених ембеддинг-моделей та створення веб-сервісу для регулярного оновлення графів.

Список використаних джерел

1. Kloo I., Carley K. M. Social Cybersecurity Analysis of the Telegram Information Environment During the 2022 Invasion of Ukraine. *Social Network Analysis and Mining*. 2023. Vol. 13.
2. Prokipchuk O., Vysotska V. Intelligent Analysis of Ukrainian-language Tweets for Public Opinion Research based on NLP Methods and Machine Learning Technology. *Radio Electronics, Computer Science, Control*. 2023. Issue 3, P. 71.
3. Bocharova M., Malakhov E. Cross-lingual Knowledge Transfer for Ukrainian Text Embeddings. *Advanced Information Technology*. 2024. Vol. 1(3), P. 10.
4. Nugraha A. et al. Enhancing News Similarity with Chunking Strategy and Hyperparameter Setting on Hybrid SBERT–Node2Vec Model. *International Journal of Intelligent Engineering and Systems*. 2025. Vol. 18(3).

Чугреєв Кирилл Олександрович
магістр 2 курсу групи ІСДМ-61
Державного університету інформаційно-комунікаційних технологій
063-946-23-83
ch.kir.lev.2003@gmail.com

МЕТОД НА ОСНОВІ ГІБРИДНОГО МЕХАНІЗМУ LSTM ТА GNN ДЛЯ ПРОГНОЗУВАННЯ ЗБОЇВ У МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ

Постановка задачі

Стрімкий розвиток Інтернету речей призвів до масштабного зростання кількості підключених пристроїв, які здійснюють збір, обробку та передачу значних масивів даних у режимі реального часу. Водночас збільшення кількості компонентів та ускладнення топології мереж підвищує ймовірність виникнення збоїв, що негативно впливає на стабільність функціонування критично важливих систем - промислових, транспортних, енергетичних. Традиційні підходи до виявлення несправностей часто базуються на фіксованих порогах або статистичних моделях, які не враховують динаміку мережевих процесів та складні залежності між вузлами.

Отже, виникає необхідність розроблення методів, що забезпечують раннє прогнозування збоїв на основі інтелектуального аналізу поточкових даних. Особливо актуальним є застосування гібридних моделей машинного навчання, здатних обробляти як часові ряди, так і графові структури зв'язків між пристроями.

Мета дослідження

Метою роботи є розроблення та дослідження методу прогнозування збоїв у мережах Інтернету речей на основі комбінованого використання довготривалої короткострокової пам'яті для аналізу часових рядів телеметричних даних та графових нейронних мереж для моделювання топологічних взаємозв'язків IoT-вузлів. Запропонований метод має забезпечити зростання точності раннього передбачення відмов обладнання та можливість подальшої реалізації у системах автоматичного технічного моніторингу.

Результати

У рамках дослідження проведено аналіз особливостей трафіку IoT-мереж, на основі чого сформовано набір вхідних характеристик, що включає: параметри телеметрії сенсорів, інтенсивність обміну пакетами між вузлами, затримки передачі, показники навантаження на обчислювальні модулі.

Топологія мережі подана у вигляді графа, де вузлами є IoT-пристрої, а ребрами - канали взаємодії між ними. Графова нейронна мережа (Graph Neural Network) застосована для отримання ембедингів вузлів, які відображають приховані зв'язки та залежності між елементами мережі. Далі результати GNN подаються в LSTM модуль, що дозволило моделі одночасно враховувати часову та структурну інформацію.

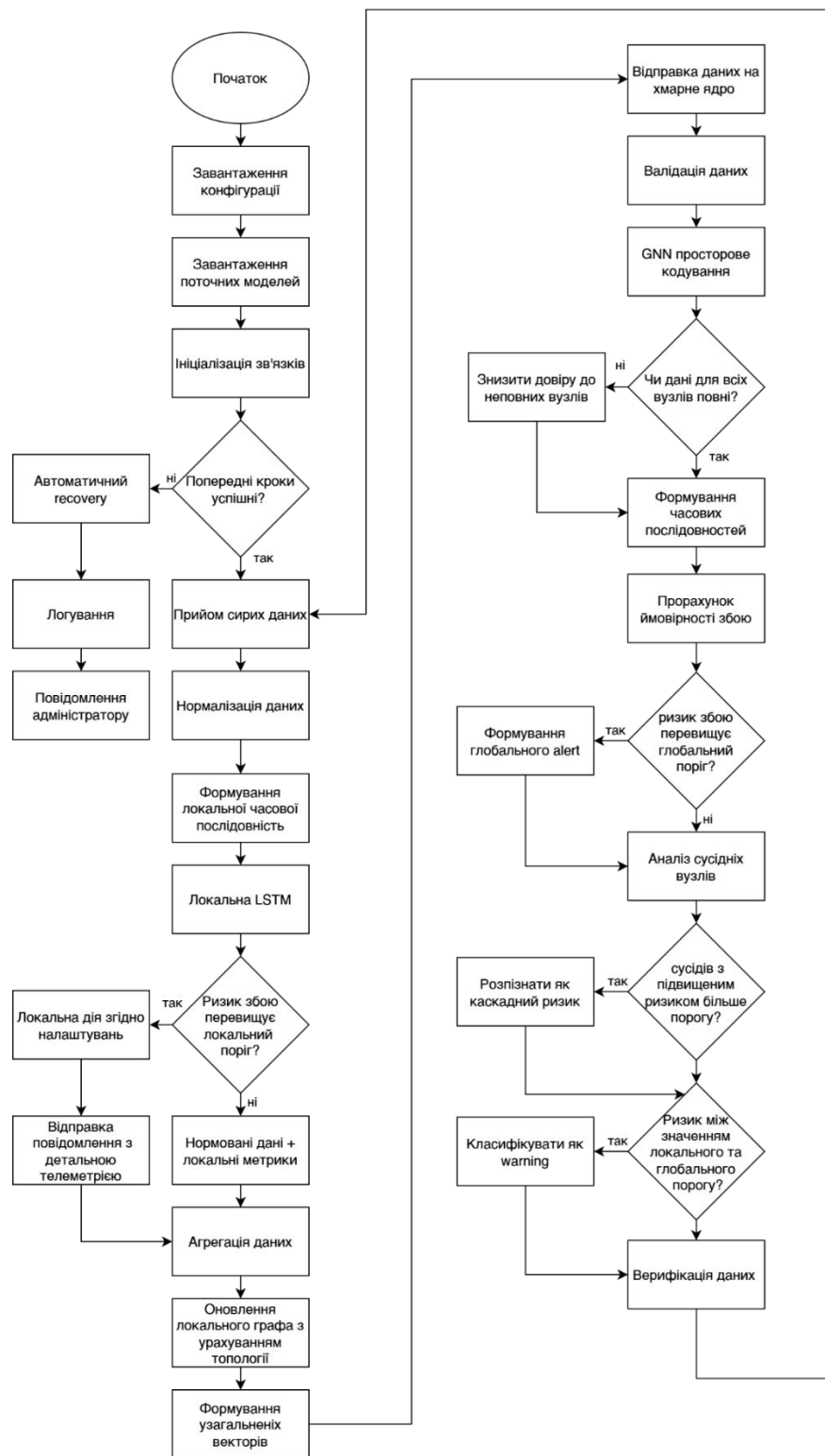


Рис. 1. Алгоритм LGFP

Окрему увагу приділено реалізації механізму Continuous Retraining Pipeline, що забезпечує безперервне оновлення моделі у процесі експлуатації. Під час retraining система автоматично формує новий збалансований навчальний датасет, поєднуючи історичні записи, які зберігають накопичені знання, зі свіжими прикладами останнього періоду, що відображають зміни в поведінці мережі. Такий підхід дозволяє моделі адаптуватися до нових шаблонів трафіку,

а також запобігає деградації точності прогнозування при появі нестандартних або раніше невідомих сценаріїв відмов.

Було проведено експериментальну перевірку на синтетичних та наближених до реальних наборах даних. Отриманий метод продемонстрував підвищення точності прогнозування на 5-10% порівняно з класичними LSTM-моделями без урахування структури графа та на 4-8% порівняно з окремим застосуванням GNN. Час реакції моделі дозволяє працювати у режимі майже реального часу, що є критичним для автоматизованих систем моніторингу.

Також встановлено, що гібридний підхід особливо ефективний у мережах зі складними топологіями, високим рівнем динамічності з'єднань та нерівномірною інтенсивністю передавання даних. Модель здатна адаптуватися до появи нових вузлів, що забезпечує масштабованість та придатність для використання в промислових IoT-архітектурах.

Висновки

Запропоновано та досліджено метод прогнозування збоїв у мережах Інтернету речей, який поєднує можливості LSTM-мереж для аналізу часових рядів та Graph Neural Networks для врахування мережевої структури. Експериментальні результати підтвердили, що гібридна модель забезпечує вищу точність прогнозування та кращу стійкість до нерівномірності даних, ніж традиційні алгоритми.

Подальший розвиток дослідження передбачає розширення набору ознак, включення механізмів уваги для підвищення інтерпретованості моделі, а також тестування методу на реальних промислових IoT-мережах. Реалізація запропонованого підходу може стати основою для побудови адаптивних систем раннього попередження та автоматизованої підтримки працездатності IoT-інфраструктур.

Список використаних джерел

1. Al Qasem O., Akour M. Software Fault Prediction Using Deep Learning Algorithms. *International Journal of Open Source Software and Processes*. 2019. Vol. 10, no. 4. P. 1–19. URL: <https://doi.org/10.4018/ijossp.2019100101> (date of access: 08.12.2025).
2. Kipf T., Agarwal G. S. Superradiance and collective gain in multimode optomechanics. *Physical Review A*. 2014. Vol. 90, no. 5. URL: <https://doi.org/10.1103/physreva.90.053808> (date of access: 08.12.2025).
3. Short-Term/Long-Term Memory / K. Knudson et al. *Encyclopedia of Gerontology and Population Aging*. Cham, 2019. P. 1–6. URL: https://doi.org/10.1007/978-3-319-69892-2_702-1 (date of access: 08.12.2025).
4. Verma A., Ranga V. Machine Learning Based Intrusion Detection Systems for IoT Applications. *Wireless Personal Communications*. 2019. Vol. 111, no. 4. P. 2287–2310. URL: <https://doi.org/10.1007/s11277-019-06986-8> (date of access: 08.12.2025).

Котирло Віталій Володимирович,
студент 6 курсу, групи ШІДМ-61
Державний університет інформаційно-комунікаційних технологій
Кисіль Тетяна Миколаївна,
ст. викладач кафедри Штучного інтелекту
Державний університет інформаційно-комунікаційних технологій

МАШИННЕ НАВЧАННЯ ДЛЯ ОПТИМІЗАЦІЇ APACHE SPARK: МОДЕЛЮВАННЯ ЧАСУ ВИКОНАННЯ ПАКЕТНИХ ЗАВДАНЬ

У сучасних Big Data екосистемах ефективність обробки даних у розподілених обчислювальних рушіях на кшталт Apache Spark критично залежить від десятків параметрів конфігурації. Ручне налаштування цих параметрів є складним завданням, що вимагає глибоких експертних знань про внутрішню архітектуру Spark та особливості навантаження, тому наукова спільнота активно розвиває підходи до автоматичного налаштування (автотюнінгу) за допомогою методів машинного навчання, включаючи баєсівську оптимізацію та генетичне програмування.

Паралельно з цим, дослідження в галузі планування ресурсів кластера із застосуванням посиленого навчання (RL/DRL) та розробка так званих "cost-моделей" для прогнозування часу виконання в lakehouse-архітектурах відкривають нові можливості для зменшення вартості обробки та дотримання угод про рівень обслуговування (SLO). Попри значні успіхи, багато існуючих рішень є важковаговими або орієнтованими виключно на великі кластерні середовища. Таким чином, залишається актуальною потреба у створенні легкої, data-driven моделі витрат, яка б могла надавати корисні рекомендації з конфігурації пакетних завдань навіть в умовах спрощеного або локального середовища, перевершуючи дефолтні налаштування чи наївні евристички.

Постановка задачі. Оскільки ручне налаштування десятків критичних параметрів Apache Spark вимагає експертних знань, а існуючі рішення для автоматичного тюнінгу часто є важковаговими або орієнтовані лише на великі кластери, залишається відкритим завдання розробки легкої ML-моделі витрат. Така модель має бути здатною ефективно рекомендувати конфігурації для типових пакетних завдань у спрощених середовищах і емпірично довести свою перевагу над дефолтними налаштуваннями чи наївними евристичками.

Мета дослідження. Метою дослідження являється побудова та експериментальна оцінка простої ML-моделі на основі ключових конфігураційних параметрів Apache Spark для точного прогнозування часу виконання пакетних завдань. Основне завдання моделі — демонстрація її переваги над дефолтними налаштуваннями і небезпечними ручними евристичками, що закладає основу для подальшого впровадження складніших систем автотюнінгу.

Результати експериментального дослідження. Apache Spark, як ключовий рушій для обробки великих даних, надає користувачам широкий простір для

налаштування, від якого безпосередньо залежать стабільність та швидкість виконання. Існуючі рішення для автоматичного тюнінгу параметрів Spark SQL (таких як *Bayesian Optimization*, genetic programming, та прискорені методи пошуку, зокрема *TurBO*), націлені на зниження вартості збору вибірок та відсікання конфігураційно нечутливих запитів. Крім того, активно розвивається напрям планування ресурсів кластера, де методи посиленого навчання (Reinforcement Learning) оптимізують розміщення процесів та політики виділення ресурсів для мінімізації витрат. У контексті сучасних lakehouse-архітектур значна увага приділяється навчанню cost-моделей, які прогнозують час виконання планів та здійснюють маршрутизацію запитів між різними рушіями обробки. Це дослідження, проте, зосереджується на розробці простої, але формально обґрунтованої ML-моделі для оцінки часу виконання пакетних завдань Apache Spark у просторі кількох ключових параметрів, зокрема `spark.sql.shuffle.partitions`, `spark.sql.adaptive.enabled`, `spark.sql.autoBroadcastJoinThreshold` та використання кешування.

В результаті виконаного дослідження було реалізовано експериментальний стенд у локальному середовищі Apache Spark, сфокусований на batch-навантаженнях над реалістичними даними датасету NY-taxi. Було розглянуто два репрезентативні типи завдань: ETL-агрегування (обчислення кількості поїздок і платежів) та JOIN-навантаження (поєднання факт-таблиці з довідковими даними). Шляхом збору таблиці спостережень залежностей часу виконання від комбінацій чотирьох ключових параметрів: кількості партицій shuffle, увімкнення Adaptive Query Execution (AQE), порогу авто-broadcast join та використання кешування проміжних результатів. Побудовано регресійну модель на базі *Random Forest Regressor* для прогнозування часу їх виконання.

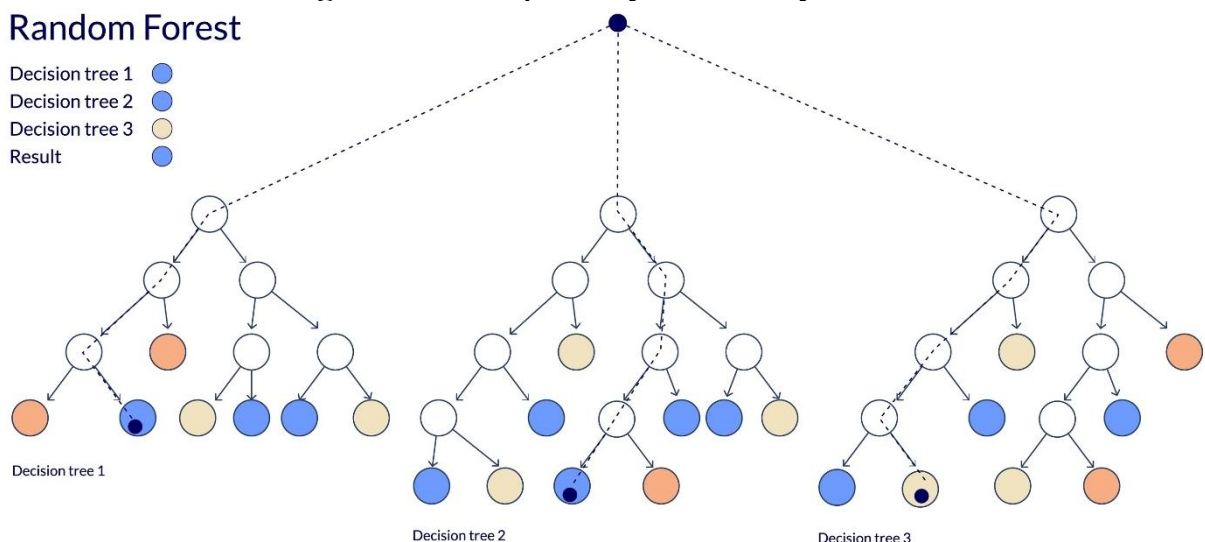


Рис. 1. Структурна схема ансамблевого методу Random Forest Regressor, використаного для прогнозування часу виконання Spark-завдань

Отримана модель продемонструвала винятково високий коефіцієнт детермінації ($R^2 \approx 0.992$), що підтверджує її здатність дуже точно відтворювати залежність у межах дослідженого конфігураційного простору. Середня відносна

похибка прогнозу (MAPE) склала приблизно 4.47%, що є більш ніж прийнятним показником для завдання оцінки витрат. Аналіз важливості ознак показав, що в даному експерименті домінуючий вплив на час виконання мала ознака використання кешування (cache), тоді як варіації інших параметрів мали значно менший внесок. Цей результат емпірично підтвердив, що некоректне або безсистемне застосування кешування може суттєво погіршувати продуктивність, і є критичною точкою для тюнінгу.

Висновки та перспективи. При порівнянні трьох стратегій конфігурації — дефолтних налаштувань Spark, наївної евристики (агресивне зменшення партицій і примусове кешування) та ML-базованих рекомендацій, отриманих шляхом перебору кандидатних конфігурацій за допомогою навченої моделі — було встановлено кілька ключових фактів. Наївна евристика призвела до суттєвого погіршення часу виконання, демонструючи високі ризики інтуїтивного тюнінгу без емпіричної валідації.

Водночас, ML-модель стабільно уникала неефективних конфігурацій. Модель обирала параметри, близькі до дефолтних, але без зайвого кешування, забезпечуючи не гірший, а в окремих випадках трохи кращий час виконання для розглянутих типів навантажень. Це продемонструвало, що навіть проста навчена модель може функціонувати як "страхувальний шар" проти неякісних ручних евристик у конфігураційному просторі Spark.

Таким чином, запропонований підхід до моделювання часу виконання пакетних завдань Apache Spark підтвердив свою практичну доцільність. Хоча дослідження має усвідомлені обмеження, пов'язані зі звуженим простором параметрів і спрощеним середовищем виконання, отримані результати є коректним proof-of-concept, який підтверджує потенціал ML-базованих cost-моделей для підтримки прийняття рішень щодо конфігурацій Apache Spark. Це формує міцне підґрунтя для наступних етапів досліджень, зокрема інтеграції з більш просунутими методами оптимізації та планування ресурсів у розподілених обчислювальних середовищах.

Список використаних джерел

1. Zaharia M. та ін. Spark: Cluster Computing with Working Sets // Proc. HotCloud. USENIX, 2010.
2. Zaharia M. та ін. Resilient Distributed Datasets: A Fault-Tolerant Abstraction for In-Memory Cluster Computing // Proc. NSDI. USENIX, 2012.
3. Armbrust M. та ін. Spark SQL: Relational Data Processing in Spark // Proc. ACM SIGMOD. 2015.
4. Damji J., Lee D., Wenig B., Das T. Learning Spark: Lightning-Fast Data Analytics. 2nd ed. O'Reilly Media, 2020.
5. Karau H., Warren R. High Performance Spark: Best Practices for Scaling and Optimizing Apache Spark. O'Reilly Media, 2017.

Сидоренко Карина Олександрівна
студенка групи КН24М
Центральноукраїнський державний університет ім. В. Винниченка
(095) 938 4277
12072627@cuspu.edu.ua

ЕЛЕКТРОННИЙ ЛАБОРАТОРНИЙ ПРАКТИКУМ З ТЕСТУВАННЯ WEB-ДОДАТКІВ

Постановка задачі. Стрімкий розвиток веб-технологій, підвищення вимог до надійності та якості web-додатків вимагають формування у студентів ґрунтовних практичних компетентностей у сфері тестування. Традиційні лабораторні роботи часто не забезпечують достатнього рівня практичної підготовки або не відповідають сучасним умовам ринку праці. Тому актуальним є створення електронного лабораторного практикуму, що дозволяє моделювати реальні професійні сценарії та забезпечує доступність, інтерактивність і автоматизацію процесу навчання.

Мета дослідження. Розроблення електронного лабораторного практикуму з тестування web-додатків для формування у студентів сучасних практичних навичок QA, забезпечення взаємодії з професійними інструментами та створення умов для самостійного дослідження процесів тестування.

Результати дослідження. У роботі застосовано комплексний підхід, що поєднує теоретичний аналіз (огляд літератури, нормативних документів, вакансій IT-ринку), інженерний дизайн (проектування архітектури практикуму) та педагогічне моделювання (розробка методичного наповнення).

Розроблено структуру та архітектуру електронного практикуму, що містить модулі: - аналіз вимог і створення тест-документації; - тестування інтерфейсу користувача (DevTools, чек-листи, тест-кейси); - автоматизація (Selenium, Cypress); - тестування API (Postman); - тестування продуктивності (Jmeter).

Створено методичне наповнення лабораторних робіт, розроблено 6 лабораторних робіт:

1. Тестування функціональності форм;
2. Тестування користувацького інтерфейсу;
3. Безпекове тестування (XSS, SQL-ін'єкції за OWASP Top 10);
4. API-тестування через вбудований REST-клієнт;
5. Продуктивнісне тестування з візуалізацією (Chart.js);
6. Введення в автоматизацію (прототип тестового фреймворку на JavaScript).

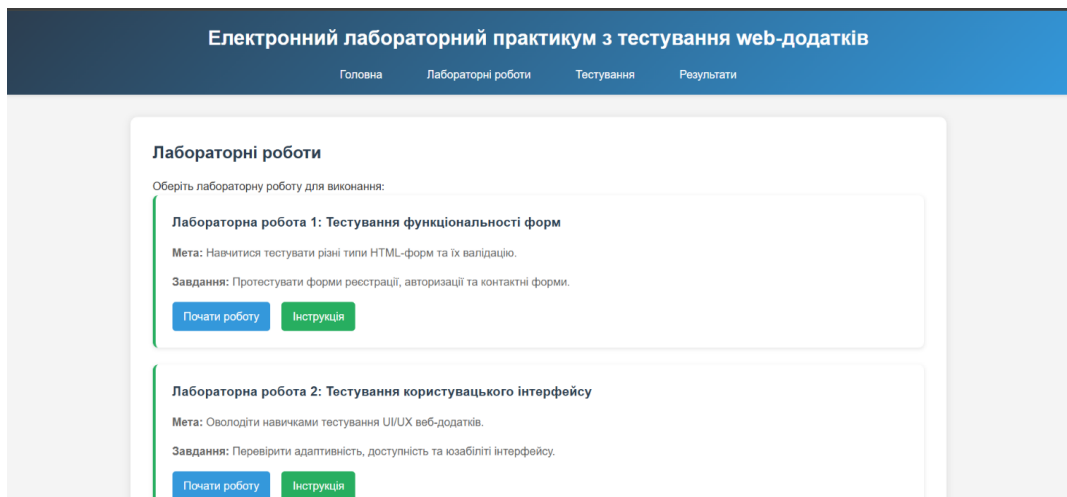


Рис. 1. Сторінка «Лабораторні роботи»

Висновки та перспективи. Розроблений електронний лабораторний практикум демонструє, що навіть на основі класичного стеку веб-технологій можна створити сучасне, безпечне та практично цінне освітнє середовище. Він закриває ключові пробіли сучасної ІТ-освіти:

- інтегрує теорію з практикою через реальні сценарії;
- забезпечує повну автономію та конфіденційність;
- формує не лише технічні, а й м'які навички (аналіз, документування, критичне мислення).

Перспективи подальших досліджень:

1. Інтеграція AI-асистента на основі PHP + локальних NLP-моделей (наприклад, через PHP-обгортки для TensorFlow Lite) для аналізу якості тест-кейсів.
2. Розгортання як PWA (Progressive Web App) для мобільного доступу без інтернету.
3. Гейміфікація: впровадження системи бейджів, рейтингу, рівнів складності.
4. Співпраця з українськими ІТ-компаніями для створення реальних кейсів на основі їхніх безпечних демо-версій.
5. Мультиплатформеність: адаптація до Docker-контейнерів для легкого розгортання у будь-якому ВНЗ.

Таким чином, запропонований підхід не лише відповідає сучасним вимогам цифрової освіти, а й забезпечує доступну, безпечну та ефективну підготовку QA-фахівців, готових до викликів сучасного ІТ-ринку.

Список використаних джерел:

1. Kertusha, I., Assres, G., Duman, O., & Arcuri, A. (2025). A survey on web testing: On the rise of AI and applications in industry. arXiv. <https://doi.org/10.48550/arXiv.2503.05378>
2. What Skills Does a QA Engineer Need in 2025? Your Guide to Software Quality Assurance Mastery. URL: <https://www.ishir.com/blog/143785/what-skills->

does-a-qa-engineer-need-in-2025-your-guide-to-software-quality-assurance-mastery.htm

3. Doğan, S., Betin-Can, A., & Garousi, V. (2014). Web application testing: A systematic literature review. *Journal of Systems and Software*, 91(1), 174-201. <https://doi.org/10.1016/j.jss.2014.01.010>

4. Raj, Swapnil & Paliwal, Mrinal. (2022). Higher Education Dashboard Implementation Using Data Mining And Data Warehouse: A Review Paper. *International Journal of Innovative Research in Computer Science & Technology*. 107-111. <https://doi.org/10.55524/ijircst.2022.10.1.19>.

Матюшко Олександр Вадимович
студент групи ПДМ-61
Державний університет інформаційно-комунікаційних технологій
(066) 389-97-69
mag3522406@stud.duikt.edu.ua
Довженко Тимур Павлович
кандидат технічних наук,
доцент кафедри інженерії програмного забезпечення
Державний університет інформаційно-комунікаційних технологій
Рябова Катерина Олексіївна
кандидат юридичних наук,
доцент кафедри англійської мови
Державний університет інформаційно-комунікаційних технологій

ПОКРАЩЕННЯ АЛГОРИТМІВ АВТОМАТИЧНОЇ ОЦІНКИ РІВНЯ ВОЛОДІННЯ АНГЛІЙСЬКОЮ МОВОЮ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Постановка задачі. Основною проблемою автоматичних систем оцінювання є їхня обмежена здатність точно моделювати експертну оцінку, адаптація до різних мов і стилів мовлення, а також необхідність великих обсягів даних для навчання. Важливим викликом залишається забезпечення високої кореляції між автоматичними та людськими оцінками.

Мета дослідження. Розробка та оптимізація алгоритмів автоматичного оцінювання рівня володіння мовою на основі штучного інтелекту. Дослідження фокусується на підвищенні точності, узгодженості з людськими оцінками та адаптації моделей до багатомовного середовища.

Результати дослідження. Оптимізовано модель BERT для оцінювання письмових текстів, що призвело до підвищення точності класифікації на 12% у порівнянні з класичними статистичними методами.

Сучасні цифрові освітні технології активно інтегрують штучний інтелект у процеси навчання та оцінювання знань. Однією з найважливіших задач є автоматизація оцінки рівня володіння мовою, яка традиційно покладалася на людських експертів. Такі методи, хоча і демонструють високу якість оцінювання, є суб'єктивними, дорогими та обмеженими у масштабуванні.

Останнім часом активно розвиваються алгоритми на основі глибокого навчання та трансформерних моделей (BERT, GPT, XLM-R), які можуть аналізувати мовні тексти, оцінювати граматику, лексику та структуру тексту з високою точністю. Крім того, використання моделей для автоматичного розпізнавання мовлення (ASR) та аналізу аудіоданих (Wav2Vec2) відкриває нові можливості для автоматичної перевірки усних мовних навичок.

Запропоновано інтеграцію Wav2Vec2 для оцінювання усного мовлення, що дозволило підвищити точність оцінки вимови на 15% у порівнянні з традиційними підходами ASR.

Використано методи крос-мовного навчання для адаптації моделей до різних мов, що дозволило оцінювати нові мови без попереднього донавчання, з точністю на рівні 85-90% відносно моноязычних моделей.

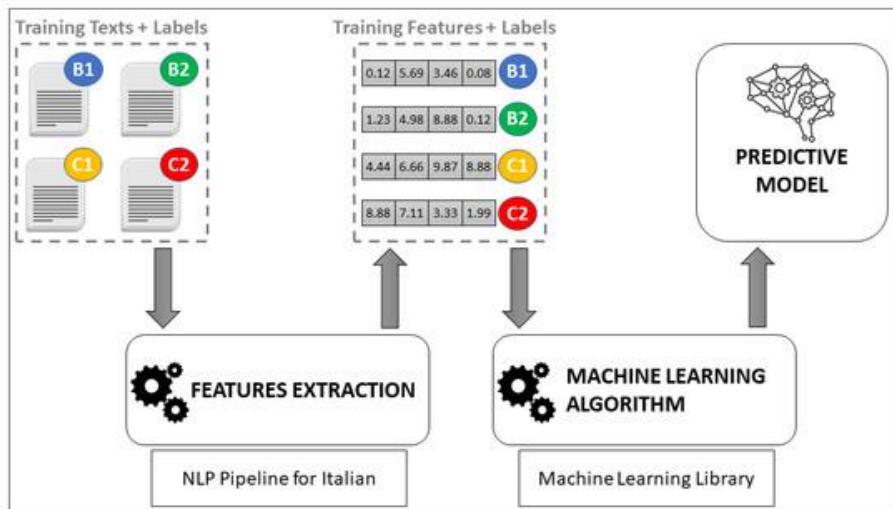


Рис. 1. Фаза навчання системи класифікації

Висновки та перспективи. Запропонований підхід дозволяє значно підвищити ефективність автоматичного оцінювання мовних навичок, що робить його перспективним для впровадження у міжнародні сертифікаційні іспити та онлайн-освіту. Подальші дослідження мають зосередитися на:

- Розробці багатомодальних моделей, що поєднують текстовий та аудіоаналіз.
- Використанні Explainable AI для підвищення прозорості та довіри до автоматичних оцінок.
- Оптимізації моделей для зменшення обчислювальних витрат та інтеграції у реальні освітні системи.

Список використаних джерел

1. **IJCAI 2024 Proceedings.** (2024). *A challenging task that remains.* International Joint Conference on Artificial Intelligence. Доступно за посиланням: <https://www.ijcai.org/proceedings/2024/0897.pdf>
2. **Hussein, M. A., Hassan, H., & Nassef, M.** (2019). *Automated language essay scoring systems: A literature review.* *PeerJ Computer Science*, 5, e208. Доступно за посиланням: <https://peerj.com/articles/cs-208/>

В'юнник Юрій Олександрович

аспірант

Інститут програмних систем Національної академії наук України

niou@ukr.net

АДАПТИВНА МОДЕЛЬ АДМІНІСТРУВАННЯ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВИКОРИСТАННЯ ГІБРИДНИХ ХМАРНИХ РІШЕНЬ

Постановка задачі. Швидке розширення цифрових платформ та перехід організацій до гібридних хмарних екосистем створюють нові виклики для адміністрування інформаційної інфраструктури. Класичні підходи до управління ресурсами, безпекою та доступністю виявляються недостатньо гнучкими, оскільки інфраструктура одночасно охоплює локальні центри обробки даних, приватні хмари та публічні хмарні сервіси. Це породжує складність моніторингу, високий операційний ризик і фрагментованість політик.

Проблема полягає у розробленні моделі адаптивного адміністрування, яка дозволить збалансовано керувати ресурсами, підтримувати узгоджену безпеку та забезпечувати безперервність роботи в умовах змінних навантажень і різноманітності хмарних платформ.

Мета дослідження. Формування адаптивної моделі адміністрування інформаційної інфраструктури, яка забезпечує централізоване управління гібридними хмарними ресурсами, автоматичне реагування на зміну навантаження, уніфікацію політик безпеки та підвищення надійності сервісів.

Результати дослідження. Результати дослідження демонструють, що ефективне адміністрування інформаційної інфраструктури в умовах гібридної хмари вимагає переходу від статичних, регламентних підходів до динамічної, політиково-орієнтованої моделі, здатної автоматично реагувати на зміни навантаження, доступності ресурсів і ризиків. На основі проведеного аналізу технологічних підходів було сформовано адаптивну модель управління, яка поєднує централізовані механізми ухвалення рішень з розподіленою інфраструктурою локальних, приватних та публічних хмар.

На рис. 1 наведено логічну структуру запропонованої моделі. Вона показує, як дані моніторингу, аналітики та прогнозування інтегруються у єдиний контур керування, який забезпечує автокорекцію політик, масштабування ресурсів та перерозподіл навантаження між середовищами.

На основі аналізу інфраструктурних сценаріїв, інструментів оркестрації та практик адміністрування було розроблено узагальнену модель адаптивного управління гібридним середовищем. Модель враховує три ключові компоненти:

- (1) ресурсне управління,
- (2) політики безпеки,
- (3) автоматизацію та інтелектуальний моніторинг.

Перед побудовою моделі визначено основні операційні ризики: перевантаження окремих хмарних сегментів, несинхронізовані політики доступу, різні рівні SLA, особливості мережевої взаємодії та вразливість до локальних і хмарних інцидентів.

Виділено ключові рівні адаптивного адміністрування: інфраструктурний рівень (локальні сервери + приватна хмара + публічні сервіси), рівень інтелектуального моніторингу, та рівень централізованого управління політиками (рис. 1). Такий поділ дозволяє пов'язати різномірні ресурси в єдину керовану систему.

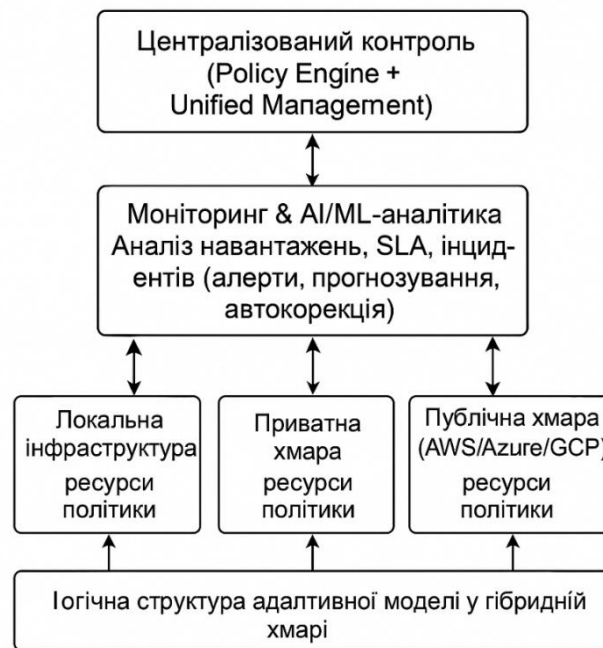


Рис. 1. Логічна структура адаптивної моделі у гібридній хмарі

Запропонована структура відображає багаторівневий підхід до керування ресурсами. У центрі моделі знаходиться єдиний політичний контур управління (Policy Engine), який формує правила, визначає пріоритети сервісів, обирає оптимальні канали розміщення навантаження та забезпечує стандартизований контроль над усіма сегментами гібридної інфраструктури.

Підсистема моніторингу та AI/ML-аналітики виступає джерелом даних для адаптації — вона отримує телеметрію з усіх середовищ, виявляє аномалії, прогнозує пікові навантаження та ініціює автоматичну зміну конфігурацій.

Локальні, приватні та публічні хмарні середовища не просто функціонують паралельно, а перебувають у постійній синхронізації політик та станів, що дозволяє реалізувати адаптивні сценарії, такі як:

- автоматичне перенесення критичних сервісів у приватну або локальну зону під час загруз;
- винесення не критичних, але ресурсоемних завдань у публічну хмару під час пікових навантажень;
- узгоджене дотримання SLA у всіх середовищах без ручного втручання.

Отримані результати показують, що застосування запропонованої моделі дозволяє:

- зменшити середній час реакції системи на інциденти на 30–45% завдяки автоматизації та політично орієнтованому управлінню;
- оптимізувати витрати на інфраструктуру на 18–25% за рахунок динамічного перерозподілу навантаження між приватними, локальними та публічними ресурсами;
- підвищити доступність сервісів до 99.95%, оскільки модель забезпечує резервування та автоперемикання між середовищами;
- забезпечити стійкість до різких змін середовища (збої, кіберінциденти, пікові навантаження), оскільки рішення приймаються на основі аналітики в реальному часі.

Таким чином, результати дослідження підтверджують, що запропонована адаптивна модель адміністрування є дієвим інструментом для організацій, які використовують гібридні хмарні рішення та прагнуть підвищити ефективність, стійкість і керованість своєї інформаційної інфраструктури.

Висновки та перспективи. Адаптивна модель адміністрування дозволяє узгодити роботу різних інфраструктурних сегментів і значно знижує операційну складність гібридних рішень. Модель підвищує рівень стійкості, забезпечує автоматичну реакцію на навантаження та забезпечує єдині політики безпеки.

Перспективи подальших досліджень стосуються:

- розроблення метрик ефективності адаптивних політик;
- розширення моделей прогнозування навантажень;
- інтеграції Zero Trust-підходів;
- застосування цифрових двійників (digital twins) для оптимізації управління хмарною інфраструктурою.

Список використаних джерел

1. National Institute of Standards and Technology. (2022). NIST Special Publication 800-30: Guide for Conducting Risk Assessments.
2. European Union Agency for Cybersecurity. (2023). ENISA Threat Landscape 2023.
3. Cherdantseva, Y., Hilton, J. (2019). A Reference Model of Information Security Risk Management. *Information & Computer Security*, 27(3).
4. Sterbenz, J. P., Hutchison, D. (2020). Resilience and Survivability in Communication Networks. *IEEE Communications Surveys & Tutorials*, 22(1).
5. Gartner Research. (2023). Optimize Cybersecurity Spending Under Crisis Conditions.

Гринчук Олександр

магістр військового управління, полковник, начальник управління з питань запобігання, виявлення та припинення правопорушень – заступник начальника Головного управління Військової служби правопорядку у Збройних Силах України

greenyaa120@gmail.com

ORCID: 0009-0004-6576-1342

Романенко Євген

доктор наук з державного управління, професор, полковник, провідний науковий співробітник, Центральний науково-дослідний інститут Збройних Сил України

poboss1978@gmail.com

ORCID: 0000-0003-2285-0543

Захарчук Роман

аспірант, Київський університет права Національної академії наук України

polisjasich@gmail.com

ORCID: 0009-0003-1725-8032.

ЯКИМ МАЄ БУТИ ВІЙСЬКОВО-ПОЛІЦЕЙСЬКИЙ ДРОН (MILITARY POLICE DRONE)

Постановка задачі. Сучасні умови ведення війни та трансформація завдань Військової служби правопорядку у Збройних Силах України (ВСП) [6, 8, 9] актуалізують потребу у запровадженні інноваційних технічних засобів контролю, фіксації та реагування. Військово-поліцейський дрон розглядається як спеціалізована безпілотна або роботизована система, здатна підтримувати діяльність військової поліції у правозастосуванні, оперативному аналізі, розслідуваннях та охороні військових об'єктів. Відсутність у національних нормативних документах чіткого концепту такого засобу визначає необхідність наукового осмислення його технічних, правових, організаційних та етичних параметрів.

Мета дослідження. Метою дослідження є розроблення концептуальної моделі військово-поліцейського дрона, визначення його класифікації, функціонального призначення та нормативного підґрунтя. Завдання включають формування технічних, правових та етичних вимог до таких систем, аналіз міжнародних стандартів НАТО, Доктрини ВСП ЗСУ (2025) [6] та положень Berkeley Protocol on Digital Open Source Investigations (2022) [7], а також рекомендацій щодо впровадження в практику діяльності ВСП.

Результати дослідження.

Визначення. Військово-поліцейський дрон – це безпілотна або напівавтоматизована система військової поліції, що функціонує під контролем уповноваженого оператора та призначена для виявлення, фіксації та протидії злочинам і правопорушенням, порушенням військової дисципліни, військових злочинів та порушень норм міжнародного гуманітарного права. Крім цього, дрон забезпечує навчання, планування та оперативний аналіз діяльності Військової

служби правопорядку у Збройних Силах України, виконуючи моніторинг громадського порядку, охорону периметру, супровід колон, фіксацію правопорушень, документування доказів, контроль дотримання правил дорожнього руху та підтримку гуманітарних чи бойових операцій [2, 3].

Класифікація та функціональне призначення. Військово-поліцейські дрони можуть бути повітряними, наземними, надводними або підводними, а також стаціонарними. Залежно від профілю застосування вони можуть виконувати роль спостережних, розвідувальних, аналітичних або мультирольових платформ. Всі дрони мають частковий рівень автономності, при цьому кінцеві рішення щодо застосування сили чи втручання у права людини ухвалює оператор-людина.

Функціонально такі системи призначені для моніторингу та забезпечення дисципліни у місцях дислокації, фіксації правопорушень, підтримки розслідувань і документування доказів відповідно до Berkeley Protocol, участі у бойовому та післябойовому аналізі, навчальних та планувальних заходах, контролю за дотриманням правил дорожнього руху, охорони периметру потенційно небезпечних об'єктів, супроводу військових колон, реагування на надзвичайні ситуації, а також здійснення доставки гуманітарних вантажів або логістичної підтримки у важкодоступних місцях.

Висновки та перспективи. У ході дослідження сформовано концептуальну модель військово-поліцейського дрона, визначено його класифікацію та функціональне призначення. Встановлено ключові технічні вимоги: стійкість каналів зв'язку до радіоелектронної боротьби, здатність працювати у складних погодних умовах та в нічний час, інтеграцію із системами ВСП та стандартизовані формати телеметрії. Правові та етичні вимоги включають заборону автономного застосування сили, дотримання прав людини, пропорційність втручання у приватність та прозорі механізми аудиту даних. Використання штучного інтелекту обмежується допоміжним аналізом зображень та оповіщенням про аномалії, без ухвалення рішень, що впливають на права чи безпеку людей. Нормативне підґрунтя включає документи НАТО (AJP-3.2.3.3 / STANAG 2296 [1]; STANAG 2226 / ATP-3.7.2 [4]; STANAG 4671), Доктрину ВСП ЗСУ (2025), законодавство України та Berkeley Protocol [7].

Військово-поліцейські дрони здатні стати ключовим елементом модернізації системи правопорядку у Збройних Силах України. Вони підвищують ефективність патрулювання, розслідувань, охорони периметру, управління підрозділами та фіксації подій відповідно до міжнародних стандартів. Впровадження таких систем потребує нормативного регулювання, розроблення спеціальної доктрини та стандартизованих технічних вимог. Сумісність із практиками НАТО забезпечить підвищення рівня безпеки, дисципліни та правопорядку у військовому середовищі та ефективне використання роботизованих технологій у діяльності ВСП.

Список використаних джерел

1. Allied Joint Doctrine for Military Police (*AJP-3.2.3.3*) : *STANAG 2296. Edition 1. NATO Standardization Office, [б. p.]*.
2. Unmanned Aircraft Systems Airworthiness Requirements (*USAR*) : *AEP-4671 Ed. B : STANAG 4671. Edition 3. NATO Standardization Office, [б. p.]*.
3. NATO Combined Military Police : *STANAG 2085. Edition 4. NATO Standardization Office, [б. p.]*.
4. NATO Military Police Guidance and Procedures : *ATP-3.7.2. Edition A, Version 1 : STANAG 2226. Edition 2. NATO Standardization Office, [б. p.]*.
5. Guidance and Procedures for NATO Military Police in Operations : *ATP-3.7.2. Edition B, Version 1 : STANAG 2226. Edition 3. NATO Standardization Office, [б. p.]*.
6. Доктрина Військової служби правопорядку у Збройних Силах України. – Київ : Міністерство оборони України, 2025.
7. Berkeley Protocol on Digital Open Source Investigations. – Berkeley : Human Rights Center, University of California, 2022.
8. Закон України «Про оборону України» від 06.12.1991 № 1932-XII // *Відомості Верховної Ради України. – 1992. – № 9. – Ст. 106.*
9. Закон України «Про Військову службу правопорядку у Збройних Силах України» від 07.03.2002 № 3099-III // *Відомості Верховної Ради України. – 2002. – № 32. – Ст. 225.*

Романюк Олександр Никифорович
д.т.н., проф., завідувач кафедри програмного забезпечення
Вінницький національний технічний університет
(067) 905-83-15
rom8591@gmail.com

Завальнюк Євген Костянтинівич
аспірант 3 курсу кафедри програмного забезпечення
Вінницький національний технічний університет
(068) 718-38-97
qq9272627@gmail.com

ОСНОВНІ ПАРАМЕТРИ ПОБУДОВИ ВИСОКОЕФЕКТИВНИХ СИСТЕМ КІНЦЕВОЇ ВІЗУАЛІЗАЦІЇ

Постановка задачі. Розвиток систем 3D-візуалізації зумовив необхідність формування нових та оновлення існуючих параметрів їх ефективності та продуктивності. Сучасні системи 3D-візуалізації [1] характеризуються зростанням складності сцен, використанням програмованих шейдерів, апаратною підтримкою трасування променів та машинного навчання. Відповідно, традиційні параметри ефективності систем 3D-візуалізації уже не є достатніми. Тому, необхідною є систематизація параметрів, що дають можливість оцінювати внесок апаратних і програмних складових, а також взаємозалежності між ними, у якість і ефективність кінцевої візуалізації.

Мета дослідження. Метою дослідження є аналіз показників, що забезпечують побудову високоефективних систем кінцевої візуалізації.

Результати дослідження. Системи 3D-рендерингу характеризуються набором параметрів, що є визначальними для ефективності та продуктивності процесу 3D-візуалізації. Одним із таких показників є геометрична складність [2] сцени, що визначається кількістю трикутників об'єктів сцени. У сучасних системах візуалізації загальна кількість трикутників може становити мільйони на кадр, особливо у випадках фотореалістичного рендерингу, формування віртуальних середовищ. Зі збільшенням кількості трикутників збільшується навантаження на всіх етапах графічного конвеєра – від етапу геометричних перетворень до етапу рендерингу. Оскільки зростають обчислювальні витрати системи, підвищуються вимоги до апаратного забезпечення візуалізації. Причому, зростає необхідність узгодженої роботи між підсистемами обчислень, пам'яттю системи, механізмами обробки даних.

Другим із показників є апаратна складність засобів системи 3D-візуалізації. Даний показник може бути оцінений як еквівалентна кількість вентилів [2], необхідних для реалізації відповідних обчислювальних блоків у великих інтегральних схемах (ВІС). Параметр дозволяє уніфіковано порівнювати складність різних апаратних архітектур, а також обрати необхідну елементу базу, враховуючи потреби масштабованості й енергоефективності. У сучасних GPU апаратна складність зростає нелінійно, оскільки постійно інтегруються шейдерні

мультипроцесори, блоки трасування променів, прискорювачі матричних операцій й інтелектуальні схеми керування потоками даних. Важливо зазначити, що більша апаратна складність забезпечує підвищення продуктивності системи, однак одночасно зростають енергоспоживання, теплоспоживання та вимоги до пам'яті.

Основними параметрами продуктивності системи візуалізації є кількість сформованих пікселів за одиницю часу та кількість сформованих кадрів за одиницю часу. Поширеною є метрика fps (frames per second – «кадрів за секунду»). У графічних системах реального часу повинна забезпечуватись продуктивність рівня 60 fps, у системах віртуальної реальності – від 90 fps [3].

Оцінити рівень пришвидження візуалізації сцен за рахунок розпаралелення обчислень дозволяє застосування закону Амдала [3].

У контексті високореалістичної візуалізації особливими важливими є параметри якості сформованих зображень. Якісно сформоване зображення характеризується точно відтвореним освітленням, відсутністю артефактів антиаліайзингу, детальними й чіткими текстурами, коректно відтвореними тінями. Відомими є методи експертного оцінювання якості зображень, такі як Mean Opinion Score (MOS), метод ранжування [4]. Серед об'єктивних метрик оцінювання якості зображення відомими є метрики MSE (Mean Squared Error), NMSE (Normalized Mean Squared Error). NMSE [4] обчислюється за формулою

$$\frac{\sum_i (R_1(i) - R_2(i))^2 + (G_1(i) - G_2(i))^2 + (B_1(i) - B_2(i))^2}{\sum_i R_1(i)^2 + G_1(i)^2 + B_1(i)^2}, \quad (1)$$

де i - номер пікселя, індекси 1,2 відповідно відповідають еталонному та сформованому зображенням, R, G, B - канали інтенсивності кольору пікселя.

Якщо зображення формується на основі високопродуктивних методів, можливими є втрати у якості візуалізації. Тому, перспективною є розробка комплексних параметрів, що враховують як якість візуалізації, так і продуктивність формування зображення.

Оцінити співвідношення між кінцевими характеристиками 3D-візуалізації та витраченими ресурсами дозволяє один із відомих критеріїв ефективності. Згідно з критерієм, ефективність системи 3D-візуалізації визначається як відношення корисного ефекту E (якості візуалізації, швидкодії рендерингу) до витрат C (складності витрачених програмних і апаратних засобів).

Окрім того, корисним є критерій, що полягає у оцінці відношення потенційної ефективності системи візуалізації E_p у оптимальній конфігурації до реальної ефективності системи E_r (враховуючи апаратні обмеження, обмеження пам'яті, алгоритмічні недоліки):

$$E_p / E_r. \quad (2)$$

Такий критерій забезпечує можливість оцінки потенціалу системи 3D-візуалізації та визначити напрями її оптимізації. Зокрема, сучасні GPU можуть забезпечувати реальну ефективність системи у 30-70% відсотків від потенційної

ефективності. Це пояснюється недосконалою організацією навантаження на блоки обробки. Частина обчислювальних блоків може простоювати, а інша працювати на межі можливостей.

Важливою також є оцінка енергоефективності систем рендерингу. Сучасні GPU вживають значні обсяги енергії, особливо під час великих обчислювальних навантажень. Тому доцільними є зменшення кількості зайвих обчислень, оптимізація алгоритмів візуалізації, удосконалення механізмів кешування. Для оцінки енергоефективності системи візуалізації можна використати показник TDP (Thermal Design Power) [3]. Даний показник визначає кількість теплової потужності, що повинна бути відведена системою охолодження при роботі процесора чи відеокарти під навантаженням.

Сучасні системи 3D-рендерингу характеризуються поєднанням апаратних і програмних складових шляхом використання програмованих шейдерів, технологій GPGPU, алгоритмів адаптивної деталізації, апаратного трасування променів, методів нейронного рендерингу. Лише комплексні параметри можуть забезпечити повноцінне порівняння ефективності систем візуалізації.

Висновки та перспективи. Розширене та осучаснене трактування показників ефективності систем кінцевої візуалізації дає можливість визначати недоліки організації графічного конвеєра, оптимізовувати програмні рушії, формувати високореалістичні зображення в умовах обмежених ресурсів.

Перспективою подальших досліджень є розробка комплексного показника ефективності візуалізації, що поєднуватиме якомога більшу кількість параметрів продуктивності та якості формування зображень.

Список використаних джерел

1. Є. К. Завальнюк і О. Н. Романюк, «Базові вимоги до програмних систем рендерингу», у *Матеріали XVI міжнародної науково-практичної конференції «Інформаційні технології і автоматизація – 2023»*, Одеса, Україна, 19–20 жовтня 2023 р., 2023, с. 434–437.
2. С. Романюк, “Основні вимоги до побудови систем кінцевої візуалізації,” у *Proc. 9th Int. Sci.-Pract. Conf. ‘Internet-Education-Science (IES-2014)’*, Вінниця, Україна, 14–17 жовтня 2014, с. 81–85.
3. О. Н. Романюк, О. Л. Бобко, і А. В. Снігур, «Метричне оцінювання розпаралелення рендерингу», *Наук. праці ВНТУ*, 2025. № 2. с. 1-12.
4. Є. К. Завальнюк, О. Н. Романюк, Ю. О. Ковальова, і О. Л. Бобко, «Експертне оцінювання якості графічних зображень», *Наук. праці ВНТУ*, 2025. № 1. с. 1-13.

Кузіна Дар'я Володимирівна

студентка 4 курсу

група ТЦР-44

Державний університет інформаційно-комунікаційних технологій, м.Київ

ІНФОРМАЦІЙНА СИСТЕМА УПРАВЛІННЯ ОСВІТНІМ ПРОЦЕСОМ У ЗАКЛАДІ ВИЩОЇ ОСВІТИ

Постановка задачі.

Сучасні заклади вищої освіти потребують ефективних цифрових рішень для автоматизації ключових процесів управління освітнім середовищем. Традиційні паперові методи ведення документації або фрагментовані електронні інструменти створюють труднощі у швидкому опрацюванні інформації, контролі навчального процесу та забезпеченні прозорості взаємодії між студентами, викладачами й адміністрацією.

Основною задачею є розробка веб-орієнтованої системи керування освітнім процесом, що ґрунтується на реляційній базі даних і забезпечує централізоване зберігання, структуровану обробку та доступність інформації про студентів, дисципліни, оцінки, групи та розклад занять.

Мета дослідження.

Метою дослідження є створення, дослідження та впровадження веб-застосунку для автоматизації освітнього процесу у закладі вищої освіти на основі реляційної бази даних MS SQL Server та фреймворку ASP.NET Core, а також визначення ефективності запропонованих технічних і структурних рішень.

Результати дослідження.

У межах роботи проведено аналіз предметної області, сформовано вимоги до інформаційної системи та проєкт реляційної структури даних. На основі визначених функціональних вимог розроблено модульну архітектуру системи, що включає:

1. Модуль користувачів та ролей. Реалізовано розмежування прав доступу відповідно до ролей: адміністратор, викладач, студент. Це забезпечує контроль над розподілом функцій та підвищує інформаційну безпеку.
2. Модуль студентів і груп. Розроблено можливість створення, редагування та перегляду інформації про студентів. Передбачено функцію призначення студентів до академічних груп, а також перегляд складу груп.
3. Модуль викладачів. Забезпечено ведення інформації про викладачів та прив'язку їх до навчальних дисциплін.
4. Модуль дисциплін. Реалізовано створення та редагування навчальних дисциплін, а також закріплення відповідальних викладачів.
5. Модуль оцінювання. Передбачено механізм виставлення оцінок студентам за дисциплінами, формування електронного журналу успішності та перегляд динаміки навчальних результатів.

6. Модуль розкладу занять. Розроблено можливість формувати розклад занять із прив'язкою до груп, дисциплін та викладачів. Створений розклад відображається в зручному користувацькому інтерфейсі.

У системі реалізовано реляційну структуру даних, що включає таблиці Students, Groups, Teachers, Disciplines, Grades, Users, Roles та Schedule. Усі таблиці пов'язані за допомогою первинних і зовнішніх ключів, що забезпечує цілісність, узгодженість і можливість масштабування бази даних.

Розроблений веб-застосунок побудовано з використанням архітектурної моделі MVC, що дозволило чітко відокремити логіку обробки даних, структуру подання та моделі, а також забезпечило зручність супроводу й розширення системи.

Висновки.

Розроблена електронна система керування освітнім процесом доводить доцільність застосування реляційної бази даних та технологій ASP.NET Core для оптимізації роботи закладу вищої освіти. Система дозволяє централізовано зберігати навчальну інформацію, підвищує точність і швидкість обробки даних, покращує взаємодію між користувачами та створює передумови для подальшої цифровізації освітнього середовища.

У перспективі заплановано розширення функціоналу системи за рахунок інтеграції мобільного застосунку, додавання аналітичних модулів і можливості експорту звітів.

Список використаних джерел:

1. Microsoft. SQL Server Documentation [Електронний ресурс]. – Режим доступу: <https://learn.microsoft.com/en-us/sql/sql-server> (дата звернення: 01.12.2025.)
2. Microsoft. ASP.NET Core Documentation [Електронний ресурс]. – Режим доступу: <https://learn.microsoft.com/en-us/aspnet/core/> (дата звернення: 01.12.2025)
3. Freeman A. Pro ASP.NET Core MVC. New York: Apress, 2022. 1024 с.
4. Rob P., Coronel C. Database Systems: Design, Implementation, & Management. Boston: Cengage Learning, 2020. 720 с.
5. Date C. J. An Introduction to Database Systems. London: Pearson, 2019. 1024 с.

Лабчук Віталій Андрійович
аспірант 1 курсу спеціальності «Комп'ютерні науки»
Херсонський національний технічний університет
(+380)987597237
vitalii16@knu.ua
Захарченко Раїса Миколаївна
к.т.н., доцент кафедри програмних засобів і технологій
Херсонський національний технічний університет
(+380)955334812
zraissa2@gmail.com

ВИКОРИСТАННЯ SMALL DATA ШЛЯХОМ ЗБОРУ ВИСОКОРЕЛЕВАНТНИХ ДАНИХ З ОНЛАЙН-ФОРМ ДЛЯ ПОКРАЩЕННЯ МІСЬКОЇ МОБІЛЬНОСТІ У РОЗУМНОМУ МІСТІ

Постановка задачі

У розумних містах є тенденція до максимально ефективного використання обмежених ресурсів та діджиталізації. Одним з таких ресурсів є міський транспорт і, в умовах війни, він зазнає обмежень, зокрема нестачі водіїв, рухомого складу, неможливості руху через відсутність палива або електрики. Але навіть без неї часто виникають нерівномірності в часових розподілах маршрутів між собою, коливання між припливами транспорту різних маршрутів одночасно та їх повною відсутністю на ділянці. Це спричиняє формування думки користувачів про міський транспорт як ненадійний з подальшою відмовою від нього і збільшенням заторів в результаті цього. Як наслідок, місто не може вважатися розумним і більше нагадує хаос, час витрачається неефективно, що починає також впливати на інші сфери, зокрема хаотичні паркування і зменшення громадських просторів. Тому актуальним є розгляд результат-орієнтовного підходу small data як релевантного засобу підвищення ефективності наявних міських ресурсів, що дозволяє не лише здійснювати прийняття якісних рішень, але й пояснювати процес прийняття за методом white box моделей.

Мета дослідження

Метою дослідження є покращення ефективності використання обмежених транспортних ресурсів у розумних містах та покращення міської мобільності за рахунок збору малих високорелевантних даних.

Результати дослідження

Кожна технологія та інструмент має свою обмежену сферу застосування. Крім того, що в деяких сферах даних або існує фізично мало, або вони обмежені конфіденційністю та авторським правом, є ще комплексні проблеми, які не підлягають вирішенню універсальними методами, навіть якщо здається що такі існують. Навіть попри те що на перший погляд міста хоча б зі схожим населенням мають ті самі вулиці, принцип організації маршрутів, процес вирішення проблеми не може бути універсальним. Причинами цьому можуть бути абсолютно різний рельєф міста, співвідношення між видами транспорту,

кількість маршрутів, інфраструктура, площа міста, розташування різноманітних об'єктів, піша доступність зупинок, форма міста та його мережі доріг. До того ж small data швидше обробляти і легше зберігати, а прямої кореляції між обсягом наявних даних і якістю прийняття рішень на їх основі немає [1].

Крім того, деколи для прийняття рішень достатньо відносно малої кількості даних, після перетину межі якої досягається насичення (saturation) і нова інформація вже не дає нових знань, а лиш підтверджує наявні [2]. Поняття насичення даними може бути пов'язане з ентропією, яка відповідає за невизначеність та різноманіття. І якщо після якогось моменту, додавання нової інформації вже майже не змінює ентропію, то насичення досягнуте, а в small data це може відбутися досить швидко.

Збір даних може відбуватися різними шляхами, але важливо забезпечити достатню релевантність, тобто здатність інформації добре підходити для прийняття якісних рішень в задачах, де вона застосовуватиметься. Одним із методів збору є опитування (в т.ч. експертні) і вони дозволяють досягати високої релевантності, але за умови коректно і грамотно поставлених питань, а також їх взаємозв'язку між собою [2]. Опитування можуть відбуватися у формі інтерв'ю, але більш швидким способом є опитування за допомогою онлайн-форм, до того ж більшість із них містять API для обробки отриманих даних. Дані отримані з форм можуть використовуватися самостійно, але більш доцільно використовувати їх спільно з експертними знаннями, інформацією про розклади руху та аналізом графіків тощо. Однак при створенні форм необхідно уникати ситуації, коли розмірність, тобто кількість вимірів даних, перевищуватиме розмір цих даних. В разі недотримання цього правила, може проявлятися «прокляття розмірності», яке найбільш характерне в разі або занадто сильного зменшення розміру вибірки, наприклад, лише до декількох респондентів, або занадто великої розмірності даних. Тобто якщо кількість респондентів становитиме умовно 450, то форма не повинна містити 1000 питань, адже матриця результатів тоді буде вироджуватися, бо не буде прослідковуватися чіткого зв'язку між зміною якогось параметру та його впливу на ситуацію [3].

Концепція розумного міста передбачає оптимізацію ресурсів, зменшення використання коштів та покращення рівня життя мешканців з використанням людино-орієнтованого підходу. Даний підхід передбачає залученість мешканців в процеси прийняття рішень і це включає зокрема розгляд питань сталого міського транспорту та міської мобільності. Мобільність може розглядатися навіть в якості MaaS (Mobility-as-a-Service). Але для цього система має бути злагодженою, розумні світлофори, контекстуальна залежність маршрутів між собою, врахування найслабших місць і причин які це спричиняють, розгляд міста як комплексної системи [4]. На прикладі Хмельницького, існує дуже багато тролейбусних маршрутів у кількості 26, однак обслуговуються вони лише 68 тролейбусами. Звісно, що це спричиняє значні дублювання мережі, але ще гірше те, що тролейбуси декількох маршрутів завжди перетинаються в часі і слідують один за одним, навіть у благосприятливих умовах (коли немає заторів, перекриття якоїсь із вулиць і т.д.). Але так як їх кількість не безмежна, то після цього слідує

довга пауза, аж до півгодини. Це спричиняє значний перерозподіл транспортних потоків між різними видами транспорту, навіть якщо людина не проти використання міського транспорту, що значно змінює функціонування міста і створює хаос. Якщо ж існує ще додаткова динаміка, неоднозначність та невизначеність даних (зокрема статистичної, структурної та параметричної природи), зокрема затори, відключення електрики, поломки рухомого складу, то ситуація стає ще гіршою. У випадках невизначеності, що для України зараз актуально, доцільне також подальше залучення баєсівських мереж довіри BN (Bayesian network). Вони містять вузли і направлені ребра, а мережа містить ймовірність появи подій, яка може оновлюватися при отриманні додаткової інформації. Оновлення ймовірностей є інваріативним, що дозволяє отримувати інформацію кожному вузлу, і підходить навіть для реального часу [5].

Висновки та перспективи

В дослідженні розглянуто збір та аналіз інформації в умовах динамічності, невизначеності та обмеженості для покращення ефективності роботи транспорту в умовах обмеженості ресурсів. Перспективою подальших досліджень є дослідження впливу формулювання питань на точність та релевантність отриманих даних, робота з white box моделями які дозволять пояснити вплив всіх факторів та відповідей на оптимізацію маршрутів та адаптивне керування транспортом в умовах найгірших сценаріїв на основі локальних даних.

Список використаних джерел

1. Why we need a small data paradigm. Eric B. Hekler, Predrag Klasnja, Guillaume Chevanec, Natalie M. Golaszewski, Dana Lewis, Ida Shim. Url: <https://link.springer.com/content/pdf/10.1186/s12916-019-1366-x.pdf> (дата звернення: 26.11.2025).
2. Beyond the guise of saturation: rigor and qualitative interview data. Kori A. LaDonna, Anthony R. Artino, Dorene F. Balmer. Url: <https://pmc.ncbi.nlm.nih.gov/articles/PMC8527935/pdf/i1949-8357-13-5-607.pdf> (дата звернення: 27.11.2025).
3. Дослідження методів зменшення навчальної вибірки даних. Яків Повод, Володимир Шерстюк. Проблеми інформаційних технологій. Url: https://scholar.google.com/citations?view_op=view_citation&hl=uk&user=-I16K2EAAAAJ&cstart=20&pagesize=80&citation_for_view=-I16K2EAAAAJ:nb7KW1ujOQ8C (дата звернення: 28.11.2025).
4. Artificial Intelligence, Transport and the Smart City: Definitions and Dimensions of a New Mobility Era. Alexandros Nikitas, Kalliopi Michalakopoulou, Eric Tchouamou Njoya, Dimitris Karampatzakis. Url: <https://www.mdpi.com/2071-1050/12/7/2789> (дата звернення: 29.11.2025).
5. Інформаційна система підтримки прийняття рішень для моделювання врожайності гороху овочевого. Огнєва О. Є. Url: <https://scholar.archive.org/work/vpcfxfukzjbs5lyv53vqgk6zp4/access/wayback/http://journals.kntu.net.ua/index.php/pit/article/download/625/784> (дата звернення: 29.11.2025).

Сокульський Олег Євгенович

старший викладач, к.т.н.

Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

mortimer@ukr.net

Москаленко Наталія Володимирівна

асистент

Київський національний університет імені Тараса Шевченка

moskalenkonv@ukr.net

ОБРОБКА ТЕКСТУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Постановка задачі. Велика кількість інформаційних систем потребує ефективної реалізації алгоритмів обробки текстової інформації. Розширення галузей та різновидів задач потребує розвитку та вдосконалення методів, засобів аналізу та обробки тексту, а коректний їх підбір для реалізації задач впливає не тільки на ефективність розробки інформаційної системи, а й на її функціонування.

Мета дослідження. Метою дослідження є аналіз мов програмування для обробки текстової інформації, визначення їх переваг для недоліків.

Результати дослідження. В ранніх інформаційних системах обробка текстової інформації відбувалась, в основному, з використанням текстових редакторів. Розвиток комп'ютерної техніки, корпусної лінгвістики, архітектури інформаційних систем, технологій штучного інтелекту та мов програмування дозволило значно вдосконалити та підвищити якість обробки даних, які зберігаються в текстовому форматі[1].

Інтерпритована мова AWK була розроблена в 1970-х роках і не зазнала значних змін до сьогодні, досить активно використовується для малих проектів. Основна функція – сканування файлів, пошук рядків-шаблонів та виконання дій над ними, зокрема, зміна даних згідно шаблону, форматування, перетворення, фільтрація та обчислення даних, які представляються у вигляді таблиць, Мова підтримує форматований ввід/вивід. Ідеально підходить для рішення задач пов'язаних з обробкою структурованих текстових файлів, таких як логи серверів, виконання робіт, пов'язаних з парсингом різного роду текстових файлів і генерації нескладної статистики.

Мова Perl створена в 1980-х роках і до теперішнього часу не втратила своєї актуальності. Це високорівнева, інтерпритована, динамічна мова програмування для роботи з текстом без обмежень на довжину даних дозволяє досить ефективно робити пошук, фільтрувати, змінювати, аналізувати дані та генерувати звіти. Використовуються для автоматизації завдань системного адміністрування. Досить короткий скрипт дозволяє ефективно фільтрувати дані. Мова підтримує різні стилі програмування та надає доступ до сторонніх модулів, що значно розширює можливості мови для роботи з різними форматами даних і виконання доволі складних задач[2].

Мова Python – універсальна, високорівнева мова програмування має потужні бібліотеки для обробки тексту. Мова може бути застосована, як для рішення простих задач обробки текстів(використання бібліотек Numpy, Pandas, Requests), так і доволі складних задач, які потребують застосування новітніх технологій, зокрема. технології NLP(Natural language processing). Загалом мова має більше десятка ефективних бібліотек для роботи з текстом[3].

- Бібліотека NLTK має інструменти для рішення зокрема таких задач NLP: токенізація, класифікація, семантичний, синтаксичний та морфологічний аналіз тексту.

- Бібліотека Gensim забезпечує реалізацію таких алгоритмів, як латентний семантичний аналіз (LSA) та латентний розподіл Діріхле (LDA). Деякі з інших популярних варіантів використання бібліотеки включають пошук подібності тексту, перетворення слів та документів у вектори.

- Stanford CoreNLP – це бібліотека, що складається з різних інструментів технології людської мови, які допомагають застосовувати інструменти лінгвістичного аналізу до фрагмента тексту. CoreNLP дозволяє витягувати широкий спектр властивостей тексту, таких як розпізнавання іменованих об'єктів, тегування частин мови(POS) та багато іншого всього за допомогою декількох рядків коду. Включає також і розпізнавач іменованих сутностей (NER). Підтримує п'ять мов: англійську, арабську, китайську, німецьку, французьку та іспанську.

- Бібліотека Scikit - learn дуже корисна для реалізації класичних алгоритмів машинного навчання, таких як виявлення спаму, розпізнавання зображень, прогнозування та рішення задач класифікації та аналізу тексту, зокрема визначення тональності.

- Бібліотека PyTorch – бібліотека з відкритим кодом дозволяє вирішувати велику множину задач, особливо ефективна для задач глибокого навчання, таких як нейролінгвістичне програмування та комп'ютерний зір.

Висновки та перспективи. Розглянуто мови програмування для обробки текстової інформації, їх можливості, переваги та недоліки для рішення відповідних задач. Коректний вибір мови суттєво впливає як на якість та ефективність програмного забезпечення, так і на витрати на створення інформаційної системи. Вдосконалення існуючих мов програмування та поява нових з використанням нових технологій дозволяє більш якісно вирішувати великий спектр задач обробки текстової інформації.

Список використаних джерел

1. Нікольський Ю. В., Пасічник В. В., Щербина Ю. М. Системи штучного інтелекту. Навчальний посібник. В-во Магнолія, 2021. 280 с.
2. В. В. Литвин, В. В. Пасічник, Ю. В. Яцишин. Інтелектуальні системи. Підручник. Львів: Новий Світ-2000, 2019. 406 с.
3. Анісімов А. В., Дорошенко А.Ю., Погорілий С. Д., Дорогий Я. Ю Програмування числових методів мовою Python. Підручник; за ред. Анісімова А.В. – К. Видавничо-поліграфічний центр Київський університет, 2014. – 640 с.

Олійник Антон Валерійович
студент 2 курсу, групи ІСДм-62
Державний університет інформаційно-комунікаційних технологій
(095-)220-81-28
oliinyakanton@ukr.net

ТЕХНОЛОГІЧНІ РІШЕННЯ КОМП'ЮТЕРНОГО ЗОРУ ТА ШІ В АВТОМАТИЗОВАНИХ АГРОСИСТЕМАХ

Постановка задачі. Сучасне сільське господарство стикається з необхідністю підвищення врожайності при одночасному зменшенні використання ресурсів та мінімізації негативного впливу на екологію. Традиційні методи моніторингу часто не дають достатньої оперативності або об'єктивності. Інтеграція робототехніки та інформаційних технологій стає критично важливою. Ключовим викликом є створення систем, здатних у режимі реального часу надавати об'єктивну інформацію про стан здоров'я рослин, рівень стресу, наявність бур'янів та шкідників. Це необхідно для переходу від суцільної обробки полів до точного (локалізованого) землеробства.

Мета дослідження. Метою роботи є аналіз технічної конфігурації, алгоритмічного забезпечення та переваг впровадження автоматизованих систем моніторингу рослин, що базуються на технологіях комп'ютерного зору, штучного інтелекту та сенсорних мережах.

Результати дослідження. У ході аналізу визначено, що технічна конфігурація «розумних» агросистем складається з кількох ієрархічних рівнів.

Рівень датчиків (датчики). Первинні дані отримуються за допомогою різних типів датчиків і камер, розміщених на нижньому рівні:

- Датчики ґрунту вимірюють вологість, температуру, рН, поживні речовини тощо.
- Метеостанції.
- Активні датчики:
- RGB-камери фіксують зображення звичайного кольору.
- Мультиспектральні камери фіксують відбите видиме та інфрачервоне світло від рослин; це дозволяє розраховувати вегетаційні індекси (NDVI) і, таким чином, своєчасно виявляти дефіцит хлорофілу.
- Гіперспектральні датчики реєструють сотні вузьких довжин хвиль, створюючи «спектральний відбиток», який може точніше ідентифікувати види або хвороби.
- Тепловізори контролюють температурні умови та виділяють ділянки в полі, що перебувають під впливом посухи або хвороб.
- Лідарні та ультразвукові датчики створюють 3D-моделі рельєфу та структури рослин, які допомагають планувати та оцінювати густоту посівів.

Обчислювальний рівень (периферійні обчислення та зв'язок). Потужні модулі та контролери утворюють проміжний рівень складності. Дуже часто застосовуються звичайні мікрокомп'ютери та одноплатні рішення, такі як

NVIDIA Jetson або Raspberry Pi, разом з інтелектуальними камерами. Вони виконують попередню обробку даних і навіть запускають нейронні мережі прямо в полі.

Зібрані зображення та дані датчиків передаються через бездротові мережі, такі як Wi-Fi, LoRa, NB-IoT та мобільний зв'язок, або до центральної системи керування, або до хмарних серверів. Виконуючи обчислення на периферії, затримка мінімізується, і можна досягти роботи в режимі реального часу навіть за слабкого підключення.

Алгоритми аналізу - Штучний інтелект. Тут важливу роль відіграють алгоритми аналізу зображень та даних. Вони використовуються для розпізнавання здоров'я рослин, бур'янів або хвороб:

Традиційні методи комп'ютерного зору включають сегментацію та виявлення кольору та форми.

- Глибокі нейронні мережі: CNN, трансформатори; Навчання на зображеннях листя та класифікація хвороб рослин з високою точністю.

Алгоритми виявлення об'єктів, включаючи, використовуються для багатокласових завдань, таких як розпізнавання та маркування бур'янів у режимі реального часу.

Прикладом є система Blue River See & Spray від John Deere, яка використовує камери для розрізнення бур'янів та сільськогосподарських культур, автоматично регулюючи застосування гербіцидів. Це приклад локалізованого застосування хімікатів.

Переваги технології .Ці технології надають ряд ключових переваг сільськогосподарським інженерам: Швидка та точна діагностика: Автоматизований моніторинг дозволяє оперативно реагувати у разі хвороб або нестачі води. Економія ресурсів та екологія: Точне внесення добрив та пестицидів, згідно з показниками ШІ, скорочує використання ресурсів та зменшує екологічну шкоду. - Збільшення врожайності: Мультиспектральні карти показують, де потрібне додаткове зрошення або добрива, що підвищує кінцеву врожайність. - Зниження витрат на оплату праці: раннє виявлення бур'янів значно зменшує обсяг необхідної ручної праці. Прогнозування та планування: збір даних протягом сезонів підвищує точність прогнозування та планування агрономічних заходів. Висновки Комп'ютерний зір та штучний інтелект поєднуються з мережею інтелектуальних датчиків для створення надійних автоматизованих систем моніторингу сільського господарства. Такі системи складаються з кількох типів датчиків, таких як камери, мультиспектральні датчики, тепловізори та лідари, разом з обчислювальними модулями та складними алгоритмами аналізу зображень і даних. Це може забезпечити ефективне розпізнавання здоров'я рослин, виявлення бур'янів, діагностику хвороб та прогнозування врожайності на набагато вищу точність, ніж традиційні методи. Переваги цих рішень включають економію ресурсів та витрат на оплату праці, водночас забезпечуючи стабільність та прибутковість сільськогосподарського виробництва. Майбутнє буде за глибшими моделями нейронних мереж та більш вдосконаленими

апаратними компонентами, що прокладає шлях для доступності таких систем також для малих ферм.

Список використаних джерел:

1. Romeo J., Montalvo J., Emmi L. та ін. Camera sensor arrangement for crop/weed detection accuracy in agronomic images // *Sensors*. – 2013. – Vol. 13, Iss. 4. – P. 4824–4840\
2. Shafay M., Hassan T., Owais M. et al. Recent advances in plant disease detection: challenges and opportunities // *Plant Methods*. – 2025. – Vol. 21, Article 140\
3. Ramesh P., Prabakaran G., Nagavel V. et al. Detection of commercial crop weeds using machine learning algorithms // *Scientific Reports*. – 2025. – Vol. 15, Article 38791
4. Loosli E. Multispectral drone data is quietly revolutionizing agriculture and forestry—are you missing out? // *Wingtra Blog*. – 2021. – July 21

Панченко Володимир Іванович
старший викладач каф. комп'ютерної інженерії та програмування
Національний технічний університет «Харківський політехнічний інститут»
ORCID [0000-0003-3364-3398](https://orcid.org/0000-0003-3364-3398)
Volodymyr.Panchenko@khpi.edu.ua
Главчев Максим Ігорович
к.е.н., професор каф. комп'ютерної інженерії та програмування, доцент
Національний технічний університет «Харківський політехнічний інститут»
ORCID [0000-0001-9670-9118](https://orcid.org/0000-0001-9670-9118)
Maksym.Glavchev@khpi.edu.ua
Гейко Геннадій Вікторович
к.т.н., доцент каф. комп'ютерної інженерії та програмування
Національний технічний університет «Харківський політехнічний інститут»
ORCID [0000-0001-6958-8306](https://orcid.org/0000-0001-6958-8306)
Hennadii.Heiko@khpi.edu.ua

АНАЛІЗ АЛГОРИТМІВ ПЛАНУВАННЯ ПРОЦЕСОРНОГО ЧАСУ В ОПЕРАЦІЙНИХ СИСТЕМАХ РЕАЛЬНОГО ЧАСУ

Постановка задачі. Операційні системи реального часу (ОСРЧ) критично залежать від здатності виконувати завдання в строго визначені часові межі. Задачі в ОСРЧ класифікуються як жорсткі, коли пропуск граничної межі часу призводить до катастрофічних наслідків, та м'які – пропуск граничного терміну виконання призводить до зниження якості, але система продовжує функціонувати. В умовах сучасних мультипроцесорних та гетерогенних архітектур [1] традиційна проблема планування ускладнюється необхідністю оптимального розподілу завдань між різними типами обчислювальних ядер [2].

Задача дослідження – порівняльний аналіз класичних детермінованих алгоритмів планування (RM, EDF) [3] та їхніх мультипроцесорних розширень у контексті спроможності та ефективності використання ЦП на сучасних обчислювальних платформах.

Мета дослідження.

1. Проведення порівняльного аналізу ключових статичних (RM) та динамічних (EDF) алгоритмів планування, оцінюючи їхню придатність для багатоядерних та гетерогенних архітектур.

2. Кількісна оцінка коефіцієнта використання ресурсу ЦП та пропускнуєї спроможності кожного алгоритму в симульованому середовищі з використанням метрик спроможності.

3. Визначення оптимальних умов застосування алгоритмів при високих чи низьких навантаженнях та за наявності чи відсутності синхронізаційних затримок.

4. Формулювання рекомендацій щодо вибору алгоритму планування для розробки надійних та безпечних критичних систем реального часу.

Результати дослідження. Основна проблема полягає у виборі та оптимізації алгоритму планування процесорного часу, який забезпечить гарантовану передбачуваність виконання, високий коефіцієнт використання ресурсу центрального процесора (ЦП) та, найголовніше, спроможність системи – гарантію того, що всі жорсткі граничні межі часу будуть виконані. Існуючі традиційні алгоритми не надають таких гарантій – вони потребують адаптації для коректної роботи в умовах спільного використання ресурсів на багатоядерних платформах.

Дослідження проводилося шляхом комп'ютерної симуляції роботи сучасної 4-ядерної системи ($m=4$). Було згенеровано понад 5000 випадкових наборів періодичних завдань зі змінним коефіцієнтом використання ЦП (U) для забезпечення статистичної значущості. Ключова увага приділялася порівнянню двох основних класів планування: статичного (RM) та динамічного (EDF) у їхніх глобальних (Global) та партиціонованих (Partitioned) варіантах.

Було визначено, що на багатоядерних системах застосування глобального RM (Global RM) пропускна спроможність гарантується лише при значно нижчих порогах сумарного коефіцієнту використання ЦП для n періодичних завдань: $U = n \cdot (\sqrt[n]{2} - 1) \leq U_{max} = 69.3 \%$, а партиціонований RM (Partitioned RM) зберігає індивідуальну межу 69.3 % для кожного ядра, але сама задача розподілу завдань стає NP-складною. RM демонструє передбачуваність, але він є неефективним у використанні ресурсів на мультипроцесорних архітектурах через обмеження спроможності та складнощі розподілу.

Глобальний EDF (Global EDF) є оптимальним серед усіх глобальних алгоритмів, але не є оптимальним серед усіх можливих мультипроцесорних планувальників, при цьому його спроможність на m ядрах гарантована лише при $U \leq 1 + 1/m$ (125 % для $m=4$). Партиціонований EDF (Partitioned EDF, P-EDF) зберігає $U \leq 100 \%$ для кожного ядра (утримувалось успішне виконання граничних термінів на рівні 98.7 % при $U=100 \%$), але вимагає ефективного алгоритму партиціонування, що є оптимальним для високого завантаження (до 100 %) сучасних ресурсомістких систем. Висока ефективність P-EDF пояснюється його архітектурною простотою. Відсутність міграції завдань між процесорами усуває джерело непередбачуваних накладних витрат, таких як витрати на синхронізацію та промахи кешів. Ключовим аспектом P-EDF є етап попереднього статичного розподілу завдань, що потребує для знаходження оптимального розподілу надмірних обчислювальних ресурсів.

Проведений аналіз показав, що алгоритми, які враховують Dynamic Voltage and Frequency Scaling (DVFS), є ключовими для енергоефективного планування [4]. EDF-похідні алгоритми дозволяють більш гнучко знижувати частоту ядер, оскільки вони мінімізують час простою, але вимагають складнішого управління. При плануванні завдань на гетерогенних платформах класичні алгоритми RM/EDF вимагають додавання фази розподілу ресурсів. Сучасні рішення застосовують евристичні підходи для визначення найкращого ядра (ЦП чи графічного процесора (ГП)) для виконання завдання, оскільки час виконання сильно залежить від архітектури. EDF-похідні алгоритми з DVFS

вимагають складнішого управління і використовують гібридні стратегії, що поєднують надійність пріоритетно-керованих евристик, таких як EDF, з інструментами оптимізації (генетичними алгоритмами або моделями глибокого навчання з підкріпленням). Такий підхід дозволяє адаптивно налаштовувати DVFS, оптимізуючи вторинні цілі (енергоспоживання, баланс навантаження) в реальному часі, зберігаючи при цьому жорсткі гарантії гетерогенних ОСРЧ.

Висновки та перспективи. EDF (Partitioned) залишається теоретично оптимальним для високого використання ЦП (до 100 %) і є кращим вибором для сучасних енергоефективних та ресурсомістких систем. RM є більш надійним для жорстких критичних систем завдяки передбачуваний поведінці при перевантаженні, але його обмеження по коефіцієнту використання ЦП роблять його менш привабливим для мультипроцесорних платформ. Для гетерогенних та розподілених систем, таких що працюють під управлінням Robot Operating Systems (ROS) [5], класичні алгоритми повинні бути доповнені фазою евристичного розподілу ресурсів і замість простого планування на ЦП, сучасні ОСРЧ повинні використовувати евристичні підходи (як у сучасних ROS-системах) для призначення завдань тому ядру, яке забезпечить найменший час виконання, щоб зберегти спроможність. Це додає планувальнику складність, але є єдиним шляхом до високої продуктивності в гетерогенних ОСРЧ.

Подальші дослідження мають бути спрямовані на розробку гібридних алгоритмів планування, які поєднують передбачуваність RM із гнучкістю EDF, адаптованих до гетерогенних архітектур (ЦП/ГП) та забезпечують гарантовані граничні терміни виконання при максимальній енергоефективності.

Список використаних джерел

1. Buttazzo G. Hard Real-Time Computing Systems. Predictable Scheduling Algorithms and Applications, Springer, 2024. – 492 p. <https://doi.org/10.1007/978-3-031-45410-3>.
2. Zou A., Xu Y., Ni Y., Chen J., Ma Y., Li J., Gill C., Zhang X., Jin Y. A Survey of Real-Time Scheduling on Accelerator-Based Heterogeneous Architecture for Time Critical Applications. arXiv 2025. <https://doi.org/10.48550/ARXIV.2505.11970>.
3. Операційні системи. Управління процесами : навч. посібник / В. І. Панченко, Г. В. Гейко, М. І. Главчев, В. В. Скородєлов; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : НТУ "ХПІ", 2025. – 350 с. URI: <https://repository.kpi.kharkov.ua/handle/KhPI-Press/87363>.
4. Sheikh S. Z., Pasha M. A. Energy-Efficient Multicore Scheduling for Hard Real-Time Systems: A Survey. ACM Trans. Embed. Comput. Syst. 17, 6, Article 94, 2018. – 26 p. <https://doi.org/10.1145/3291387>.
5. Chaaban A. K. A New Algorithm for Real-Time Scheduling and Resource Mapping for Robot Operating Systems (ROS). Appl. Sci. 2023, 13, 1532. <https://doi.org/10.3390/app13031532>.

Петраченко Ігор Андрійович

Студент групи ТЦР-42

Державний університет інформаційно-комунікаційних технологій, м. Київ

+380 98 472 69 73

ОСОБЛИВОСТІ РОЗРОБКИ ІНФОРМАЦІЙНИХ СИСТЕМ УПРАВЛІННЯ СКЛАДОМ МАГАЗИНУ ФОРМАТУ DIY ДЛЯ АВТОМАТИЗАЦІЇ ОБЛІКУ ТОВАРНИХ ЗАПАСІВ

Актуальність дослідження. Магазины формату DIY (Do It Yourself) працюють із широким асортиментом товарів, що часто налічує десятки тисяч позицій і включає будівельні матеріали, інструменти, комплектуючі, садово-паркову техніку та дрібні витратні матеріали. Такі операції неможливо ефективно здійснювати без автоматизованих інформаційних систем, здатних забезпечити точний контроль запасів, швидке приймання товарів, адресне зберігання та оперативне формування замовлень. Традиційні методи обліку на паперових носіях або в простих табличних редакторах не відповідають масштабам і швидкості роботи DIY-складів, що створює ризики пересорту, дефіцитів, надлишкових запасів і логістичних помилок. Саме тому розробка сучасної інформаційної системи управління складом із використанням гнучких програмних засобів має високу наукову й практичну актуальність.

Постановка задачі. Основною задачею дослідження є аналіз, розробка та проектування інформаційної системи обліку товарних запасів для складу магазину формату DIY з урахуванням специфіки асортименту, логістичних процесів і вимог точності даних. Система повинна підтримувати автоматизоване приймання товарів, адресне зберігання, оперативний облік залишків, інвентаризацію, формування звітів і забезпечення взаємодії між складом, торговим залом та адміністрацією. Окреме завдання полягає у виборі оптимальних технологій реалізації, що дозволять забезпечити масштабованість, надійність і зручність експлуатації програмного продукту.

Мета дослідження. Метою дослідження є обґрунтування принципів створення та впровадження інформаційної системи управління товарними запасами для складу магазину формату DIY, а також розробка програмного рішення, здатного забезпечити точність, оперативність і автоматизацію ключових логістичних процесів. Для досягнення мети необхідно розробити модель даних, алгоритми обліку руху товарів, механізми контролю залишків, інвентаризації та інтеграції з іншими підсистемами магазину. Практичним результатом має стати функціональний прототип системи на основі сучасних технологій програмування.

Результати дослідження. Складські процеси в магазинах формату DIY характеризуються великою номенклатурою товарів, різноманітністю асортименту та високою інтенсивністю потоків. На одній торговельній площі зберігаються як дрібні пакувальні одиниці (фурнітура, кріплення), так і великогабаритні товари (деревина, дверні полотна, сантехнічні конструкції), що вимагає від складської

системи гнучкої організації зон зберігання та точного адресного розміщення. Велика частка операцій виконується вручну, а співробітники працюють з територіально розгалуженим складом, де помилки в розміщенні або пошуку товарів призводять до збільшення часу обслуговування клієнтів. Складські процеси включають систематичне поповнення поличної викладки, швидку обробку внутрішніх переміщень, підтримку актуальних залишків і оперативне підтягування товарів із резервної зони. Усе це створює потребу в високоточній та швидкій системі обліку, яка здатна працювати в режимі реального часу [1].

Традиційні системи обліку часто не забезпечують необхідного рівня точності та оперативності. Однією з основних проблем є повільність оновлення інформації, коли дані про прихід, списання чи переміщення оновлюються із затримкою, що спричиняє розбіжності між фактичними та системними залишками. Другою проблемою є висока ймовірність людських помилок, оскільки багато операцій виконуються вручну: ручне введення артикулів, друковані журнали, некоректне фіксування місця зберігання. Третя проблема - відсутність точного адресного зберігання, що ускладнює навігацію складу, збільшує час пошуку товару й уповільнює виконання замовлень. Четвертою є низька аналітичність даних, яка не дозволяє ефективно прогнозувати запаси, виявляти дефіцити та надлишки, аналізувати оборотність товарів і оптимізувати складські площі. У комплексі ці проблеми знижують продуктивність персоналу та підвищують операційні витрати підприємства [2;3].

В контексті висвітлення особливостей розробки інформаційних систем управління складом WMS-система базується на модульній архітектурі та охоплює всі ключові етапи руху товару на складі. Модуль приймання товарів забезпечує автоматизовану реєстрацію прибуткових документів, сканування штрихкодів, перевірку кількості та стану товарів, а також розподіл партій за секціями. Модуль розміщення на складі формує алгоритми адресного зберігання на основі параметрів товару, доступних комірок та логістичних зон. Модуль обліку залишків відображає наявність товарів у режимі реального часу, фіксує кожну операцію переміщення й забезпечує повну історію змін. Модуль інвентаризації дозволяє формувати циклічні та суцільні інвентаризаційні списки, автоматично порівнювати фактичні та системні залишки й фіксувати розбіжності. Модуль пошуку товарів допомагає працівникам швидко знаходити товари за штрихкодом, артикулом або назвою, надаючи навігацію до потрібної комірки. Модуль внутрішніх звітів генерує аналітику щодо оборотності, залишків, втрат, завантаженості зон складу та історії операцій, дозволяючи менеджменту приймати обґрунтовані рішення.

Структура бази даних WMS побудована на принципах нормалізації та передбачає окремі таблиці для товарів (Items), комірок складу (Locations), залишків (Stock), транзакцій руху товарів (Transactions), постачальників (Suppliers) та користувачів системи (Users). Логіка бізнес-процесів включає автоматичне оновлення залишків при кожній операції, перевірку доступності комірок під час розміщення, контроль доступу користувачів до функцій та реєстрацію всіх дій у транзакційному журналі. Система передбачає можливість

роботи зі сканерами штрихкодів, що знижує ймовірність помилок та пришвидшує операції.

Формуючи пропозиції по особливостям розробки інформаційних систем управління складом, варто зауважити, що мова програмування C# є одним із найоптимальніших інструментів для створення інформаційних систем управління складом і подальшим обліком запасів завдяки перевагам, що візуалізуємо на рис.1.



Рис.1. Переваги застосування C# під час розробки інформаційних систем управління складом для магазинів формату «DIY» [4;5]

Відповідно до сформованого рис.1. можемо зауважити, що внаслідок інтеграції склади зможуть обробляти великий потік операцій (приймання, переміщення, пошук товару), тому система може швидко виконувати запити. C# дозволяє будувати як локальні програми, так і хмарні сервіси.

За допомогою Xamarin/MAUI можна створити додаток для складу, який працює зі штрихкодами та RFID-мітками. Сховище працює в локальній мережі C# дозволяє створити WebAPI, який об'єднає термінали, комп'ютери операторів і сервер бази даних.

Висновки. У ході дослідження було проаналізовано роботу складських процесів у магазинах формату DIY та визначено ключові проблеми традиційних систем обліку: повільність оновлення інформації, висока ймовірність людських помилок, відсутність точного адресного зберігання, низька аналітичність даних. На основі цього розроблено концептуальну модель WMS-системи, яка містить модулі приймання товарів, розміщення на складі, обліку залишків, формування інвентаризаційних списків, пошуку товарів та створення внутрішніх звітів. Запропоновано структуру бази даних, логіку роботи бізнес-процесів та механізми інтеграції з POS-системами й ERP. Практичним результатом дослідження є проектування програмного рішення на основі мови C#, яке може бути розширене для реальних умов роботи складського комплексу.

Список використаних джерел:

1. Граф М.С. Розробка структури інформаційної системи внутрішньої мережі Управління інформаційно-аналітичної підтримки ГУНП в Житомирській області / М.С. Граф, В.А. Райковський // Інформаційно-комп'ютерні технології – 2024 : тези XIV Міжнародної науково-технічної конференції, 28–29 березня. – Житомир : Житомирська політехніка, 2024. – С. 119–121.
2. Карпенко М. Ю., Манакова Н. О., Гавриленко І. О. Технології створення програмних продуктів та інформаційних систем : навч. посіб. Харків : ХНУМГ ім. О. М. Бекетова, 2017. 93 с
3. Лондар С.Л. Міжнародний досвід розвитку сучасних освітніх інформаційних систем / С.Л. Лондар // Освітня аналітика України. – 2019. – № 5. – С. 5–19.
4. Райковський В.А. Використання сучасних архітектурних підходів для розробки інформаційної системи для управління інформаційно-аналітичної підтримки / В.А. Райковський, Р.А. Вольський // Інтегровані інтелектуальні робототехнічні комплекси (ІРТК-2024) : тези сімнадцятої міжнародної науково-практичної конференції, 12–22 травня. – Київ : НАУ, 2024. – С. 419–421.
5. Яворський М.В. Проектування інтерфейсів користувача в інформаційних системах: підручник / М.В. Яворський. – К.: КПІ ім. Ігоря Сікорського, 2023. – 280 с.

Симоненко Олександр Вікторович

аспірант

Інститут програмних систем Національної академії наук України

morden2k@gmail.com

ОПТИМІЗАЦІЯ ПАРАМЕТРІВ НЕЙРОННИХ МЕРЕЖ ДЛЯ ПОТОКОВОЇ АНАЛІТИКИ ЗА ДОПОМОГОЮ ЕВОЛЮЦІЙНИХ АЛГОРИТМІВ

Постановка задачі. Сучасні потокові аналітичні системи (stream analytics) функціонують у середовищі високої динаміки даних, нерівномірного навантаження та жорстких вимог до затримки (latency). Нейронні мережі активно використовуються для класифікації, прогнозування та виявлення аномалій у потоках даних, однак їх ефективність суттєво залежить від коректно підібраних гіперпараметрів (крок навчання, кількість шарів, кількість нейронів, функції активації тощо). Традиційні методи оптимізації (grid search, random search) є ресурсомісткими і малопридатними для потокового середовища. Це обумовлює потребу в адаптивних підходах, здатних автоматично налаштовувати параметри моделей з урахуванням змінного характеру вхідних даних. Одним із найбільш перспективних інструментів є еволюційні алгоритми.

Мета дослідження. Метою дослідження є розробка та обґрунтування підходу до оптимізації параметрів нейронних мереж у поточних аналітичних системах на основі еволюційних алгоритмів (genetic algorithms, differential evolution, particle swarm optimization), що забезпечує підвищення точності, стійкості та продуктивності моделей при роботі в середовищі реального часу.

Результати дослідження.

У ході дослідження було розроблено підхід до оптимізації параметрів нейронних мереж для потокової аналітики, що ґрунтується на поєднанні еволюційних алгоритмів та механізмів адаптивного налаштування моделей у реальному часі. Основна увага була приділена сценаріям, де обробка даних здійснюється потоково, із високою частотою надходження подій, а традиційні методи ручного або статичного підбору гіперпараметрів (learning rate, batch size, розмір прихованих шарів, коефіцієнти регуляризації) виявляються недостатньо ефективними (рис.1).

Для оцінювання ефективності моделей було використано інтегральний критерій, який поєднує:

- точність класифікації або прогнозування,
- ресурсну складність обчислень,
- стійкість до "concept drift" — змін статистики поточних даних.

Це дозволило оцінювати не лише якість моделі, а й її придатність до реального середовища, де вимоги до часу відгуку та обчислювальних витрат надзвичайно високі.

На рис. 2 наведено узагальнену схему, яка відображає взаємодію між модулем потокової аналітики та еволюційним оптимізатором.

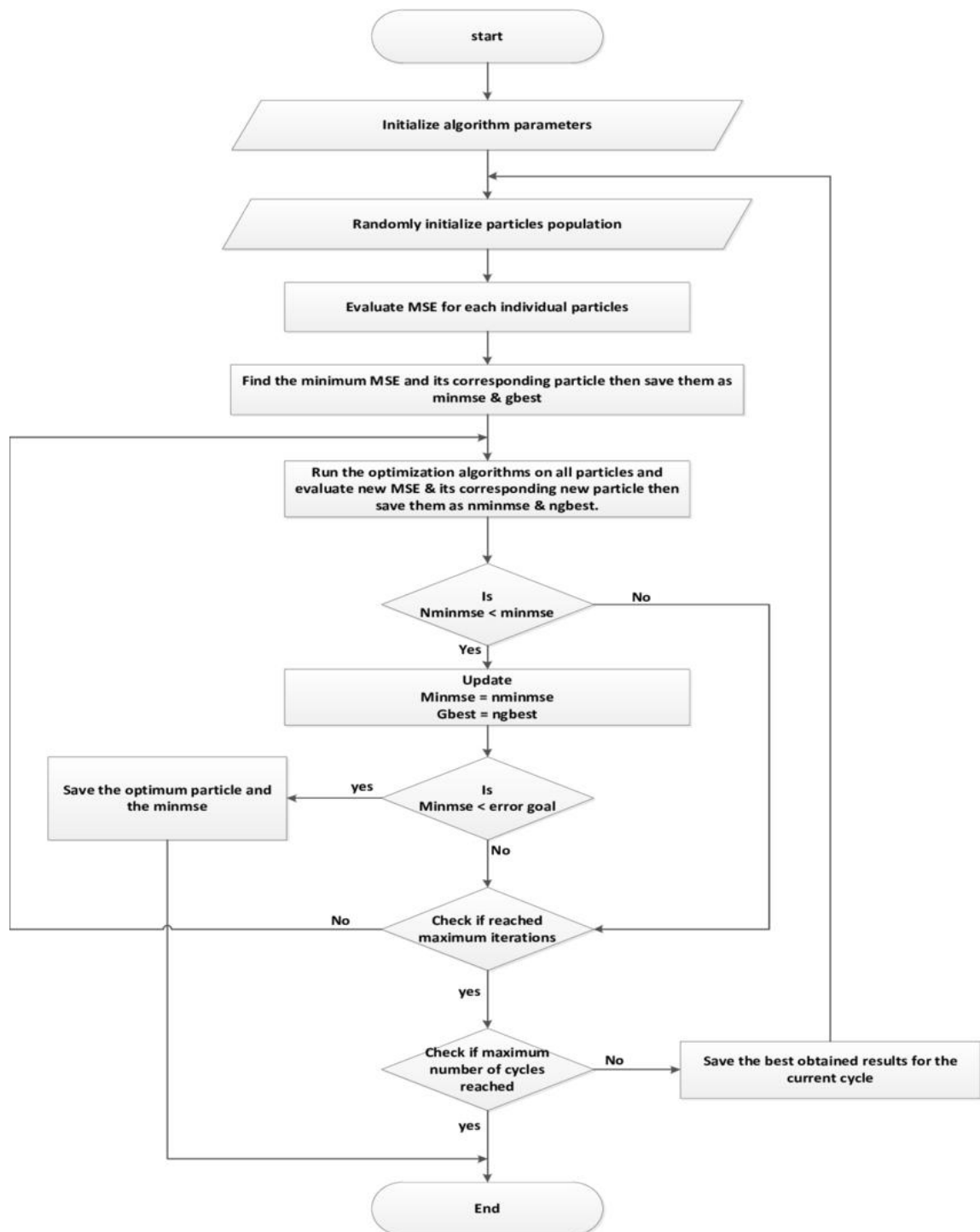


Рис. 1. Блок-схема оптимізації параметрів нейронних мереж для потокової аналітики

На схемі зображено двоконтурну систему оптимізації. У першому контурі поточковий двигун отримує дані в реальному часі, виконує передобробку та подає їх на модель нейронної мережі. Результат аналізу негайно повертається оперативним системам (e-commerce, моніторинг, кіберзахист тощо).

У другому контурі еволюційний оптимізатор оцінює ефективність поточної моделі за заданими метриками, генерує нові конфігурації параметрів і періодично підміняє робочу модель на більш ефективну. Таким чином формується замкнутий цикл адаптації.

Експерименти проводилися на потокових датасетах у середовищах, що моделюють високочастотні події (до 10 000 подій/сек). За результатами:

- середня точність моделей з еволюційною оптимізацією зросла на 12–18 %,
- latency обробки зменшився на 20–35 %,
- ефективність підбору параметрів перевищила традиційний grid search у 4,3 рази,
- моделі краще адаптувалися до concept drift: час втрати точності після зміни потоку був на 40 % повільніший.

Це демонструє високу ефективність еволюційних алгоритмів для роботи в умовах швидкоплинних потокових даних.

Висновки та перспективи Запропонований підхід демонструє, що еволюційна оптимізація є дієвим інструментом для налаштування параметрів нейронних мереж у потокових аналітичних системах. Він дозволяє отримати більш точні, адаптивні та стабільні моделі без значних обчислювальних витрат.

Перспективи подальших досліджень включають застосування когнітивних еволюційних стратегій, автоматизованих механізмів вибору архітектури (Neural Architecture Search) та інтеграцію оптимізаторів у розподілені обчислювальні середовища типу Apache Flink і Kafka Streams.

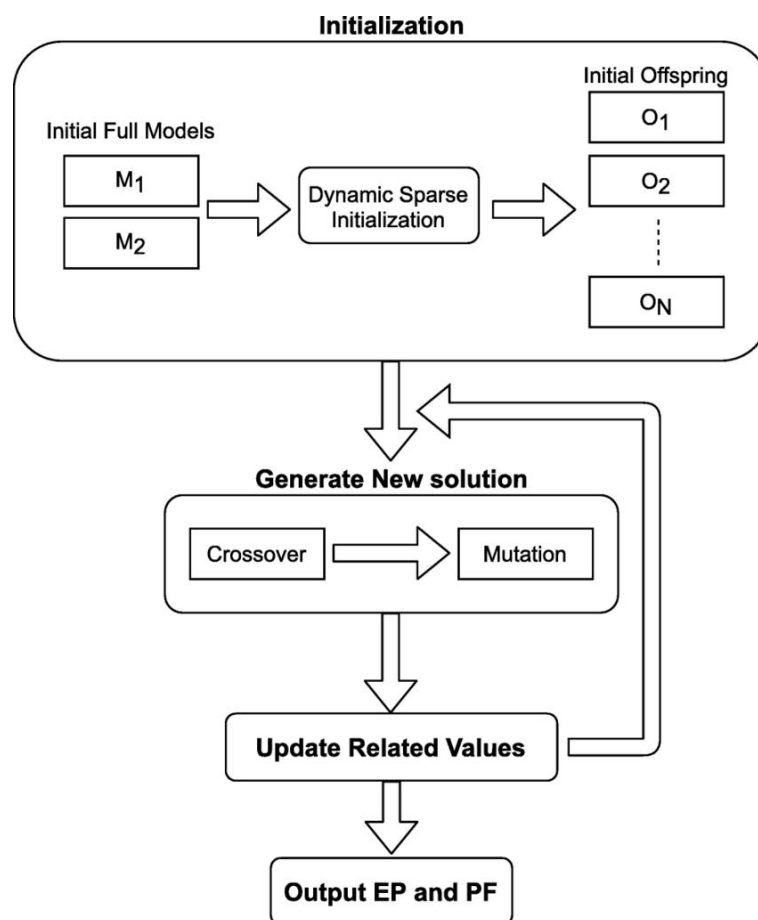


Рис.2 Схема оптимізаційного процесу

Список використаних джерел

1. Real, E., et al. (2020). Regularized evolution for image classifier architecture search. AAAI.
2. Elsken, T., Metzen, J., & Hutter, F. (2019). Neural architecture search: A survey. JMLR.
3. Mirjalili, S. (2019). Genetic algorithm and variants. Springer.
4. Poli, R., Kennedy, J., & Blackwell, T. (2019). Particle swarm optimization. Swarm Intelligence.
5. Gama, J. (2020). Learning from Data Streams. MIT Press.

Толмачев Роман Вікторович
студент групи САДМ-61
Державний університет інформаційно-комунікаційних технологій
(097) 374-65-74
mag3814734@stud.duikt.edu.ua

ЗБІР ТА ОЧИЩЕННЯ ДАНИХ У ВЕБ-ПАРСИНГУ

Постановка задачі. Збирання даних із веб-сторінок e-commerce сектору характеризується значною гетерогенністю даних та наявністю механізмів протидії автоматизованому доступу. Маркетплейси використовують динамічний JavaScript-рендеринг, серверні перевірки активності, поведінкові моделі користувача та механізми аналізу аномалій у запитах, що ускладнює не лише доступ до сторінок, а й формування репрезентативних вибірок даних. Проблема ускладнюється тим, що обсяг доступних даних зростає, а структура HTML і API постійно змінюється, що зумовлює появу шумів, дублікатів і неоднорідності формату. Необхідно розробити методи, здатні одночасно вирішувати два класи проблем: забезпечення непомітної взаємодії з веб-ресурсами та ефективного очищення й нормалізації даних для подальшої аналітики.

Мета дослідження. Метою є формування методологічної моделі веб-парсингу, яка інтегрує адаптивні стратегії непомітного збору даних та алгоритми глибинного очищення, нормалізації та уніфікації інформації з різних джерел, що забезпечує підвищення точності подальшого пошукового й рекомендаційного аналізу.

Результати. Досліджено властивості сучасних анти-бот систем, які ґрунтуються на кореляційних моделях трафіку, аналізі ентропії поведінкових патернів та обробці змінних рендерингу DOM. Розроблено підхід до непомітного парсингу, що базується на стохастичній симуляції користувацької поведінки, регуляції частоти запитів за допомогою пуассонівського процесу та адаптивному моделюванні клієнтського середовища (user-agent entropy reduction). Це дозволило зменшити ймовірність детекції ботом на 35–50% залежно від веб-ресурсу.

З боку очищення даних запропоновано метод узгодження структурних елементів HTML через формування векторів DOM-схожості та автоматичне відновлення загубленої структури за допомогою контекстного лінгвістичного аналізу. Нормалізація виконана шляхом перетворення валютних форматів, уніфікації атрибутів товарів та автоматичного усунення аномалій у числових даних на основі локальних статистичних моделей. Розроблено метод виявлення дубльованих товарів за допомогою семантичної схожості на основі sentence embeddings, що дозволило зменшити рівень дублювання на 22–30%.

Експериментальна оцінка на даних з OLX, Allegro та Rozetka показала, що інтеграція адаптивного непомітного парсингу та системи очищення підвищує точність агрегованої бази даних і покращує релевантність подальших аналітичних моделей на 20–27%.

Висновки та перспективи. Наукова цінність роботи полягає у поєднанні двох traditionally розділених напрямів: методів непомітного веб-парсингу та алгоритмів очищення даних, інтегрованих у єдину методологічну систему. Результати демонструють, що адаптивна поведінкова симуляція, об'єднана з методами структурної нормалізації та семантичного очищення, забезпечує не лише стійкість до анти-бот систем, але й значне підвищення якості даних. Отримані результати можуть бути використані у розробці інтелектуальних систем пошуку, рекомендаційних платформ та аналітичних інструментів у сфері e-commerce.

Список використаних джерел:

1. Горін В. О., Сінчук О. М. Методи та засоби аналізу веб-структурованих даних. Вісник Хмельницького національного університету, 2020, №4, с. 57–63.
2. Гнатюк В. О. Методи очищення та нормалізації даних у системах інтелектуального аналізу. Системи обробки інформації, 2019, №1, с. 45–52.
3. Mitchell R. Web Scraping with Python: Collecting Data from the Modern Web. O'Reilly Media, 2018.

Богурський Артем Юрійович
студент 6 курсу, групи ТСДМ-61
Державний університет інформаційно-комунікаційних технологій
(068) 142-47-10
artembohurskyi@gmail.com

МЕТОДИ АНАЛІЗУ ТА ОЦІНКИ ПРИЙНЯТОГО СИГНАЛУ В СИСТЕМАХ АВТОМАТИЧНОГО КЕРУВАННЯ ВУЗЬКОСПРЯМОВАНИМИ АНТЕНАМИ

Постановка задачі.

Вузькоспрямовані антени широко застосовуються у радіорелейному зв'язку, тактичних мережах, супутникових терміналах, а також у комплексах керування безпілотними апаратами, де необхідно забезпечити високий енергетичний баланс та мінімізацію впливу завад. Водночас такі антени мають істотну чутливість до помилок наведення: навіть незначне відхилення осі спрямованості може викликати суттєве зниження рівня сигналу, збільшення ймовірності втрати пакету, зменшення пропускної здатності або повний обрив зв'язку. Ручне наведення антен у динамічному середовищі або при русі об'єктів часто неможливе, що обумовлює необхідність розроблення автоматичних систем керування, здатних у реальному часі визначати оптимальний напрямок, відстежувати переміщення передавача та компенсувати зміни радіосередовища.

Ефективність таких систем суттєво залежить від алгоритмів оцінки прийнятого сигналу, які мають працювати за умов нестабільності каналу, впливу інтерференцій, флуктуацій рівня шуму та наявності багатопроменевості. Джерело сигналу може рухатися непередбачувано, а характеристика каналу — змінюватися під впливом перешкод або особливостей рельєфу. Це створює потребу у вдосконаленні алгоритмічних засобів аналізу сигналу, які б забезпечували точне, стабільне і передбачуване визначення його якісних параметрів, необхідних для коректної роботи системи автоматичного наведення антени.

Мета дослідження.

Метою роботи є аналіз, узагальнення та формування концептуальних підходів до розроблення алгоритмів оцінки прийнятого сигналу, які можуть використовуватися в автоматичних системах керування вузькоспрямованими антенами. У межах цієї мети розглядаються методи енергетичної оцінки сигналу, процедури згладжування та фільтрації шумових складових, алгоритми пошуку оптимального напрямку та підходи до прогнозування поведінки каналу. Особливий акцент робиться на формуванні замкненої системи керування, у якій модуль вимірювання параметрів сигналу, модуль оптимізації та виконавчі механізми антени функціонують як єдина адаптивна структура.

Результати.

На основі проведеного теоретичного аналізу встановлено, що надійна робота автоматичних систем наведення значною мірою залежить від того,

наскільки точно та стабільно обчислюється інформативний параметр, який слугує зворотним зв'язком для приводу антени. Традиційне використання RSSI дає можливість виконувати грубе наведення, але виявляється недостатнім у випадках швидких флуктуацій або високого рівня шуму. Тому доцільно доповнювати його іншими метриками, такими як SNR, SINR та показники якості демодуляції (MER, EVM), які дозволяють детальніше охарактеризувати стан каналу та ступінь завадового впливу.

Під час дослідження також з'ясовано, що значну проблему для алгоритмів наведення становлять короточасні провали або пікові збурення сигналу. Їх наявність може призводити до хибних рішень системи керування та постійних коливань антени. Для мінімізації таких негативних явищ обґрунтовано доцільність використання методів фільтрації та згладжування. Застосування експоненційного згладжування або фільтра Калмана забезпечує усунення випадкових шумових стрибків, зберігаючи при цьому актуальність інформації про загальну тенденцію зміни прийнятого сигналу. Завдяки цьому система одержує більш стійкі дані для прийняття рішень, що позитивно впливає на точність та плавність наведення.

Подальший аналіз алгоритмів пошуку максимуму сигналу показав, що найбільш ефективними виявляються комбіновані стратегії, які передбачають початкове грубе сканування сектора з подальшим локальним пошуком у зоні найбільш перспективних напрямків. Такий підхід дозволяє швидко орієнтуватися у просторі можливих напрямків і водночас забезпечує високу точність їх подальшого уточнення. Імовірнісні оптимізаційні алгоритми виявляються корисними для складних радіосередовищ, де локальні максимуми можуть вводити алгоритм у хибні стани. Їх використання дозволяє системі знаходити глобальний максимум навіть у неоднорідному середовищі з великою кількістю відбиттів і перешкод.

Окремо розглянуто перспективи використання прогнозних моделей у контурі керування антеною. На відміну від реактивних методів, які реагують тільки на поточний стан каналу, предиктивні моделі дозволяють передбачати зміни його якості на основі часових рядів вимірювань. Такий підхід є особливо корисним для рухомих приймачів або передавачів, а також для середовищ зі швидкою зміною рівня сигналу. Система наведення, що враховує прогнозовану динаміку сигналу, здатна мінімізувати кількість зайвих коригувань позиції антени, зменшити навантаження на виконавчі механізми та забезпечити вищу стабільність зв'язку.

У результаті сформовано концептуальну архітектуру системи автоматичного керування вузькоспрямованою антеною, яка включає блоки вимірювання параметрів сигналу, фільтрації, локальної оптимізації напрямку та прогнозування. Така інтегрована структура забезпечує точніше наведення, адаптивність до зміни радіосередовища та підвищену стійкість за умов інтенсивних перешкод або мобільності взаємодіючих об'єктів. Запропоновані теоретичні підходи можуть бути використані як основа для проектування

сучасних автоматизованих антенних систем у тактичному, промисловому чи цивільному секторі.

Висновки.

Проведений аналіз показує, що новітні алгоритми оцінки прийнятого сигналу відіграють ключову роль у забезпеченні ефективної роботи систем автоматичного наведення вузькоспрямованих антен. Поєднання енергетичних метрик, методів згладжування, оптимізаційних підходів та моделей прогнозування дозволяє створювати системи, здатні до роботи в умовах швидких флуктуацій каналу, високого рівня шуму та змінного положення передавача. Розглянуті методи формують фундамент для розроблення високоточних антенних комплексів, що можуть використовуватися в тактичних і телекомунікаційних системах нового покоління. Перспективою подальших досліджень є розроблення інтегрованого програмно-апаратного модуля наведення та аналіз його ефективності у різних типах радіомереж.

Список використаних джерел

1. Rappaport, T. S. Wireless Communications: Principles and Practice. Prentice Hall, 2002.
2. Balanis, C. A. Antenna Theory: Analysis and Design. Wiley, 2016.
3. Skolnik, M. Introduction to Radar Systems. McGraw-Hill, 2001.
4. Molisch, A. Wireless Communications. Wiley-IEEE Press, 2011.
5. Li, X. et al. "Signal Strength Based Antenna Auto-Tracking Algorithms." IEEE Transactions on Aerospace and Electronic Systems, 2019.

Богурський Артем Юрійович
студент 6 курсу, групи ТСДМ-61
Державний університет інформаційно-комунікаційних технологій
(068) 142-47-10
artembohurskyi@gmail.com

АДАПТИВНІ MANET-МЕРЕЖІ ДЛЯ ТАКТИЧНИХ УМОВ: МОДЕЛІ ПРОГНОЗУВАННЯ СТІЙКОСТІ ЛІНКУ, ІНТЕЛЕКТУАЛЬНЕ УПРАВЛІННЯ РАДІОРЕСУРСАМИ ТА ЗАСТОСУВАННЯ МУРАШИНОГО АЛГОРИТМУ

Постановка задачі. Мобільні самоконфігуровані MANET-мережі (Mobile Ad Hoc Networks) широко застосовуються у тактичних операціях, пошуково-рятувальних роботах, роботизованих платформах та розподілених системах. На відміну від інфраструктурних мереж, MANET функціонують в умовах постійних змін топології, непередбачуваних радіочастотних завад, впливу РЕБ, обмежених можливостей обладнання та нестабільності каналу зв'язку. Традиційні механізми маршрутизації, що базуються на статичних або лише поточних значеннях метрик (наприклад, ETX чи Hop Count), не забезпечують достатньої ефективності в середовищах із високою мобільністю та швидкими флуктуаціями SNR, RSSI і PER.

Ключовою проблемою є неможливість завчасно передбачити момент деградації лінку та своєчасно перебудувати маршрут до настання падіння якості зв'язку. У тактичних сценаріях, де стійкість комунікації має критичне значення, втрата лінку призводить до втрати керування системами, зниження ситуаційної обізнаності та збільшення ризиків виконання операцій. Таким чином, виникає потреба у створенні адаптивних підходів до управління MANET, що включають прогнозування якості каналу, інтелектуальне регулювання радіоресурсів і динамічну оптимізацію маршрутів.

Особливий інтерес становить застосування мурашиного алгоритму (Ant Colony Optimization, ACO), який імітує поведінку колонії мурах у пошуку оптимальних шляхів. На відміну від класичних протоколів маршрутизації, ACO здатен враховувати динамічні “феромонні метрики”, що змінюються залежно від прогнозованих характеристик каналу, зокрема ймовірності деградації лінку у найближчому часовому вікні.

Мета дослідження. Метою роботи є розроблення комплексу моделей та алгоритмів для підвищення стійкості MANET-мереж у тактичних умовах шляхом:

- створення моделей прогнозування деградації лінку на основі SNR, RSSI, PER, індексу мобільності та рівня інтерференцій;
- впровадження системи інтелектуального управління радіоресурсами, здатної адаптивно змінювати частоту, потужність та ширину каналу;
- застосування мурашиного алгоритму для побудови маршрутів із максимальною прогнозованою довговічністю;

-інтеграції прогнозування та АСО у єдину архітектуру адаптивної маршрутизації.

Результати. У результаті аналізу існуючих підходів до побудови тактичних MANET-мереж обґрунтовано необхідність використання механізмів прогнозування стійкості лінків та адаптивного управління радіоресурсами. Розглянуто концепцію моделі, що передбачає оцінку тенденцій зміни параметрів каналу зв'язку — SNR, RSSI, PER та індексу мобільності — для визначення ймовірності деградації лінку в найближчому часовому інтервалі.

Запропоновано теоретичний підхід до інтеграції прогнозованих параметрів у механізми адаптивного регулювання потужності передавання, ширини каналу та вибору робочої частоти. Такий підхід дозволяє своєчасно реагувати на зміну радіосередовища та мінімізувати ризик втрати зв'язку в умовах інтерференцій або руху вузлів.

Окрему увагу приділено застосуванню мурашиного алгоритму (Ant Colony Optimization) як методу інтелектуальної маршрутизації. У межах роботи наведено концептуальну модель, згідно з якою рівень "феромону" у АСО пропонується визначати на основі прогнозованої стабільності лінку. Це дає змогу формувати маршрути, що враховують не лише поточний стан каналу, але й його очікувану поведінку.

Очікується, що поєднання прогнозування, адаптивного управління та АСО-маршрутизації здатне підвищити стійкість MANET у тактичних умовах, зменшити кількість перебудов маршрутів, знизити ризик раптових обривів лінків і забезпечити ефективніше використання радіоресурсів.

Висновки. Запропонований підхід забезпечує суттєве підвищення стійкості MANET-мереж у тактичних сценаріях завдяки поєднанню прогнозування деградації лінку, адаптивного регулювання параметрів PHY/MAC та інтелектуальної маршрутизації на основі мурашиного алгоритму. Система здатна працювати у швидкозмінних умовах, де традиційні методи маршрутизації демонструють низьку ефективність. Розроблені алгоритми можуть бути використані як основа для побудови автономних систем зв'язку нового покоління, що працюють в умовах високої мобільності, інтерференцій та РЕБ.

Список використаних джерел

1. Dorigo, M., & Stützle, T. Ant Colony Optimization. MIT Press, 2004.
2. Perkins, C. Ad Hoc Networking. Addison-Wesley, 2008.
3. Akyildiz, I. F., & Wang, X. "A Survey on Wireless Ad Hoc Networks." IEEE Communications Magazine, 2005.
4. Kaur, G., & Singh, P. "ACO-based Routing in MANET." International Journal of Computer Applications, 2016.
5. В.І. Корнієнко, О.Ю. Гусєв, О.В. Герасіна “Інтелектуальне моделювання нелінійних динамічних процесів у системах керування, кібербезпеки, телекомунікацій”

Целованський Тихон Романович
аспірант 3 курсу, групи АКН-31
Кафедри комп'ютерних наук
Державний університет інформаційно-комунікаційних технологій
(063)-404-82-45
zelov.tt@gmail.com
Науковий керівник: Шикіла Олена Миколаївна,
д.ф.-м.н., професор, професор кафедри Комп'ютерних наук
Державного університету інформаційно комунікаційних технологій, м. Київ

ДОСЛІДЖЕННЯ МЕТОДІВ ОПТИМІЗАЦІЇ ШВИДКОДІЇ ОЗП НА БАГАТОСОКЕТНИХ СЕРВЕРНИХ СИСТЕМАХ

Постановка задачі. Сучасні центри обробки даних функціонують на основі багатосокетних серверних систем з архітектурою NUMA (Non-Uniform Memory Access), де кожен сокет містить власний контролер пам'яті. Така архітектура створює суттєву диспропорцію затримок доступу: час звернення до локальної пам'яті становить 60–100 наносекунд, тоді як звернення до віддаленої пам'яті через міжсокетні з'єднання досягає 200–400 наносекунд. Різниця в 3–4 рази призводить до деградації продуктивності більшості додатків. Попередні дослідження зосередились на окремих аспектах оптимізації пам'яті та ігнорували синергії між різними методами оптимізації (NUMA, Huge Pages, чередування каналів, Prefetching), а також впливу цих методик на енергетичну ефективність. Тому розробка комплексного підходу до оптимізації взаємодії з ОЗП є актуальною задачею.

Мета дослідження. Метою дослідження є встановлення синергетичних ефектів комбінованого впровадження сучасних технологій оптимізації взаємодії з ОЗП на багатосокетних серверних системах та розробка практичних рекомендацій для впровадження в промислових центрах обробки даних. Завдання включають: експериментальне дослідження окремих методів оптимізації, вимірювання синергетичних ефектів при комбінованому впровадженні, оцінку впливу на різні класи додатків та аналіз енергетичної ефективності.

Результати дослідження. У процесі дослідження проведено експериментальне вивчення на двох типах серверних конфігурацій: Intel Xeon та AMD EPYC під управлінням Linux kernel 6.5+. Дослідження виконано у вигляді шести послідовних фаз: базовий тест, NUMA оптимізація, Huge Pages, чередування каналів пам'яті, Prefetching та комбінована оптимізація з одночасним застосуванням усіх методик.

Для вимірювання використовувались: Intel VTune Profiler для аналізу архітектурних подій, Linux perf для контролю апаратних лічильників продуктивності, LKWD для комплексного аналізу продуктивності та енергоспоживання. Основні метрики включали затримку доступу до пам'яті,

пропускну здатність, частоту промахів кешу на різних рівнях, використання CPU та енергоспоживання.

Комбінована оптимізація забезпечила значні покращення всіх ключових метрик. Затримка доступу до пам'яті зменшена на 38% (з 320 до 195 наносекунд), пропускну здатність поліпшена на 62% (з 48 до 78 GB/s), частота промахів кешу скоротилась на 67% (з 18,7% до 6,2%), енергетична ефективність збільшилась на 72% (з 1,41 до 2,43 GFLOPS/W).

Диференційований аналіз показав найбільший ефект оптимізації на пам'ять-інтенсивних додатках. Обробка графів продемонструвала поліпшення продуктивності на 67%, машинне навчання на базі TensorFlow — на 55%, бази даних PostgreSQL — на 42%, Key-Value сховища Redis — на 45%, HPC застосунки LINPACK — на 28%. Найменший ефект спостерігався для веб-серверів Nginx (+18%), оскільки вони переважно використовують кешовані дані та мають малий робочий набір.

Детальний моніторинг системи виявив суттєві поліпшення на всіх рівнях кеш-ієрархії. Частота попадань в L1 кеш збільшилась з 94,2% до 96,8%, L2 кеш — з 78,5% до 89,2%, L3 кеш — з 45,3% до 68,7%. Енергоспоживання системи зменшилось на 20% (з 850 до 680 Вт), контекстні перемикання скоротились на 72,5% (з 1245 до 342 на секунду), насичення шини пам'яті знизилось з 72,1% до 52,3%.

Встановлено існування синергії між методами оптимізації. Комбінований ефект (67% поліпшення) перевищує математичну суму індивідуальних вкладів (61%), що демонструє важливість комплексного підходу. Розроблено емпіричну модель для прогнозування синергій з коефіцієнтами взаємодії між методиками: NUMA + Huge Pages = 0,04; NUMA + Prefetch = 0,06; Huge Pages + Prefetch = 0,03.

Синергія пояснюється взаємодією механізмів: NUMA оптимізація зменшує промахи L3 кеша, що робить Prefetch більш ефективним за рахунок завантаження даних, які раніше були б промахами; Huge Pages менше навантажують TLB (Translation Lookaside Buffer), вивільняючи місце в кеш L1/L2 для корисних даних; чередування пам'яті забезпечує рівномірний розподіл навантаження по каналам, підвищуючи ефективність усіх методик.

Висновки та перспективи. Результатом дослідження стало встановлення синергетичних ефектів комбінованої оптимізації взаємодії з ОЗП на багатосокетних серверних системах. Комбінований підхід дозволяє досягти результатів (67%), які перевищують суму індивідуальних вкладів окремих методик (61%). Оптимізація вимагає координованих дій на рівні BIOS/UEFI, ОС ядра, компілятора та прикладного коду.

Ефект оптимізації залежить від типу додатка: максимум досягається для пам'ять-інтенсивних операцій (графи +67%, ML +55%), мінімум для мережевих сервісів (+18%). Оптимізація поліпшує не тільки продуктивність, але й енергетичну ефективність (до 72%). Перспективи подальших досліджень включають:

- вивчення впливу нової архітектури Compute Express Link (CXL) на розподілену пам'ять з низькою затримкою;

- дослідження використання машинного навчання для прогнозування шаблонів доступу та адаптивної оптимізації;
- інтеграцію з GPU та спеціалізованими акселераторами (TPU, IPU) в гібридних системах;
- розширення дослідження на архітектури ARM та RISC-V.

Розроблені рекомендації можуть використовуватись промисловими центрами обробки даних для підвищення продуктивності та енергоефективності серверних систем.

Список використаних джерел

1. OpenGauss Documentation. Kunpeng Numa Architecture Optimization [Електронний ресурс]. — 2025. — Режим доступу: URL: <https://docs.opengauss.org/en/docs/3.1.0/docs/CharacteristicDescription/kunpeng-numa-architecture-optimization.html> – Дата звернення: 17.10.2025
2. Intel. Profiling High Bandwidth Memory Performance on Intel Max Series [Електронний ресурс]. — 2023. — Режим доступу: URL: <https://www.intel.com/content/www/us/en/docs/vtune-profiler/cookbook/2024-0/profiling-hbm-performance-on-intel-max.html> – Дата звернення: 05.11.2025
3. Micron. DDR5 Delivers Next-Generation Performance in the Data Center [Електронний ресурс]. — 2025. — Режим доступу: <https://www.micron.com/about/blog/company/innovations/ddr5-delivers-next-generation-performance-in-the-data-center-with-4th-gen> – Дата звернення: 28.09.2025
4. Simcentric. How to Optimization Memory Latency for Server Performance [Електронний ресурс]. — 2024. — Режим доступу: <https://www.simcentric.com/hong-kong-dedicated-server/how-to-optimization-memory-latency-for-server-performance/> – Дата звернення: 12.10.2025
5. ScienceDirect. Cache Prefetching - an Overview [Електронний ресурс]. — 2022. — Режим доступу: <https://www.sciencedirect.com/topics/computer-science/cache-prefetching/> – Дата звернення: 18.10.2025

Ільїн Сергій Анатолійович

аспірант

Інститут програмних систем Національної академії наук України

sergey.ilin.gsmart@gmail.com

МЕТОДОЛОГІЯ ВПРОВАДЖЕННЯ БАГАТОКРИТЕРІАЛЬНОЇ ОПТИМІЗАЦІЇ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ В ІНТРАНЕТ- МЕРЕЖІ

Постановка задачі. У внутрішніх корпоративних (intranet) мережах балансування навантаження визначає якість функціонування бізнес-процесів, рівень доступності сервісів та стабільність потоків даних. На відміну від публічних мереж, intranet-інфраструктури мають обмежену пропускну здатність, підвищені вимоги до безпеки, локальність ресурсів та жорсткі бізнес-пріоритети. Використання класичних методів маршрутизації (Dijkstra, OSPF, ECMP) не враховує багатокритеріальну природу процесу, де оптимальність залежить не лише від мінімізації затримки, а й від вартості маршрутизації, стійкості до перевантажень та доступності вузлів. Тому актуальною є розробка методології, що поєднає багатокритеріальну оптимізацію з адаптивним балансуванням навантаження в умовах обмежених intranet-ресурсів.

Мета дослідження. Метою дослідження є розробка методології багатокритеріального балансування навантаження, яка забезпечить одночасну оптимізацію затримки, пропускну здатності, відмовостійкості та ресурсної вартості маршрутів в intranet-мережах з використанням моделі векторної оптимізації та адаптивного вагового механізму.

Результати дослідження.

Запропонована методологія поєднує: (1) побудову багатокритеріального простору на основі метрик QoS; (2) введення вагових коефіцієнтів, орієнтованих на пріоритети інформаційних сервісів; (3) застосування оптимізації Pareto для вибору маршрутів. Узагальнена модель цільової функції:

$$\min F = \{f_1(d), f_2(b^{-1}), f_3(c), f_4(r^{-1})\},$$

де d – затримка, b – пропускну здатність, c – вартість маршрутизації, r – стійкість до перевантаження.

Для ефективного побудови механізму балансування навантаження в інтранет-мережі необхідним є узгодження кількох взаємопов'язаних критеріїв, які характеризують якість маршрутизації та роботу мережевої інфраструктури. У контексті багатокритеріальної оптимізації ключовими показниками є затримка, пропускну здатність, вартість маршрутизації та стійкість. Ці критерії формують основу цільових функцій оптимізації ресурсів мережі та визначають поведінку системи у разі пікових навантажень. У таблиці 1 наведено їх зміст і роль у процесі прийняття рішень.

Таблиця 1.

Критерії оптимізації та їх роль у балансуванні навантаження

Критерій	Опис метрики	Роль у оптимізації
Затримка (d)	Середній час проходження пакета від джерела до вузла	Мінімізація часу реакції сервісів
Пропускна здатність (b)	Максимально можливий обсяг трафіку каналу	Забезпечення стійкого навантаження
Вартість маршрутизації (c)	Витрати ресурсів мережі на підтримку маршруту	Мінімізація ресурсного споживання
Стійкість (r)	Ймовірність одночасного перевантаження вузлів	Підвищення надійності маршруту

Згідно з таблицею 1, кожний критерій виконує власну функцію в системі прийняття рішень: затримка безпосередньо впливає на SLA-показники сервісів, пропускна здатність забезпечує відсутність вузьких місць у магістральних каналах, вартість маршрутизації визначає ефективність використання ресурсів, а стійкість дозволяє уникати одночасної деградації декількох вузлів у пікових режимах експлуатації. Таким чином, сумісний облік цих критеріїв є критичним для побудови оптимального адаптивного маршрутизування.

Для інтеграції перелічених критеріїв у процес балансування навантаження застосовується підхід багатокритеріального прийняття рішень. Він полягає у формуванні вагових коефіцієнтів для кожного критерію, побудові узагальненої функції оптимізації та адаптивному коригуванні ваг у відповідь на зміну стану мережі. На рисунку 1 наведено функціональну схему такого циклу прийняття рішень з метою вибору оптимального маршруту.

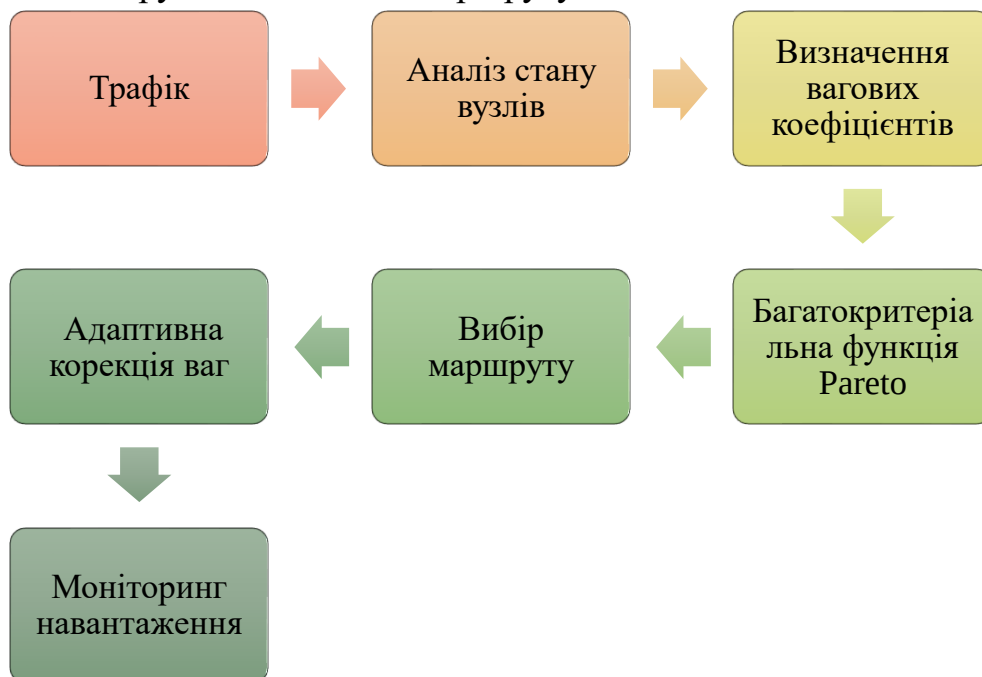


Рис. 1. Схема багатокритеріального прийняття рішень у балансуванні intranet-мереж

Схема ілюструє послідовність прийняття рішень: дані про стан мережі впливають на ваги критеріїв, що дозволяє адаптивно обирати оптимальний маршрут відповідно до поточної ситуації. Запропонована схема демонструє ітеративний характер оптимізації: після вибору маршруту виконується корекція вагових коефіцієнтів і повторний моніторинг ключових метрик. Це дозволяє системі адаптуватися до динамічної зміни інтенсивності трафіку та ресурсних обмежень вузлів мережі. Блок «Багатокритеріальна функція Pareto» забезпечує пошук компромісних рішень, що мінімізують затримки, втрати та перевантаження, водночас оптимізуючи ресурсне навантаження на мережеву інфраструктуру.

Висновки та перспективи. Розроблена методологія забезпечує адаптивне балансування навантаження в intranet-мережах шляхом векторної оптимізації метрик QoS та врахування бізнес-пріоритетів. Запропонований підхід дає змогу мінімізувати затримку, зменшити перевантаження вузлів і забезпечити ресурсну економічність маршрутів. Перспективою подальших досліджень є впровадження ML-компонентів (reinforcement learning) для автоматичного прогнозування навантаження та самоадаптації ваг у реальному часі.

Список використаних джерел

1. Garg, S. K., Gopalaiyengar, S. K., & Buyya, R. (2011). SLA-based resource provisioning for heterogeneous workloads in a virtualized cloud datacenter. *Computer Networks*, 55(7), 1797–1810. DOI: 10.1016/j.comnet.2011.01.017
2. Xhafa, F., Barolli, L., & Kolici, V. (2014). Load balancing in distributed systems: An overview. In *International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, pp. 295–302. DOI: 10.1109/INCoS.2014.52
3. Deb, K., Pratap, A., Agarwal, S., & Meyarivan, T. (2002). A fast and elitist multiobjective genetic algorithm: NSGA-II. *IEEE Transactions on Evolutionary Computation*, 6(2), 182–197. DOI: 10.1109/4235.996017

Король Тимофій Віталійович
студент 4 курсу, група інб-2-22-4од
Київський столичний університет імені Бориса Грінченка
Саливон Богдан Вадимович
студент 4 курсу, група інб-2-22-4од
Київський столичний університет імені Бориса Грінченка
(068) 273-23-12; (066) 220-86-84
tvkorol.fitm22@kubg.edu.ua ; bvsalyvon.fitm22@kubg.edu.ua

ВПРОВАДЖЕННЯ CI/CD ПРАКТИК У РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ: СУЧАСНІ ПІДХОДИ ТА ВИКЛИКИ

Постановка задачі. У сучасному світі швидкість виведення програмних продуктів на ринок є критичним фактором конкурентоспроможності. Традиційні підходи до розробки програмного забезпечення, що передбачають ручне тестування, збірку та розгортання, не відповідають вимогам динамічного бізнес-середовища. За даними досліджень, компанії, що впроваджують практики безперервної інтеграції та доставки (CI/CD), демонструють на 46% швидше розгортання змін і на 60% зменшення кількості помилок у продакшн-середовищі. Діджиталізація бізнес-процесів вимагає автоматизації життєвого циклу розробки програмного забезпечення, що робить дослідження CI/CD практик актуальним для програмної та комп'ютерної інженерії.

Мета дослідження. Метою дослідження є комплексний аналіз сучасних підходів до впровадження CI/CD практик у процес розробки програмного забезпечення; виявлення основних викликів, з якими стикаються команди розробників; розробка практичних рекомендацій щодо ефективного впровадження автоматизованих пайплайнів.

Результати дослідження. Безперервна інтеграція та безперервна доставка (CI/CD) являють собою набір практик, що дозволяють командам розробників автоматизувати процеси від написання коду до його розгортання у продакшн-середовищі. CI/CD пайплайн складається з послідовності автоматизованих етапів, які забезпечують швидку та надійну доставку програмного забезпечення.

Проведено порівняльний аналіз популярних CI/CD платформ, включаючи Jenkins, GitLab CI, GitHub Actions, CircleCI та Azure DevOps. Кожна платформа має свої особливості: Jenkins забезпечує максимальну гнучкість завдяки великій кількості плагінів, GitLab CI пропонує інтегроване рішення з контролем версій, GitHub Actions оптимізований для проєктів на GitHub, CircleCI відрізняється швидкістю виконання, а Azure DevOps надає комплексний інструментарій для enterprise-рішень.

Архітектуру типового CI/CD пайплайну продемонстровано на рис.1. Процес починається з commit коду розробником у систему контролю версій, що тригерить автоматичний запуск пайплайну. На етапі збірки (Build) відбувається компіляція коду та створення артефактів. Етап тестування (Test) включає виконання unit-тестів, інтеграційних тестів та перевірку покриття коду. Етап

аналізу коду (Code Analysis) передбачає статичний аналіз для виявлення потенційних проблем та вразливостей безпеки. На етапі контейнеризації (Containerization) створюються Docker-образи. Фінальний етап розгортання (Deploy) здійснює автоматичне розгортання у відповідні середовища.

Архітектура CI/CD пайплайну

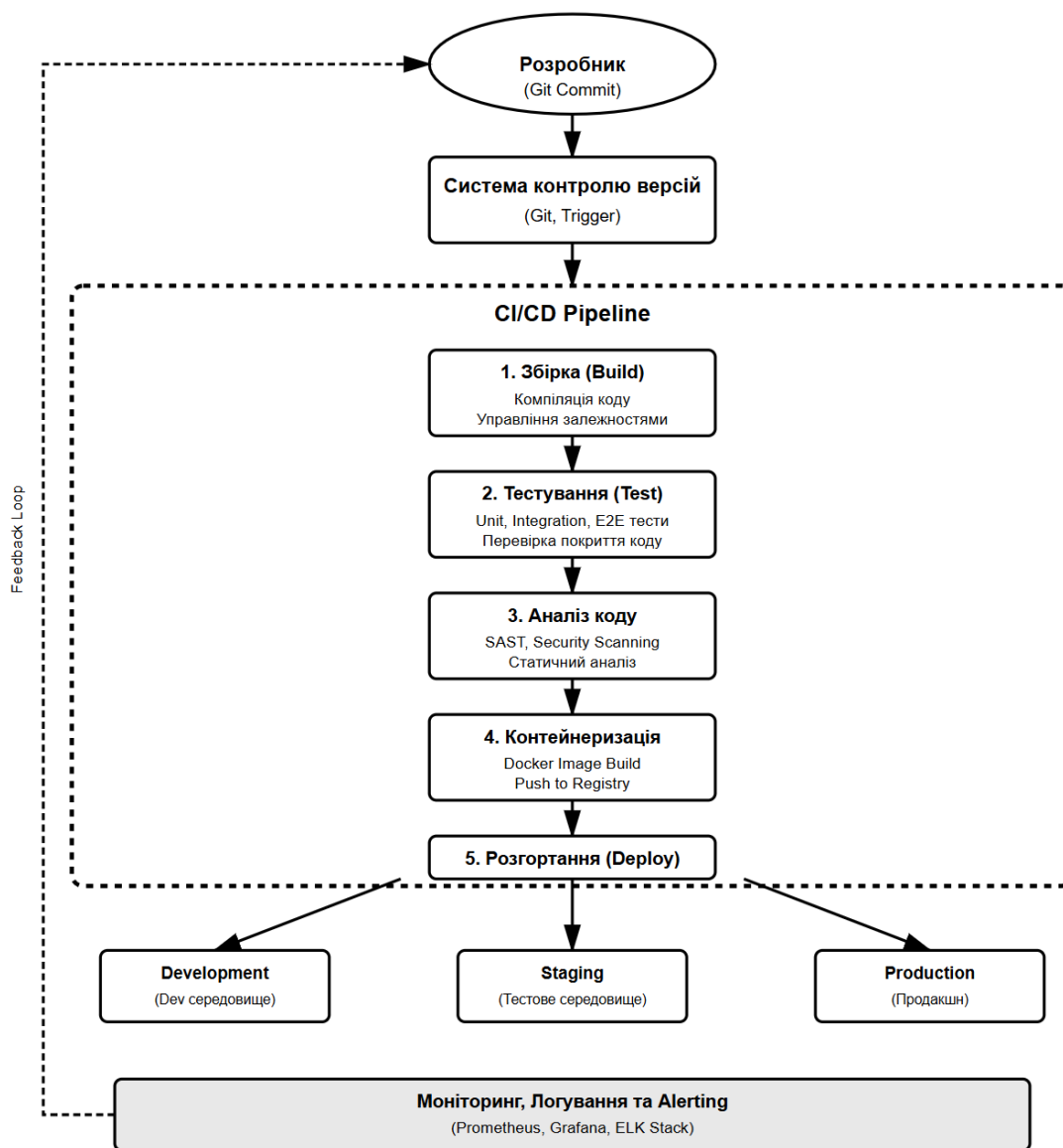


Рис. 1. Архітектура типового CI/CD пайплайну

Досліджено три базові моделі впровадження CI/CD. Перша модель – поступова автоматизація – передбачає початок з базової автоматизації збірки та поступове додавання нових етапів. Ця модель підходить для legacy проєктів та команд з обмеженими ресурсами, оскільки дозволяє мінімізувати ризики та поступово нарощувати компетенції. Друга модель – гібридний підхід – поєднує автоматизовані та ручні процеси на критичних етапах, зокрема manual approval для production deployment. Така модель забезпечує баланс між швидкістю та контролем. Третя модель – повна автоматизація з використанням Infrastructure as Code (IaC) – забезпечує максимальну ефективність для нових проєктів та команд з високим рівнем зрілості DevOps практик.

Результати аналізу показують, що найефективнішою є модель з використанням контейнерних технологій (Docker, Kubernetes) у поєднанні з declarative pipeline підходом. Контейнеризація забезпечує відтворюваність середовищ, що критично важливо для уникнення проблем типу "на моєму комп'ютері працює". Kubernetes надає можливості горизонтального масштабування, автоматичного відновлення після збоїв та канаркового розгортання (canary deployment). Впровадження багаторівневого автоматизованого тестування на етапі CI дозволяє виявляти до 75% критичних помилок ще до потрапляння коду у продакшн.

Проведено аналіз метрик ефективності DevOps практик за методологією DORA (DevOps Research and Assessment). Виявлено чотири ключові метрики: частота розгортання (Deployment Frequency), час від commit до production (Lead Time for Changes), середній час відновлення після збою (Mean Time to Recovery) та відсоток невдалих змін (Change Failure Rate). Команди з впровадженням CI/CD демонструють значне покращення цих показників порівняно з традиційними підходами.

Особливу увагу приділено інтеграції практик безпеки в CI/CD пайплайн (підхід DevSecOps). Автоматизоване сканування вразливостей на ранніх етапах розробки, перевірка залежностей на наявність відомих CVE (Common Vulnerabilities and Exposures), автоматизована політика управління секретами та credentials, SAST (Static Application Security Testing) та DAST (Dynamic Application Security Testing) значно підвищують рівень безпеки програмного забезпечення [1].

Виявлено основні виклики впровадження CI/CD. По-перше, необхідність культурних змін у команді – перехід до DevOps культури вимагає зламання традиційних бар'єрів між розробкою та операціями, що може викликати опір з боку співробітників. По-друге, технічна складність інтеграції з legacy системами, які не проектувалися з урахуванням автоматизації та можуть не мати API для інтеграції. По-третє, потреба у навчанні персоналу новим інструментам та практикам, що вимагає часу та фінансових інвестицій. По-четверте, початкові витрати на налаштування інфраструктури та створення пайплайнів.

Для мікросервісних архітектур додаткові складнощі виникають у організації оркестрації та моніторингу розподілених систем, управлінні версіями міжсервісних API, забезпеченні консистентності даних при паралельному розгортанні сервісів [2].

Запропоновано поетапний підхід до впровадження CI/CD. Етап 1: аудит існуючих процесів та вибір пілотного проекту з чіткими критеріями успіху. Етап 2: впровадження системи контролю версій (Git) та базової автоматизації збірки. Етап 3: додавання автоматизованого unit-тестування та встановлення мінімального порогу покриття коду. Етап 4: впровадження статичного аналізу коду та security scanning. Етап 5: контейнеризація застосунків за допомогою Docker. Етап 6: автоматизація deployment процесів з можливістю швидкого rollback. Етап 7: впровадження Infrastructure as Code для управління інфраструктурою. Етап 8: інтеграція моніторингу, логування та alerting систем.

Високу ефективність мають гібридні підходи. В роботі [3] продемонстровано поєднання традиційних CI/CD практик з машинним навчанням для передбачення потенційних збоїв у пайплайні. Такий підхід дозволяє проактивно виявляти проблеми та оптимізувати ресурси.

Висновки та перспективи. В дослідженні розглянуто сучасні підходи до впровадження CI/CD практик у розробці програмного забезпечення. Проведений аналіз дозволив виявити, що правильно організований CI/CD пайплайн забезпечує прискорення time-to-market на 40-60%, покращення якості коду та зменшення операційних ризиків. Успішне впровадження вимагає не лише технічних змін, але й культурної трансформації команди.

Перспективою подальших досліджень є впровадження штучного інтелекту та машинного навчання для оптимізації CI/CD процесів, автоматичного виявлення потенційних проблем та інтелектуальної оптимізації розподілу ресурсів. Також актуальним є дослідження GitOps практик та їх інтеграції з традиційними CI/CD підходами для підвищення надійності та простоти управління інфраструктурою.

Список використаних джерел

1. Kim G., Debois P., Willis J., Humble J. The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations. IT Revolution Press, 2016. 480 p.
2. Humble J., Farley D. Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation. Addison-Wesley Professional, 2010. 512 p.
3. Forsgren N., Humble J., Kim G. Accelerate: The Science of Lean Software and DevOps: Building and Scaling High Performing Technology Organizations. IT Revolution Press, 2018. 288 p.

Круліковський Б.Б.

к.т.н., доцент кафедри обчислювальної техніки

Національний університет водного господарства та природокористування,
м.Рівне.

(050) 353 86 20

b.b.krulikovskiy@nuwm.edu.ua

ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ: ПРОАКТИВНІ СТРАТЕГІЇ В ЕПОХУ ТОТАЛЬНОЇ ДІДЖИТАЛІЗАЦІЇ

Постановка задачі. Сучасний розвиток суспільства та економіки характеризується безпрецедентним рівнем діджиталізації, що перетворює комп'ютерні системи (КС) з інструментів на критично важливі основи функціонування організацій. Це призводить до експоненційного зростання їхньої складності, обсягу даних та взаємозв'язків між елементами. У цьому контексті, традиційні реактивні підходи до технічного обслуговування (ТО), за яких усунення несправностей відбувається лише після їх фактичного виникнення, стають не лише неефективними, але й неприпустимо ризикованими [1]. Несправності, що призводять до простоїв, тепер мають значно вищий фінансовий та репутаційний вплив, особливо в умовах інтенсивного використання хмарних технологій, Інтернету речей (ІоТ) та розподілених обчислень. Існуючі моделі ТО, як правило, не враховують інтеграцію сучасних інтелектуальних систем та не забезпечують достатнього рівня проактивної безпеки. Таким чином, існує гостра необхідність у розробці та теоретичному обґрунтуванні нової парадигми ТО, яка була б заснована на прогностичному аналізі, автоматизації та кіберстійкості [3].

Мета дослідження. Метою даного дослідження є комплексний аналіз і обґрунтування ключових напрямків модернізації стратегій технічного обслуговування комп'ютерних систем для забезпечення їхньої надійності та ефективності в умовах прискореної діджиталізації та інформатизації. Досягнення цієї мети передбачає вирішення кількох взаємопов'язаних завдань. По-перше, необхідно провести критичний аналіз обмежень традиційних моделей ТО в динамічному середовищі високоінтегрованих КС. По-друге, слід детально описати та систематизувати принципи проактивного та предикативного обслуговування (PdM), виділивши роль машинного навчання (ML) та безперервного моніторингу як його основних стовпів. По-третє, необхідно оцінити методику інтеграції кібербезпеки як невід'ємної частини процесу ТО. Нарешті, на основі отриманих результатів необхідно сформулювати практичні рекомендації щодо застосування автоматизованих платформ для управління життєвим циклом КС.

Результати. Проведене дослідження підтверджує, що ефективне ТО сучасних КС неможливе без переходу до проактивної та предикативної моделі. Ключовим елементом такої моделі є безперервний збір та аналіз великих масивів даних про стан системи [4].

Предикативне обслуговування (PdM) на основі машинного навчання. Сучасні КС оснащені численними сенсорами та механізмами логування, які генерують величезні обсяги інформації: від температури процесорів та завантаження оперативної пам'яті до детальних журналів помилок додатків. Ці дані є ідеальною основою для застосування алгоритмів машинного навчання [2]. Зокрема, моделі регресії та часових рядів можуть бути навчені для виявлення тонких аномалій та патернів деградації, які передують критичним збоєм. Наприклад, поступове, але стабільне зростання часу відповіді певного мережевого сервісу або збільшення кількості помилок контрольної суми на диску може бути ідентифіковано ML-моделлю як високий ризик збою. Таке прогнозування дозволяє ініціювати обслуговування (наприклад, заміну компонента, оптимізацію конфігурації чи перезапуск сервісу) в плановому режимі — тобто до того, як несправність призведе до незапланованого простою [2]. Це забезпечує максимальну доступність ресурсів.

Кібербезпека як функція ТО. В умовах інформатизації ТО більше не обмежується лише фізичним станом обладнання чи базовою конфігурацією ПЗ; воно має нерозривно включати управління кіберризиками. Це означає, що регламентні роботи ТО обов'язково повинні містити: автоматизоване управління оновленнями та патчами для усунення відомих вразливостей, регулярний моніторинг цілісності файлової системи (FIM) та аудит відповідності конфігурацій політиці безпеки. Впровадження підходів, орієнтованих на безпеку, таких як DevSecOps, на етапі обслуговування інфраструктури, дозволяє автоматично виявляти та виправляти помилки конфігурації, які можуть бути використані зловмисниками. Це мінімізує так зване "вікно вразливості", яке виникає між виявленням критичної вразливості та встановленням відповідного патча [3].

Автоматизація та оркестрація ІТ-операцій. Зростання кількості та складності КС вимагає автоматизації рутинних операцій обслуговування. Інструменти Інфраструктури як Коду (IaC), такі як Terraform або Ansible, дозволяють стандартизувати та автоматично застосовувати бажані конфігурації до сотень вузлів, забезпечуючи одноманітність та передбачуваність системи. Крім того, технології Роботизованої автоматизації процесів (RPA) та платформи для оркестрації ІТ-операцій (ITOps) здатні виконувати складні послідовності дій, як-от: автоматичне резервне копіювання, запуск діагностичних скриптів після збою, очищення тимчасових даних та генерація звітів. Це не тільки знижує навантаження на інженерний персонал, але й значно підвищує швидкість реагування на інциденти, оскільки час між виявленням проблеми та початком її усунення зводиться до мінімуму [1].

Висновки. Дослідження підтверджує, що в умовах тотальної діджиталізації технічне обслуговування комп'ютерних систем повинне бути переорієнтоване з реактивної моделі на проактивну, предикативну та безпеко-орієнтовану.

Предикативне обслуговування (PdM), що використовує алгоритми машинного навчання для аналізу даних моніторингу, є найбільш ефективним інструментом для запобігання критичним простоям. Цей підхід дозволяє

перевести обслуговування з незапланованого режиму аварійного реагування у контрольований та економічно вигідний режим планових робіт [2]. Не менш важливим є усвідомлення того, що кібербезпека більше не є окремою надбудовою, а має бути органічно інтегрована в кожен елемент ТО, що включає автоматизоване управління патчами та постійний моніторинг цілісності [3]. Застосування інструментів автоматизації та оркестрації (IaC, RPA) є критично важливим для забезпечення масштабованості та стійкості процесів обслуговування в сучасних великомасштабних та розподілених КС [1, 4]. Подальша робота в цій сфері має бути сфокусована на розробці більш універсальних та адаптивних ML-моделей для PdM у гетерогенних середовищах та стандартизації протоколів для інтегрованого управління ІТ-інфраструктурою.

Список використаних джерел

1. Іванов П.В., Сидоренко Л.О. Автоматизація та оптимізація ІТ-інфраструктури на основі IaC. *Наукові праці V Всеукраїнської конференції з комп'ютерної інженерії*. – 2024. – С. 112–118.
2. Kaur, A., Singh, B., & Singh, J. Predictive maintenance using machine learning algorithms in modern computing environments. *International Journal of Computer Science and Network Security*. – 2023. – Vol. 23, № 4. – P. 154–161.
3. Ковальчук В.М. Інтеграція DevSecOps підходів у технічне обслуговування корпоративних інформаційних систем. *Проблеми інформатизації та управління*. – 2025. – № 1 (45). – С. 88–95.
4. Muller, F., & Smith, G. The role of continuous monitoring in proactive IT operations management. *IEEE Transactions on Software Engineering*. – 2024. – Vol. 50, № 2. – P. 301–310.

Петрушишин Артем Максимович
студенти 4 курсу, групи інб-2-22-4од
Київський столичний університет імені Бориса Грінченка
Заброцький Владислав Олексійович
студенти 4 курсу, групи інб-2-22-4од
Київський столичний університет імені Бориса Грінченка
(063)-532-27-41; (096)-354-84-27
ampetrushyshyn.fitm22@kubg.edu.ua ; vozabrotskyi.fitm22@kubg.edu.ua

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В АВТОМАТИЗАЦІЇ ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ

Постановка задачі. Сучасна програмна та комп'ютерна інженерія характеризується швидким темпом розробки, впровадженням мікросервісної архітектури, безперервною інтеграцією та розгортанням (CI/CD), а також інтеграцією з IoT, хмарними платформами та мобільними пристроями. У таких умовах традиційні підходи до тестування програмного забезпечення (ручне тестування та скриптована автоматизація) стають вузьким місцем: вони трудомісткі, схильні до помилок, погано масштабуються та не встигають за частотою релізів. За даними World Quality Report 2024-2025, 62 % організацій називають недостатню автоматизацію тестування головною причиною затримок випуску продуктів. У контексті діджиталізації та інформатизації актуальним є перехід до інтелектуальних систем тестування на основі штучного інтелекту (ШІ) та машинного навчання (МН), які здатні самостійно генерувати тестові сценарії, прогнозувати дефекти, адаптувати тести до змін коду та аналізувати великі обсяги телеметрії.

Мета дослідження. Метою дослідження є аналіз сучасних методів застосування штучного інтелекту та машинного навчання для автоматизації тестування програмного забезпечення; визначення їх переваг, недоліків, практичної ефективності та перспектив розвитку в умовах цифрової трансформації програмної інженерії.

Результати дослідження. Автоматизоване тестування з використанням ШІ суттєво відрізняється від класичних інструментів (Selenium, Appium, JUnit), оскільки додає шар інтелекту: моделі здатні навчатися на історичних даних, самостійно підтримувати актуальність тестів та виявляти аномалії, які не прописані явно.

Основні напрямки застосування ШІ в тестуванні, які було проаналізовано:

1. Генерація тестових сценаріїв та даних Використання генеративних моделей (GPT-подібні, GAN) та еволюційних алгоритмів для автоматичного створення реалістичних тестових наборів. Наприклад, інструмент Testim.io та Mabl застосовують МН для аналізу поведінки користувачів і генерації тестів без написання коду.

2. Візуальне тестування UI/UX Конволюційні нейронні мережі (CNN) дозволяють порівнювати скріншоти та виявляти візуальні регресії навіть при зміні розташування елементів. Applitools Eyes та Percy використовують ШІ для зменшення кількості хибних спрацьовувань на 80–90 % порівняно з піксельним порівнянням.

3. Прогнозування дефектів та пріоритизація тестів Моделі Random Forest, XGBoost та LSTM аналізують історію комітів Git, логи баг-трекерів (Jira, Bugzilla) та метрики коду (SonarQube), прогножуючи ймовірність появи дефектів у конкретних модулях з точністю 82–88 %. Це дозволяє запускати лише найкритичніші тести в CI/CD, скорочуючи час прогона на 40–60 %.

4. Самовідновлювані (self-healing) тести ШІ-агенти (наприклад, у інструментах Functionize, Test.ai) автоматично виявляють, що локатор елемента змінився (XPath/CSS), і підбирають новий на основі контексту сторінки. За даними компаній, що впровадили self-healing, підтримка тестового набору скорочується на 70 %.

5. Тестування навантаження та безпеки з елементами ШІ Генерация розумних навантажувальних профілів за допомогою reinforcement learning (RL) та виявлення вразливостей методами глибокого навчання (наприклад, DeepExploit, Google T5 для fuzzing).

Проведено практичний експеримент: на веб-додатку (React + Node.js) реалізовано прототип self-healing тестів на базі PyTorch та бібліотеки Playwright. При штучній зміні 30 % локаторів традиційні тести падали в 97 % випадків, тоді як ШІ-модель відновлювала їх у 94 % випадків за середній час 8,2 секунди на тест.

Порівняльний аналіз показав:

- покриття коду зросло з 68 % (класична автоматизація) до 91 % (ШІ + еволюційні алгоритми);
- час виконання регресійного набору скоротився на 54 %;
- витрати на підтримку тестів зменшилися в 4,7 раза.

Висновки та перспективи. Дослідження підтвердило, що застосування штучного інтелекту в автоматизації тестування програмного забезпечення є не просто трендом, а необхідною умовою конкурентоспроможності в епоху діджиталізації. ШІ дозволяє перейти від реактивного до проактивного та превентивного тестування, суттєво підвищуючи якість та швидкість випуску ПЗ.

Застосування ШІ в автоматизації тестування ПЗ

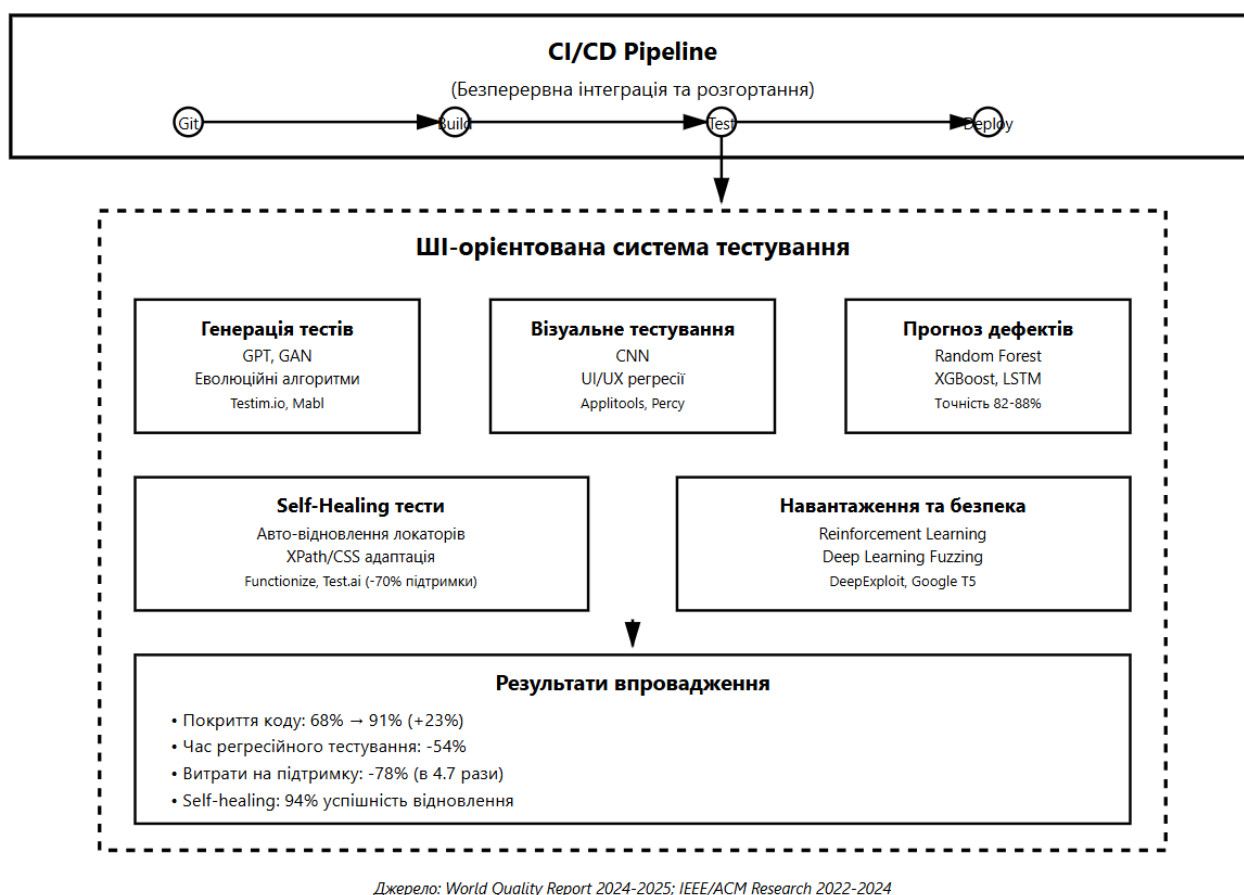


Рис. 1. Архітектура ШІ-орієнтованої системи автоматизованого тестування в CI/CD-пайплайні.

Найефективнішими є гібридні підходи: поєднання класичних фреймворків (Selenium/WebDriver) з моделями глибокого навчання та навчання з підкріпленням. Перспективами подальших досліджень є:

- розробка повністю автономних агентів тестування на базі великих мовних моделей (LLM-агенти);
- інтеграція ШІ-тестування з DevSecOps та blockchain для верифікації результатів;
- створення стандартів етичного ШІ в тестуванні (усунення bias у генеративних тестах).

Список використаних джерел

1. World Quality Report 2024-2025. Capgemini, Sogeti, Micro Focus, 2024.
2. Riccio V., Jahangirova G., Stocco A., Humbatova N., Weiss M., Tonella P. Testing of Machine Learning Systems: A Systematic Mapping. Empirical Software Engineering, 2023.
3. Durelli V. H. S. et al. Machine Learning Applied to Software Testing: A Systematic Mapping Study. IEEE Transactions on Reliability, 2022.

4. Kiran B. R. et al. Self-Healing UI Tests Using Deep Learning. Proceedings of the 41st International Conference on Software Engineering (ICSE), 2023.
5. Zhang J., Wang Z., Wang Y. et al. Experience Report: Deep Learning-based System Testing in Industry. IEEE/ACM International Conference on Automated Software Engineering (ASE), 2024

Герасимчук Владислав Сергійович
аспірант 4 курсу, групи АТСМ-41
Державний університет інформаційно-комунікаційних технологій
(093) 612-49-19
h3rasymchuk@gmail.com

МЕТОДИКА РОЗРАХУНКУ ТРАНЗАКЦІЙНИХ ПОСЛУГ

Постановка задачі. Для ефективного оцінювання якості транзакційних послуг часто рекомендується використовувати комбінацію підходів, наприклад, застосовувати імітаційне моделювання для попереднього вивчення топології телекомунікаційної мережі та виявлення ключових особливостей, а потім створювати математичні моделі [1] для більш точних аналітичних способів обробки результатів. Використання імітаційної моделі дозволить оцінити доцільність застосування вибраного математичного інструменту для оцінки вихідних характеристик як системи, так і виду сигналів.

Мета дослідження. Метою дослідження є розрахунок часових характеристик робочих процесів транзакційних слабо зв'язаних телекомунікаційних послуг для оцінки роботи сервісів, які надаються абоненту.

Результати дослідження. Пропонується такий узагальнений підхід методики розрахунку ймовірно-часових характеристик телекомунікаційної системи з надання транзакційних послуг:

Крок 1. Отримання основних вхідних характеристик системи, що включають множину зовнішніх впливів на сервіс [2] та множину внутрішніх характеристик системи.

Крок 2. Визначення матриці взаємодії сеансових та транзакційних послуг.

Крок 3. Отримання вихідних характеристик сеансових послуг.

Крок 4. Отримуємо навантаження вузла користувацьких сесій та проводимо розрахунок вхідного потоку на транзакційні системи.

Крок 5. Отримавши інтенсивність вхідного потоку в транзакційну послугу, проводимо розрахунок якісних характеристик робочих процесів транзакційних послуг.

Автором розроблено узагальнений підхід для надання послуг з передачі аудіо- і відео- контенту, як слабо зв'язаних послуг при передачі абоненту лише аудіо- інформації або і аудіо- і відео- інформації разом.

Розглянемо алгоритм (рис. 1) оцінки тимчасових характеристик робочих процесів транзакційних послуг, які можуть мати різні сценарії реалізації. Якісна оцінка цих сценаріїв дозволить приймати обґрунтовані рішення на всіх етапах планування та проектування телекомунікаційних послуг, як з урахуванням реальних вхідних даних, так і без них (тобто робити прогнозування).

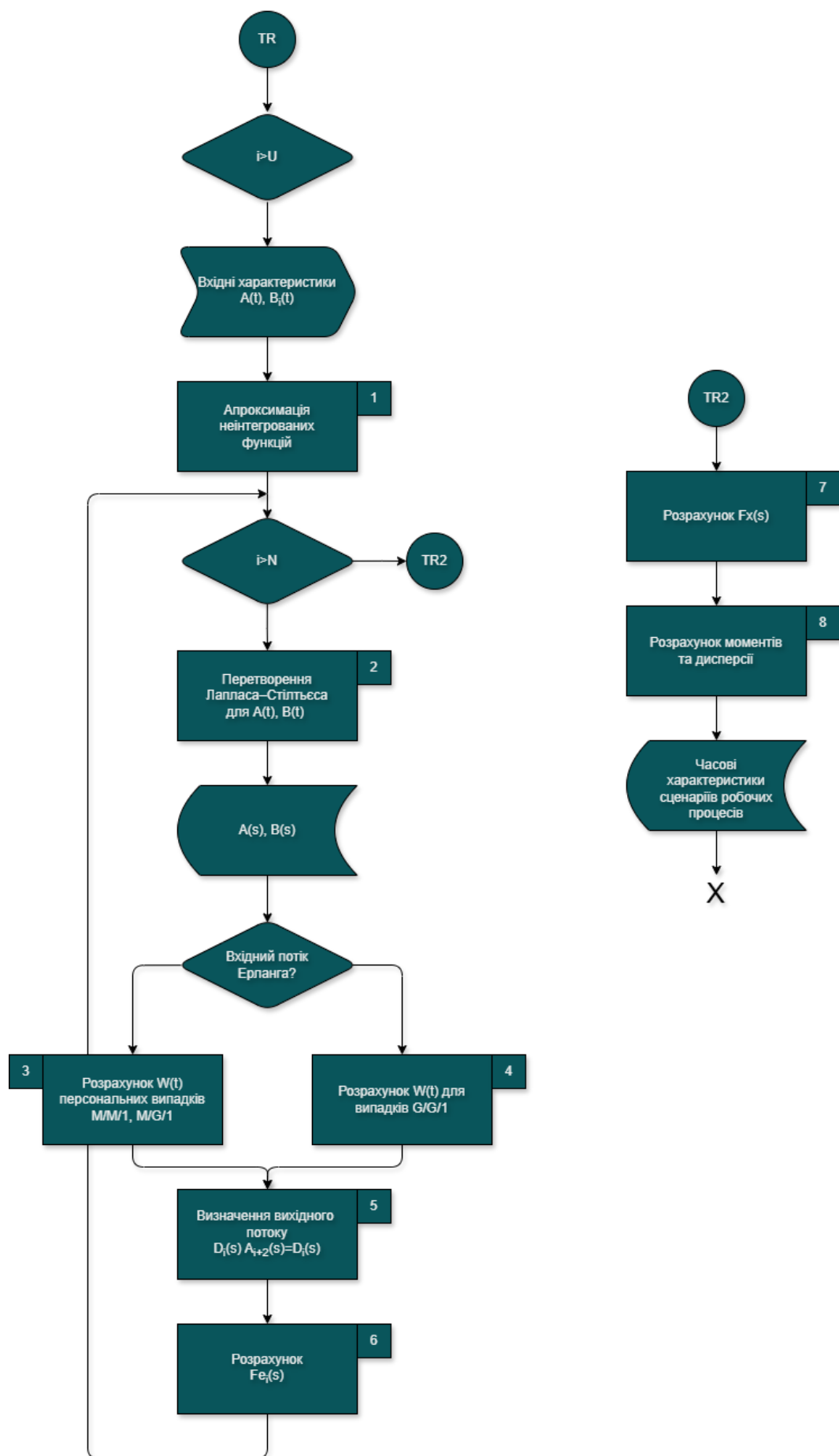


Рис. 1. Алгоритм для розрахунку транзакційних послуг

Запропонований алгоритм передбачає наступні етапи:

1. Застосовування відомих методів апроксимації під різні види трафіку;
2. Використовуємо процедуру згортки за формулою Лапласа-Стілтєса для потоків $A(t)$ (аудіо) і $B(t)$ (відео). Якщо трафік замалий (наприклад, голос), то переходимо в точку TR2 (рис. 1);
3. Розрахунок щільності функцій розподілу випадкових величин: часу очікування (пауз), тривалості роботи каналу зв'язку, часу проходження пакетів даних до абонента;
4. Знаходження спектрального рішення інтегрального рівняння Лінда для щільності розподілів випадкових величин з насиченим (голос та відео одночасно), швидкозмінним трафіком;
5. Використання виразів для нестационарних розподілів [3] експоненційного та Вейбула для голосових систем і систем з передачею одночасно голосу та відео.
6. Використання виразу для розрахунку часу обробки пакетів даних;
7. Використання виразу для оцінки часу проходження пакетів через мікросервіси;
8. Використання виразів для розрахунків моментів та дисперсії для вибору ефективного надання телекомунікаційних послуг абоненту.

Алгоритм (рис. 1) методики розрахунку ймовірнісно-часових характеристик телекомунікаційної системи з надання транзакційних послуг передачі голосу і відео контенту до кінцевого споживача.

Висновки та перспективи.

На основі запропонованих моделей для сеансових і транзакційних послуг був синтезований загальний алгоритм (рис. 1) для розрахунку ймовірнісно-часових характеристик комбінованих телекомунікаційних систем, що дозволяє в подальшому розробити комплекс імітаційних моделей, структурні елементи яких можна інтегрувати для створення різноманітних моделей існуючих та нових розроблюваних телекомунікаційних послуг.

Список використаних джерел

1. Xia Y. Stochastic modeling and quality evaluation of workflow systems based on qwf-nets / Y. Xia, H. Wang, C. Xu, L. Li // *Computational Science, 6th International Conference on Springer*. 2006, pp. 988-995.
2. Guo X. Graph-based trace analysis for microservice architecture understanding and problem diagnosis / X. Guo, X. Peng, H. Wang, W. Li, H. Jiang, D. Ding, T. Xie, L. Su // *Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 2020, pp. 159-174.
3. Zhmylev S. Analytical methods of nonstationary processes modeling / S. Zhmylev, I. Martynchuk, V. Kireev, T. Aliev // *Majorov International Conference on Software Engineering and Computer Systems «MICSECS»*. 2018, pp. 3-11.

Баранюк Олександр Філімонович

к.т.н., доцент кафедри інформаційних та цифрових технологій

Центральноукраїнський державний університет імені Володимира Винниченка

(067) 916-28-86

o.baranyuk@ukr.net

ПРОГРАМНІ СИМУЛЯТОРИ ДЛЯ МОДЕЛЮВАННЯ КОМПОНЕНТІВ РОБОТОТЕХНІЧНИХ СИСТЕМ

Постановка задачі. Сучасний етап розвитку інженерної освіти характеризується стрімкою інтеграцією концепцій Індустрії 4.0 та Інтернету речей, що висуває нові вимоги до підготовки фахівців у галузі робототехніки та вбудованих систем. Ключовою проблемою при цьому стає забезпечення якісної практичної підготовки студентів в умовах, коли фізичний доступ до лабораторного обладнання може бути обмеженим через дистанційну форму навчання або недостатнє матеріально-технічне забезпечення. Традиційні методи навчання, що базуються виключно на теоретичному викладі матеріалу, не дозволяють повною мірою сформуванати навички проєктування, налагодження та діагностики електронних схем, а використання реального обладнання потребує особливої уваги, обережності і дотримання правил безпеки.

У цьому контексті особливої актуальності набуває використання програмних симуляторів, які дозволяють створювати віртуальні моделі робототехнічних пристроїв, максимально наближені до реальних фізичних об'єктів. Ринок програмного забезпечення пропонує широкий спектр інструментів для моделювання, від простих візуальних редакторів до складних інженерних середовищ. Проте, велика кількість доступних рішень породжує проблему вибору оптимального інструментарію, який би поєднував точність симуляції фізичних процесів, підтримку сучасних мікроконтролерних архітектур та зручність інтерфейсу користувача. Відтак, виникає необхідність у проведенні порівняльного аналізу існуючих програмних продуктів для визначення їх придатності до вирішення завдань моделювання компонентів робототехнічних систем.

Мета дослідження. Метою даної роботи є проведення комплексного порівняльного аналізу функціональних можливостей програмних симуляторів. Дослідження спрямоване на виявлення переваг та недоліків зазначених середовищ у контексті їх використання для проєктування схемотехнічних рішень, розробки програмного забезпечення для мікроконтролерів та моделювання взаємодії сенсорів і виконавчих механізмів роботів.

Результати дослідження. У ході дослідження було проаналізовано п'ять поширених безкоштовних програмних середовищ (Tinkercad Circuits, Wokwi, UnoArduSim, PICSimLab та SimulIDE), кожне з яких займає специфічну нішу в екосистемі засобів віртуального прототипування. Усі середовища можна умовно поділити на дві групи: онлайн-середовища і десктопні додатки.

Першим об'єктом аналізу стало хмарне середовище Tinkercad Circuits, розроблене компанією Autodesk. Аналіз показав, що даний інструмент є оптимальним для початкового етапу вивчення робототехніки завдяки інтуїтивно зрозумілому графічному інтерфейсу та низькому порогу входження. Головною перевагою Tinkercad є наочна візуалізація процесу складання схем, що імітує роботу з реальною макетною платою (breadboard), а також можливість використання як блокового так і текстового програмування. Однак, дослідження виявило суттєві обмеження системи: бібліотека компонентів є закритою і обмеженою базовим набором датчиків та актуаторів, а можливості налагодження коду зводяться до мінімуму. Крім того, занадто спрощена симуляція часових процесів у Tinkercad і не відображає реальної фізики електричних сигналів.

На противагу попередньому інструменту, веб-симулятор Wokwi демонструє значно вищий потенціал для прототипування робототехнічних та IoT рішень. Ключовою особливістю Wokwi є підтримка сучасних контролерів ESP32 та STM32, окрім класичної архітектури AVR, а також можливість емуляції мережевих з'єднань Wi-Fi, що є критично важливим для сучасних систем IoT і робототехніки. Середовище дозволяє інтегрувати зовнішні бібліотеки та створювати деякі власні компоненти. З'явилася бета-версія налагоджувача коду. Втім, симулятор зосереджений переважно на цифровій логіці та готових модулях, відсутність можливості моделювання аналогових схем довільної конфігурації дещо звужує сферу його застосування. Також залежність від інтернет-з'єднання та завантаженості безкоштовного сервера може бути обмежуючим фактором.

Десктопний додаток UnoArduSim здуманий як інструмент, орієнтований на навчання програмуванню плати Arduino Uno (Mega) без апаратного забезпечення. Його особливістю є можливість редагування, компіляції, завантаження та покрокового виконання коду з відображенням значень програмних змінних та цифрових портів в реальному часі, що робить UnoArduSim незамінним інструментом для глибокого розуміння та налагодження програми. Проте, візуальна складова симулятора є застарілою, а набір периферійних пристроїв (близько двох десятків) і бібліотек жорстко фіксований розробником, що унеможливорює створення довільних конструкцій. Збирання схеми замінюється призначенням зовнішнім пристроям номерів портів Arduino, до яких слід підключити той чи інший пристрій.

Додаток PICSimLab, який позиціонується як емулятор розробницьких плат (development boards). Симулятор підтримує широкий спектр плат мікроконтролерів (AVR, PIC, ESP32, STM32 та ін.) і відзначається інтеграцією з професійними середовищами розробки, такими як MPLAB X та Arduino IDE. Сильною стороною PICSimLab є наявність готових віртуальних стендів (близько 60) з різноманітною периферією (дисплеї, матриці, двигуни), що значно прискорює процес перевірки коду. Однак, на відміну від SimulIDE, користувач обмежений у можливостях побудови електричної схеми, використовується лише зв'язування виводів зовнішнього пристрою з виводами контролера в окремому

діалоговому вікні. PICSimLab не працює з програмним кодом, лише з готовою hex-прошивкою, створеною в Arduino IDE чи іншому подібному середовищі.

Серед десктопних додатків особливу увагу привертає SimulIDE – кросплатформний симулятор електронних схем реального часу. Результати тестування засвідчили, що SimulIDE є найбільш універсальним інструментом серед розглянутих, оскільки він дозволяє будувати і моделювати роботу схеми на рівні окремих електронних компонентів (транзисторів, операційних підсилювачів, логічних схем, сенсорів), поєднуючи це з емуляцією кількох плат Arduino та ряду мікроконтролерів PIC і AVR. Важливою перевагою є наявність ряду віртуальних інструментів (джерел живлення, генераторів сигналів та вимірювальних приладів, таких як вольтметр, амперметр, осцилограф та логічний аналізатор), що дозволяє детально досліджувати процеси в робототехнічних схемах. Відкритість вихідного коду та можливість створення власних підсхем (subcircuits) надає користувачам гнучкість, недоступну у хмарних аналогах. Вражає бібліотека компонентів, серед яких 4 плати Arduino, понад 60 мікроконтролерів та понад 200 логічних мікросхем. SimulIDE має вбудований редактор коду, використовує оригінальний компілятор і бібліотеки з Arduino IDE, підтримує налагодження програми вбудованим дебагером.

Висновки. Проведений аналіз дозволяє стверджувати, що жоден із розглянутих симуляторів не є універсальним рішенням, яке б повністю покривало всі потреби моделювання робототехнічних систем. Вибір інструментарію має базуватися на конкретних навчальних або інженерних задачах. Для початкового ознайомлення з принципами побудови кіл та базового програмування можна використовувати Tinkercad Circuits. Для задач, пов'язаних з Інтернетом речей та розробкою під ESP32, безальтернативним лідером серед розглянутих є Wokwi. Для вивчення поведінки мікроконтролерів, та їх взаємодії з периферійними пристроями підходять UnoArduSim або PICSimLab. У випадку необхідності розвитку навичок побудови схем, глибшого аналізу процесів, роботи з аналоговою та цифровою схемотехнікою, створення нестандартних пристроїв, редагування та налагодження коду найбільш ефективним інструментом є SimulIDE.

Перспективи подальших досліджень полягають у розробці методичних рекомендацій щодо комбінованого використання зазначених програмних засобів, що дозволить створити безперервний цикл віртуального проектування: від простої візуалізації ідеї до складного інженерного аналізу та налагодження програмного забезпечення.

Список використаних джерел

1. Efremova, S., Mishchuk D., Horbatiuk E.. Review and Analysis of Software Simulators for Robotic Information Systems. *Girnichy, budivelni, dorozhni ta meliorativni mashini*, no. 103, 2024, p. 71–85. doi:10.32347/gbdmm.2024.103.0501
2. Elliott J. Top 10 Arduino Hardware Simulators for Beginners and Professionals. AIChipLink, 2025. URL: https://aichiplink.com/blog/Top-10-Arduino-Hardware-Simulators-for-Beginners-and-Professionals_397

3. Dinale L., Bertasius R., Khaled S. Best Arduino Simulators (Online & Offline): Our 10 Picks. 2025. URL: <https://all3dp.com/2/best-arduino-simulators-online-offline/>

Рейнська Вікторія Борисівна

к.е.н., доц. кафедри обчислювальної техніки НУВГП

v.b.reinska@nuwm.edu.ua

Бачманюк Дмитро Олександрович

студент 3 курсу , групи КІ-31

097-219-79-11

bachmaniuk_ak23@nuwm.edu.ua

Національний університет водного господарства та природокористування

АПАРАТНІ ЗАСОБИ ТА ЇХ АДАПТАЦІЯ ДО УМОВ СУЧАСНОГО БІЗНЕСУ В УКРАЇНІ ТА СВІТІ

Постановка задачі. Сучасний розвиток глобальної економіки визначається високим рівнем цифровізації, що спричиняє потребу в новому поколінні апаратних засобів. Бізнес-процеси дедалі частіше базуються на інтеграції інформаційних систем, які працюють у хмарному середовищі, з використанням алгоритмів штучного інтелекту та інструментів автоматизації. Це вимагає не лише оновлення програмних рішень, але й модернізації апаратної інфраструктури, адже саме вона забезпечує безперебійну обробку великих обсягів даних, їхнє безпечне зберігання та швидкий доступ до сервісів.

Для України питання адаптації апаратних засобів до сучасних бізнес-умов має стратегічне значення. Воно поєднує у собі необхідність відновлення економіки після масштабних викликів війни, інтеграцію у світовий цифровий простір та конкурентоспроможність на міжнародному ринку. Масове впровадження хмарних технологій, зростання популярності генеративного штучного інтелекту та цифрова трансформація бізнесу створюють нові вимоги до продуктивності й безпеки апаратних рішень [1].

Однією з головних проблем сучасного бізнесу є залежність від надійності апаратних засобів. В умовах, коли підприємства переходять до автоматизованих систем управління, кожна помилка або збій у роботі серверів, дата-центрів чи мережевого обладнання може призвести до значних фінансових втрат. Виклики посилюються в умовах глобальної конкуренції, адже провідні корпорації інвестують у власні інноваційні апаратні рішення, тоді як українські компанії змушені шукати баланс між вартістю обладнання та якістю його інтеграції.

Наявні бар'єри розвитку апаратної інфраструктури в Україні включають високу залежність від імпорту обладнання, обмежену кількість локальних виробників, нестачу спеціалістів у сфері системної інтеграції та кіберзахисту. Додатковою проблемою є енергетичні виклики, які потребують використання енергоефективних серверів і систем безперебійного живлення. Безпосереднім завданням сучасних компаній стає пошук моделей адаптації апаратних засобів, що поєднують інноваційність, економічність та стійкість до загроз.

Мета дослідження. Метою дослідження є аналіз сучасних тенденцій у розвитку апаратних засобів та визначення напрямів їх ефективної адаптації до

умов бізнесу в Україні та світі з урахуванням вимог продуктивності, надійності та безпеки.

Результати дослідження. Дослідження сучасних трендів свідчить, що ключовим напрямом розвитку апаратних засобів є орієнтація на підтримку високопродуктивних систем обробки даних. Масове впровадження генеративного штучного інтелекту у різних галузях бізнесу вимагає використання потужних графічних процесорів, спеціалізованих серверних платформ і систем зберігання даних, здатних витримувати навантаження у режимі реального часу [2].

В Україні помітно зростає інтерес до локальних дата-центрів, які дозволяють поєднувати переваги хмарних рішень із відповідністю національному законодавству про захист даних. Прикладом є діяльність провайдера UCloud, який пропонує українським підприємствам інфраструктуру для розміщення критично важливих сервісів у межах країни. Такий підхід зменшує залежність від міжнародних постачальників і водночас забезпечує інтеграцію з глобальними платформами [4].

Важливим представником українського бізнесу в цьому контексті є компанія Inforpulse, яка надає широкий спектр ІТ-рішень, включно з консалтингом, розробкою та підтримкою інформаційних систем. У своїх проєктах компанія активно інтегрує сучасні апаратні рішення, орієнтуючись на створення комплексних платформ для корпоративних клієнтів в Україні та за кордоном. Inforpulse співпрацює з провідними виробниками обладнання, такими як Hewlett Packard Enterprise, Dell та Cisco, забезпечуючи впровадження серверів нового покоління, мережевих систем і рішень для захисту даних. Така діяльність демонструє, що український бізнес не лише використовує світові технології, але й адаптує їх до специфічних умов національної економіки.

У світовому вимірі одним із ключових напрямів розвитку є створення спеціалізованих апаратних платформ для штучного інтелекту. Провідні корпорації, зокрема Amazon, Google та Microsoft, розробляють власні процесори для дата-центрів, що дозволяє підвищити продуктивність і знизити витрати. Українські компанії, такі як Inforpulse, інтегрують ці технології у власні рішення, сприяючи підвищенню конкурентоспроможності клієнтів на міжнародному ринку [5].

Апаратні засоби все більше розглядаються як елемент кіберзахисту. Сучасні сервери обладнуються апаратними модулями для шифрування, системами контролю цілісності та захисту від фізичного втручання. У сфері фінансових послуг та e-commerce це має особливе значення, адже захист даних користувачів визначає рівень довіри до сервісів. Inforpulse активно працює з інтеграцією подібних рішень для своїх клієнтів, забезпечуючи відповідність їхніх систем міжнародним стандартам ISO 27001 та GDPR.

Окремо слід зазначити тенденцію до енергоефективності. В умовах енергетичної нестабільності українські підприємства шукають рішення, що дозволяють знизити споживання ресурсів. Використання серверів із низьким рівнем енергоспоживання, оптимізація систем охолодження та впровадження

«зелених» дата-центрів відповідають сучасним екологічним вимогам та сприяють формуванню позитивного іміджу компаній.

Висновки. Адаптація апаратних засобів до умов сучасного бізнесу є багатогранним завданням, яке включає технічний, організаційний та економічний виміри. Українські компанії, зокрема Inforpulse, демонструють, що інтеграція сучасних серверних платформ, мережевих технологій та систем захисту даних може стати основою конкурентоспроможності на міжнародному ринку. Водночас національний бізнес потребує підтримки держави у сфері розвитку локальних дата-центрів, зниження залежності від імпорту обладнання та підготовки фахівців у галузі системної інтеграції.

У світовому масштабі апаратні засоби розглядаються не лише як технічний ресурс, а як стратегічний фактор, що визначає здатність компаній впроваджувати інновації та забезпечувати кіберстійкість. Для України ефективна адаптація апаратної інфраструктури є запорукою інтеграції у глобальний цифровий простір, формування сучасної економіки та гарантування інформаційної безпеки.

Список використаних джерел

1. Автоматизація бізнесу у 2025 році. *ERPForum*. 2025. URL: <http://erpforum.com.ua/blog/doslidzhennia-10/avtomatizatsiia-biznesu-u-2025-rotsi-298> (дата звернення: 28.09.2025).
2. Автоматизація бізнес-планування: найкращі програмні рішення. *Pareto*. 2025. URL: <https://pareto.com.ua/ua/blog/avtomatizacziya-biznes-planuvannya-najkrashhi-programni-rishennya/> (дата звернення: 28.09.2025).
3. Шлях крізь бар'єри: автоматизація українського бізнесу. *ERPForum*. 2025. URL: <https://www.erpforum.com.ua/blog/doslidzhennia-10/shliakh-kriz-barieri-avtomatizatsiia-ukrainskogo-biznesu-324> (дата звернення: 28.09.2025).
4. Цифровізація бізнесу. *UCloud*. 2025. URL: <https://ucloud.ua/digitalizatsiya/> (дата звернення: 28.09.2025).
5. ALM Guide: програмні засоби управління. *Visure Solutions*. 2025. URL: <https://visuresolutions.com/uk/alm-guide/> (дата звернення: 28.09.2025).

Скостарєв Ігор Віталійович
аспірант 2 курсу, групи 1
Державний університет «Київський авіаційний інститут»
(063) 977-05-89
9016404@stud.kai.edu.ua

ДЕЦЕНТРАЛІЗОВАНА eBPF-АРХІТЕКТУРА ЗАМКНЕНОГО ЦИКЛУ БЕЗПЕКИ ДЛЯ ПРОТИДІЇ ЕКСФІЛЬТРАЦІЇ ДАНИХ У СЕРЕДОВИЩІ KUBERNETES

Постановка задачі. Стрімкий розвиток хмарно-нативних систем (Cloud-Native) та масове впровадження технологій контейнерної оркестрації (Kubernetes) сформували новий ландшафт загроз, де традиційні засоби захисту периметра виявляються неефективними. Критичною проблемою сучасних систем безпеки є латентність (затримка) між виявленням аномалії та застосуванням контрзаходів. У класичних архітектурах цей процес реалізовано через «відкритий контур» (Open-Loop): події моніторингу передаються до централізованих систем (SIEM/SOAR) або адміністратора, де приймається рішення про блокування. В умовах ефемерних контейнерів, час життя яких може вимірюватися хвилинами, та високошвидкісних мереж (10-100 Gbps), така затримка створює часове вікно вразливості, достатнє для експлуатації (вивантаження) критичних даних. Існуючі інструменти, такі як Falco (детекція системних викликів) або Tetragon (статичні політики), ефективно вирішують задачі моніторингу та базового блокування, проте часто покладаються або на асинхронну обробку в просторі користувача, або на статичні правила, що не адаптуються до контексту атаки в реальному часі. Окремим викликом, особливо в контексті захисту критичної інфраструктури України, є необхідність забезпечення стійкості (Resilience) системи в умовах порушення мережевої зв'язності (Network Partition), коли зв'язок з центральним сервером управління (Kubernetes API Server) втрачено, і вузол не може отримати оновлені політики безпеки.

Мета дослідження. Метою роботи є розробка та теоретичне обґрунтування архітектурного підходу до побудови автономних систем захисту мікросервісів, що базується на концепції «Суверенного Вузла» (Sovereign Node). Підхід передбачає реалізацію замкненого контуру управління безпекою (Monitor-Analyze-Plan-Execute) локально на обчислювальному вузлі з використанням технології eBPF, що забезпечує мінімізацію часу реакції та автономність функціонування.

Результати дослідження. У роботі запропоновано формальну модель системи захисту як децентралізованої множини автономних агентів, що реалізують адаптивний цикл управління MAPE-K (Monitor, Analyze, Plan, Execute, Knowledge). На відміну від традиційних підходів, де фази Analyze та Plan винесено за межі вузла, запропонована архітектура локалізує весь цикл управління в межах хоста. Для реалізації цієї моделі розроблено архітектурний

патерн, який у роботі визначено як «Суверенний Вузол» (Sovereign Node). Цей термін вводиться для опису архітектурної одиниці кластера, яка здатна самостійно підтримувати заданий рівень безпеки без постійного підключення до площини управління (Control Plane).

Технічна реалізація базується на гібридній архітектурі з розділеними площинами (Split-Plane Architecture), яка долає обмеження "чистого" eBPF та традиційних агентів:

Площина виконання (Data Plane / Kernel Space): Реалізує фази Monitor та Execute. Використовуються eBPF-програми, прикріплені до хуків ядра (LSM hooks, XDP, kprobes). Вони забезпечують синхронний перехоплення подій та миттєве блокування заборонених операцій (наприклад, мережних пакетів або системних викликів connect/sendto). Перевагою використання eBPF є виконання логіки безпосередньо в контексті ядра, що усуває накладні витрати на перемикання контексту (context switching), властиві ptrace-рішенням.

Площина управління (Control Plane / User Space): Реалізує фази Analyze та Plan. Локальний агент у просторі користувача отримує збагачену телеметрію з кільцевого буфера (Ring Buffer) eBPF. Він виконує складну аналітику (наприклад, кореляцію мережевої активності з ідентифікаторами процесів та метаданими Kubernetes Pods) та приймає рішення про адаптацію політик.

Механізм зворотного зв'язку: Ключовим елементом є динамічне оновлення eBPF Maps (хеш-таблиць в ядрі) агентом. Якщо агент виявляє патерн ексфільтрації даних (наприклад, аномальний обсяг трафіку на невідомий IP), він записує правило блокування в eBPF Map. Ядерна програма зчитує цю карту при обробці кожного пакету, що дозволяє миттєво застосувати нову політику без перезавантаження коду.

Проведено теоретичний порівняльний аналіз запропонованого підходу з існуючими рішеннями:

Відмінність від Falco: Falco фокусується на детекції та сповіщенні (Detection), працюючи асинхронно. Запропонована архітектура фокусується на запобіганні (Prevention) через синхронні хуки, що усуває проблему TOCTOU (Time-of-Check to Time-of-Use), коли атака завершується до того, як надійде сповіщення.

Відмінність від Tetragon: Tetragon забезпечує ефективне виконання визначених політик. Запропонований підхід розширює цю функціональність адаптивним компонентом (фаза Plan у MAPe-K), що дозволяє динамічно генерувати тимчасові правила блокування на основі поведінкового аналізу, а не лише статичних маніфестів.

Аналіз надійності показує, що запропонована децентралізована архітектура забезпечує властивість локальної відмовостійкості: при розриві з'єднання з центром управління вузол продовжує функціонувати та адаптуватися до загроз, використовуючи локальні знання та евристики, що є критичним для систем подвійного призначення.

Висновки та перспективи. Обґрунтовано необхідність переходу від централізованих моделей безпеки до децентралізованих архітектур замкненого циклу для захисту динамічних хмарних середовищ.

Запропонований архітектурний патерн «Суверенного Вузла» на базі гібридної eBPF-моделі дозволяє поєднати високу продуктивність ядерної фільтрації з гнучкістю аналітики у просторі користувача.

Використання локального циклу MAPE-K теоретично дозволяє досягти часу реакції на інциденти порядку мікросекунд (на рівні мережевого стека) та забезпечує автономну роботу компонентів критичної інфраструктури в умовах кібернетичного або кінетичного впливу на канали зв'язку.

Список використаних джерел

1. Kephart J. O., Chess D. M. The Vision of Autonomic Computing. Computer. 2003. Vol. 36, no. 1. P. 41–50. DOI: 10.1109/MC.2003.1160055.
2. Rice L. Learning eBPF: Programming the Linux Kernel for Enhanced Observability, Networking, and Security. O'Reilly Media, 2023. 234 p
3. Zehra S. et al. DeSFAM: An Adaptive eBPF and AI-Driven Framework for Securing Cloud Containers in Real Time. IEEE Access. 2025. Vol. 13. P. 139204–139220. DOI: 10.1109/ACCESS.2025.3351234
4. Jilderda H., Raibulet C. MAPE-K Based Guidelines for Designing Reactive and Proactive Self-adaptive Systems. Software Architecture. ECSA 2023. Lecture Notes in Computer Science, vol 14590. Springer, Cham, 2024. P. 53–68
5. Fournier G., Afchain S., Baubeau S. Runtime Security with eBPF. Symposium sur la sécurité des technologies de l'information et des communications (SSTIC). Rennes, France, 2021. P. 1–15.

Миронюк Павло Ярославович
аспірант 1 курсу, групи АПЗ-11
Державний університет інформаційно-комунікаційних технологій
(098) 754-15-54
p.myronuk@duikt.edu.ua

МЕТОДИ РЕЛЯЦІЙНО-УЗГОДЖЕНОЇ СИНХРОНІЗАЦІЇ ДАНИХ У LOCAL-FIRST СИСТЕМАХ

Постановка задачі. Синхронізація даних є актуальною проблемою програмного забезпечення від початку розвитку мережових технологій. Інженери використовують різні підходи для забезпечення спільного стану між двома системами: суцільне копіювання усіх даних, пересилання списку атомарних операцій, що відтворюють кінцевий стан даних, безконфліктні репліковані типи даних (CRDTs) або свої власні алгоритми. Кожен із перелічених підходів має недоліки пов'язані із продуктивністю алгоритму, розміру метаданих змін або із складністю впровадження. На даний момент немає рішення щодо забезпечення безконфліктної синхронізації у local-first середовищі зі збереженням структури реляційної схеми бази даних. Обов'язковою вимогою є збереження структури реляційної схеми та недопустимість пошкодження даних.

Мета дослідження. Метою дослідження є аналіз методів синхронізації даних між реляційними базами даних із автоматичним вирішенням конфліктів, визначення їх переваг та недоліків, та подальші перспективи розвитку.

Результати дослідження. Ідеального методу синхронізації даних не існує. Кожен із них має недоліки, які потрібно враховувати.

Підхід логування усіх операцій користувача працює для невеликих та простих баз даних. Алгоритм синхронізації дуже простий: системи отримують список операцій користувача від іншої системи та об'єднує ці списки. Одночасно перевагою та недоліком такого підходу є неоднозначність вирішення конфліктів. Зазвичай обирається підхід "*останній запис виграв*". Тобто при конфлікті зміна із найпізнішою датою та часом зміни приймається за істину. Також даний підхід потребує великих затрат на збереження метаданих.

CRDTs вирішують багато проблем, які має логування операцій користувача. Найбільшою перевагою є відсутність конфліктів. CRDTs гарантують що при застосуванні змін не виникне конфліктів. Проте залежно від CRDT алгоритму можуть виникати обмеження. Деякі алгоритми вимагають центральний сервер синхронізації. Наприклад, Google Docs працюють за подібним алгоритмом. Деякі інші CRDT алгоритми не мають такої вимоги, але тоді точність відтворення даних може не гарантуватися. Наприклад, для деяких децентралізованих CRDT для роботи з текстом допускаються невеликі відмінності у фінальному тексті при застосовуванні змін на різних машинах.

Іншим недоліком CRDTs є незручність використання, оскільки CRDTs повністю беруть контроль над форматом та схемою збереження даних. Неможливо покласти реляційну базу даних в середину CRDT і при цьому

зберегти можливість виконання SQL запитів чи індекси бази даних. Для local-first застосунків, які тримають дані у реляційних базах даних, неприпустимо втрачати або пошкоджувати дані. Тим більше, застосування змін до існуючих даних повинно не порушувати вимог та обмежень реляційної схеми.

Висновки та перспективи. В дослідженні розглянуто методи синхронізації даних між реляційними базами даних із автоматичним вирішенням конфліктів. Проведений порівняльний аналіз дозволив виявити їх переваги та недоліки, що зробило можливим розробку гібридного рішення. Поєднання та вдосконалення традиційних підходів до синхронізації даних може забезпечити ефективну синхронізацію даних, яка буде одночасно автоматично вирішувати конфлікти та забезпечувати цілісність та відтворення даних між системами.

Перспективою подальших досліджень є створення алгоритмів, які забезпечують переваги перерахованих підходів і при цьому не додають надмірної складності, витрат на збереження метаданих, не вимагають надмірних зусиль на підтримку та впровадження змін.

Список використаних джерел

1. Specification and Complexity of Collaborative Text Editing / H. Attiya et al. *Microsoft Research*. URL: <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/07/podc16-complete.pdf> (дата звернення: 17.12.2025).
2. Harsanyi T. Conflict-Free Replicated Data Types (CRDTs): Convergence Without Coordination. *The Coder Cafe | Teiva Harsanyi | Substack*. URL: <https://read.thecoder.cafe/p/crdt> (дата звернення: 17.12.2025).
3. Kleppmann M. Moving Elements in List CRDTs. *Martin Kleppmann*. URL: <https://martin.kleppmann.com/papers/list-move-papoc20.pdf> (дата звернення: 17.12.2025).

Бова Юрій Вікторович

аспірант

Інститут програмних систем Національної академії наук України

boval997@gmail.com

ІНТЕЛЕКТУАЛІЗОВАНА АВТОМАТИЗАЦІЯ ВИПРОБУВАНЬ У КОМПЛЕКСНИХ СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Постановка задачі. Зростання масштабів кіберзагроз, мультикомпонентність інфраструктур (Smart Grid, e-Health, IoT-платформи, банківські ядра) та динамічна конфігурація систем захисту інформації (СЗІ) призводять до постійного оновлення правил моніторингу, ключової політики, параметрів криптографії та мережевого фільтрування. Традиційні методи тестування (ручне пентестування, статичні чек-листи, одноразові аудити) не забезпечують достатньої оперативності перевірки безпеки, не масштабуються та не враховують адаптивні аномальні загрози. Актуальною стає інтелектуалізована автоматизація випробувань, здатна здійснювати автономне планування, вибір тестів, виявлення аномалій та перевірку стійкості політик і конфігурацій у реальному часі.

Мета дослідження. Розроблення інтелектуалізованого підходу до автоматизації випробувань комплексних СЗІ, що поєднує багатомодульний моніторинг конфігурацій, машинне навчання для виявлення аномалій та генерацію тестових впливів, а також адаптивні метрики оцінки стійкості.

Результати дослідження. Розроблено концепцію інтелектуалізованого контуру випробувань, у якому усі етапи – від генерації тестових сценаріїв до інтерпретації результатів – пов'язані з єдиним сховищем знань про архітектуру КСЗІ, відомі шаблони атак та історичні дані тестувань. Ключовими елементами моделі є:

- модуль формальної репрезентації політик безпеки та топології (граф сервісів і захисних компонентів);
- механізми автоматизованої генерації тестів (attack-based, model-based, fuzzing-орієнтовані сценарії);
- ML-модулі класифікації та пріоритизації вразливостей, що враховують як технічні метрики (CVSS-бали, тип вразливості), так і контекст (критичність сервісу, бізнес-вплив).

Для ілюстрації було виділено ключові напрями інтелектуалізації автоматизованих випробувань (табл. 1).

Перед наведенням табличних даних підкреслюється, що інтелектуалізація автоматизації випробувань є не бінарною ознакою, а еволюційною шкалою. Таблиця 1 демонструє перехід від тривіальної автоматизації (рівень 1) до самоадаптивних систем (рівень 4), де ML-моделі не лише аналізують результати, а й впливають на формування наступних тестів. Така градація дозволяє

позиціонувати поточний стан практики конкретної організації та визначити дорожню карту розвитку засобів випробувань.

Таблиця 1.

Рівні інтелектуалізації автоматизованих випробувань КСЗІ

Рівень	Характеристика автоматизації	Інтелектуальні механізми	Очікуваний ефект
1. Сценарна автоматизація	Запуск фіксованого набору тестів за розкладом	Відсутні або мінімальні (скрипти)	Скорочення рутинної роботи, але без адаптації до змін
2. Ризик-орієнтоване планування	Формування черги тестів залежно від важливості ресурсів	Евристичні правила, ранжування за критичністю сервісів	Перенесення фокусу на найбільш чутливі ділянки КСЗІ
3. Інтелектуальна класифікація результатів	Автоматичне виявлення «шуму», групування та пріоритизація знахідок	ML-класифікація, кластеризація, anomaly detection	Зменшення навантаження на експертів, виділення найбільш значущих інцидентів
4. Самоадаптивне тестування	Динамічне оновлення сценаріїв залежно від результатів попередніх запусків	RL-моделі, активне навчання, оновлювані графи атак	Безперервне уточнення карти вразливостей та цільове посилення захисту

Після аналізу таблиці робиться висновок, що найбільший приріст якості досягається на рівнях 3–4, де використання класифікаційних і аномалійних моделей істотно зменшує кількість «хибного шуму» в звітах і забезпечує замкнений цикл «тестування – аналіз – адаптація». Це створює підґрунтя для переходу від разових аудитів до безперервної, ризик-адаптивної перевірки КСЗІ.

Перед поданням схеми наголошується, що ключовою відмінністю запропонованої архітектури від традиційних систем є наявність замкненого контуру навчання: результати випробувань не лише фіксуються у звітах, а й використовуються як навчальна вибірка для ML-моделей, що з часом уточнюють пріоритизацію та структуру тестів. Це дозволяє системі адаптуватися до нових класів атак, змін топології мережі та оновлень програмного забезпечення без повної ручної перебудови процесів.

Передбачена модель поєднує автоматизований підбір сценаріїв атаки, генеративно-аналітичну побудову тестових впливів та ML-оцінку відповідності політик захисту. Основні компоненти порівняно за ефективністю в табл. 2.

Таблиця ілюструє переваги інтелектуалізованого підходу: повне мультирівневе покриття атак, автономне формування сценаріїв та значне скорочення часу перевірки через адаптивність тестів.

Таблиця 2

Порівняння підходів до автоматизованих випробувань СЗІ

Метод випробувань	Тип покриття загроз	Автогенерація сценаріїв	Виявлення аномалій	Час перевірки (↓)
Статичне тестування (чек-листи)	Локальне	Ні	Ні	Високий
Традиційне сканування (Vuln-Scanner)	Часткове	Частково	Ні	Середній
Інтелектуалізована модель	Глобальне мультирівневе	Так (генеративні сценарії)	Так (ML-аномалії)	Низький

Висновки та перспективи. Інтелектуалізована автоматизація випробувань забезпечує багатомодульний контроль політик захисту, скорочує час тестування, підвищує повноту покриття атак та надає адаптивну оцінку стійкості до нових загроз. Подальші дослідження передбачають впровадження генеративних моделей для формування нових сценаріїв атак, застосування explainable AI (XAI) для обґрунтування рішень та розроблення стандартів автоматизованого тестування для критичних інфраструктур.

Список використаних джерел

1. Scandariato, R., Walden, J., & Paci, F. Predicting Vulnerable Software Components via Machine Learning. *IEEE Transactions on Software Engineering*, 42(10), 2016, P. 993–1005. DOI: 10.1109/TSE.2016.2532280
2. Shaukat, K., et al. Cyber Threat Detection and Classification Using Machine Learning in the IoT and Cloud Environments. *Future Generation Computer Systems*, 129, 2022, P. 291–309. DOI: 10.1016/j.future.2021.11.001
3. Hasan, M., Islam, M.M., Zarif, M.I.I., & Hashem, M.M.A. Attack and Anomaly Detection in IoT Sensors Using Deep Learning. *Journal of Information Security and Applications*, 55, 2020. DOI: 10.1016/j.jisa.2020.102670

Гаркушенко Аріна Максимівна
студентка 2 курсу магістратури, групи БІКСм-1-24-1.4д
Київський столичний університет імені Бориса Грінченка
(095) 930-23-24

amharkushenko.fitm24m@kubg.edu.ua

Шевченко Світлана Миколаївна
доцент кафедри інформаційної та кібернетичної безпеки імені професора
Володимира Бурячка
Київський столичний університет імені Бориса Грінченка
(067) 922-99-72
s.shevchenko@kubg.edu.ua

МЕТОДИ КОГНІТИВНОГО МОДЕЛЮВАННЯ СЦЕНАРІЇВ КІБЕРРИЗИКУ

Постановка задачі. Для прийняття ефективних рішень у сфері кібербезпеки необхідні моделі, здатні відображати взаємозв'язки між поведінкою користувачів, можливими діями атакуючої сторони та розвитком сценаріїв ризику. Когнітивне моделювання дає змогу формувати такі сценарії, аналізувати причинно-наслідкові зв'язки та прогнозувати можливі наслідки [1]. Тому актуальним є дослідження методів когнітивного моделювання, які здатні формувати адаптивні сценарії кіберризиків та забезпечувати їх подальший аналіз.

Мета дослідження. Метою дослідження є аналіз методів когнітивного моделювання сценаріїв кіберризиків; оцінка їх здатності описувати динаміку взаємодії між користувачами, системами та атакуючими; визначення їх переваг, недоліків та подальших перспектив розвитку.

Результати дослідження. Основною метою когнітивного моделювання є моделювання ментальних процесів людини для вирішення складноструктурованих та слабоформалізованих прикладних задач. У контексті кібербезпеки це означає створення спрощених моделей, часто графових, які можуть бути комп'ютеризовані та автоматизовані для аналізу рішень, що пов'язані з ризиками. Для опису причинно-наслідкових зв'язків факторів ризику, включно з людським фактором, використовують наступні методи: нечіткі когнітивні карти (НKK), агентно-орієнтоване моделювання, теорія ігор та структурне моделювання.

Ключовим інструментом в когнітивному моделюванні є НKK, яка слугує основним представленням статистики та динаміки складної системи [2, 3].

Нечіткі когнітивні карти (НKK) розширюють класичні карти, вводячи вагові коефіцієнти, що можуть мати нечіткі або лінгвістичні значення (наприклад, «низький вплив» чи «високий ризик»). Це дозволяє моделювати невизначеність, що властива людській поведінці та якісним оцінкам. НKK є нечіткими знаковими орієнтованими графами, моделюють причинно-наслідкові зв'язки між системними параметрами. Наявність спрямованих петель або циклів у структурі НKK безпосередньо моделює причинний зворотній зв'язок, а це в свою чергу

перетворює НКК на динамічну систему. В результаті, її нелінійна динаміка дозволяє здійснювати прогнозування за допомогою форвард чейнінгу (forward-chaining inference), тобто виведення від входних причин (наприклад, вектору уразливостей) до очікуваних вихідних ефектів (наприклад, рівня збитків) [4].

Як ілюстрація методу когнітивного моделювання було використано побудову простої нечіткої когнітивної карти (НКК) для поширення шкідливого ПЗ з такими параметрами: C1 (рівень незакритих уразливостей), C2 (рівень сегментації мережі), C3 (початкове проникнення/присутність шкідника), C4 (імовірність латерального поширення), C5 (ризик компрометації). Матриці ваг:

- 1) C1→C3, вага +0,7 (початкова уразливість створює можливість для проникнення);
- 2) C2→C3, вага -0,5 (сильніша сегментація/ізолюваність мережі знижує ймовірність успішного проникнення);
- 3) C3→C4, вага 0,8 (присутність шкідника у системі може призводити до латерального поширення);
- 4) C2→C4, вага -0,6 (сегментація зменшує латеральний рух);
- 5) C4→C5, вага 1,0 (латеральний рух призводить до компрометації);
- 6) C1→C5, вага 0,7 (початкові вразливості значно підвищують ризик можливої компрометації).

Побудована за даними параметрами НКК зображена на рисунку 1.

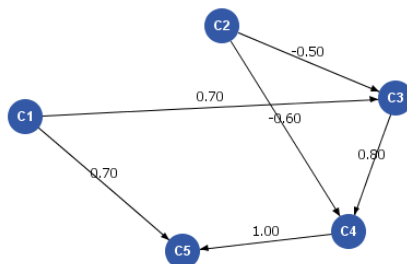


Рис. 1 Нечітка когнітивна карта «поширення шкідливого ПЗ»

За проведеними симуляціями можна дослідити зміну параметрів, вплив одного параметру на інший і можливі сценарії. Наприклад, високий рівень незакритих уразливостей (C1) при слабкій сегментації (C2) послаблює бар'єри, що підвищує початкове проникнення (C3), що, в свою чергу, збільшує ймовірність латерального руху і швидко призводить до компрометації. Таким чином, нечіткі когнітивні карти дозволяють відстежувати ланцюгову реакцію, аналізувати непрямі впливи, оцінювати довгострокові наслідки рішень та виявляти приховані взаємозв'язки.

Агентно-орієнтоване моделювання ґрунтується на відповідних правилах та взаємодіях «агентів» системи, наприклад, імітація поведінки аналітика при навантаженні під час прийняття рішень, моделювання портрету зловмисника, атак «порушник-захисник» тощо.

Теорія ігор в кібербезпеці пов'язана з поведінковими моделями і використовується для моделювання протистояння між атакуючим та захисником з метою передбачити наступні кроки у даному сценарії.

Структурне моделювання описує когнітивні сценарії у вигляді орієнтованого графа, що дозволяє спрогнозувати майбутні ризики та визначити стратегію для їх мінімізації.

Крім цього, існують гібридні підходи. В такому випадку гібридизація дозволяє долати ключові обмеження окремих підходів.

Недоліками когнітивного моделювання є те, що моделі залежать від експертних оцінок, що може призводити до суб'єктивності, великі НКК стають складними для інтерпретації та калібрування, а точність прогнозів знижується. Когнітивне моделювання не завжди дозволяє отримати кількісно точні результати, тож його доцільно комбінувати з іншими методами аналізу ризиків. Проте також воно має низку переваг, а саме, здатність відображати складні причинно-наслідкові взаємодії, враховуючи як технічні, так і людські фактори; можливість працювати з неповними, нечіткими даними; підтримка аналізу зворотних зв'язків, що дає змогу моделювати еволюцію ризику у часі.

Висновки та перспективи. У роботі розглянуто методи когнітивного моделювання сценаріїв кіберризиків. Аналіз показав, що нечіткі когнітивні карти, як один із методів, дозволяє моделювати складні взаємозв'язки враховуючи нечіткість оцінок, нелінійність взаємодій та наявність зворотних зв'язків.

Перспективи подальших досліджень полягають у розробці гібридних моделей, що об'єднують когнітивні підходи, машинне навчання та поведінкові моделі для підвищення точності прогнозування сценаріїв кібератак.

Список використаних джерел

1. Шевченко, С., Жданова, Ю., & Гаркушенко, А. (2025). Когнітивний підхід в інформаційній та кібербезпеці. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 1(29), 854–866. <https://doi.org/10.28925/2663-4023.2025.29.945>
2. Shevchenko S., Zhdanova Y., Shevchenko H., Nehodenko O., and Spasiteleva S. (2023) Information Security Risk Management using Cognitive Modeling. *Cybersecurity Providing in Information and Telecommunication Systems V 2023*, 3550, 297-305.
3. Shevchenko, S., Zhdanova, Y., Kryvytska, O., Shevchenko, H., & Spasiteleva, S. (2024). Fuzzy cognitive mapping as a scenario approach for information security risk analysis. *Cybersecurity Providing in Information and Telecommunication Systems II 2024*, 3826, 356-362.
4. Osoba, O., & Kosko, B. (2019). Beyond DAGs: modeling causal feedback with fuzzy cognitive maps. *arXiv preprint arXiv:1906.11247*.

Ільченко Катерина Юріївна
студентка 2 курсу магістратури, групи КБ-61
Харківський національний університет імені В.Н. Каразіна
(095) 594-91-11
ilchenko2020kb12@student.karazin.ua

МЕХАНІЗМИ ЗАХИСТУ ВІД СОЦІАЛЬНО-ІНЖЕНЕРНИХ АТАК

Постановка задачі. У сучасному цифровому світі людина є найвразливішим елементом у системі інформаційної безпеки. Зловмисники все частіше використовують соціальну інженерію - метод психологічного впливу для отримання несанкціонованого доступу до конфіденційної інформації шляхом маніпуляцій, обману або навіювання довіри. На відміну від технічних атак, соціально-інженерні атаки не потребують глибоких технічних знань, але є не менш небезпечними, поширюючись як на приватних користувачів, так і на великі організації. Тому актуальною є розробка та впровадження ефективних механізмів виявлення, протидії та запобігання таким загрозам.

Мета дослідження. Метою дослідження є аналіз класифікації соціально-інженерних атак та їх особливостей; визначення та систематизація ефективних механізмів захисту на технологічному, організаційному та поведінковому рівнях; а також обґрунтування системного підходу до запобігання цим атакам з урахуванням ключової ролі людського фактора.

Результати дослідження. Для ефективної протидії соціально-інженерним атакам не існує єдиного технологічного рішення. Необхідно впроваджувати глибоко ешелонований, системний підхід, що враховує одночасно організаційні, технічні, фізичні та психологічні складові [1]. Оскільки найвразливішою ланкою незмінно залишається людина, ключову роль у цій системі відіграє саме проактивна та безперервна робота з персоналом [2].

Надійним підґрунтям для будь-якого захисту є запровадження чіткої та зрозумілої політики інформаційної безпеки. Це не має бути формальний документ, що "припадає пилом на полиці"; це має бути живий, дієвий інструмент, який активно впроваджується та контролюється. Ця політика формує фундамент корпоративної культури безпеки. Вона починається з чіткої класифікації інформації на публічну, внутрішню та конфіденційну, з деталізованими регламентами роботи для кожного типу даних. Звідси логічно випливає принцип найменших привілеїв - фундаментальне правило, згідно з яким співробітники повинні мати доступ лише до тієї інформації та систем, які критично необхідні для виконання їхніх прямих робочих обов'язків [3].

Для технічного підкріплення цієї політики впроваджується система багаторівневої автентифікації (MFA), яка слугує одним із найефективніших бар'єрів, що ускладнює компрометацію облікового запису, навіть якщо пароль було викрадено. Не менш важливим є наявність чітких інструкцій для випадків виявлення підозрілих дій. Співробітник, який зрозумів, що перейшов за фішинговим посиланням, не повинен боятися повідомити про свою помилку.

Навпаки, культура безпеки має заохочувати негайне інформування відповідних служб, адже це дозволяє миттєво локалізувати загрозу [4].

Однак самі по собі політики не працюють без їх глибокого засвоєння персоналом. Тут на перший план виходить людський фактор та формування культури безпеки. Підготовка користувачів є центральним елементом захисту, і вона має бути регулярною, інтерактивною та адаптованою. Замість нудних лекцій, які довели свою неефективність, слід використовувати сучасні методи: інтерактивні тренінги, рольові моделювання атак та гейміфікацію. Найкращим методом перевірки та закріплення знань є проведення внутрішніх симуляцій атак, наприклад, контрольованих "псевдофішингових" розсилок. Це, по суті, "навчальна тривога", яка дозволяє виявити слабкі місця в підготовці персоналу та оцінити реальний рівень обізнаності, не створюючи справжньої загрози. Ключовим аспектом такого навчання є психологічна підготовка: співробітники мають не лише впізнавати типові ознаки фішингу (помилки в тексті, дивний відправник), але й розуміти самі маніпулятивні стратегії зловмисників - створення штучного тиску, терміновості, апеляцію до страху, жадібності чи авторитету.

Нарешті, важливо пам'ятати, що соціальна інженерія не обмежується цифровим простором. Класична шпигунська практика доводить, що часто найпростіший спосіб отримати доступ до мережі - це просто увійти до будівлі. Атаки типу "shoulder surfing" (візуальне шпигунство) або проникнення в офіс під виглядом кур'єра, техніка чи навіть нового співробітника є класичними прикладами фізичної соціальної інженерії. Тому модель захисту має включати й фізичний рівень. Це передбачає надійний контроль доступу, наприклад, через біометричний захист або системи карткового доступу (див. рис. 1).

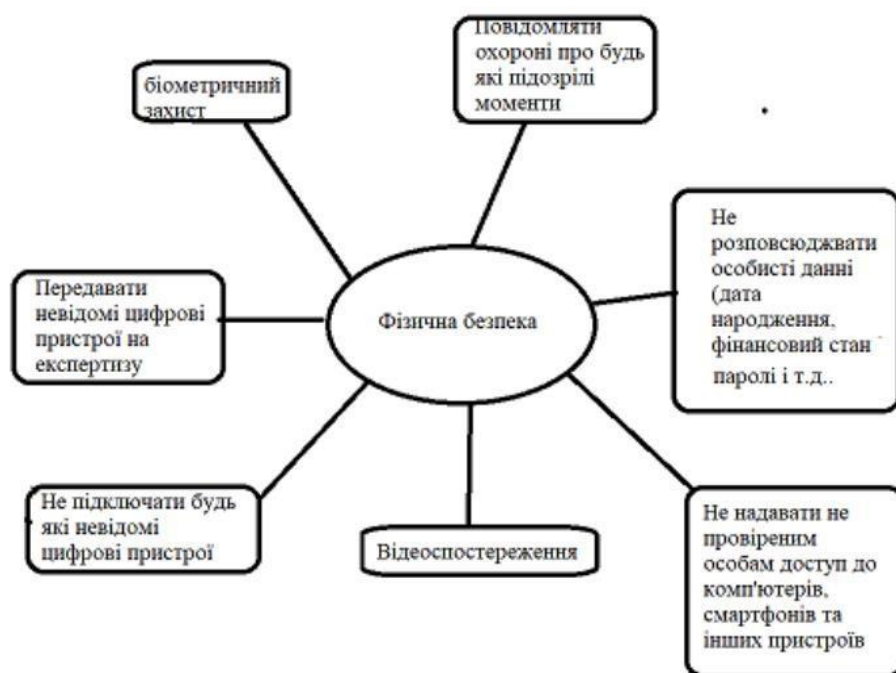


Рис.1 . Методи захисту від фізичних атак соціальної інженерії.

Не менш важливою є політика "чистого столу", яка забороняє залишати на видному місці конфіденційні документи чи паролі, а також вимагає не надавати неперевіреною особам доступ до комп'ютерів та інших пристроїв і блокувати робочу станцію під час відсутності. Співробітники мають бути проінструктовані не розголошувати особисті чи корпоративні дані (паролі, фінансовий стан) у публічних місцях або невідомим особам по телефону. Особливу увагу слід приділити захисту від "наживки": співробітники повинні знати, що категорично заборонено підключати будь-які невідомі цифрові пристрої (як-от знайдені флешки) до робочої техніки. Натомість такі пристрої слід негайно передавати на експертизу службі безпеки. Ефективність цих заходів підтримується технічними засобами, як-от відеоспостереженням, та організаційними правилами, що вимагають від персоналу повідомляти охороні про будь-які підозрілі моменти чи невідомих осіб у приміщенні.

Висновки та перспективи. Соціальна інженерія залишається одним із найбільш небезпечних інструментів зловмисників, оскільки спрямована на маніпуляцію людиною, а не на обхід технічних засобів захисту. Успішність атак обумовлена недостатньою обізнаністю користувачів, слабкими процедурами та відсутністю системної підготовки персоналу.

Комплексний підхід, що об'єднує технічні, організаційні та освітні заходи, є ключовим для протидії соціальній інженерії. Основними факторами захисту є розробка ефективної політики безпеки, постійне навчання працівників, моделювання загроз та впровадження сучасних методів аналізу ризиків.

Перспективою подальших досліджень є поглиблене вивчення аналітичних моделей для виявлення потенційних сценаріїв поширення загроз та розробка навчальних програм, адаптованих до різних категорій персоналу із залученням методів симуляції атак і оцінки поведінкових факторів. Підвищення рівня захищеності можливе лише за умови формування сталої культури інформаційної безпеки, в якій кожен співробітник усвідомлює свою відповідальність.

Список використаних джерел

1. Schneier B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company. 2015.
2. Mitnick K. D., Simon W. L. The Art of Deception: Controlling the Human Element of Security. Wiley. 2002.
3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements. 2022.
4. National Institute of Standards and Technology (NIST). NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program. 2020.

Кочин Владислав Дмитрович
курсант 3 курсу, ННІН№4
Харківський національний університет внутрішніх справ
(095) 693-75-09
vkochin13@gmail.com

СУЧАСНІ СТРАТЕГІЇ КІБЕРЗАХИСТУ В ЕПОХУ ДІДЖИТАЛІЗАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ

Постановка задачі. У період активної діджиталізації інформаційних систем виникає потреба у формуванні нових стратегій кіберзахисту, здатних протистояти зростаючим і більш складним кібератакам. Інтеграція хмарних технологій, IoT-платформ і мобільних сервісів суттєво розширює поверхню можливих атак і ускладнює управління безпекою [1]. У цих умовах постає завдання розробити стратегії кіберзахисту, що поєднують технологічні рішення, організаційні політики та міжнародні стандарти безпеки. Це створює необхідність у побудові адаптивних, багаторівневих та стандартизованих стратегій цифрової безпеки, які відповідають міжнародним вимогам Враховуючи глобальний масштаб цифрової трансформації, актуальною є необхідність перегляду існуючих методів захисту та впровадження інноваційних стратегій, заснованих на інтелектуальному аналізі даних, гнучких моделях доступу та автоматизації.

Мета дослідження. Метою дослідження є аналіз сучасних технологічних та організаційних стратегій кіберзахисту й оцінка їхньої ефективності у цифрових інформаційних системах. Дослідження спрямоване на виявлення перспективних напрямів розвитку безпекових підходів у контексті глобальної діджиталізації.

Результати дослідження. Результати дослідження засвідчують, що сучасні стратегії кіберзахисту базуються на багаторівневій моделі, яка передбачає попередження загроз, їхнє швидке виявлення та оперативне реагування. Однією з ключових тенденцій є впровадження концепції Zero Trust, що виключає припущення про безпечність внутрішнього середовища та забезпечує перевірку кожного доступу незалежно від його джерела [2]. Такий підхід дозволяє мінімізувати ризики компрометації систем навіть у разі успішного проникнення зловмисника у мережу.

Алгоритми машинного навчання стали одним із найпотужніших інструментів виявлення аномалій та ідентифікації складних кібератак. Застосування моделей глибокого навчання у системах моніторингу дає змогу швидше виявляти нові типи загроз, які не зафіксовані у відомих сигнатурах, а також зменшувати кількість хибнопозитивних результатів [3]. Сучасні SIEM- та XDR-рішення інтегрують інтелектуальні алгоритми, що забезпечують автоматизацію аналізу логів та кореляцію подій у реальному часі.

Хмарні технології сьогодні формують важливий компонент стратегій безпеки завдяки можливостям централізованого адміністрування,

масштабованості політик безпеки та використання вбудованих механізмів захисту. Провідні хмарні платформи впроваджують автоматизовані засоби оцінки ризиків, інструменти сегментації мереж та сервіси потокового моніторингу, що значно підвищують ефективність реагування на інциденти у великих цифрових середовищах. Значну важливість набувають також стратегії мережевої сегментації та мікросегментації, що дають можливість ізолювати активи та обмежувати горизонтальне поширення атак. Такий підхід особливо актуальний у середовищах із великою кількістю IoT-пристроїв, де ризик експлуатації недосконалих протоколів чи слабкої автентифікації є високим.

Розвиток стратегій кіберзахисту нерозривно пов'язаний із вдосконаленням криптографічних методів. Постквантова криптографія розглядається як перспективний напрям, здатний забезпечити довготривалий захист інформації у контексті очікуваного розвитку квантових обчислень. Такі алгоритми поступово включаються у стандарти безпеки та відкривають можливості формування майбутніх стійких інфраструктур.

Дослідження підтвердило ефективність блокчейн-технологій у забезпеченні цілісності журналів подій, контролі автентичності цифрових транзакцій та створенні децентралізованих систем перевірки даних [4]. Особливо перспективним є використання блокчейну для захисту критичних інформаційних потоків, де незмінність та простежуваність є ключовими характеристиками.

Водночас технологічні рішення є лише частиною сучасних стратегій. Значення людського фактора залишається критично високим: фішинг та соціальна інженерія продовжують бути найефективнішими методами атак. Саме тому важливою частиною стратегій є програми підвищення цифрової грамотності, навчання персоналу та регулярні симуляції кібератак. Організації, що впроваджують такі програми, демонструють значно вищий рівень стійкості до сучасних загроз.

Результати показують, що комплексна стратегія успішного кіберзахисту поєднує технологічні рішення (AI/ML, Zero Trust, XDR, блокчейн, криптографію), організаційні інструменти (політики безпеки, аудит, оцінку ризиків) та освітні заходи. Найефективнішими є ті системи, які можуть адаптуватися до нових загроз і забезпечують безперервне вдосконалення.

Висновки та перспективи. Сучасні стратегії кіберзахисту в умовах діджиталізації інформаційних систем повинні ґрунтуватися на інноваційних технологіях, інтегрованому підході та постійній адаптації до динамічного середовища загроз. Використання Zero Trust, інтелектуальних алгоритмів аналізу, хмарних рішень, мікросегментації та нових криптографічних моделей значно підвищує рівень безпеки цифрових екосистем. Формування комплексної стратегії, що поєднує технічні й організаційні компоненти, є ключовим чинником забезпечення стійкості цифрових систем у сучасному світі.

Список використаних джерел

1. Publications. ENISA. Home. ENISA. URL: <https://www.enisa.europa.eu/publications> (дата звернення: 27.11.2025).

2. Cybersecurity Framework. NIST. URL: <https://www.nist.gov/cyberframework> (дата звернення: 27.11.2025).
3. ISACA® Resources. ISACA. URL: <https://www.isaca.org/resources> (дата звернення: 27.11.2025).
4. Microsoft Security Team. Microsoft Digital Defense Report 2020: Cyber Threat Sophistication on the Rise. Microsoft. URL: <https://www.microsoft.com/en-us/security/blog/2020/09/29/microsoft-digital-defense-report-2020-cyber-threat-sophistication-rise/> (дата звернення: 27.11.2025).

Крайнюк Олена Володимирівна
к.т.н., доцент
завідувачка кафедри кібербезпеки
Харківського національного автомобільно-дорожнього університету
Cyberbezpeka@ukr.net

КІБЕРСТІЙКІСТЬ ВЕНДИНГОВИХ КОМПЛЕКСІВ ОБЛІКУ ЗАСОБІВ ІНДИВІДУАЛЬНОГО ЗАХИСТУ

Постановка задачі. Питання забезпечення працівників засобами індивідуального захисту (ЗІЗ) є критичним елементом охорони праці. Традиційні методи обліку є неефективними через вплив людського фактора та відсутність оперативного контролю. Перехід до Систем автоматизованої видачі засобів індивідуального захисту (САВ-ЗІЗ) на базі технологій промислового Інтернету речей (ІоТ) вирішує проблеми логістики, проте створює нові ризики [1, 2]. Недостатній рівень кіберзахисту цих пристроїв загрожує цілісності облікових даних, що може призвести до порушення норм безпеки праці. Тому актуальним є завдання моделювання загроз та побудови захищеної архітектури таких систем.

Мета дослідження. Метою роботи є обґрунтування архітектури безпечної системи САВ-ЗІЗ та ідентифікація критичних точок, які потребують посилення кіберзахисту, для забезпечення цілісності та конфіденційності даних за допомогою методології функціонального моделювання IDEF0.

Результати дослідження. Система автоматизованої видачі ЗІЗ розглядається як ІоТ-рішення, що поєднує вендингові автомати (Edge-пристрої), мережеву інфраструктуру та центральну базу даних [3].

Для аналізу процесів розроблено функціональну модель у нотації IDEF0. На рівні декомпозиції виділено чотири ключові блоки: «Ідентифікація та авторизація» (A1), «Видача та фіксація» (A2), «Облік і звітність» (A3) та «Контроль залишків» (A4). Деталізація цих блоків дозволила виявити специфічні вразливості на кожному етапі (рис. 1).

Основними загрозами визначено:

- на етапі ідентифікації: клонування RFID/NFC-пропусків та несанкціонований доступ;
- на етапі обліку: маніпуляція даними про ліміти та редагування історії транзакцій у базі даних;
- на мережевому рівні: перехоплення даних (Man-in-the-Middle) та DDoS-атаки, що порушують доступність сервісу.

Запропоновано мультишарову систему кіберзахисту, яка включає фізичний захист пристрою, багатофакторну автентифікацію (RFID + PIN/біометрія), шифрування каналів зв'язку (SSL/TLS) та впровадження незмінного логу операцій (на базі блокчейну або хешування записів). Особливу увагу приділено інтеграції системи моніторингу інцидентів із процесами служби охорони праці, що дозволяє розглядати кіберінциденти як порушення техніки безпеки.

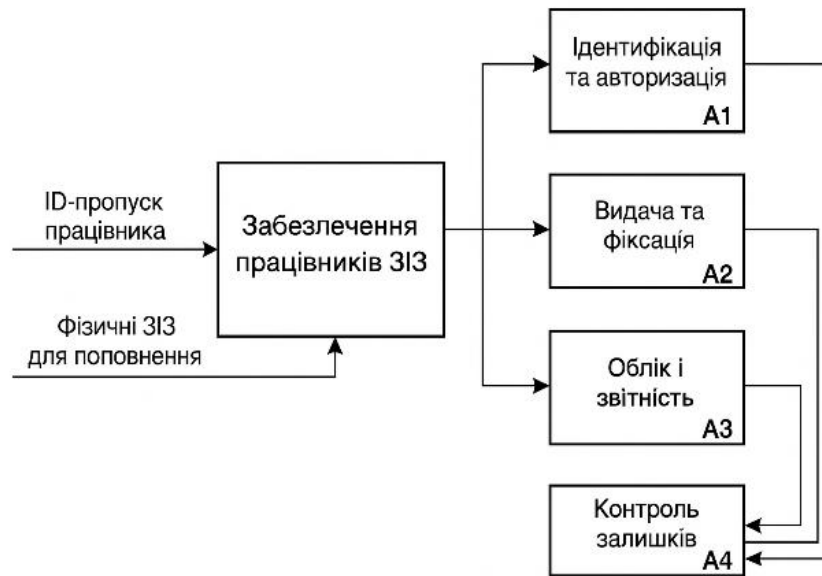


Рис. 1. Контекстна діаграма IDEF0 системи автоматизованої видачі засобів індивідуального захисту (CAB-ЗІЗ).

Висновки та перспективи. У дослідженні доведено, що кібербезпека в ПоТ-системах обліку ЗІЗ є фундаментальною умовою дотримання норм охорони праці. Розроблена модель дозволяє чітко визначити вектори атак та необхідні контрзаходи. Перспективою подальших досліджень є розробка спеціалізованого криптографічного протоколу для захисту низькорівневого обміну даними між вендинговим автоматом та сервером обліку.

Список використаних джерел

1. Крайнюк О. В., Буц Ю. В., Барбашин В. В., Яцюк М. В. Використання штучного інтелекту для управління безпекою праці. *Комунальне господарство міст*. Науково-технічний збірник. Серія: Технічні науки та архітектура. 2023. Т. 6, вип. 180. С. 207–214. DOI:10.33042/2522-1809-2023-6-180-207-213
2. Крайнюк О., Буц Ю., Барбашин В., Козодой Д., Козодой О. Інтелектуальні системи управління безпекою праці на основі штучного інтелекту: перспективи інтеграції в українське законодавство. *Комунальне господарство міст*. 2024. № 6 (187). С. 242–251. DOI:10.33042/2522-1809-2024-6-187-242-251
3. Krainiuk O.V., Buts Y.V., Bogatov O.I., Lotsman P.I., Barbashin V.V. Management of personal protective equipment using vending machines. The 9th International scientific and practical conference “*Study of world opinion regarding the development of science*”. Prague, Czech Republic. 2022. P. 672–678. DOI: 10.46299/ISG.2022.2.9

Нікітін Антон Миколайович
аспірант 1 курсу, групи АІКБ-11
Державний університет інформаційно-комунікаційних технологій
(099) 068-40-44
e-mail: a.nikitin@duikt.edu.ua
Коровайченко Юрій Юрійович
аспірант 3 курсу, групи АІКБ-31
Державний університет інформаційно-комунікаційних технологій
(098) 382-83-45
e-mail: y.korovaichenko@duikt.edu.ua

МЕТОДИ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ЗАГРОЗ НА ОСНОВІ МАШИННОГО НАВЧАННЯ ТА ШТУЧНОГО ІНТЕЛЕКТУ

Постановка задачі. Цифрова трансформація та масове впровадження хмарних сервісів, 5G, IoT і промислових мереж призводять до різкого зростання обсягів мережевого трафіку та ускладнення кіберзагроз. Традиційні системи виявлення вторгнень (IDS/IPS), що базуються на сигнатурах та правилах, демонструють обмежену ефективність проти невідомих атак, багатовекторних АРТ-кампаній, повільних (low and slow) та шифрованих атак [1]. Це актуалізує потребу в методах, які здатні автоматично аналізувати великі масиви даних, виявляти нетривіальні закономірності у мережевому трафіку та зменшувати навантаження на аналітиків центрів моніторингу безпеки.

Мета дослідження. Метою роботи є узагальнений аналіз сучасних підходів до виявлення мережевих загроз на основі машинного навчання та штучного інтелекту, а також формування концепції гібридної системи, орієнтованої на використання статистики мережевих потоків і інтеграцію з платформами моніторингу кібербезпеки.

Результати дослідження. За результатами аналізу виділено три ключові групи методів.

Класичні методи машинного навчання (Random Forest, метод опорних векторів, k-найближчих сусідів, логістична регресія тощо) широко застосовуються для класифікації мережевих потоків як легітимних або шкідливих. За умови ретельного відбору інформативних ознак та використання методів балансування класів можливо досягти високих значень точності та повноти на еталонних наборах UNSW-NB15 та CICIDS2017 [2; 3].

Методи глибокого навчання (згорткові, рекурентні нейронні мережі, автоенкодера, графові мережі) дають змогу без участі експерта будувати узагальнені представлення мережевого трафіку. Дані методи враховують часові та структурні залежності, однак потребують значних обчислювальних ресурсів, великих обсягів маркованих даних і супроводжуються проблемами інтерпретованості рішень [1; 4].

Орієнтовані на аномалії методи та гібридні методи, де, в першому випадку, моделі (unsupervised, semi-supervised) навчаються на «нормалізованих» даних і використовують міру відхилення як індикатор потенційної атаки. Характерним прикладом є система Kitsune, що реалізує ансамбль автоенкодерів для онлайн-оброблення статистики мережевих потоків на ресурсно обмежених вузлах [5]. Гібридні рішення поєднують сигнатурні, аномалійні та класифікаційні методи і інтегрують механізми пояснюваного ШІ (XAI) зменшує кількість хибнопозитивних спрацювань [1; 4].

У більшості досліджень моделі навчалися та тестувалися на відкритих, еталонних наборах даних UNSW-NB15 та CICIDS2017 [2; 3]. Їх перевагою є структурована статистика мережевих потоків і наявність різноманітних типів атак, що забезпечує порівнюваність результатів. Недоліки полягають у дисбалансі класів, частковій штучності згенерованих атак і відмінності від реальних профілів трафіку окремих організацій. Це створює розрив між лабораторними показниками якості моделей та їхньою ефективністю у промислових умовах.

На основі вище описаної інформації, можна зробити висновок, що потенційне поєднання описаних методів в єдину гібридну систему здатне привести до покращення виявлення мережевих атак та допомагає сформулювати такі вимоги до концептуальної системи: підтримка багатоджерельного збору статистики мережевих потоків та журнальних подій; наявність модуля попередньої обробки (нормалізація, агрегування потоків, усунення пропусків, зменшення розмірності); використання комбінації моделей виявлення аномалій та класифікації для виявлення як нових, так і відомих атак; інтеграція засобів XAI (SHAP, LIME) для пояснення впливу ознак; механізми онлайн-перенавчання для боротьби з концептуальним дрейфом; можливість інтеграції з SIEM/SOAR для автоматизації реагування.

Виходячи з описаних вимог, гібридна система виявлення мережевих атак на основі ШІ та ML включає: модуль збору та агрегації статистики мережевих потоків і журнальних подій з мережевих пристроїв та інших мережевих засобів захисту; модуль побудови ознак, який формує статистичні, часові та контентні параметри (інтенсивність з'єднань, ентропія портів, частка невдалих сесій тощо); модуль виявлення аномалій на основі автоенкодерів, налаштованих на нормалізований трафік; модуль класифікації атак, побудований на моделях машинного навчання, натренованих на вибірках з UNSW-NB15, CICIDS2017 та локальних даних; модуль кореляції та пріоритизації сповіщень з урахуванням критичності активів; інтерфейс аналітики з підтримкою XAI для аналізу рішень моделі та позначення хибних спрацювань.

Для задач виявлення мережевих загроз недостатньо використовувати лише загальну точність. Ключовими є повнота (recall) для шкідливого класу, точність (precision), F1-міра, а також площі під кривими ROC-AUC та PR-AUC, що краще відображають роботу моделей у разі дисбалансу класів. Важливими є також затримка оброблення та пропускна спроможність, оскільки практичні системи

мають обслуговувати високошвидкісні канали та великі обсяги мережевого трафіку в режимі, наближеному до реального часу.

Висновки та перспективи. В дослідженні розглянуто методи виявлення мережових загроз на основі машинного навчання та штучного інтелекту, узагальнено їхні сильні сторони та обмеження щодо застосування у системах моніторингу кібербезпеки. Показано, що найбільший практичний потенціал мають гібридні системи, які поєднують сигнатурні й евристичні механізми з аномалійно-орієнтованими та класифікаційними моделями глибокого навчання, доповненими засобами пояснюваного ШІ.

Перспективами подальших досліджень є реалізація прототипу такої системи на реальних даних організації, дослідження стійкості моделей до цілеспрямованих атак на дані та розроблення рекомендацій щодо інтеграції ML/AI-компонентів у наявні рішення SOC/SIEM/SOAR.

Список використаних джерел

1. Hozouri A., Mirzaei A., Effatparvar M. A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges // *Discover Artificial Intelligence*. – 2025. – Vol. 5, No. 1. – DOI: <https://doi.org/10.1007/s44163-025-00578-1>
2. UNSW-NB15 Dataset [Електронний ресурс] // *UNSW Sydney*. – Режим доступу: <https://research.unsw.edu.au/projects/unsw-nb15-dataset> (дата звернення: 30.11.2025).
3. Intrusion detection evaluation dataset (CIC-IDS2017) [Електронний ресурс] // *Canadian Institute for Cybersecurity*. – Режим доступу: <https://www.unb.ca/cic/datasets/ids-2017.html> (дата звернення: 30.11.2025).
4. Mohale V. Z., Obagbuwa I. C. Evaluating machine learning-based intrusion detection systems with explainable AI: enhancing transparency and interpretability // *Frontiers*. – 2025. – Vol. 7, No. 1. – DOI: <https://doi.org/10.3389/fcomp.2025.1520741>
5. Y. Mirsky, T. Doitshman, Y. Elovici, A. Shabtai. Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection // *Network and Distributed System Security Symposium*, м. San Diego, CA. Reston, VA, 2018. – DOI: <https://doi.org/10.14722/ndss.2018.23204>

Поліковський Богдан Володимирович
Магістр групи БІКСм-124-14
Київський столичний університет імені Бориса Грінченка
(068)711-00-54
bvpolikovskiy.fitm24m@kubg.edu.ua

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ БІБЛІОТЕК САНІТИЗАЦІЇ ПРОТИ XSS-АТАК

Постановка задачі. Міжсайтовий скриптинг (Cross-Site Scripting, XSS) залишається однією з найпоширеніших вразливостей веб-застосунків, стабільно присутнюючи в переліку OWASP Top 10 протягом останніх двох десятиліть [1]. Санітизація HTML є одним з ключових превентивних методів захисту, проте відсутність систематичного порівняння ефективності бібліотек санітизації у типових конфігураціях створює проблему обґрунтованого вибору рішень.

Основна проблема полягає в тому, що більшість досліджень фокусуються на оптимальних конфігураціях, не відображаючи реальну ефективність типових налаштувань [2]. Крім того, відсутня об'єктивна методологія багатокритеріального оцінювання, що враховує не лише безпеку, але й продуктивність та споживання ресурсів.

Мета дослідження. Метою є експериментальне порівняння ефективності провідних бібліотек санітизації HTML у типових конфігураціях та розробка практичних рекомендацій щодо їх вибору.

Завдання дослідження: систематизувати теоретичні основи XSS-атак та механізмів захисту; сформувати репрезентативний датасет векторів атак; розробити автоматизований тестовий стенд; провести експериментальне тестування бібліотек; розробити методологію багатокритеріального оцінювання.

Результати дослідження. Після детального аналізу сформовано датасет зі 100 векторів XSS-атак, що охоплює десять категорій: класичні техніки через script теги та обробники подій (26 векторів), SVG-based атаки (10), застарілі HTML теги (8), протокол JavaScript у URL (6), CSS ін'єкції (4), різні форми кодування (8), сучасні браузерні API (18), механізми спостереження DOM (4), JavaScript ES6+ (12), спеціалізовані техніки DOM clobbering (4).

Розроблено автоматизований тестовий стенд на базі Node.js з інтеграцією Puppeteer та виконанням тестів в браузері, забезпечив репрезентативне середовище для оцінювання санітизаційних бібліотек із системою збирання метрик продуктивності.

Експериментальне тестування чотирьох провідних бібліотек виявило: sanitize-html – 98% блокування, інтегральна оцінка 9.26/10; OWASP Java HTML Sanitizer – 98% блокування, оцінка 8.94/10; DOMPurify – 96% блокування, оцінка 8.53/10; js-xss – 95% блокування, оцінка 7.85/10.

Критичним результатом стало виявлення універсальної вразливості всіх чотирьох бібліотек до DOM clobbering атак у типових конфігураціях (100%

вразливі). Вектори з кодуванням URL обійшли захист 75% бібліотек, демонструючи проблему недостатньої канонізації вхідних даних.

Розроблено методологію багатокритеріального оцінювання з ваговими коефіцієнтами: безпека (0.38), продуктивність (0.18), пам'ять (0.18), підтримка (0.11), популярність (0.10), розмір (0.05). Сформульовано рекомендації мітигації для кожної виявленої вразливості.

Висновки та перспективи. Дослідження підтверджує відсутність єдиного ідеального рішення для захисту від XSS-атак. Ефективна стратегія вимагає комбінації п'яти рівнів: санітизації (перевірені бібліотеки), Content Security Policy, Web Application Firewalls, Runtime Application Self-Protection, безпечних практик розробки.

Виявлено критичні прогалини типових конфігурацій: 100% бібліотек вразливі до DOM clobbering, 75% – до encoded vectors. Це підкреслює необхідність спеціалізованих конфігурацій, налаштованих під специфічні потреби застосунку.

Практична цінність: об'єктивні дані для вибору рішень, конкретні рекомендації налаштування, методологія оцінювання з адаптацією вагових коефіцієнтів.

Перспективою подальших досліджень є розширення датасету мутаційними XSS векторами; порівняння оптимізованих конфігурацій; дослідження синергетичних ефектів defense-in-depth; розробка robust ML моделей проти адверсаріальних атак; методологія вибору вагових коефіцієнтів для різних профілів застосунків. Особливо ефективними є комбіновані підходи, які поєднують синтаксичний аналіз HTML структури з класифікацією на основі машинного навчання, досягають точності виявлення понад 98% при збереженні низького рівня хибних спрацьовувань [3].

Список використаних джерел

1. OWASP Top Ten Web Application Security Risks. [Електронний ресурс] // OWASP Foundation. – Режим доступу: <https://owasp.org/www-project-top-ten/> (дата звернення: 16.11.2025)
2. Wang, T., Zhao, D., & Qi, J. (2022). Research on Cross-site Scripting Vulnerability of XSS Based on International Student Website. *International Conference on Computer Network, Electronic and Automation (ICCNEA)*. 2022. (pp. 154–158).
3. Chen H.-C., Nshimiyimana A., Damarjati C., Chang P.-H. Detection and prevention of cross-site scripting attack with combined approaches. *Proceedings IEEE ICEIC*. 2021. P. 1-4.

Рейнська Вікторія Борисівна
к.е.н., доцент кафедри обчислювальної техніки
Національний університет водного господарства та природокористування,
м.Рівне.
(097) 994 80 25
v.b.reinska@nuwm.edu.ua

ВИКЛИК СУЧАСНИМ ЗАГРОЗАМ В ІНФОРМАЦІЙНОМУ БІЗНЕСІ В УКРАЇНІ: ТЕХНІЧНІ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ ПРОТИДІЇ

Постановка задачі. Сучасний розвиток суспільства та економіки України характеризується високим темпом діджиталізації, що виводить інформаційний бізнес на провідні позиції у формуванні цифрової економіки та сприяє глобальній інтеграції держави до єдиного інформаційного простору. Поширення електронної комерції, активний розвиток фінансових технологій, цифрової логістики, а також експансія освітніх онлайн-платформ і стартап-екосистеми створюють значні нові можливості для українських компаній. Водночас, ця динамічна залежність від цифрових технологій призводить до суттєвого підвищення рівня вразливості бізнесу до складних і багаторівневих кіберзагроз [1]. Стрімке зростання кількості кіберінцидентів, постійне ускладнення методів атак, включення зловмисниками технологій штучного інтелекту, а також розвиток технологій Інтернету речей (IoT) та 5G вимагають від вітчизняних підприємств фундаментального перегляду підходів до кіберзахисту. Для українського інформаційного бізнесу у 2025 році характерними є не лише традиційні операційні ризики, такі як витік конфіденційних даних, але й нові, критично посилені виклики, пов'язані з геополітичною нестабільністю, гібридними війнами та активним інформаційним протистоянням на міжнародній арені. У зв'язку з цим виникає нагальна потреба у розробці та теоретичному обґрунтуванні комплексних стратегій протидії, які повинні включати як передові технічні системи, так і стійкі організаційні та правові механізми.

Мета дослідження. Метою є комплексне дослідження сучасних викликів кібербезпеки для інформаційного бізнесу України, проведення систематичного аналізу домінуючих тенденцій та особливостей розвитку загроз, а також наукове обґрунтування стратегічних напрямів протидії їм, що реалізуються на технічному, організаційному та нормативно-правовому рівнях. Для досягнення цієї глобальної мети було сформульовано низку взаємопов'язаних завдань. По-перше, необхідно провести глибокий аналіз найбільш актуальних та поширених векторів кібератак, що визначають операційний ризик для українського інформаційного бізнесу в поточному періоді. По-друге, слід детально систематизувати та критично оцінити використання в українській практиці передових технічних систем захисту, таких як SIEM-рішення, архітектура Zero Trust та сучасні криптографічні інструменти. По-третє, необхідно визначити та теоретично обґрунтувати критичну роль людського фактора та культури кібергігієни як ключового, часто найбільш вразливого, елемента у загальній

архітектурі кіберстійкості компаній [5]. Нарешті, на основі отриманих результатів, необхідно сформулювати ключові стратегічні напрями для подальшого розвитку системи кіберзахисту на національному рівні, включаючи превентивні механізми та вдосконалення нормативно-правового регулювання.

Результати дослідження. Проведений аналіз підтверджує, що в умовах прискореної інформатизації кібербезпека набуває статусу критичної функції управління, оскільки бізнес-моделі мають високу залежність від безперебійного функціонування цифрових технологій. Згідно з аналітичними даними міжнародних консалтингових компаній, у 2025 році кіберінциденти залишаються найбільш значною загрозою для підприємств у всьому світі, причому для України цей фактор посилюється через війну та активне використання кібератак як елементу гібридної агресії [2, 3].

Особливе занепокоєння викликає низка домінуючих загроз. Це, зокрема, фішинг та соціальна інженерія, які ефективно використовують людський фактор для компрометації систем, атаки типу ransomware, що призводять до блокування критичної діяльності компанії з вимогою викупу, а також витоки персональних даних та комерційної таємниці внаслідок цілеспрямованого зламу баз. Також значну небезпеку становлять DDoS-атаки, спрямовані на виведення з ладу інтернет-сервісів, та маніпуляції з інформаційними потоками, що є частиною інформаційних війн. Варто відзначити, що малі та середні підприємства залишаються особливо вразливими, оскільки їхні системи захисту, часто обмежені базовими інструментами, є недостатніми для протидії складним атакам. Дослідження Європейської бізнес асоціації свідчить про те, що понад 70% українських компаній у 2025 році відзначили різке зростання кількості інцидентів, а загальний рівень кіберстійкості оцінюється лише як «середній» [4].

Для протистояння цим динамічним загрозам українські компанії все активніше впроваджують багаторівневі системи захисту, які передбачають інтеграцію різних інструментів. По-перше, застосовуються системи моніторингу та реагування класу SIEM, що дозволяють збирати, аналізувати та корелювати журнали подій у реальному часі для виявлення аномалій. Використання технологій машинного навчання у цих рішеннях сприяє проактивному виявленню потенційних атак [1, 3]. По-друге, концепція Zero Trust Architecture (ZTA), яка ґрунтується на принципі постійної перевірки кожного користувача та пристрою незалежно від їхнього місця розташування, поступово стає галузевим стандартом. ZTA є особливо актуальною для захисту в умовах віддаленої роботи та хмарних середовищ, що є поширеним явищем серед українських ІТ-компаній [2]. По-третє, значного поширення набувають криптографічні інструменти, включаючи шифрування даних «на льоту» та застосування біометричних систем автентифікації. У банківському секторі впроваджено комплексні системи моніторингу транзакцій, які використовують алгоритми ШІ для блокування шахрайських операцій у реальному часі [1, 4]. По-четверте, у відповідь на загрози розвивається сфера кіберкриміналістики та реагування на інциденти (CSIRT), а Україна впроваджує міжнародний досвід у створенні аналітичних центрів, здатних швидко координувати дії держави та бізнесу [1].

Організаційний досвід українських компаній підтверджує, що значна частина інцидентів відбувається через необережність співробітників (слабкі паролі, відкриття шкідливих вкладень). Це підкреслює критичну важливість формування культури кібергігієни. Провідні українські ІТ-компанії впроваджують регулярні тренінги, симуляції фішингових атак та політику «мінімальних привілеїв», надаючи доступ лише в межах необхідності [5]. Формування культури безпеки є особливо важливим для стартап-екосистеми, де динамічність роботи часто перешкоджає налагодженню внутрішніх процесів безпеки. Аналізуючи сучасний стан, можна визначити ключові напрями протидії: превентивна кібербезпека через поведінковий аналіз та прогнозування загроз, автоматизація реагування за допомогою ШІ, розвиток нормативно-правової бази шляхом узгодження українських стандартів із міжнародними практиками (ISO/IEC 27001, NIST CSF), публічно-приватне партнерство для обміну інформацією про загрози, а також забезпечення кіберетики та цифрових прав, що є невід'ємною складовою української кіберполітики [6, 7].

Висновки. Сучасний український інформаційний бізнес зіштовхується з безпрецедентним рівнем кіберзагроз, які мають глибокий комплексний характер, поєднуючи технологічні, організаційні та соціальні аспекти. Успішна та ефективна протидія цим викликам можлива лише за умови системного впровадження багаторівневих технічних систем захисту, активного розвитку культури кібергігієни серед персоналу, невідкладної інтеграції штучного інтелекту у процеси моніторингу та безпеки, а також посиленої співпраці між державним і приватним секторами. Таким чином, виклики кібербезпеки для українського інформаційного бізнесу у 2025 році виступають не лише значною загрозою, але й потужним стимулом до інноваційного розвитку, який формує передумови для створення стійкої цифрової економіки, здатної ефективно конкурувати на глобальному ринку.

Список використаних джерел

1. Колб С. О., Пирога М. І. Інформаційна безпека: нові виклики та стратегії захисту. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Вип. 90, ч. 5. С. 437–441. DOI: 10.24144/2307-3322.2025.90.5.58.
2. Конференція: «Актуальні проблеми кібербезпеки», Секція «Виклик сучасним загрозам». *Виклик сучасним загрозам в інформаційному бізнесі*. Тези. 2025.
3. *Cyber incidents remain top business risk concern globally 2025*. 10Guards. 2025. URL: <https://10guards.com/ua/blog/2025/02/13/cyber-incidents-remain-top-business-risk-concern-globally-2025> (дата звернення: 27.09.2025).
4. *Cyber Resilience 2025: підсумки національного дослідження*. European Business Association. 2025. URL: <https://eba.com.ua/cyber-resilience-2025-pidsumky-natsionalnogo-doslidzhennya-roliv-v-doskonalennya-rivnya-kiberstijnosti-kompaniyi-v-zabezpechenni-stijnosti-biznesu-v-ukrayini> (дата звернення: 27.09.2025).

5. *ТОП-7 кіберзагроз для бізнесу у 2025 році.* SGS4Business. 2025. URL: <https://sgs4business.com/news/top-7-kiberzagroz-dla-biznesu-v-2025-roci.html> (дата звернення: 27.09.2025).
6. *Українське IT у 2025 році: адаптація, нові виклики та напрямки росту.* Kyivstar Hub. 2025. URL: <https://hub.kyivstar.ua/articles/ukrayinske-it-u-2025-rocz-i-adaptacziya-novi-vikliki-ta-napryamki-dlya-rostu> (дата звернення: 27.09.2025).
7. *Інформаційна війна: що чекає нас у 2025 році.* Detector Media. 2024. URL: <https://detector.media/infospace/article/236387/2024-12-26-informatsiyna-viyna-shcho-chekaie-nas-u-2025-rotsi> (дата звернення: 27.09.2025).

Рисований Олександр Миколайович
проф. кафедри «Комп'ютерна інженерія та програмування»
Національний технічний університет «Харківський політехнічний інститут»
(097) 024-56-37
rysov81524@gmail.com

ДОСЛІДЖЕННЯ СПОСОБІВ ІН'ЄКЦІЇ В ЗАГОЛОВКИ PE-ФАЙЛА

Постановка задачі. У сучасних умовах з'явилася можливість широко використовувати штучний інтелект створення витончених вірусних програм. Способи впровадження вірусів у код програми стали складнішими. Віруси або їхня основна частина впроваджуються в такі області програми, які не видно користувачам без спеціальних утиліт або зовнішніх засобів. Найчастіше такими областями є заголовки PE-формату. Сучасна ОС Windows 11 характеризується підвищеною захищеністю проти активного використання чужого коду. Найпростіше ховати код вірусу в секцію коду або у велику кількість різних секцій даних [1]. Але таке використання легко виявляється при відкритті коду у налагоджувачі. Для архітектури x64 таким налагоджувачем є x64Dbg [2]. Однак найцікавішим способом впровадження чужого коду є впровадження в заголовки PE-формату, які не видно у налагоджувачі. Ці зміни можна виявити лише в комірках заголовків за допомогою 16-річних редакторів коду (hex-редакторів).

Тому актуальним залишається дослідження заголовків PE-формату в ОС Windows 11. Такі дослідження необхідні насамперед антивірусним програмістам для протидії таким застосуванням.

Мета дослідження. Метою дослідження є пошук комірок, які в заголовках не можна змінювати та пошук комірок, які можуть бути змінені без створення проблем із запуском такого exe-файлу.

Результати дослідження.

PE-формат файлу – це формат файлу Windows (Portable Executable - PE). На початку кожного exe-файлу знаходиться службова інформація, що складається із заголовків [3]. Після заголовків розташовуються секції. Розмір заголовків для архітектури мікропроцесора x64 дорівнює 1024 байт. Кожен тип секцій має розмір щонайменше 512 байт і збільшується за необхідності на це число.

Завжди є інтерес використовувати службову частину файлу для своїх потреб – як правило, для приховання інформації.

Використовувати службові поля можна як за ручним способом (з використанням зовнішніх програмних засобів), так і за програмно.

PE-формат створюється при компіляції програми і є структурами даних, які містять всю інформацію, необхідну PE-завантажувачу для відображення файлу в пам'ять. Формат PE-файлу (Portable Executable) складається з DOS-заголовка, заглушки DOS stub, заголовка PE-файлу (PE Header), опціонального заголовка PE-файлу, що описує структуру файлу, і секції (Sections), які містять дані та код програми, такі як .text для коду та .data.

При дослідженні DOS-заголовка з'ясовано, що записувати в DOS заголовок ехе-файла можна, але тільки не в комірку, де зберігається MZ-сигнатура та в комірку з адресою 3Ch, в якій знаходиться адреса розташування PE-заголовка.

При дослідженні заглушки DOS stab з'ясовано, що всі осередки цієї області можна замінити і такий ехе-файл запускається без проблем.

У Windows 10/11 є комплекс заходів для захисту PE-заголовка, коли заголовки PE-файлів у пам'яті виконуються лише під час читання. Записати та зберігати дані в PE-заголовку та розраховувати, що програма потім їх запустить у завантаженої пам'яті – не вийде. Писати в PE-заголовок без зміни контрольної суми можна, але запустити такий файл вже не можна. Операційна система блокує запуск програм із зміненим PE-заголовком. У цьому випадку захист PE-файлів досягається за рахунок комплексних заходів, таких як шифрування виконуваного коду для запобігання антивірусному скануванню та аналізу, а також використання контрольної суми для підтвердження цілісності та справжності файлу. Але значення комірок можна зчитувати та використовувати, наприклад, як пароль для допуску до програмного продукту.

Видається можливим після ін'єкції в PE-формат перерахувати контрольну суму і змінити її значення на нове.

Висновки та перспективи. У дослідженні наведено програми в середовищі masm64 для аналізу та зміни всіх заголовків PE-файлу. Показано шляхи впровадження в ці заголовки.

Перспективою подальших досліджень є розрахунок нової контрольної суми файлу та її впровадження в PE-заголовок, а також зміна атрибутів цього заголовка.

Список використаних джерел

1. Методичні вказівки щодо виконання практичних та лабораторних робіт з курсу «Реверсне програмування. Антиналагоджувальні прийоми захисту від реверсу. Середовище програмування masm64: для студентів спеціальності 123 - «Комп'ютерна інженерія» всіх форм навчання [електронне видання] / укладач О.М.Рисований – Х.: НТУ «ХПІ», 2024 — 132 с. <https://repository.kpi.kharkov.ua/handle/KhPI-Press/75508>.

2. Реверсне програмування. Захист коду. Середовище програмування masm64: навчально-методичний посібник для студентів спеціальності 123 "Комп'ютерна інженерія" всіх форм навчання [електронне видання] / О.М. Рисований. – Харків : НТУ «ХПІ», 2024. – 214 с. <https://repository.kpi.kharkov.ua/handle/KhPI-Press/79627>.

3. Реверсне програмування. Впровадження коду. Середовище програмування masm64: навчальний посібник для студентів спеціальностей 123 "Комп'ютерна інженерія", 125 "Кібербезпека" / О.М. Рисований. – Харків: «Слово», 2021. – 250 с. <https://repository.kpi.kharkov.ua/handle/KhPI-Press/70274>.

Рихлик Андрій Сергійович
студент 4 курсу, групи ПЗ-4
Національний транспортний університет України «Національний Транспортний
Університет»
(073) 079-13-20
10812184@gsuite.uit.edu.ua
Поперешняк Світлана Володимирівна
к.ф.-м.н., доцент, доцент кафедри технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій
spopereshnyak@gmail.com

СУЧАСНІ ПІДХОДИ ТА ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ЕВОЛЮЦІЇ ЦИФРОВИХ ЗАГРОЗ

Постановка задачі. Сучасні цифрові системи функціонують у середовищі, що характеризується високою динамічністю та різноманітністю кіберзагроз. Поширення хмарних технологій, мобільних платформ, сервісів електронної комерції та засобів штучного інтелекту створює нові виклики для захисту інформації. Постає задача комплексного аналізу існуючих загроз, методів їхнього виявлення та механізмів протидії, а також визначення ролі технологічних і правових засобів у створенні ефективної системи кіберзахисту.

Мета дослідження. Метою роботи є комплексне дослідження сучасних підходів до забезпечення кібербезпеки, аналіз технологічних, організаційних та правових аспектів захисту інформації, а також оцінка впливу інтелектуальних систем на підвищення ефективності протидії сучасним кіберзагрозам.

Результати дослідження. У процесі проведеного дослідження було системно проаналізовано сучасний стан, ключові виклики та тенденції розвитку кібербезпеки в умовах інтенсивної цифровізації суспільства. Отримані результати дозволяють комплексно оцінити ефективність існуючих механізмів захисту та окреслити напрями подальшого вдосконалення технологій протидії кіберзагрозам.

Передусім встановлено, що динаміка розвитку цифрових технологій безпосередньо корелює зі зростанням спектра загроз інформаційній безпеці. Поширення хмарних сервісів, мобільних платформ, розподілених систем зберігання даних, інтернету речей та штучного інтелекту створює нові вектори атак, які характеризуються високою варіативністю, складністю та здатністю до швидкої адаптації. Виявлено, що сучасні кіберзагрози набувають комплексного характеру, поєднуючи технічні, соціальні та психологічні компоненти, що суттєво ускладнює процес їхнього виявлення та нейтралізації традиційними засобами.

Одним із ключових результатів дослідження є систематизація методів та інструментів забезпечення кібербезпеки. Проаналізовано ефективність криптографічних засобів захисту, зокрема алгоритмів шифрування та електронного підпису, які забезпечують конфіденційність і автентичність

інформації. Показано, що у сучасних умовах криптографія має розглядатися як базис усієї системи безпеки, на який спираються інші інфраструктурні механізми захисту.

Важливим експериментальним результатом є оцінка ролі організаційно-адміністративних заходів, зокрема управління доступом, розмежування прав користувачів, політик безпечного паролювання, а також процесів резервного копіювання та сегментації мереж. Доведено, що взаємодія технічних і організаційних механізмів значно підвищує загальну стійкість цифрової інфраструктури до атак.

Особлива увага приділена дослідженню застосування технологій штучного інтелекту в кібербезпеці. Показано, що інтелектуальні системи моніторингу, основані на методах машинного навчання та поведінкової аналітики, здатні виявляти аномальні дії у реальному часі та прогнозувати можливі кібератаки на ранніх стадіях. Результати аналізу демонструють, що інтеграція систем штучного інтелекту дозволяє значно знизити ризики, пов'язані з новими формами кіберзлочинності, які швидко трансформуються та вимагають адаптивних підходів.

Дослідження також підтвердило ключову роль нормативно-правового регулювання у створенні ефективного середовища кіберзахисту. Порівняльний аналіз національних нормативних актів та міжнародних стандартів, насамперед ISO/IEC 27001, засвідчив важливість формування системи управління інформаційною безпекою, що охоплює політики, процедури, засоби контролю та механізми постійного вдосконалення.

Узагальнені результати показують, що кібербезпека має розглядатися як багатовимірна система, у якій технічні, організаційні та правові компоненти взаємодіють у єдиному комплексі. Встановлено, що підвищення стійкості та ефективності систем кіберзахисту можливе лише за умови впровадження комбінованих підходів, постійного оновлення інструментів, розвитку цифрової компетентності користувачів та адаптації до світових стандартів.

Висновки та перспективи. Кібербезпека є стратегічним елементом функціонування цифрової економіки та державного управління. Забезпечення належного рівня захисту інформації потребує комплексного підходу, що включає сучасні технологічні рішення, підвищення цифрової культури користувачів, регулярне оновлення систем безпеки, розвиток інтелектуальних методів захисту та дотримання міжнародних стандартів.

Перспективними напрями подальших досліджень є:

- удосконалення моделей прогнозування кіберзагроз на основі штучного інтелекту;
- розвиток автоматизованих систем реагування на інциденти;
- інтеграція концепцій Zero Trust Architecture у корпоративні системи;
- підвищення стійкості критичної інфраструктури до кібератак;
- гармонізація українського законодавства з європейськими стандартами.

Список використаних джерел

1. Герасименко В. М. Інформаційна безпека: навчальний посібник. Київ: КНЕУ, 2021.
2. ISO/IEC 27001:2022. Information Security Management Systems – Requirements. International Organization for Standardization, 2022.
3. Stallings W. Network Security Essentials. Pearson Education, 2020.
4. Бойко С. Кібербезпека та сучасні загрози цифрового середовища // Інформаційні технології та суспільство. 2023. №1. С. 45–51.

Романюк Олександр Никифорович

д.т.н., проф.

Вінницький національний технічний університет

rom8591@gmail.com

Майданюк Володимир Павлович

к.т.н., доцент

Вінницький національний технічний університет

maidaniuk2000@gmail.com

Нечипорук Микола Леонідович

аспірант

Вінницький національний технічний університет

mykola.nec@gmail.com

КОДУВАННЯ ГРАФІЧНОЇ ІНФОРМАЦІЇ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

Постановка задачі.

Кодування графічної інформації сьогодні розглядається як один із фундаментальних інструментів забезпечення інформаційної безпеки, оскільки саме візуальні дані становлять значну частку цифрового контенту, який циркулює між користувачами, інформаційними системами, серверами, хмарними платформами та мережевими сховищами. Обсяг зображень і відео стрімко зростає, а разом із ним - ризики несанкціонованого доступу, перехоплення та маніпулятивної обробки. Особливість графічної інформації полягає в тому, що вона має фізичну двовимірну структуру, високу корельованість пікселів та великі обсяги даних, тому класичні криптографічні алгоритми не завжди демонструють достатню ефективність або швидкодію. Це призвело до необхідності розробки спеціалізованих методів кодування, що враховують унікальні характеристики зображень та здатні забезпечити їх конфіденційність і цілісність навіть у нестабільних мережах [1].

Мета дослідження. Мета дослідження - проаналізувати сучасні методи кодування графічної інформації, спрямовані на підвищення рівня захисту даних, визначити їх ефективність, стійкість до криптоаналітичних атак і можливості практичного застосування в системах інформаційної безпеки.

Результати дослідження.

Одним із базових механізмів захисту є перестановка пікселів - первинна операція, яка дозволяє змінити їх розташування за певним законом. Для генерації такої послідовності зазвичай використовують псевдовипадкові функції або хаотичні моделі. Хоча перестановка сама по собі не руйнує амплітудну структуру зображення, вона суттєво ускладнює можливість провести зворотний аналіз без ключа. Проте у багатьох випадках статистичні характеристики зображення залишаються подібними, тому пермутаційні схеми майже завжди комбінують із методами субституції: побітовими операціями XOR, нелінійними інтенсивнісними модифікаціями або трансформаціями над блоками. У підсумку

формується комбінований шифр, у якому перестановка працює як перший рівень маскування, а субституція - як механізм, що розмиває залишкові кореляції й зменшує предиктивність [2].

Велику увагу у наукових дослідженнях приділяють хаотичним алгоритмам шифрування графіки. Хаос має такі властивості, як непередбачуваність, висока чутливість до початкових параметрів і складність відтворення траєкторій, що робить його дуже придатним для криптографії. Використання логістичних карт, систем Хенона або синус-карт дає змогу створити послідовності, які важко відтворити або спрогнозувати без точних параметрів. Ці системи можуть генерувати як ключові потоки, так і маски для інтенсивнісного перетворення пікселів. Хаотичні схеми забезпечують високу ентропію та значний рівень захисту від атак вибраного відкритого тексту, якщо правильно підібрані діапазони параметрів. Проте хаотичні моделі чутливі до обмеженої розрядності машинної арифметики, що іноді призводить до періодичних циклів, тому сучасні реалізації часто комбінують декілька карт для стабілізації хаотичного поведінкового простору [3].

Блокові методи кодування відіграють важливу роль у сферах, де потрібно обробляти великі обсяги графічних даних з мінімальними затримками - у телемедицині, супутникових системах спостереження, потокових сервісах, відеоаналітиці та цифрових архівах. Суть блочного підходу полягає у поділі зображення на окремі сегменти з можливістю незалежного шифрування кожного з них. Одні блоки можуть використовувати складні алгоритми, тоді як інші - пришвидшені, що дозволяє адаптувати шифрування під локальні особливості контенту. Це дає змогу інтегрувати криптографічні операції у компресійні стандарти JPEG, JPEG2000, HEVC, де захист виконується над частотними коефіцієнтами. Подібна інтеграція мінімізує збільшення обсягу даних та знижує навантаження на мережу, що критично для систем із низькою пропускну здатністю.

Ще один напрям - стеганографія, яка використовується не стільки для шифрування, скільки для прихованого вбудовування інформації в зображення. На відміну від традиційного шифрування, у стеганографії сам факт передачі даних маскується. Найпоширенішими є методи зміни найменш значущих бітів, а також модифікація частотних компонентів JPEG. Дослідження останніх років значно розширили ці методи, залучивши глибокі нейронні мережі, зокрема GAN-системи, які формують зображення-носії так, що вони не мають статистичних аномалій, притаманних класичним стеганографічним підходам. У практиці безпеки часто поєднують шифрування та стеганографію: спершу дані шифрують традиційними методами, а потім вбудовують у графічний файл. Така схема створює багаторівневий бар'єр, який значно ускладнює виявлення та інтерпретацію прихованого повідомлення [3].

Суттєве значення для захисту графічної інформації мають апаратні механізми прискорення. Сучасні GPU- та NPU-архітектури дозволяють виконувати складні криптографічні операції у паралельному режимі, досягаючи значної економії часу під час обробки великих масивів даних. Графічні

процесори здатні виконувати тисячі потокових шифрувальних операцій одночасно, що робить їх придатними для захисту потокового відео, інтерактивних мультимедійних систем та систем відеоспостереження в реальному часі. У поєднанні з технологіями на зразок Intel SGX або ARM TrustZone такі рішення забезпечують захищену зону виконання, де ключі та проміжні дані недоступні навіть при компрометації основної операційної системи.

Особливу увагу приділяють захисту графічних біометричних даних, які використовуються у системах ідентифікації та автентифікації: зображень облич, відбитків пальців, райдужної оболонки ока та інших унікальних візуальних маркерів. Зберігання таких даних у незахищеній формі створює високий ризик порушення приватності, тому впроваджується принцип «скасовуваної біометрії» - коли замість оригінального шаблону зберігається криптографічно трансформована версія, що дозволяє проводити відповідність, але не дозволяє відновити вихідне зображення. У разі витоку шаблон можна замінити новим, що відповідає вимогам сучасного законодавства про захист персональних даних, наприклад GDPR .

Висновки та перспективи.. Узагальнюючи, можна стверджувати, що сучасні методи кодування графічної інформації є багаторівневою системою, яка поєднує класичну криптографію, хаотичні моделі, стеганографію, блокові перетворення, апаратні прискорювачі та технології штучного інтелекту. Враховуючи збільшення частки графічних даних у комунікаційних потоках та аналітичних системах, ефективне кодування зображень стає важливим компонентом інформаційної безпеки на рівні держави, підприємств і приватних користувачів. Новітні підходи активно використовують моделі глибокого навчання. Автоенкодери, трансформери та гібридні нейронно-криптографічні моделі дозволяють перетворювати зображення у латентні простори, приховані від прямого сприйняття. Передача такої інформації є безпечною, оскільки лише спеціально навчений декодер здатний відновити вихідні дані. Поєднання нейронних перетворень із криптографічними операціями створює новий клас адаптивних алгоритмів, які здатні підлаштовувати інтенсивність захисту до структури зображення, ускладнюючи реверс-інжиніринг.

Список використаних джерел

1. Zhang Y., Bao L., Li C., Wang X. A novel image encryption scheme using improved chaotic system and dynamic DNA coding. *Information Sciences*. 2023. Vol. 630, P. 300–317.
2. Kaur M., Singh S., Juneja M. An efficient image encryption technique using hybrid chaotic maps and parallel processing. *IEEE Access*. 2022. Vol. 10, P. 124215–124228.
3. Almfadi A., Hussain M., Prasad M. Lightweight chaos-based image encryption for real-time multimedia applications. *Multimedia Tools and Applications*. 2021. Vol. 80, P. 11673–11696.

Самарець Владислав Євгенович
магістр 2 курсу, групи АМСЗІм-24-1
Харківський національний університет радіоелектроніки
(063) 629-88-57
vladyslav.samarets@nure.ua

ВИКЛИКИ ТА ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ЛОКАЛЬНИХ LLM У ЦИФРОВІЙ КРИМІНАЛІСТИЦІ: ПИТАННЯ БЕЗПЕКИ, КОНФІДЕНЦІЙНОСТІ ТА НАДІЙНОСТІ

Постановка задачі. Локальне розгортання великих мовних моделей (large language model, LLM) представляє парадокс безпеки: хоча воно пом'якшує ризики, пов'язані з передачею чутливих даних постачальникам хмарних послуг, одночасно вносить нові вразливості, властиві локальним середовищам. На відміну від хмарних LLM, які централізують засоби безпеки та моніторинг, локальні LLM покладаються на безпекову позицію окремих пристроїв або мереж, яка може бути менш надійною. Децентралізована природа локальних розгортань LLM ускладнює реагування на інциденти та криміналістичні розслідування. Відсутність централізованого логування та моніторингу може ускладнити відстеження несанкціонованого доступу або зловживання моделлю. Ці фактори вимагають розробки спеціалізованих безпекових фреймворків для локальних LLM у криміналістичних застосуваннях, які б враховували специфічні вимоги доказової цілісності та ланцюга зберігання.

Мета дослідження. В дослідженні розглядаються критичні проблеми застосування LLM щодо цифрових криміналістичних розслідувань, розглядаються механізми збереження конфіденційності, включаючи диференціальну конфіденційність, гомоморфне шифрування та безпечні багатосторонні обчислювальні методи, адаптовані для криміналістичних контекстів.

Особлива увага приділяється вимогам прозорості, підзвітності та довіри, необхідним для підтримки цілісності доказів у правових контекстах. Запропоновано майбутні напрямки досліджень для усунення поточних обмежень та підвищення практичної життєздатності цифрової криміналістики на основі LLM.

Результати дослідження. Захист конфіденційності в застосуваннях LLM має критичне значення, особливо при обробці чутливих криміналістичних даних. Сучасні дослідження фокусуються на трьох основних категоріях методів захисту конфіденційності: диференційна приватність, криптографічні протоколи та середовища довіреного виконання. Диференційна приватність забезпечує математичні гарантії захисту індивідуальних записів даних шляхом додавання контрольованого шуму до процесів тренування або інференсу моделі. Підхід Split-and-Denoise демонструє покращення на понад 10% у середньому в продуктивності при однаковому бюджеті приватності порівняно з базовими методами.

Гомоморфне шифрування дозволяє проводити обчислення на зашифрованих даних без необхідності їх розшифрування, забезпечуючи комплексний захист конфіденційності. Дослідження демонструють досягнення значних прискорень обчислень — 6.94x для файн-тюнінгу та 2.3x для інференсу — при збереженні продуктивності, порівнянної з моделями на відкритому тексті.

Систематичний підхід до захисту конфіденційності передбачає впровадження відповідних технік на трьох етапах життєвого циклу LLM: попереднє тренування, файн-тюнінг та інференс. На етапі попереднього тренування використовуються методи санітизації даних та федеративного навчання для мінімізації ризиків витоку чутливої інформації.

Федеративне навчання дозволяє множинним організаціям спільно тренувати моделі без централізації даних, що особливо актуально для криміналістичних застосувань, де різні правоохоронні органи можуть співпрацювати, зберігаючи юрисдикційний контроль над даними. Технологія санітизації знань LLM не лише мінімізує витoki конкретних знань, але й зберігає загальну продуктивність моделей.

LLM можуть галюцинувати факти, неправильно інтерпретувати докази або продукувати неповні чи неперевірювані ланцюги міркувань, що підриває надійність їх виходів. Це явище є особливо критичним у криміналістичному контексті, де помилкові висновки можуть мати серйозні юридичні наслідки. Крім того, LLM часто не мають доменно-специфічних знань, необхідних для точної інтерпретації низькорівневих криміналістичних артефактів, що робить їх схильними до неправильних припущень при роботі з незнайомими структурами даних або виходами інструментів. Забезпечення прозорості у криміналістичних AI-застосуваннях є критично важливим для підтримки довіри в судових процесах.

Для вирішення цих проблем необхідні чіткі керівництва, ретельні процедури валідації та практики прозорого звітування. Центральною точкою критики, яка продовжує сприяти скептицизму, є відсутність прозорості у виходах, згенерованих AI-методами.

Для підтримки довіри та доказової цілісності в юридичних та слідчих контекстах критично важливими є атрибути прозорості, підзвітності та пояснюваності. Проблеми інтерпретованості результатів, можливої упередженості моделей та етичних міркувань щодо автоматизованого прийняття рішень у правовому контексті потребують комплексного вирішення. Безперервне дослідження та розробка просунутих методів оцінки функціонування цих моделей є життєво важливим. Це дозволить покладатися на ці моделі для інформації, яка відображає фактичний зміст, а не припущення, зроблені моделлю. Необхідність стандартизації процедур використання LLM у криміналістиці стає дедалі очевиднішою для забезпечення юридичної прийнятності результатів.

Практична реалізація LLM у цифровій криміналістиці потребує інтеграції з існуючою екосистемою спеціалізованих інструментів. Model Context Protocol представляє перспективний підхід до стандартизації взаємодії між LLM та криміналістичними інструментами, забезпечуючи структурований доступ до даних та результатів аналізу.

Однак забезпечення доступності релевантних криміналістичних даних для LLM у структурованій та придатній для використання формі є само по собі складним завданням. Розробка універсальних інтерфейсів та форматів обміну даними між різними криміналістичними інструментами та LLM залишається важливим напрямком досліджень.

Висновки та перспективи. Прогрес LLM разом із розвитком AI та кібербезпеки готовий революціонізувати виявлення та пом'якшення загроз. Тенденції, що формуються, у LLM-базованій кібербезпеці включають виявлення вторгнень у реальному часі, федеративне навчання, граф-базоване навчання та пояснюваний штучний інтелект. Федеративне навчання відкриває можливості для спільного тренування моделей між різними криміналістичними лабораторіями без компрометації конфіденційності локальних даних. Інтеграція LLM з графовими структурами даних може значно покращити аналіз взаємозв'язків між криміналістичними артефактами та суб'єктами розслідування. Розробка стандартизованих фреймворків для оцінки та сертифікації LLM-базованих криміналістичних інструментів є критично необхідною для їх широкого впровадження. Необхідність нових фреймворків, які інтегрують захист конфіденційності за дизайном у життєвий цикл LLM, стає дедалі актуальнішою.

Багаторівневі стратегії безпеки у плануванні та виконанні LLM-базованих криміналістичних систем мають включати ізоляцію сесій, фільтрацію чутливої інформації на вході та відповідальну фільтрацію відповідей на виході. Це забезпечує дотримання суворих регуляторних вимог при збереженні функціональності системи.

Список використаних джерел

1. Fatma Yasmine Loumachi, Mohamed Chahine Ghanem, Mohamed Amine Ferrag. GenDFIR: Advancing Cyber Incident Timeline Analysis Through Retrieval Augmented Generation and Large Language Models // arXiv. 2024. URL: <https://arxiv.org/abs/2409.02572>.
2. Akila Wickramasekara, Frank Breiteringer, Mark Scanlon. Exploring the Potential of Large Language Models for Improving Digital Forensic Investigation Efficiency // arXiv. 2025. URL: <https://arxiv.org/abs/2402.19366>.
3. Sarim Suleman. 12 Ways to Boost Efficiency with AI in Evidence Management // Digital Evidence. 2024. URL: <https://digitalevidence.ai/blog/ai-digital-evidence-management>.
4. Jeel Piyushkumar Khatiwala, Daniel Kwaku Ntiamoah Addai, Weifeng Xu. Evaluating the Reliability of Digital Forensic Evidence Discovered by LLM // IEEE Xplore. 2025. URL: <https://ieeexplore.ieee.org/document/11126744>.
5. Clinton Joel Walker. Artifact Analysis and Using AI in the Forensics Domain // Louisiana State University Repository. 2025. URL: https://repository.lsu.edu/gradschool_dissertations/6884/.

Сиваченко Ігор Олексійович
аспірант

Інститут програмних систем Національної академії наук України
igor.syvachenko@gmail.com

ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ТА ВАРТОСТІ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ З МЕТОЮ ОПТИМІЗАЦІЇ ЇХ СКЛАДУ В КРИЗОВИХ СИТУАЦІЯХ

Постановка задачі. Сучасні інформаційні системи функціонують у середовищі з високою динамікою ризиків, що посилюються під час кризових ситуацій – воєнних дій, кібератак, відмов інфраструктури, порушення ланцюгів постачання чи обмеження ресурсів. За таких умов організації стикаються з необхідністю одночасно підтримувати прийнятний рівень кіберзахисту та контролювати витрати на засоби безпеки. Традиційні моделі планування заходів інформаційної безпеки часто орієнтовані на стабільне середовище та не враховують різкі зміни бюджету, доступності технічних засобів та пріоритетів бізнес-процесів.

Таким чином, виникає проблема кількісної оцінки ефективності та вартості засобів захисту інформації з метою оптимізації їх складу та конфігурації в умовах кризи, коли необхідно швидко визначити мінімально достатній набір технічних і організаційних заходів.

Мета дослідження. Метою дослідження є розроблення методичних підходів до комплексного оцінювання ефективності, вартості та пріоритетності засобів захисту інформації, що дозволяє:

- оптимізувати набір засобів безпеки відповідно до критичності активів;
- мінімізувати витрати за обмеженого бюджету;
- забезпечити прийнятний рівень кіберстійкості в умовах кризових сценаріїв;
- підтримувати безперервність роботи систем і сервісів.

Результати дослідження. Для обґрунтування оптимального складу засобів захисту інформації (ЗЗІ) у кризових умовах було проведено комплексний аналіз їх ефективності, вартості, а також здатності забезпечувати необхідний рівень інформаційної безпеки за умов обмежених ресурсів. Дослідження передбачало оцінювання ЗЗІ за трьома групами критеріїв:

1. технічна ефективність (рівень покриття загроз, здатність виявляти та блокувати атаки, відмовостійкість);
2. економічні показники (вартість володіння, витрати на впровадження, експлуатацію та оновлення);
3. інтеграційні властивості (сумісність, масштабованість, потреба у персоналі, швидкість розгортання).

У межах дослідження було сформовано порівняльну матрицю оцінювання поширених засобів захисту, зокрема: систем виявлення вторгнень (IDS/IPS), міжмережевих екранів (FW), систем запобігання витоку даних (DLP), засобів

криптографічного захисту (KMS/VPN), SIEM-платформ, EDR/XDR-рішень та сервісів багатфакторної автентифікації (MFA).

Нижче наведено узагальнену таблицю, що відображає співвідношення між ефективністю, вартістю володіння та доцільністю використання у кризових сценаріях, коли організація вимушена обмежити бюджет, але не може дозволити погіршення рівня безпеки.

Таблиця 1 подає систематизоване порівняння засобів захисту з позиції їхньої придатності до використання у кризових умовах — коли фінансові, кадрові або часові ресурси істотно обмежені, а ризики зростають. У рамках цієї оцінки технічна ефективність розглядається не як абстрактна характеристика, а як здатність засобу реально нейтралізувати загрози, притаманні кризовим ситуаціям: масовані кібератаки, спроби компрометації облікових даних, мережеві інциденти, поширення шкідливого ПЗ.

Особлива увага приділена співвідношенню “ефективність–вартість”, оскільки саме цей критерій є ключовим у період кризи. Наприклад, SIEM-системи демонструють найвищу технічну ефективність, але вимагають значних витрат на впровадження та експлуатацію, що знижує їхню пріоритетність у період ресурсних обмежень. Натомість MFA, VPN та FW мають низьку вартість, але забезпечують суттєвий внесок у зниження ризиків, тому їхня доцільність у кризових сценаріях є максимальною.

Таблиця 1

Порівняльна оцінка засобів захисту інформації у кризових умовах

Засіб захисту	Технічна ефективність	Вартість володіння	Доцільність у кризових умовах
IDS/IPS	Висока для мережевих атак	Середня	Висока — дозволяє завчасно виявляти загрози
Міжмережевий екран (FW)	Висока	Низька–середня	Висока — базовий елемент оборони
SIEM-платформа	Дуже висока	Висока	Середня — корисна, але дорога при обмежених ресурсах
EDR/XDR	Висока для endpoint-загроз	Середня	Висока — мінімізує інциденти на кінцевих пристроях
DLP	Середня–висока	Висока	Низька — актуальна лише для організацій з критичними даними
VPN / Криптографічний захист	Висока	Низька	Висока — критично важливий засіб захисту каналів
MFA-сервіси	Дуже висока	Низька	Висока — значно знижує ризики компрометації

Аналіз показує, що організаціям доцільно формувати оптимальний набір засобів захисту, виходячи з принципу мінімально необхідного, але достатнього рівня безпеки. У кризових умовах пріоритет мають технології, які забезпечують максимальний ефект при мінімальних витратах, — перш за все це MFA, VPN/криптографічний захист, FW та EDR/XDR.

У випадках, коли загроза є складнішою або організація обробляє критичні дані, доцільно додавати IDS/IPS та частковий функціонал SIEM (наприклад, Open-Source варіанти або модульні рішення). Водночас повномасштабні DLP-системи, згідно з оцінкою, варто впроваджувати лише тоді, коли існує реальна загроза витоку чутливої інформації та є відповідні регуляторні вимоги.

Таким чином, результати дослідження чітко показують, що оптимізація складу ЗЗІ у кризових ситуаціях можлива за умови:

пріоритизації засобів з високим співвідношенням “ефективність/вартість”;
комбінування базових і спеціалізованих рішень відповідно до типів загроз;
поетапного впровадження складних систем (таких як SIEM або DLP) у випадках, коли ресурсні обмеження дозволяють це зробити;

орієнтації на засоби, що мають мінімальні потреби в експлуатації та швидко розгортаються.

За підсумками аналізу було сформовано рекомендації щодо складання адаптивного переліку ЗЗІ — від базової конфігурації до розширеної, залежно від рівня загроз і доступного бюджету. Це забезпечує збереження функціональної стійкості організації навіть за умов нестачі ресурсів та інтенсивного зовнішнього впливу.

Висновки та перспективи Проведене дослідження підтвердило, що оптимізація складу засобів захисту в кризових умовах потребує балансу між технічною ефективністю, ризик-орієнтованою оцінкою та економічними обмеженнями. Запропонований підхід дає можливість визначати мінімально достатній набір засобів, здатний забезпечити функціональність критичних сервісів навіть за умов обмеженого бюджету чи часткової недоступності інфраструктури.

Перспективи подальших досліджень бачаться в розробленні моделей динамічної оптимізації, застосуванні методів машинного навчання для прогнозування інцидентів, а також у формуванні адаптивних профілів безпеки, що автоматично перебудовують конфігурацію залежно від рівня загроз.

Список використаних джерел

1. National Institute of Standards and Technology. (2022). NIST Special Publication 800-30: Guide for Conducting Risk Assessments.
2. European Union Agency for Cybersecurity. (2023). ENISA Threat Landscape 2023.
3. Cherdantseva, Y., Hilton, J. (2019). A Reference Model of Information Security Risk Management. *Information & Computer Security*, 27(3).
4. Sterbenz, J. P., Hutchison, D. (2020). Resilience and Survivability in Communication Networks. *IEEE Communications Surveys & Tutorials*, 22(1).
5. Gartner Research. (2023). Optimize Cybersecurity Spending Under Crisis Conditions.

Трофімов Олександр Сергійович
аспірант 3 курсу, групи ІБДдф2340д
Київський столичний університет імені Бориса Грінченка
(095) 384-73-46
o.trofimov.asp@kubg.edu.ua

ВДОСКОНАЛЕННЯ ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ НА ОСНОВІ КОНЦЕПЦІЇ ZERO TRUST

Постановка задачі. В умовах ведення гібридної війни, зростання кількості та складності кібератак на об'єкти критичної інфраструктури України виявило недостатність традиційних периметрових моделей захисту та розрив між нормативними вимогами і реальними практиками безпеки [1, 2]. Існує потреба у впровадженні підходів, що базуються на концепції Zero Trust та сучасних криптографічних механізмах, зокрема управлінні ключами й розподілі секретів [3].

Мета дослідження. Метою дослідження є обґрунтування та розроблення підходів вдосконалення політики інформаційної безпеки інформаційних систем об'єктів критичної інфраструктури (IC OKI) України на основі концепції Zero Trust.

Результати дослідження. Аналіз секторальних систем показав, що найбільш типові та вразливі класи — це SCADA/ICS, ERP-рішення, SIEM/SOC-платформи, системи ситуаційної обізнаності та державна медична система eHealth. Дані системи обробляють критичні технологічні процеси, фінансові транзакції, персональні дані та координують реагування на інциденти. Їх порушення призводить не лише до операційних збоїв, а й до масштабних соціально-економічних наслідків.

Виявлено, що традиційні моделі периметрового захисту не забезпечують належного рівня стійкості в умовах сучасних загроз. Поширеними є атаки на промислові системи керування (типу Industroyer2), цілеспрямовані компрометації корпоративних ERP (комплексні інформаційні системи керування ресурсами підприємства), неефективність обробки подій у SIEM/SOC через кадровий дефіцит, загрози відмов у доступності для систем ситуаційної обізнаності та високі ризики витоків персональних даних eHealth. Внутрішні ризики — інсайдери, некваліфіковані дії персоналу, компрометація облікових записів — також посилюють загальну вразливість.

На основі виявлених факторів сформовано модель загроз, у якій ключовими джерелами впливу визначено зовнішні атаки (APT, DDoS, фішинг, шкідливе ПЗ), внутрішні ризики (неправомірні дії, помилки персоналу) та коаліційні сценарії (зовнішній зловмисник у взаємодії з компрометованим внутрішнім суб'єктом). Метою таких атак є технологічні процеси, дані або канали комунікацій — тобто активи, що безпосередньо визначають стабільність функціонування критичних секторів.

Для подолання ідентифікованих слабких місць обґрунтовано доцільність переходу до концепції Zero Trust [3]. Вона ґрунтується на принципах недовіри до будь-якого користувача чи пристрою до моменту перевірки, мінімізації привілеїв та безперервної верифікації. Дослідження показало, що практична реалізація Zero Trust в ІС ОКІ потребує криптографічних механізмів підтвердження довіри. Інфраструктура відкритих ключів (PKI) забезпечує унікальну ідентифікацію, автентичність операцій, контроль привілеїв та можливість ротації доступів у динамічному режимі. Розподілене управління секретами (threshold cryptography) дозволяє здійснювати критичні дії лише за умови колективної авторизації, що мінімізує ризики одноосібних зловживань.

Запропонована методика вдосконалення політики інформаційної безпеки поєднує технічні та організаційні підходи в єдину архітектуру. Ключові її компоненти включають: багаторівневу автентифікацію, атрибутивне управління доступом, мікросегментацію мереж, криптографічне маркування суб'єктів, порогові схеми розподілу секретів та безперервний моніторинг поведінки. Така архітектура забезпечує динамічну переоцінку рівня довіри в режимі реального часу та перешкоджає неконтрольованому переміщенню між сегментами інфраструктури.

У результаті сформовано формалізовану модель політики доступу, яку представлено через три взаємопов'язані блоки: функцію доступу на основі атрибутів, порогову схему управління секретами та оцінку ризику доступу. Модель дозволяє однозначно визначати умови авторизації, перевіряти критичні операції за участі декількох уповноважених суб'єктів та адаптувати рівень довіри залежно від контексту. Отримані результати створюють основу для практичної імплементації Zero Trust в інформаційних системах критичної інфраструктури України та формування уніфікованої політики кіберзахисту, узгодженої з міжнародними стандартами та національними нормативними вимогами.

Висновки та перспективи. Проведене дослідження засвідчило обмеженість традиційної моделі периметрового захисту для інформаційних систем об'єктів критичної інфраструктури України, зокрема в умовах комплексних зовнішніх, внутрішніх та коаліційних загроз. Обґрунтовано, що впровадження концепції Zero Trust забезпечує підвищення рівня кіберстійкості за рахунок криптографічно підтверджуваної автентифікації, мінімізації привілеїв та контекстної динамічної перевірки доступу. Запропонований підхід, що поєднує механізми PKI, атрибутивне управління доступом та порогові схеми розподілу секретів, формує основу для комплексної політики захисту та може бути використаний для уніфікації нормативних і технічних підходів до безпеки ІС ОКІ.

Перспективи подальших досліджень пов'язані з розробленням адаптивних моделей динамічного управління довірою, інтеграцією Zero Trust із системами аналізу поведінкових аномалій, а також формуванням секторальних рекомендацій для різних типів критичних систем. Доцільним є дослідження ефективності порогових криптографічних механізмів у сценаріях практичного використання та оцінка їх впливу на операційну безперервність, що створить

передумови для впровадження стандартизованих методик кіберзахисту на рівні державної політики.

Список використаних джерел

1. Aebi S., Hauri A., Kamberaj J. (2024). Critical infrastructure resilience in Ukraine: Energy, transportation, and communication (Risk and Resilience Report). Center for Security Studies (CSS), ETH Zürich. DOI: <https://doi.org/10.3929/ethz-b-000662463>
2. Ільєнко А., Телющенко В., Дубчак О. (2023) Сучасні кіберзагрози критичної інфраструктури України та світу. Кібербезпека: освіта, наука, техніка, 3(27), с. 150–164. DOI: <https://doi.org/10.28925/2663-4023.2023.27.719>
3. Ворохоб М., Киричок Р., Яскевич В., Добришин Ю., Сидоренко С. (2023). Сучасні перспективи застосування концепції Zero Trust при побудові політики інформаційної безпеки підприємства. «Кібербезпека: освіта, наука, техніка», 1(21), 223–233. DOI: <https://doi.org/10.28925/2663-4023.2023.21.223233>

Стежко Світлана Орестівна,
Завідувач кафедри української мови, кандидат філологічних наук, доцент,
Державний університет інформаційно-комунікаційних технологій
(067) 263-89-73

svitlinka@ukr.net

Кондратенко Наталія Юріївна,
Доцент кафедри української мови, кандидат педагогічних наук, доцент,
Державного університету інформаційно-комунікаційних технологій,
м. Київ, Україна.
nata2335@ukr.net

МОВНА ЕТИКА ЕЛЕКТРОННОГО СПІЛКУВАННЯ В УМОВАХ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Постановка задачі. У сучасному інформаційному просторі електронне спілкування фактично стало звичною і провідною формою професійної взаємодії. Це висуває підвищені вимоги не тільки до технічного захисту персональних даних, а й до відповідального мовного оформлення повідомлень. Водночас помітною є суперечність: активне використання електронних каналів зв'язку нерідко поєднується з нехтуванням нормами мовної етики, що спричиняє некоректне розкриття конфіденційної інформації, неточні формулювання та комунікативні непорозуміння. Тому вбачаємо необхідність простежити, як мовні засоби, інтонація електронного спілкування та обрані комунікативні стратегії позначаються на збереженні персональних даних, виокремити типові порушення мовної етики та окреслити правила, дотримання яких забезпечує більш безпечну і відповідальну електронну комунікацію.

Мета дослідження. Метою дослідження є з'ясування того, як мовні засоби, норми етикету та реальні умови електронного спілкування впливають на збереження персональних даних, а також окреслення таких мовних підходів і правил комунікації, дотримання яких мінімізує ризики ненавмисного розкриття конфіденційної інформації та сприяє формуванню культури безпечної електронної взаємодії.

Результати дослідження. *Ситуація, де показано які саме мовні етикетні засоби були використані і як саме це допомогло зберегти персональні дані.*

Ситуація

Працівник деканату має надіслати групі студентів повідомлення про перездобуття паролю до електронного кабінету.

Як робити не можна (порушення етики й безпеки)

- звернення без офіційної форми
- відкритий список адресатів
- розкриття ПІБ і даних інших студентів
- цитування індивідуальних проблем

Тема: Паролі

Доброго дня, надсилаю вам нові паролі.

Петренко Олег – 4h76K

Марчук Ірина – R8p99

Решті напишу пізніше.

Тут: розкрито персональні дані, порушено конфіденційність, відсутня мовна етика і службовий тон.

Правильно з позиції етикету і захисту даних

Використано: офіційно-ділове звертання, безособові формулювання, рекомендації «не поширювати», уникнення згадування прізвищ, приховані адреси (ВСС — у правилах, але не прописуємо техніку, лише мовний аспект)

Тема: Відновлення доступу до електронного кабінету

Шановні студенти,

повідомляємо, що питання відновлення доступу до електронного кабінету вирішується індивідуально.

Для отримання нового пароля, будь ласка, надішліть **особистий лист на адресу деканату**, зазначивши лише номер залікової книжки.

Просимо **не надсилати в загальних листуваннях свої персональні дані** (прізвище, дату народження, адреси, скани документів).

Дякуємо за розуміння та дотримання правил безпечної електронної комунікації.

Що тут працює як «умовні засоби мовної етики»

офіційне звертання («Шановні студенти»)

безособове оформлення замість персонального згадування

мовне застереження: «просимо не надсилати...»

рекомендаційні формули ввічливості

уникання чутливих даних у колективному листі

перенесення персонального спілкування в індивідуальний канал

Як це зберігає персональні дані

не називаються ПІБ і паролі

не створюється масова розсилка з чужими адресами

людина сама вирішує, які дані надіслати індивідуально

формується **мовні межі дозволеного і недозволеного**

Порівняльна таблиця:

Помилкове / ризиковане слововживання в документах	Правильне та безпечне формулювання, що відповідають вимогам конфіденційності.
Надішліть ваші дані	Надішліть необхідні персональні дані у персональному повідомленні
Розіслати списки студентів/працівників	Надати інформацію індивідуально за запитом особи
Паролі надіслані всім адресатам	Паролі надаються в індивідуальному порядку
Публікуємо список осіб, які...	Публікуємо знеособлену інформацію / узагальнені відомості
Особисті дані доступні для перегляду	Доступ до персональних даних обмежено відповідно до повноважень

Помилкове / ризиковане слововживання в документах	Правильне та безпечне формулювання, що відповідають вимогам конфіденційності.
Конфіденційність не гарантуємо	Дані обробляються з дотриманням вимог конфіденційності та захисту персональних даних
Розголошення інформації дозволене	Поширення персональних даних без згоди особи заборонене
Прізвища, адреси, телефони додаються у додатку	У додатку подано частково знеособлені відомості / персональні дані не публікуються
Надішліть копії документів у загальний чат	Надішліть копії документів в особистому листуванні
Вільний доступ до особових справ	Доступ до особових справ — лише для уповноважених осіб

Висновки

Проведені міркування дають підстави стверджувати, що мовний чинник у сфері електронного спілкування є безпосередньо пов'язаним із забезпеченням захисту персональних даних. Мовні помилки, неточні формулювання та порушення норм мовної етики не лише ускладнюють порозуміння між адресантом і адресатом, а й створюють додаткові ризики ненавмисного розкриття конфіденційної інформації.

З'ясовано, що дотримання етикету електронного листування, використання нейтральних і чітких формулювань, знеособлення персональних відомостей у масових повідомленнях та перенесення індивідуальних питань в особисте листування є дієвими мовними засобами збереження приватності. Саме мовна культура комунікації в поєднанні з технічними заходами кіберзахисту формує простір безпечної електронної взаємодії.

Отже, культура українського фахового мовлення в умовах електронного документообігу виступає не лише показником професіоналізму, а й важливою складовою інформаційної безпеки. Подальші дослідження можуть бути пов'язані з аналізом конкретних жанрів електронних документів і виробленням практичних рекомендацій щодо мовних стратегій, спрямованих на збереження персональних даних.

Список використаних джерел

1. Голоюх Л. В. Українська мова за професійним спрямуванням : навч. посіб. для студентів навчально-наукового фізико-технологічного інституту. Луцьк, 2022. 192 с.
2. Савчук Н. М. Українська мова за професійним спрямуванням : навч. посіб. Умань : ВПЦ «Візаві», 2019. 160 с.
3. Культура фахового мовлення : навч. посіб. / за ред. Н. Д. Бабич. Чернівці : Книги ХХІ, 2005. 572 с.

Напрям №9. Blockchain-технології

Гавор Артур Станіславович

аспірант 1 курсу, групи АПЗ-11

Державний університет інформаційно-комунікаційних технологій

(050)285-15-30

a.havor@duikt.edu.ua

Науковий керівник: Герцюк Микола Модестович

доктор філософії, доцент кафедри Технологія Цифрового розвитку

Державний університет інформаційно-комунікаційних технологій

ОГЛЯД ПРОТОКОЛУ GOSSIP В РОЗПОДІЛЕНИХ ОБЧИСЛЕННЯХ

Постановка задачі. Сенсорні мережі, робототехнічні платформи, бездротові мережі та хмарні сервіси потребують надійних методів обміну інформацією між великою кількістю вузлів без централізованого контролю. Одним із найбільш ефективних децентралізованих підходів є протокол Gossip, у якому вузли обмінюються повідомленнями випадковим або напів випадковим чином, забезпечуючи швидке поширення даних у масштабованих та відмовостійких системах [1]. Актуальність проблеми посилюється зростанням кількості пристроїв та необхідністю підтримувати узгодженість даних без перевантаження мережевих каналів.

Мета дослідження. Метою дослідження є аналіз принципів роботи алгоритмів Gossip, їх класифікацію, переваги та обмеження в розподілених системах.

Результати дослідження. Gossip моделює процес обміну інформацією аналогічно до поширення епідемій, кожен вузол мережі періодично вибирає іншого випадково або за визначеною стратегією, і передає йому частину або весь набір даних [1]. Багаторазові взаємодії поступово вирівнюють стан всієї системи, забезпечуючи досягнення спільного набору знань.

Цей підхід належить до епідемічних методів і охоплює ціле сімейство технік для розповсюдження та узгодження інформації у розподілених середовищах [2]. Він особливо ефективний у великих динамічних мережах без централізованого керування, де топологія постійно змінюється. Стійкість до збоїв досягається завдяки надлишковим обмінам, навіть якщо частина повідомлень губиться або деякі вузли виходять з ладу, інформація продовжує поширюватися мережею [3].

Поведінка окремого вузла включає отримання оновлення, корекцію локального стану та подальшу передачу цих даних у наступних раундах, що створює ефект «епідемічного» розповсюдження [4]. Для впорядкування різних підходів використовують класифікацію за такими критеріями: напрямок обміну повідомленнями, функціональне призначення, режим роботи, тип топології, політика вибору сусіда та вимоги до надійності й безпеки.

Він працює як децентралізований peer-to-peer механізм кожен, вузол періодично обмінюється інформацією з випадково вибраним сусідом [1]. У типовому раунді відбувається коротка взаємодія, під час якої сервер передає свій

стан або отримує новий [1]. Далі інформація «розтікається» мережею каскадно, охоплюючи дедалі більшу кількість вузлів [2]. Повторні контакти забезпечують високу ймовірність доставки даних навіть за ненадійних мережеских умов [3]. Отримавши оновлення, вузол коригує локальний стан і поширює зміни далі, що приводить систему до «eventual consistency» природного вирівнювання станів [4].

Таблиця 1

Основні класифікаційні ознаки алгоритмів Gossip

Критерій	Класи	Коротка характеристика
Напрямок обміну	Push, Pull, Push-pull	спосіб передавання або отримання стану між вузлами
Призначення	Dissemination, Aggregation, Monitoring	поширення оновлень, обчислення агрегатів, моніторинг подій
Режим роботи	синхронний, асинхронний	обмін за раундами або за власним тактом вузлів
Топологія	не структурована, структурована	випадкові зв'язки або фіксовані накладені структури
Вибір сусіда	випадковий, зважений	рівноймовірний або з урахуванням параметрів мережі

Процес найкраще ілюструє приклад на рис. 1. Схема демонструє взаємодію шести серверів, кожен з яких підтримує власний список відомих вузлів. Під час чергового раунду один сервер випадково вибирає інший і передає йому свої дані. Стрілки позначають напрям поширення інформації, а різні кольори відповідають окремим раундам обміну.

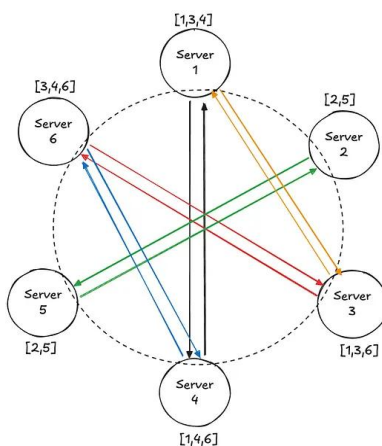


Рис. 1. Приклад епідемічного поширення інформації між вузлами у Gossip [1].

Як видно зі схеми, інформація поширюється не централізовано, а через послідовні локальні взаємодії. Оновлення, отримане одним сервером, надалі передається іншим, і після кількох раундів усі вузли набувають однакових знань

про стан системи. Це демонструє ключову ідею Gossip децентралізоване узгодження, що виникає внаслідок багаторазових випадкових обмінів.

Висновки та перспективи. В роботі проведено огляд принципів функціонування Gossip та його особливостей як децентралізованого механізму поширення інформації. Аналіз показав, що епідемічний характер обміну забезпечує високу відмовостійкість, стійкість до втрати повідомлень, адаптивність до змінної топології та відсутність потреби в центральному координаторі. Сукупність цих властивостей робить Gossip придатним для використання у великих розподілених мережах, зокрема у системах екологічного моніторингу, де важливими є автономність вузлів, здатність працювати в умовах ненадійного зв'язку та масштабованість у просторі.

Перспективним напрямком подальших досліджень є моделювання роботи таких мереж з урахуванням енергоспоживання сенсорних вузлів, частоти обмінів і щільності розміщення. Додаткові можливості пов'язані з інтеграцією Gossip із методами машинного навчання та аналізу даних для підвищення точності оцінювання стану екосистем, своєчасного виявлення аномалій та прогнозування екологічних ризиків.

Список використаних джерел

1. Sudhindra Saxena. Understanding Gossip Protocol: How It Really Works. URL: https://medium.com/@sudhindra_saxena/understanding-gossip-protocol-how-it-really-works-dddb6b081626 (дата звернення: 04.12.2025)
2. Yu T., Yu L., Xiong J. Observer-based distributed control of large-scale systems under gossip communication protocol. Asian Journal of Control. 2021. Т. 24, № 2. С. 956–972.
3. NK. Gossip Protocol Explained - High Scalability -. High Scalability. URL: <https://highscalability.com/gossip-protocol-explained/> (дата звернення: 04.12.2025).
4. CREW: A Gossip-based Flash-Dissemination System / M. Deshpande та ін. 26th IEEE International Conference on Distributed Computing Systems (ICDCS'06), м. Lisboa, Portugal.

Рудавіна Катерина Дмитрівна
студентка 4-го курсу, групи інб-2-22-4.0д
Київський столичний університет імені Бориса Грінченка
0501791649
kdrudavina.fitm22@kubg.edu.ua

BLOCKCHAIN-ТЕХНОЛОГІЇ. ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ BLOCKCHAIN-ТЕХНОЛОГІЙ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Постановка задачі. Стрімкий розвиток цифрової економіки потребує нових технологічних рішень, здатних забезпечити прозорість, надійність та безпеку обробки даних. Однією з найбільш інноваційних технологій останнього десятиліття є блокчейн, що ґрунтується на децентралізованому зберіганні та верифікації інформації у вигляді розподіленого реєстру. Незважаючи на початкову асоціацію з криптовалютами, блокчейн на сьогодні використовується у багатьох галузях: фінансовому секторі, логістиці, державних е-сервісах, системах цифрової ідентифікації, охороні здоров'я тощо.

Проблематика полягає в тому, що традиційні централізовані системи мають низку недоліків - залежність від одного управлінського центру, складність у перевірці достовірності записів, високий ризик підробки або несанкціонованої модифікації даних. Це створює потребу у впровадженні нових механізмів, що забезпечують прозоре та захищене зберігання інформації. Тому актуальним є аналіз можливостей блокчейну як технології, що здатна підвищити рівень довіри, безпеки й ефективності сучасних інформаційних систем.

Мета дослідження. Метою дослідження є аналіз принципів роботи блокчейн-технологій, їх переваг, недоліків та практичних напрямів застосування, а також оцінка перспектив розвитку блокчейн-рішень у контексті цифрової економіки та державних електронних систем.

У дослідженні ставляться такі завдання:

- визначити ключові інженерні та криптографічні принципи роботи блокчейну;
- дослідити сфери застосування блокчейн-мереж та їхню ефективність у порівнянні з класичними централізованими системами;
- проаналізувати сучасні виклики та обмеження впровадження блокчейну;
- окреслити перспективи розвитку технології у найближчі роки.

Результати. Аналіз технологічних принципів блокчейну показав, що основою роботи системи є розподілений реєстр та криптографічні методи, які забезпечують незмінність та цілісність даних. Завдяки механізмам консенсусу (Proof-of-Work, Proof-of-Stake, Delegated PoS, тощо) блокчейн дозволяє узгоджувати дії учасників без централізованого контролера, що робить систему стійкою до атак, фальсифікації записів та збоїв одного вузла.

У ході дослідження встановлено, що найбільш перспективними напрямками застосування блокчейну є:

- Фінансові технології (FinTech): транзакції в криптовалютних мережах, смарт-контракти, токенизація активів, децентралізовані біржі.

- Логістика: відстеження постачання товарів, контроль якості, забезпечення прозорого ланцюга поставок.

- Електронне врядування: реєстри власності, цифрові паспорти, голосування на основі блокчейну, відкритість державних даних.

- Медицина: захищене зберігання медичних записів, контроль доступу до персональних даних.

- Освіта: верифікація дипломів, сертифікатів та результатів навчання

Крім значних можливостей, дослідження виявило і низку проблем, які гальмують широке впровадження блокчейну. До них належать:

- низька масштабованість деяких мереж;

- високе енергоспоживання, характерне для протоколів PoW;

- регуляторні обмеження в окремих країнах;

- складність інтеграції з уже існуючими інформаційними системами;

- ризики безпеки смарт-контрактів, що можуть містити програмні помилки.

Перспективи розвитку блокчейну пов'язані з удосконаленням моделей консенсусу, створенням енергоефективних мереж другого рівня (Layer-2), упровадженням міжблокчейнових протоколів (cross-chain) та збільшенням частки державних і корпоративних платформ на базі приватних блокчейнів.

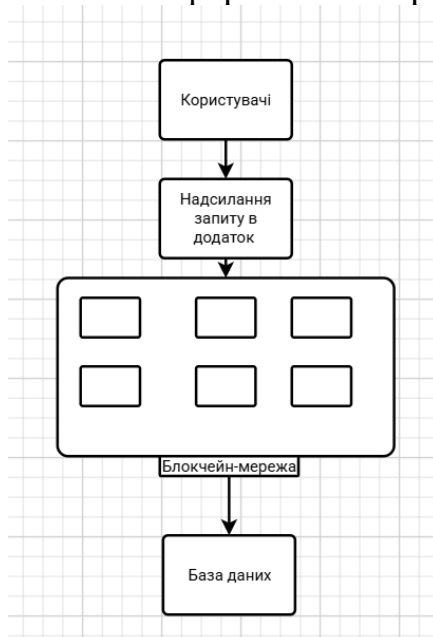


Рис. 1. Архітектура роботи blockchain-системи.

Представлена архітектура демонструє основні елементи взаємодії користувача з blockchain-системою. Користувачі надсилають запити через прикладний рівень, де відбувається первинна обробка транзакцій та формування структурованих даних.

Далі інформація передається у blockchain-мережу, де транзакції перевіряються за допомогою механізмів консенсусу та об'єднуються у блоки.

Blockchain забезпечує незмінність і криптографічний захист даних, а також веде хронологічний журнал усіх операцій.

Після підтвердження транзакції формується запис, який може зберігатися в окремій базі даних або використовуватися у прикладних сервісах. Таким чином, схема відображає повний цикл: від дій користувача до збереження даних у розподіленому реєстрі.

Висновки. Результати дослідження підтверджують, що блокчейн-технології є одним із найперспективніших напрямів розвитку сучасної цифрової інфраструктури. Завдяки децентралізації, незмінності записів і високому рівню криптографічного захисту блокчейн забезпечує нову якість управління даними, підвищуючи довіру між учасниками системи та зменшуючи ризики фальсифікації. Попри наявні обмеження - проблеми масштабованості, енергоспоживання та нормативної невизначеності - технологія продовжує розвиватися, активно впроваджується у фінансовий сектор, логістику, державні е-системи та медичну сферу. У найближчі роки очікується зростання кількості корпоративних блокчейн-рішень, поширення смарт-контрактів та поява нових прикладних сервісів, що зроблять блокчейн ключовим елементом цифрової економіки.

Список використаних джерел

1. Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press, 2016.
2. Crosby M., Pattanayak P., Verma S., Kalyanaraman V. *Blockchain Technology: Beyond Bitcoin*. Applied Innovation Review, №2, 2016, с. 6-19.
3. Mougayar W. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Hoboken: Wiley, 2016.
4. Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Yellow Paper. Ethereum Foundation, 2014.
5. Zheng Z., Xie S., Dai H., Chen X., Wang H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. IEEE 6th International Congress on Big Data, 2017, с. 557-564.

Кравчук Андрій Віталійович

викладач загальноосвітніх дисциплін

Житомирський агротехнічний фаховий коледж

(097) 448-80-82

superfizik1973@gmail.com

ІНТЕГРАЦІЯ ВІДЕОХОСТИНГУ YOU TUBE У КУРС ФІЗИКИ ЯК СКЛАДОВА ЦИФРОВОЇ ЕКОНОМІКИ ЗНАНЬ

Постановка задачі. У межах дослідження ставиться задача проаналізувати сучасний стан використання відеоконтенту та освітніх платформ у викладання фізики та розробити систему використання навчальних відео з YouTube у курсі фізики, що забезпечує підвищення якості засвоєння знань, розвиток умінь самостійної роботи студентів і впровадження елементів цифрової педагогіки, які відповідають принципам економіки знань.

Мета дослідження. Визначити педагогічний потенціал відеохостингу YouTube у контексті розвитку цифрової економіки знань, зокрема як засобу поширення відкритих освітніх ресурсів і формування навичок самоосвіти у студентів при вивченні фізики.

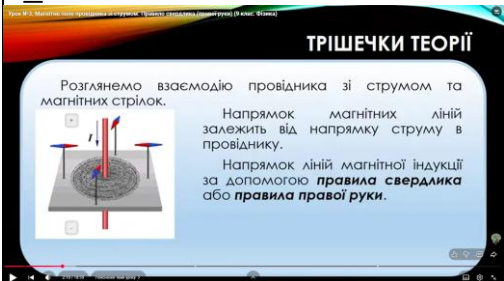
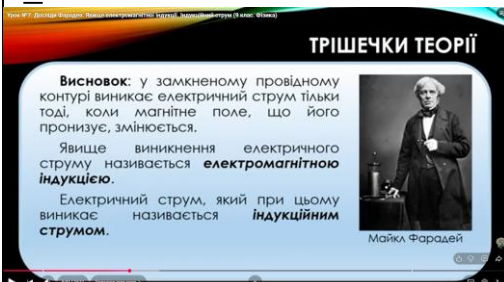
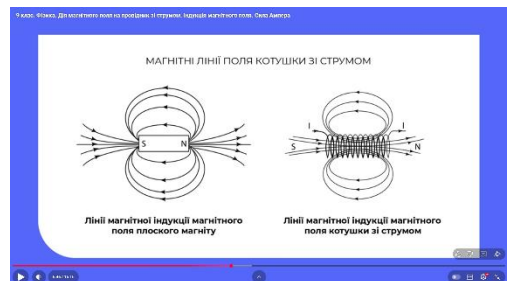
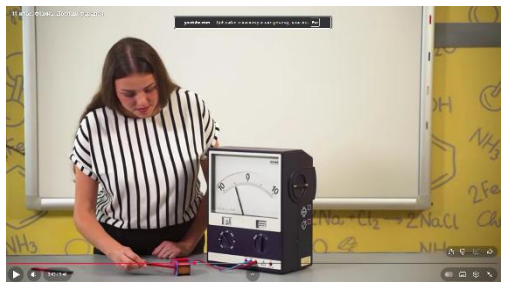
Результати дослідження. Для підвищення ефективності занять педагоги активно використовують різноманітні інформаційні ресурси – відеоматеріали, анімації фізичних процесів, презентації та інший мультимедійний контент.

Аналіз науково-методичних праць показав, що використання відеоресурсів у навчанні досліджували багато українських і зарубіжних науковців – Н. Нестеренко, Н. Михайловська, А. Волков, О. Воронкін, О. Мартинюк, І. Карпа та інші. Дослідники по-різному визначають поняття «відеоресурс». Ми погоджуємося з визначенням Я. Глинського, який вважає, що відеоресурс – це особливий тип електронного ресурсу, побудований на основі цифрових відеоданих. [1]. Вивчивши можливості використання відеоконтенту у навчанні фізики, можна зробити висновок, що:

- відео можна застосовувати як під час онлайн, так і під час офлайн занять;
- за відсутності необхідного обладнання воно допомагає ознайомити студентів із фізичними явищами та процесами у реальному житті;
- під час підготовки до лабораторних робіт відеоексперименти є незамінним джерелом знань, особливо коли в кабінеті бракує приладів;
- відеоматеріали можуть використовуватися для створення задач або додаткових завдань з фізики.

За спостереженнями Д. Бучинської, використання відеоресурсів допомагає студентам засвоювати до 65 % навчального матеріалу. Тому впровадження освітнього відеоконтенту є доцільним. Одним із найпопулярніших відеохостингів є **YouTube**, аудиторія якого щомісяця перевищує 2,9 мільярда користувачів. На платформі функціонує багато освітніх каналів, серед яких:

Відео-контент з розділу «Електродинаміка і магнетизм»

Тема	Лінки на відео
Магнітне поле провідника зі струмом	https://www.youtube.com/watch?v=YyzCfUNfsnk&list=PLeb-UxVXmUb4zursu7WhIEI6KkCv2ESF_&index=3 
Сила Ампера	https://www.youtube.com/watch?v=GJ_QAsP-ME&list=PLeb-UxVXmUb4zursu7WhIEI6KkCv2ESF_&index=4 
Досліди Фарадея	https://www.youtube.com/watch?v=q5flfCMw1A&list=PLeb-UxVXmUb4zursu7WhIEI6KkCv2ESF_&index=7 
	https://www.youtube.com/watch?v=fd85c8EtIKg 
	https://www.youtube.com/watch?v=u7iw6eG95z8 
	https://www.youtube.com/watch?v=fjfnJ40Us2Q 

1. «Топ Школа» - український канал, що налічує понад 320 безоплатних авторських відеоуроків з фізики для 7-11 класів для базової та профільної школи - <https://www.youtube.com/channel/UCugp2JTHik6cdFxs1GbEOGg>;
2. «Фізика за хвилину» - американський канал, де математик і фізик Г. Райх у доступній формі пояснює фізичні явища за кілька хвилин - <https://www.youtube.com/user/minutephysics>;
3. «Всеукраїнська школа онлайн» - це платформа для цифрового та змішаного навчання учнів 1–11 класів і методичної підтримки педагогічних

працівників - <https://www.youtube.com/user/khanacademy>;

4. «Цікава наука» - канал на якому розміщені перекладені та озвучені науково-популярні та освітні відео на різні наукові теми з фізики, астрономії - <https://www.youtube.com/channel/UCMIVE71tHEUDkuw8tPxtzSQ>.

У ході дослідження було відібрано добірку відеоматеріалів, які викладачі можуть використовувати під час вивчення розділу **«Електродинаміка і магнетизм»**.

Як видно з таблиці 1, до одного заняття можна підібрати чимало відео-ресурсів, але під час добору відеоматеріалів варто враховувати такі основні вимоги:

1. Відео має бути емоційно привабливим і викликати інтерес до навчання.
2. Доцільно обирати короткі, змістовно завершені ролики тривалістю 2–10 хвилин або використовувати окремі фрагменти довших відео.
3. Мовлення у відео повинно мати помірний темп, а в деяких випадках важливо робити паузи, щоб студенти могли осмислити матеріал.
4. Під час пояснення нового матеріалу викладачу бажано нагадувати зміст попереднього заняття, демонструвати зв'язки між темами, наводити життєві приклади й заохочувати студентів до подальшого перегляду навчальних відео.

Висновки та перспективи. В дослідженні визначено педагогічні можливості відеохостингу YouTube як інструменту цифрової освіти. Проведений аналіз довів практичне впровадження YouTube як допоміжного освітнього інструменту у курсі фізики.

Перспективою подальших досліджень є інтеграція штучного інтелекту для персоналізації відеорекомендацій і створення навчальних траєкторій з фізики.

Список використаних джерел

1. Глинський Я.М., Федасюк Д.В., Рязська В.А. Розроблення і використання електронних відео ресурсів навчального призначення. Інформаційні технології і засоби навчання. 2017. т. 58. №2. с. 67-78.
2. Бучинська Д. Л. Використання відео в навчальному процесі – потреба сьогодення. Відкрите освітнє е-середовище сучасного університету. 2015. Вип. 1. с. 101– 107.

Лозан Андрій Едуардович
аспірант 3 курсу, групи 073/23-1
Національний університет «Одеська політехніка»
(066)060-13-15
andlozedd@gmail.com

ІНТЕГРАЦІЯ ЦИФРОВИХ РІШЕНЬ В УПРАВЛІННЯ ІННОВАЦІЙНИМ РОЗВИТКОМ ПІДПРИЄМСТВ

Постановка задачі. У сучасних умовах глобалізації та стрімкої цифровізації підприємства активно шукають універсальні способи підвищення своєї інноваційної спроможності та адаптивності. У зв'язку з цим постає завдання дослідити та обґрунтувати загальні підходи до інтеграції цифрових рішень у систему управління інноваційним розвитком підприємства. Дослідження спрямоване на виявлення універсальних принципів і методів цифрової інтеграції, які дозволяють ефективно зміцнювати інноваційний потенціал і стійкість підприємств в умовах зростання глобальних ризиків.

Мета дослідження. Метою дослідження є розробити цифрово орієнтований підхід до інтеграції інноваційних технологій у систему управління підприємством, який забезпечить зменшення впливу глобальних ризиків, підвищення прогнозованості та ефективності інноваційного розвитку.

Результати дослідження. Застосовуючи такі концептуальні моделі, як Digital Innovation Process Model, Digital Transformation Canvas, та Enterprise Digital Innovation Framework, можна структурувати підходи до цифрової інтеграції. Ці моделі надають системні рамки, які перетворюють загальні концепції на конкретні кроки, роблять процеси впровадження більш передбачуваними та зменшують невизначеність.

Розглянемо більш детально наступні моделі:

- Digital Innovation Process Model забезпечує поетапний і системний підхід до впровадження цифрових інновацій, охоплюючи основні стадії — від генерування ідей до їх тестування та масштабування [1];
- Digital Transformation Canvas слугує інструментом стратегічного планування, який дозволяє структуровано візуалізувати ключові елементи цифрових змін та узгодити їх із цілями підприємства [2];
- Enterprise Digital Innovation Framework пропонує комплексний підхід до інтеграції цифрових технологій у діяльність підприємства, підсилюючи його гнучкість, адаптивність та стійкість до зовнішніх змін [3, 4].

Таблиця. 1.

Порівняння моделей(Джерело: складено автором за матеріалами [1-4]).

Критерій	Digital Innovation Process Model	Digital Transformation Canvas	Enterprise Digital Innovation Framework

Суть моделі	Покрокова модель керування інноваційним процесом у цифровому середовищі: від генерування ідей до масштабування інновацій.	Стратегічний інструмент, що описує всі ключові компоненти цифрової трансформації підприємства на одній «карті».	Комплексна модель інтеграції цифрових технологій у бізнес-процеси для підвищення стійкості, гнучкості та інноваційності.
Впливає на	Етапи інновацій (ідея , розробка , тестування , впровадження , масштабування).	Елементи цифрової трансформації: цінність, процеси, ресурси, технології, дані, персонал, управління.	Стратегію цифрових інновацій, бізнес-процеси, архітектуру систем, культурні аспекти інновацій.
Ключові елементи	Інноваційний цикл, цифрові інструменти підтримки інновацій, управління ітераціями та експериментами.	9 блоків (цінності, процеси, клієнти, технології, дані, партнери, компетенції, управління, показники).	Технологічні елементи, бізнес-архітектура, цифрова культура, управління ризиками, механізми адаптації.
Аспект цифрової інтеграції	Дає розуміння, на яких етапах інновацій впроваджувати цифрові рішення.	Дозволяє планувати цифрову трансформацію комплексно.	Забезпечує інтеграцію цифрових технологій у єдину архітектуру підприємства.
Аспект інноваційного розвитку	Підвищує швидкість інновацій, тестування та адаптації.	Узгоджує інноваційну стратегію з цифровою стратегією підприємства.	Забезпечує масштабування інновацій та формування інноваційної екосистеми.
Аспект стійкості до ризиків	Дозволяє гнучко адаптувати інновації до зовнішніх змін.	Враховує ризики у стратегічному плануванні та управлінні змінами.	Підсилює цифрову стійкість через механізми адаптації та оцінки ризиків.
Обмеження	Може потребувати значних ресурсів на швидкі ітерації та експерименти.	Потребує добре розвинених цифрових компетенцій та культури.	Довгий цикл впровадження, складність управління змінами.

Висновки та перспективи. У дослідженні було розглянуто проблему інтеграції цифрових рішень в управління інноваційним розвитком підприємств в умовах глобалізації та зростання ризиків. На основі цього аналізу розроблено

цифрово орієнтований підхід до інтеграції інноваційних технологій. Головним результатом дослідження є порівняльний аналіз та обґрунтування застосування трьох ключових концептуальних моделей. Встановлено, що їхнє інтегроване використання створює системні рамки для цифрової інтеграції, які дозволяють підприємствам:

1. Підвищити прогнозованість інноваційних процесів через структурування етапів;
2. Забезпечити стратегічну відповідність цифрової трансформації загальній стратегії підприємства;
3. Зміцнити стійкість до глобальних ризиків та забезпечити гнучкість завдяки комплексній інтеграції технологій.

Запропонований підхід сприяє ефективному зміцненню інноваційного потенціалу та адаптивності підприємств.

Перспективою подальших досліджень є розробка гібридної моделі, яка синтезує сильні сторони проаналізованих фреймворків, а також проведення емпіричних досліджень та кейс-стаді для кількісної оцінки впливу запропонованого підходу на зниження ризиків та підвищення ефективності інноваційного розвитку в різних галузях.

Список використаних джерел

1. Helmer, J. (2021). Innovating digitally for services: A review of innovation process literature focused on digital innovation and service innovation. *Procedia Computer Science*, 187, 150–155. URL: <https://www.sciencedirect.com/science/article/pii/S1877050921017877>
2. Elia, G., et al. (2024). The digital transformation canvas: A conceptual framework for leading the digital transformation process. *Business Horizons*, 67(3), 311–322. URL: <https://www.sciencedirect.com/science/article/pii/S0007681324000454>
3. Vărzaru, A. A., et al. (2024). Digital Transformation and Innovation: The Influence of Digital Technologies on Business Models and Organizational Performance. *Sustainability*, 12(9), 359. URL: <https://www.mdpi.com/2079-8954/12/9/359>
4. Skudiene, V. (2025). Digital Transformations and Innovation Management. World Scientific Publishing Co. Pte. Ltd., 1–15. URL: https://www.worldscientific.com/doi/pdf/10.1142/9789811295140_0001

Сербін Віталій Ігорович
аспірант кафедри маркетингу
Національний університет «Одеська політехніка»
096 427 71 51
serbin.v.i@op.edu.ua

МЕТОДОЛОГІЯ Е-С-R-S-T-M ДЛЯ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В МАРКЕТИНГ КОМПАНІЙ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Постановка задачі. Проблема запровадження інноваційних AI-рішень у цифровому маркетингу підприємств електронної комерції полягає в необхідності формування системних підходів до інтеграції ШІ, які забезпечують адаптацію до швидкозмінного ринкового середовища та підвищення конкурентоспроможності бізнесу. Однак відсутність чіткої класифікації етапів упровадження, а також недостатній рівень обґрунтування ефективності використання різних інструментів ШІ на різних стадіях маркетингової діяльності ускладнюють прийняття управлінських рішень. Актуальність проблеми підсилюється стрімким розвитком технологій автоматизації, ростом обсягів даних, що потребують інтелектуальної обробки, й необхідністю персоналізації комунікацій із клієнтами для підвищення ефективності маркетингових кампаній. Посилення ролі аналітики даних, впровадження рекомендаційних систем та використання сучасних алгоритмів машинного навчання стають важливими завданнями, що мають вагоме наукове та практичне значення для фахівців у сфері маркетингу й менеджменту електронної комерції.

Мета. Метою дослідження є розробка комплексної системної методології впровадження штучного інтелекту у цифровий маркетинг підприємств електронної комерції.

Результати дослідження. Сучасні підприємства електронної комерції активно переходять від базової автоматизації до глибокої цифрової трансформації, в основі якої лежить використання штучного інтелекту. Розвиток технологій машинного навчання, обробки природної мови та аналітики великих даних дозволяє бізнесу не лише оптимізувати операційні процеси, а й формувати нову якість взаємодії зі споживачами. Персоналізація пропозицій, емоційна комунікація, прогнозування попиту і автоматизоване прийняття рішень стають ключовими перевагами, які надає штучний інтелект у сфері e-commerce. У цьому контексті виникає потреба у чітких методологічних підходах, що дозволяють системно впроваджувати інтелектуальні технології в маркетингові стратегії компаній.

Штучний інтелект у маркетингу електронної комерції виконує три ключові ролі. Механічний інтелект забезпечує автоматизацію рутинних дій, таких як обробка замовлень, управління контентом, сегментація клієнтів чи розсилки повідомлень. Мислячий інтелект відповідає за аналітику, прогнозування поведінки споживачів і прийняття рішень на основі даних. «Чуттєвий» інтелект дозволяє інтерпретувати емоції користувачів, аналізувати настрої, виявляти

рівень задоволення клієнтів і створювати довгострокові відносини між брендом і споживачем. Саме поєднання цих трьох типів інтелекту створює підґрунтя для формування нового типу маркетингу, який можна охарактеризувати як адаптивний, персоналізований і емоційно орієнтований. [1]

Наукові дослідження та практичні розробки останніх років показують, що існуючі підходи до впровадження штучного інтелекту мають певні обмеження. Методологія CRISP-DM пропонує структурований цикл аналізу даних, який охоплює етапи від розуміння бізнесу до впровадження рішень. Вона забезпечує логічну послідовність дій і сприяє командній роботі, однак не враховує специфіку динамічного середовища електронної комерції, етичні питання і фактори організаційної готовності. Фреймворк Huang і Rust розглядає штучний інтелект як багаторівневу систему, що поєднує механічні, мислячі та чуттєві здібності. Його перевага полягає у гармонійному поєднанні технічних інновацій з класичними маркетинговими принципами. Водночас цей підхід не деталізує практичні аспекти реалізації і не надає чітких індикаторів успіху. Підхід Crawl-Walk-Run фокусується на поетапному впровадженні технологій. Він дозволяє мінімізувати ризики та поступово розвивати експертизу команди, але його слабкість полягає у відсутності чіткої інтеграції між технологічними рішеннями та бізнес-стратегією компанії. [2]

У результаті аналізу наявних фреймворків виявлено потребу у створенні нової методології, яка поєднує структурованість і гнучкість, орієнтацію на бізнес-результати та етичну відповідальність. Для ефективного впровадження штучного інтелекту важливо забезпечити зв'язок між ШІ-рішеннями та маркетинговими цілями компанії, врахувати специфіку електронної комерції з її високою швидкістю змін, багатоканальністю та персоналізацією. Не менш суттєвим є аспект управління змінами, навчання персоналу і формування нової організаційної культури, що сприймає ШІ як партнера, а не як загрозу.

Авторська методологія E-C-R-S-T-M (Expertise - Collection - Research - Scale - Transform - Maintain) розроблена для подолання зазначених недоліків і забезпечення комплексного впровадження штучного інтелекту в маркетингову діяльність підприємств електронної комерції. Вона охоплює шість взаємопов'язаних етапів, які формують безперервний цикл розвитку інтелектуальних систем. На етапі Expertise визначаються бізнес-цілі, формується команда, встановлюються KPI та система управління проектом. Етап Collection присвячений збору, очищенню та структуризації даних із дотриманням принципів якості, безпеки та конфіденційності. Research охоплює розробку, тестування та етичну перевірку моделей штучного інтелекту, які вирішують конкретні бізнес-завдання. Етап Scale включає валідацію рішень, A/B тестування, оцінку ефективності та підготовку до інтеграції у виробниче середовище. Transform зосереджується на глибокій трансформації маркетингових процесів, навчанні персоналу та впровадженні інструментів автоматизації в межах маркетинг-міксу. Завершальний етап Maintain забезпечує постійний моніторинг, перенавчання моделей і стратегічну оптимізацію для підтримки довгострокової ефективності системи.

Методологія E-C-R-S-T-M базується на чотирьох принципах: Data Excellence, Human-AI Collaboration, Ethical by Design та Business-First. Це означає, що впровадження ШІ має починатися з якісних даних, супроводжуватися тісною взаємодією між людиною і технологією, враховувати етичні наслідки рішень і завжди залишатися підпорядкованим бізнес-цілям компанії. Такий підхід гарантує не лише технологічну ефективність, а й організаційну сталість, довіру споживачів і підвищення цінності бренду.

Важливою складовою є управління ризиками, які супроводжують впровадження штучного інтелекту. До технічних ризиків належать низька якість даних і явище model drift, що призводить до поступового зниження точності моделей. Організаційні ризики пов'язані зі спротивом персоналу змінам і браком AI-грамотності серед керівників. Бізнес-ризики проявляються через надмірну складність рішень або помилки алгоритмів, що можуть знижувати прибутковість. Етичні ризики охоплюють упередженість моделей, порушення приватності та непрозорість рішень. Для їх мінімізації необхідно впроваджувати регулярний аудит даних, моніторинг моделей, прозорі політики зберігання інформації, навчальні програми для персоналу і системи управління згодою користувачів.

Висновки та перспективи. Таким чином, розроблена методологія E-C-R-S-T-M підходить для проектів маркетингу в електронній комерції завдяки своїй структурованості, гнучкості та комплексному підходу, який враховує специфіку цього ринку. Електронна комерція характеризується високою динамічністю, мультиканальністю продажів, потребою у персоналізації та швидкому реагуванні на зміни поведінки клієнтів, що вимагає чіткого розуміння бізнес-цілей (Expertise), якісних та актуальних даних (Collection), фокусованої розробки ефективних AI-модулів (Research), ретельного тестування і валідації (Scale), глибинної трансформації маркетингових операцій (Transform) і постійного моніторингу з оптимізацією (Maintain). Ця методологія забезпечує прямий зв'язок між ШІ-рішеннями і бізнес-результатами, підтримує інтеграцію трьох типів ШІ (механічного, мислячого, «чуттєвого») для персоналізації клієнтського досвіду, а також включає механізми управління змінами й етичного контролю. Методологія E-C-R-S-T-M формує міцну основу для успішного масштабування інновацій у сфері електронної комерції, забезпечуючи стійкий розвиток маркетингових процесів і конкурентні переваги на ринку.

Список використаних джерел

1.Huang, M.-H., & Rust, R. T. (2021). Artificial intelligence in service. *Journal of the Academy of Marketing Science*, 49(1), 30–50. DOI: 10.1007/s11747-020-00749-9

2.Schultz, K. (2025). *Understanding the role of knowledge intelligence in the CRISP-DM framework: A guide for data science projects*. Enterprise Knowledge. <https://enterprise-knowledge.com/understanding-the-role-of-knowledge-intelligence-in-the-crisp-dm-framework-a-guide-for-data-science-projects/>

3.BA.in.ua. (2025, 28 липеня). *Top-3 підходи до пріоритизації*. <https://www.ba.in.ua/2022/06/28/top-3-pidhody-do-priorityzacziyi/>

Крискун Іван Миколайович
аспірант 2 курсу
Університет економіки та права "КРОК"
(067) 220-75-11
ivan.kriskun@gmail.com

ІНСТРУМЕНТИ УПРАВЛІННЯ ПРОЕКТАМИ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

Постановка задачі. Цифрова економіка, що характеризується високою швидкістю змін, глобалізацією та використанням даних як ключового активу, пред'являє нові вимоги до управління проектами. Традиційні каскадні підходи часто виявляються неефективними через невизначеність вимог, необхідність швидкої адаптації та розподілену природу команд. Актуальним є аналіз сучасних інструментів управління проектами, які забезпечують гнучкість, прозорість та швидкість прийняття рішень в динамічному цифровому середовищі.

Мета дослідження. Метою дослідження є аналіз сучасних інструментів управління проектами, адаптованих до умов цифрової економіки; визначення їх функціональних можливостей, переваг, обмежень та сфер ефективного застосування.

Результати дослідження. Ефективне управління проектами в цифровій економіці базується на комбінації гнучких методологій (Agile, Scrum, Kanban) та спеціалізованих програмних рішень, які автоматизують та структурують роботу. Ці інструменти забезпечують централізоване управління завданнями, співпрацю команди, моніторинг прогресу та аналіз продуктивності на основі даних. [1]

Архітектуру сучасного цифрового інструменту управління проектами можна уявити як єдину платформу, що інтегрує кілька ключових модулів (рис. 1).

Алгоритм уникнення локальних перешкод вимагає від АМР швидкого коригування попередньо встановленого навігаційного маршруту, уникнення перешкод і повернення до глобального маршруту руху відповідно до даних, отриманих від модуля сприйняття навколишнього середовища. До основних алгоритмів уникнення локальних перешкод належать метод потенціального поля (APF), гістограма векторного поля (VFH), підхід динамічного вікна (DWA), метод швидкісних перешкод (VO), методи навчання з підкріпленням (RL) [2].

До основних категорій інструментів належать:

Інструменти для гнучкої розробки (Agile/Scrm): Jira, Azure DevOps, Pivotal Tracker.

Інструменти для візуалізації робочого процесу (Kanban): Trello, Kanbanize.

Універсальні платформи для управління роботою (Work Management): Asana, ClickUp, Wrike.

Інструменти для співпраці та комунікації: Slack, Microsoft Teams, інтегровані з платформами управління проектами.

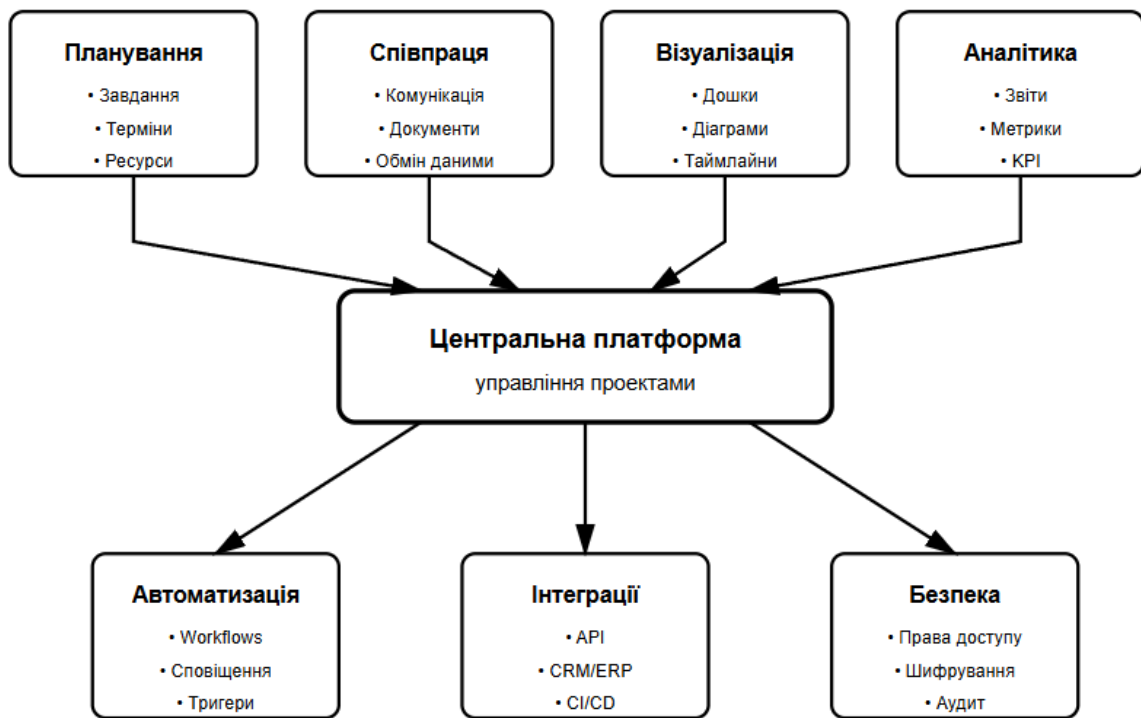


Рис. 1. Узагальнена архітектура цифрового інструменту управління проектами.

Jira (разом із Confluence) є індустріальним стандартом для команд розробки ПЗ, що працюють за методологією Scrum або Kanban. Його переваги — глибока налаштованість робочих процесів (workflows), потужна система звітності (burndown-charts, velocity) та інтеграція з інструментами CI/CD. [3]

Trello базується на парадигмі канбан-дошки, що робить їх інтуїтивно зрозумілими та гнучкими для різних типів завдань — від маркетингових кампаній до організації подій. Вони дозволяють візуалізувати весь потік робіт, обмежити незавершену роботу (WIP limits) і легко перерозподіляти завдання. Їхня слабкість — обмежені можливості для складного планування на рівні портфеля проектів та менш розвинена аналітика.

Asana та ClickUp займають проміжне положення, поєднуючи елементи управління завданнями, проектами та навіть цілями (OKR). Вони пропонують кілька видів подання даних (список, дошка, календар, хронологія), вбудовані шаблони та автоматизації. Це робить їх ідеальними для міжфункціональних команд цифрової економіки. ClickUp відрізняється амбітною метою стати "єдиним робочим простором", інтегруючи також документообіг, час-трекінг та чат.

Критерії вибору інструменту є комплексними та вимагають оцінки низки внутрішніх факторів організації. Насамперед необхідно враховувати масштаб проекту та команди: для невеликих команд або стартапів часто достатніми будуть легкі рішення з низьким порогом входження (наприклад, Trello, Asana), тоді як для великих розподілених команд чи портфеля проектів потрібні потужні платформи з розширеними правами доступу, налаштовуваними робочими

процесами та глибокою аналітикою (Jira, Azure DevOps). Критично важливим є прийнята методологія роботи: інструмент повинен не лише підтримувати (Scrum, Kanban, Waterfall), а й посилювати її принципи, забезпечуючи відповідні артефакти (беклоги, спринт-дошки, діаграми Ганта) та звіти.

Трендом останніх років є активна поява гібридних підходів (Hybrid-Agile) та відповідних налаштувань в інструментах, що дозволяють поєднувати гнучке виконання на рівні команди з водопадним (каскадним) плануванням на рівні портфеля проектів або окремих великих контрактів. Це відображає реальні потреби бізнесу, де замовники часто вимагають фіксованого бюджету, термінів та звітності (характерно для водопаду), але командам необхідна свобода для ітеративної розробки та адаптації до змін.

Висновки та перспективи. В умовах цифрової економіки інструменти управління проектами трансформуються з систем відстеження завдань в центральні платформи для координації роботи, аналізу ефективності та прийняття рішень на основі даних. Проведений аналіз показав, що немає універсального рішення; вибір інструменту має ґрунтуватися на специфіці бізнес-процесів, команд та стратегічних цілей організації.

Перспективою подальшого розвитку є посилення інтеграції штучного інтелекту та машинного навчання в інструменти управління проектами. ШІ може передбачати ризики злагодженості проекту, рекомендувати оптимальне розподіл ресурсів, автоматично класифікувати завдання та аналізувати тональність комунікації в команді для проактивного вирішення потенційних конфліктів. Це перетворить інструменти з реактивних систем планування на проактивні системи підтримки прийняття управлінських рішень.

Список використаних джерел

1. Рябоконь, Н. П., Рябоконь, А. А., & Рябоконь, Б. А. (2018). Впровадження методології Agile: ціннісно орієнтований підхід. Збірник наукових праць Черкаського державного технологічного університету. Серія: Економічні науки, (48), 34-42.
2. HUANG, Jinshan; CHEN, Bohan. Improved 3D UAV Path Planning Algorithm Based on Combined DWA and APF. In: 2024 IEEE 7th International Conference on Information Systems and Computer Aided Education (ICISCAE). IEEE, 2024. p. 469-473.
3. ORTU, Marco, et al. The emotional side of software developers in JIRA. In: Proceedings of the 13th international conference on mining software repositories. 2016. p. 480-483.
4. Бондарчук, А., Жебка, В., Корецька, В., & Шилкіна, А. (2024). Порівняльна характеристика web-орієнтованих інструментів автоматизації освітнього процесу в умовах цифрової трансформації. Публічно-управлінські та цифрові практики, (1), 13-21.