МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ТЕХНОЛОГІЙ ЦИФРОВОГО РОЗВИТКУ

ІІ Міжнародна науково-практична конференція

«СУЧАСНІ АСПЕКТИ ДІДЖИТАЛІЗАЦІЇ ТА ІНФОРМАТИЗАЦІЇ В ПРОГРАМНІЙ ТА КОМП'ЮТЕРНІЙ ІНЖЕНЕРІЇ»

19-21 грудня 2024 року

ЗБІРНИК ТЕЗ

м. Київ

II Міжнародна науково-практична конференція «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії». Збірник тез. – К.: ДУІКТ, 2024.

Даний збірник містить тези учасників конференції, представлених на II Міжнародній науково-практичній конференції «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії», яка проводилась 19-21 грудня 2024 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: digitaldut2022@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

Напрям 1. ДОСВІД СУЧАСНИХ ІТ-КОМПАНІЙ.

Ананченко Олексій Євгенович
Application Security Engineer
компанії Playtech
ananchenko.oe@gmail.com

ДОСВІД ВПРОВАДЖЕННЯ ПРОГРАМИ БЕЗПЕЧНОЇ РОЗРОБКИ В ОРГАНІЗАЦІЯХ

Постановка задачі.

В програму безпечної розробки входить достатньо багато компонентів. Як загальні так і практичних. Але головним компонентом є діалог між AppSec командою і командою розробників. Це такий собі договір між двома командами, AppSec зобов'язується інформувати про усі ризики що пов'язано з вразливостями до команди. Розробники забовязуються виправляти ці ризики у визначений термін. Це можуть бути результати дизайн ревью, сканувань вразливостей у коді, у працюючих программах і тд. Без цього забовязання программа безпечної розробки працювати не буде. Усі сторони мають бути зацікавлені у тому щоб зменшити кількість вразливостей до мінімуму, чим зменшити ризики для бізнесу.

Мета дослідження.

Головною метою програми безпечної розробки є включити елементи безпеки з самого раннього етапу SDLC. Включення безпеки на ранніх етапах розробки програмного забезпечення допомагає мінімізувати потенційних ризиків та забезпечення цілісності продукту. Виправлення вразливостей на початкових стадіях розробки економічно ефективніше, оскільки вартість усунення вад безпеки після впровадження може бути в десятки разів вищою.

Результати дослідження.

Загальним етапом програми безпечної розробки завжди є навчання. Щорічні навчання розробників по написанню безпечного коду є вимогою для успішного проходження сертифікації ISO270001.

Можна використовувати як існуючі платформи для навчання так і створювати свої власні курси.

Вимоги є першим етапом SDLC. Є декілька джерел запитів для нового функціоналу: замовники, користувачі, бізнес аналітики і тд. Коли новий запит попадає в команду розробки він має бути спочатку оброблений, до нього мають бути сформовані конкретні вимоги і очікуваний результат. Тому на цьому етапі також підключають AppSec спеціаліста який перегляне суть нового функціоналу, оцінить наскільки він має вплив на безпеку та додасть рекомендації чи вимоги які потрібно буде врахувати при розробці.[1]

На цьому етапі інженери мають можливість переглянути вже готовий дизайн візуально оцінити які можуть бути ризики і додати свої коментарі. Якщо це велика розробка то також вимагається супроводити дизайн діаграмою інфраструктури, потоків даних, компонентів та логічних зв'язків застосунка.

А також під час дизайн рев'ю робиться моделювання потенційних загроз щоб визначити потенційні загрози в майбутній розробці.

На наступному етапі розробки використовуються автоматизовані інструменти для пошуку вразливостей безпосередньо в вже написаному коді.

Static Application Security Testing (SAST) - це метод аналізу безпеки, який перевіряє вихідний код програми без її виконання, шукаючи відомі шаблони вразливостей та потенційні проблеми безпеки на рівні коду. SAST-інструменти аналізують код рядок за рядком, перевіряючи потенційно небезпечні конструкції, неправильне використання API, небезпечні функції та інші проблеми безпеки, створюючи дерево абстрактного синтаксису (AST) для глибокого аналізу.

Хоча цей сканер проводить найглибше сканування коду, він також генерує велику кількість False Positive, банально через те що він не має ширшої картини нашого додатку, не розуміє інфраструктуру, не розуміє звязки між різними сервісами. Тому проводиться тріаж знайдених вразливостей. Верифікується чи дійсно вони несуть загрозу, а також відбувається тісна робота з вендором який може налаштовувати свій інструмент під потреби команди.

Software Composition Analysis (SCA) - це автоматизований сканер якийм ми перевіряємо та аналізуємо сторонні компонентів, бібліотек та залежностей, які використовуються у програмному забезпеченні, на предмет відомих вразливостей та проблем безпеки.

Цей інструмент дозволяє побачити які бібліотеки використовують розробники, які з них давно вже потрібно було оновити і в яких є вразливості. Інструмент порівняє знайдені бібліотеки і підкаже до якої версії слід оновитись.

Також важливо щоб не було проблем з ліцензіями. Коли сторонній компонент поширюється безкоштовно тільки за умови що продукт в якому його використовують теж буде безкоштовним.

Сканування відбувається набагато швидше ніж у SAST, SCA намагається збілдити софт, при цьому дістає усі залежності які використовуються в продукті, робить їх хеш і відсилає до вендора на сервер, де той порівнюється з вже існуючою базою вразливостей і повертає результат.[2]

Коли застосунок готовий і є робоча версія відбувається динамічне сканування (DAST) та сканування на проникнення (Pen.Test)

Тестування проходять у форматі емуляції атаки на застосунок. Виконуються усі ті ж техніки які б виконував зловмисник.

DAST може інтегруватись в CI/CD pipeline і виконуватись автоматично під час кожного білда.

Також на цьому етапі часто користуються послугами контракторів, яким замовляють тестування функціональності.

Виміряти результат роботи програми безпечної розробки складно, особливо коли виправлення вразливостей залежить від інших команд.

Є декілька метрик за якими можна слідкувати:

- Як зменшується бізнес-ризик протягом певного періоду часу (місяць, квартал, рік)
- Наскільки швидко команди реагують на нові ризики

- Як часто вразливості повторно зявляться в додатку
- Який рівень покриття мають SAST, SCA, DAST і тд.

Якщо программа безпечної розробки тільки впроваджується то доцільно почати з вимірювання кількість вразливостей, і їх трендів, кількість збільшується чи зменшується.

Висновки та перспективи.

Щоб побудувати ефективну програму безпечної розробки потрібно визначитись з планом своїх дій на найближчі 3 роки. Зрозуміти які цілі перед собою ставить бізнес Чи планується отримусвати сертифікати і проходити аудити. Чи будуть працювати з персональними данними користувачів які підпадають під міжнародні стандарти GDPR. Потрібно ідентифікувати прогалини в безпеці, чого не вистачає. Спланувати де мають бути впроваджені додаткові заходи безпеки які наразі відсутні. Визначити потенційні загрози які можуть загрожувати організації і відштовхуючись від цього будувати свою програму безпечної розробки.

Список використаних джерел

1. Microsoft. Security Development Lifecycle (SDL) Practices Url: https://www.microsoft.com/en-us/securityengineering/sdl/practices?oneroute=true (date of access: 01.01.2024)
2. Fisher D., Application Security Program Handbook. MANNING Shelter Island, 2022. 207-210p.

Свириденко Микола Олександрович
Agile Coach
компанії MINT
(073)-090-59-19
kswiridenko@gmail.com

GENERATIVE AI: ТЕХНОЛОГІЧНИЙ ПРОРИВ ЧИ ВИКЛИК ДЛЯ ТЕХНІЧНИХ КОМАНД

Постановка задачі. Generative AI (генеративний штучний інтелект) декларується як технологія, що значно оптимізує робочі процеси, скорочуючи час виконання задач до 30-40%. Очікується, що це призведе до підвищення якості та швидкості доставки функціоналу. Водночас постає питання адаптації технічних команд до нових інструментів та інтеграції AI у складні проєкти.

Мета дослідження. Дослідити реальний вплив Generative AI на ефективність роботи технічних команд, виявити виклики та можливості інтеграції технології в існуючі процеси. Визначити ключові фактори, що впливають на успішність використання AI.

Результати дослідження. Дослідження виявило, що Generative AI суттєво скорочує час виконання рутинних завдань, таких як генерація програмного коду або текстів, що дозволяє знижувати навантаження на розробників. Водночас залишаються виклики, що пов'язані зі системними аспектами інтеграції результатів AI у складні процеси.

Необхідні додаткові ресурси для перевірки та рефакторингу згенерованих результатів, оскільки якість роботи AI потребує підтвердження людиною. Крім того, залишаються невизначеності у розподілі відповідальності за помилки, що з'являються лише на етапі тестування або експлуатації.

Generative AI допомагає зменшувати технічний борг за рахунок автоматизації рутинних завдань, таких як оновлення документації або створення тестових сценаріїв. Однак успішне впровадження цієї технології вимагає чіткого стратегічного планування для уникнення хаотичного впровадження, що може призвести до неефективного використання ресурсів. Завдяки можливості автоматизувати процеси, Generative AI дозволяє технічним командам зосередитися на складніших та інноваційних завданнях, що вимагають творчого підходу.

Соціальний аспект інтеграції технології включає необхідність навчання співробітників для ефективного використання AI. Це також стосується розробки нових підходів до взаємодії команд із штучним інтелектом, що включає етичні аспекти та стандарти оцінки результатів. Слід зазначити, що впровадження Generative AI викликає певний опір серед співробітників через страх втрати робочих місць або зниження значущості їхньої роботи. Подолання цих бар’єрів потребує комунікації переваг технології та її безпосереднього впливу на розвиток компаній.

Висновки. Використання Generative AI відкриває значні можливості для оптимізації процесів і підвищення ефективності роботи технічних команд. Успіх залежить від якісної інтеграції, навчання співробітників і врахування соціально-організаційних факторів. Generative AI може стати ключовим інструментом у реалізації інноваційних рішень за умови правильної адаптації до специфіки організацій. Майбутні дослідження повинні зосереджуватися на вдосконаленні методів контролю якості, адаптації процесів та оцінці довгострокових соціальних і економічних наслідків інтеграції AI в бізнес-процеси.

Список використаних джерел

1. Brown T., Mann B., Ryder N. et al. (2020). Language Models are Few-Shot Learners. Advances in Neural Information Processing Systems, 33, 1877-1901.

2. Ramesh A., Pavlov M., Goh G. et al. (2021). Zero-Shot Text-to-Image Generation. Proceedings of the International Conference on Machine Learning, 139, 8821-8831.

3. Dosovitskiy A., Beyer L., Kolesnikov A. et al. (2021). An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale. International Conference on Learning Representations, Vienna, Austria, 12-14.

4. Patterson D., Gonzalez J., Le Q. et al. (2021). Carbon Emissions and Large Neural Network Training. Communications of the ACM, 64(12), 44-48.

Напрям 2. СУЧАСНІ АСПЕКТИ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.

Аронов Андрій Олексійович,
к.т.н., доцент кафедри технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій
a.aronov@duikt.edu.ua

ВПЛИВ LAZY LOADING НА ПРОДУКТИВНІСТЬ ЗАВАНТАЖЕННЯ СТОРІНОК ВЕБ-САЙТІВ

Постановка задачі. Швидкість завантаження сторінок веб-сайтів є важливим чинником, який безпосередньо впливає на користувацький досвід і загальну ефективність веб-сайтів. З накопиченням все більшої кількості інформації на веб-сайтах, наприклад, з накопиченням кількості замовлень у особистому кабінеті клієнта в інтернет-магазині, швидкість завантаження всіх замовлень суттєво знижується. Lazy loading — це технологія завантаження контенту на сторінці веб-сайту, при якій ресурси-компоненти завантажуються не відразу при первинному завантаженні сторінки, а тоді, коли вони стають необхідними для відображення [1].

Мета дослідження. Підвищити швидкість завантаження сторінок веб-сайту зменшуючи навантаження на сервер за допомогою Lazy loading, основна ідея якого полягає у запиті тільки необхідної інформації для відображення на даний момент часу. Дослідити вплив використання вказаної технології на досвід використання веб-сайту.

Результати дослідження. При наявності у базі даних інтернет-магазину декількох тисяч замовлень, які складаються з декількох різних товарів кожне – час, витрачений на завантаження сторінки із замовленнями одного активного клієнта може сягати десятки секунд, що є неприпустимим для роботи веб-сайту. Надмірне навантаження на сервер можна суттєво знизити використовуючи технологію Lazy loading, яка дозволяє скоротити час до першого рендеру сторінки FCP (First Contentful Paint) та швидкості завантаження сторінки. Технологія дозволяє завантажувати лише той контент, який видимий на екрані користувача, в той час як інші ресурси залишаються неактивними до тих пір, поки вони не стануть необхідними [2].

Для відкладеного завантаження зображень та фреймів можна використовувати атрибут *loading* з параметром *lazy.*

```
<img src="order.jpg" loading="lazy" alt="image title" />
```

Для завантаження не тільки зображень а, наприклад, частини історії замовлень можна використати найпростішу функцію з параметром дати і вивантажувати тільки останні замовлення. Блок-схема процесу завантаження сторінки із замовленнями представлено на рис.1.

```
function load_cabinet_orders(month, year) {
```

```
        if( $("#date_" + month + "_" + year).html() == "" )
            $("#date_" + month + "_" + year).load("/orders/load/" + month + "/" + year);
}
```

Користувачі веб-сайту швидше отримують одну і ту ж кількість видимої інформації на сторінці сайті за менший час.

Під час скролінгу сторінки автоматично надсилається запит на отримання наступної порції даних.

```
$(window).scroll(function() {
    if($(this).scrollTop() > n) { ... load_cabinet_orders(month, year) }
}
```

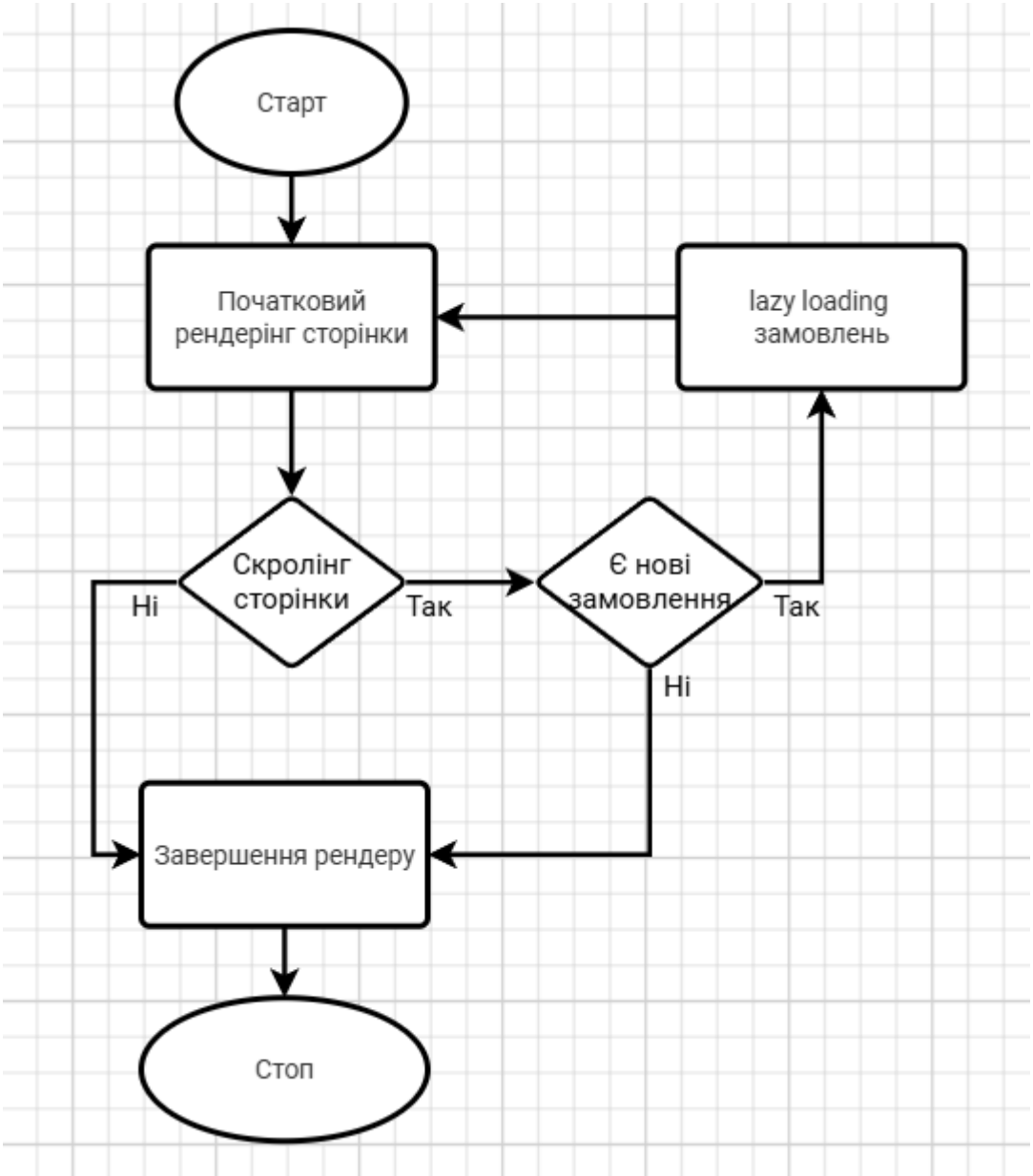

Рис. 1. Блок-схема процесу завантаження сторінки

Дослідження показало що для інтернет-магазину з кількістю замовлень 40 тисяч за допомогою технології Lazy loading параметр FCP було знижено з 9 секунд до 1,2 секунди, а завантаження особистої сторінки клієнта стало швидше на більш ніж 20 секунд і становило 3.4 секунди при цьому кількість інформації,

замовлень, яку бачить клієнт, коли сторінка завантажується в обох випадках однакова.

Висновки. Lazy loading — це ефективна технологія для оптимізації роботи веб-сайтів, особливо для покращення швидкості завантаження їх сторінок та зменшення навантаження на сервер. Використання цієї технології дозволяє значно покращити користувацький досвід, особливо на мобільних пристроях, де швидкість інтернет-з'єднання є важливим фактором.

Список використаних джерел

1. Lazy loading – Web Perfomance MDN URL: https://developer.mozilla.org/en-US/docs/Web/Performance/Lazy_loading

2. First Contentful Paint Lighthouse | Chrome for Developers URL: https://developer.chrome.com/docs/lighthouse/performance/first-contentful-paint.

Коваль Софія Олегівна
студентка 3 курсу, групи ІП-21
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
(096) 190-36-37
sofiiakoval5555@gmail.com
Науковий керівник: **Поперешняк Світлана Володимирівна**
к.ф.-м.н., доцент, доцент кафедри ІПІ ФІОТ
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
(098)-645-546-2
spopereshnyak@gmail.com

ІННОВАЦІЇ У СИСТЕМАХ УПРАВЛІННЯ ПОДІЯМИ: МУЛЬТИПЛАТФОРМЕННИЙ ПІДХІД ДО ПОБУДОВИ ПЕРСОНАЛІЗОВАНИХ РЕКОМЕНДАЦІЙ

Постановка задачі. У сучасному світі організація соціальних заходів вимагає врахування індивідуальних потреб та уподобань користувачів. Більшість платформ для управління подіями (наприклад, Eventbrite, Meetup) фокусуються лише на базових критеріях вибору заходів, таких як місце проведення, час та тип події. Однак вони частково враховують настрій та особисті інтереси користувачів, що обмежує персоналізацію. Це призводить до зниження зацікавленості та залученості учасників [1].

Задачею є розробка системи управління подіями, яка використовує рекомендаційні алгоритми, що базуються на аналізі настрою та інтересів користувачів. Система повинна забезпечити мультиплатформенну доступність (мобільний і веб-додаток) та ефективно обробляти дані за допомогою сучасних технологій.

Мета дослідження. Метою цього дослідження є створення інноваційної системи управління подіями, яка надає персоналізовані рекомендації на основі настрою та інтересів користувачів. Для досягнення цієї мети було визначено такі підходи: розробка рекомендаційного модуля з використанням машинного навчання; реалізація мультиплатформенного клієнтського інтерфейсу на основі React Native; використання монолітної архітектури серверної частини з Node.js і MongoDB для оптимізації процесу розробки і підтримки.

Результати дослідження. Результатом дослідження стала розробка прототипу системи, що складається з трьох основних компонентів. Серверна частина, реалізована на Node.js з базою даних MongoDB, забезпечує обробку запитів, зберігання інформації про події та користувачів, а також роботу рекомендаційного алгоритму. Рекомендаційний модуль використовує машинне навчання для аналізу настрою користувачів, базується на їхніх оцінках, відгуках або інтеграції з соціальними мережами, а також визначає інтереси користувачів за категоріями подій, які вони відвідували раніше. Клієнтська частина,

побудована на React Native з використанням Expo [3], забезпечує одночасну підтримку веб- та мобільних додатків.

Використання Expo як надбудови над React Native дозволило інтегрувати функціонал, що забезпечує роботу додатку нативно на iOS, Android та в веб-середовищі. Expo також спрощує масштабування додатку та впровадження функцій, таких як live-оновлення та швидкий доступ до нових можливостей платформи. Такий підхід значно підвищив ефективність розробки та забезпечив зручність у підтримці проєкту [2].

Рекомендаційний механізм включає збір даних, аналіз настрою за допомогою NLP-моделей, кластеризацію користувачів за інтересами та настроєм, а також формування рекомендацій через ранжування подій за рівнем релевантності для кожного користувача [4].

Схема архітектури системи представлена нижче на рисунку 1.1. Ця діаграма детально зображує компоненти системи, такі як веб- та мобільний інтерфейси, бекенд-сервер, база даних та зовнішні сервіси. Вона також показує, як ці компоненти взаємодіють між собою через HTTP-запити, зберігання даних та взаємодію з Google API для обробки адрес.

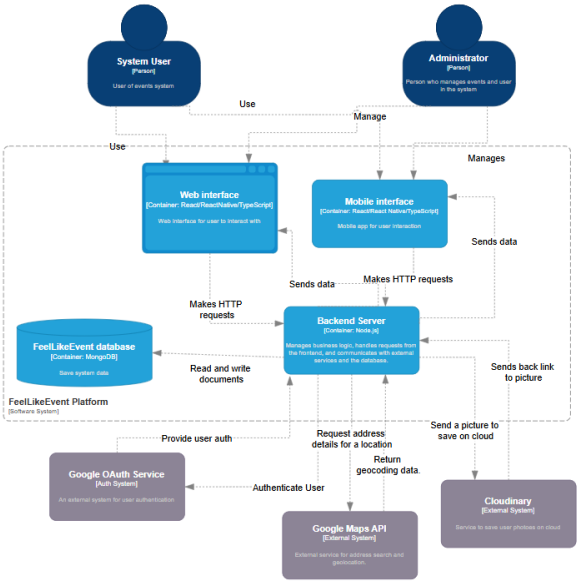

Рис. 1. Діаграма контейнерів

Висновки та перспективи. У результаті дослідження було створено прототип системи управління подіями з рекомендаційним модулем, який дозволяє персоналізувати вибір заходів відповідно до настрою та інтересів користувачів. Запропоновані рішення демонструють високу ефективність рекомендаційного алгоритму та гнучкість мультиплатформенної реалізації. Основними перевагами системи є підвищення рівня персоналізації користувацького досвіду, зниження витрат на розробку завдяки використанню React Native і Expo, а також спрощення підтримки та масштабування системи. Подальші кроки включають інтеграцію додаткових джерел даних, наприклад API соціальних мереж, та вдосконалення алгоритмів прогнозування для підвищення точності рекомендацій.

Список використаних джерел

1. Jain, S., & Srivastava, S. (2022). "Personalized Event Recommendation Systems: A Review." International Journal of Computer Applications, 175(4), 25-30.
2. Mehta, D., & Patel, M. (2022). "Multi-platform Approach to Building Scalable Event Management Systems." Proceedings of the 2022 International Conference on Cloud Computing and Virtualization, 172-179.
3. Expo Documentation. [Online resource]. Available: https://expo.dev .
4. Frontiers in Big Data, "Natural Language Processing for Recommender Systems," Frontiers in Big Data, 2024. Available at: https://www.frontiersin.org/research-topics/49105/natural-language-processing-for-recommender-systems .

Колодюк Андрій Васильович
аспірант 3 курсу, спеціальність 121 Інженерія програмного забезпечення,
Державного університету інформаційно-комунікаційних технологій
a.kolodiuk@duikt.edu.ua
Науковий керівник: **Жебка Вікторія Вікторівна**,
доктор технічних наук, професор, завідувач кафедри Технологій цифрового розвитку
Державного університету інформаційно-комунікаційних технологій, м.Київ

ОЦІНКА ЕФЕКТИВНОСТІ МІКРСЕРВІСНОЇ АРХІТЕКТУРИ В УМОВАХ ВИСОКИХ НАВАНТАЖЕНЬ: ДОСВІД ТА ПЕРСПЕКТИВИ ДЛЯ КОРПОРАТИВНИХ ВЕБ-ДОДАТКІВ

Постановка задачі. Сучасні корпоративні веб-додатки потребують високої надійності, масштабованості та здатності адаптуватися до значних змін в обсязі запитів. Мікросервісна архітектура (МСА) стає основою для побудови таких додатків завдяки своїй здатності забезпечити незалежне масштабування та високу доступність [1]. Однак, при значних навантаженнях важливо оцінити ефективність застосування МСА для забезпечення стабільної роботи додатків в умовах високої інтенсивності запитів [2].

Мета дослідження. Метою дослідження є оцінка ефективності мікросервісної архітектури у корпоративних веб-додатках, коли система працює в умовах високих навантажень, а також аналіз її впливу на споживчі характеристики, такі як швидкість обробки запитів, масштабованість, доступність та стійкість до відмов. Також планується розглянути методи оптимізації роботи мікросервісів для досягнення максимальної продуктивності в умовах великих навантажень.

Результати дослідження. У дослідженні було проведено кілька експериментів для оцінки ефективності мікросервісної архітектури в умовах високих навантажень. Тестування проводилось на корпоративних веб-додатках, розроблених за допомогою мікросервісної та монолітної архітектури, з метою порівняння їх ефективності за різними параметрами: швидкість обробки запитів, час відгуку, масштабованість та стійкість до відмов.

1. Швидкість обробки запитів: Мікросервісна архітектура показала суттєве зниження часу обробки запитів при збільшенні кількості паралельних запитів завдяки можливості окремого масштабування мікросервісів, які мають більшу потребу у ресурсах. Це забезпечує гнучке управління ресурсами та дозволяє швидко збільшувати обробку запитів при високих навантаженнях.

2. Масштабованість: Мікросервіси продемонстрували значно більшу гнучкість у масштабуванні. В умовах високих навантажень, наприклад, при проведенні тестів навантаження на 100 000 паралельних запитів, система, побудована на мікросервісах, змогла автоматично масштабувати окремі компоненти, що забезпечило збереження стабільності роботи системи. У порівнянні з монолітною архітектурою, де для масштабування необхідно було

масштабувати всю систему цілком, мікросервіси забезпечили значно вищу ефективність.

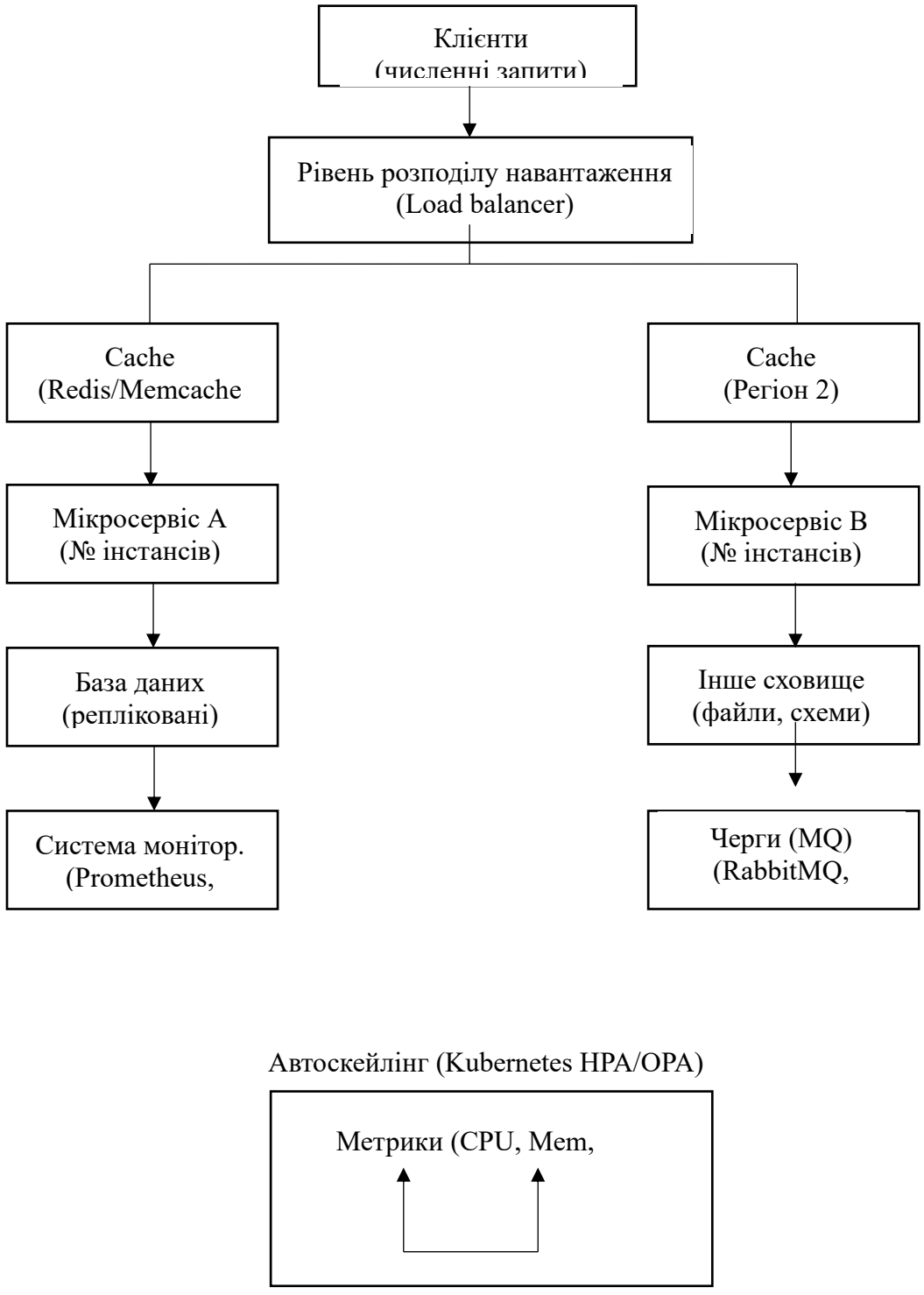

Рис. 1. Умовна ASCII-схема

3. Доступність та стійкість до відмов: Однією з ключових переваг мікросервісної архітектури є підвищена доступність. Завдяки принципу автономності, навіть у разі відмови одного з мікросервісів, решта системи продовжувала працювати без значних збоїв. В умовах великих навантажень мікросервіси продемонстрували меншу кількість відмов та кращу стійкість до

навантажень в порівнянні з монолітними системами, де відмова одного з компонентів може призвести до збою всього додатку.

4. Оптимізація через кешування та балансування навантаження: Одним із найбільш ефективних методів оптимізації в рамках мікросервісної архітектури є використання кешування на рівні мікросервісів та застосування розподіленого балансування навантаження. Це дозволяє знизити навантаження на основні сервіси та зменшити затримки при обробці запитів. Тести показали, що з правильно налаштованим кешуванням час обробки запитів можна зменшити на 30-40%. Нижче подана схема, яка показує, як оптимізація через кешування та розумне балансування навантаження, у поєднанні з динамічним масштабуванням та моніторингом, забезпечує ефективну роботу мікросервісної архітектури при високих навантаженнях.

Висновки та перспективи. Мікросервісна архітектура забезпечує значну перевагу в умовах високих навантажень завдяки можливості гнучкого масштабування, автономному управлінню ресурсами та високій стійкості до відмов.

Враховуючи результати дослідження, можна зробити висновок, що мікросервісна архітектура є оптимальним рішенням для корпоративних веб-додатків, що повинні працювати в умовах постійного зростання трафіку та високих навантажень.

Для забезпечення високої ефективності мікросервісів необхідно використовувати сучасні методи оптимізації, такі як кешування, балансування навантаження та автоматичне масштабування, що допомагає мінімізувати затримки та підвищити продуктивність системи.

Дослідження також показало, що хоча мікросервіси забезпечують вищу гнучкість і ефективність, їх впровадження вимагає ретельного проектування, налаштування інфраструктури та використання інструментів моніторингу для досягнення оптимальних результатів.

Список використаних джерел

1. Indrasiri, K., Siriwardena, P. Microservices for the Enterprise: Designing, Developing, and Deploying. 2nd ed. Apress, 2023. – p. 35-48.

2. Mohanty, S. R., Scott, A., Davis, J. Cloud-native Microservices with Kubernetes: Building Scalable and Resilient Cloud-native Architectures. Packt Publishing, 2023. – p. 45-60.

Копич Данило Олексійович
молодший науковий співробітник
Інститут спеціального зв'язку та захисту інформації
(050) 636-73-22
danyla.kopych@gmail.com

ПІДТРИМКА ПРОЦЕСУ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЙ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ

Постановка задачі. Розвиток інформаційних технологій та інтенсивне впровадження штучного інтелекту (ШІ) докорінно змінюють підходи до створення програмного забезпечення. ШІ уже сьогодні демонструє значний потенціал в оптимізації процесів розробки, автоматизації рутинних завдань і підвищенні якості програмних продуктів. Актуальність дослідження обумовлена необхідністю адаптації сучасних інструментів і методологій, включаючи генеративний ШІ, до вимог швидкозмінного ринку.

Мета дослідження. Метою дослідження є підвищення ефективності основних процесів життєвого циклу програмного забезпечення за рахунок використанням сучасних інструментів генеративного штучного інтелекту.

Результати дослідження. У сучасному світі інформаційних технологій процес розробки програмного забезпечення стає дедалі складнішим, вимагаючи впровадження передових технологій для підвищення ефективності та забезпечення високої якості кінцевого продукту. Інтеграція ГШІ у процес створення програмного забезпечення сприяє автоматизації рутинних завдань, генеруванню рекомендацій, підвищенню якості коду та зменшенню ймовірності помилок. Ефективні запити відіграють ключову роль в отриманні корисних відповідей від моделей ШІ. Важливість добре сформульованих запитів полягає у мінімізації непорозумінь між користувачем та моделлю ШІ [1].

Генеративний штучний інтелект знаходить застосування на всіх етапах розробки програмного забезпечення, надаючи командам розробників цінну допомогу та інструменти для підвищення продуктивності [2].

У рамках роботи пропонується методика для автоматизації ключових етапів розробки програмного забезпечення з використанням ГШІ. Розроблена підсистема надає інтелектуальну підтримку командам розробників, допомагаючи вирішувати різноманітні завдання, від аналізу вимог до генерації коду та тестування.

Підсистема використовує ГШІ для аналізу вхідних даних і технічних завдань від замовників, що дозволяє формувати структуровані та зрозумілі вимоги. Вона уточнює та пропонує варіанти формулювань, зменшуючи ризик неоднозначностей. Крім того, ШІ автоматично створює документ специфікацій, готовий до інтеграції у робочий процес.

На етапі проектування підсистема надає рекомендації щодо архітектури системи та вибору відповідних патернів проектування. Вона сприяє створенню

оптимальних структур для великих проєктів, підвищуючи ефективність проектування. Система також пропонує варіанти організації модулів і компонентів, що допомагає уніфікувати підхід до проєктування.

У процесі програмування ГШІ забезпечує автоматичне написання фрагментів коду та шаблонних функцій, орієнтуючись на контекст завдання. Він може генерувати вихідний код, зменшуючи обсяг ручної роботи, а також допомагає в рефакторингу існуючого коду, підвищуючи його якість і підтримуваність [3].

На етапі тестування підсистема генерує тестові сценарії на основі специфікацій, що суттєво скорочує час на їх ручне створення. Вона аналізує результати тестування, виявляє слабкі місця у коді та пропонує варіанти їх покращення.

Функція автоматизації документування забезпечує генерацію актуальних технічних інструкцій і користувацької документації. Це дозволяє швидко оновлювати документацію після внесення змін у код, підтримуючи її релевантність і повноту.

Завдяки автоматизації рутинних завдань, інтелектуальним рекомендаціям та можливості генерувати код, така підсистема значно знижує навантаження на фахівців, дозволяючи їм зосередитися на стратегічно важливих аспектах проекту.

Висновки та перспективи. Впровадження підсистеми підтримки процесу розробки програмного забезпечення, що базується на генеративному штучному інтелекті, відкриває нові горизонти для оптимізації роботи розробників. Така підсистема сприяє автоматизації повторюваних завдань, мінімізуючи витрати часу та ресурсів, і дозволяє зосередитися на більш складних та творчих аспектах роботи. Використання генеративного ШІ сприяє підвищенню якості програмного коду, вдосконаленню архітектурних рішень, а також спрощенню процесів тестування та супроводу. У перспективі це не лише підвищить продуктивність команд розробників, але й створить передумови для інтеграції більш складних і масштабних рішень у програмне забезпечення.

Список використаних джерел

1. White, Jules, et al. A prompt pattern catalog to enhance prompt engineering with chatgpt. arXiv preprint arXiv:2302.11382, 2023. URL: https://arxiv.org/pdf/2302.11382.

2. Hamdi, Mohammed, and Lewy D. Kim. "A Prompt-Based Approach for Software Development." 2023 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, 2023. URL: https://american-cse.org/csci2023-ieee/pdfs/CSCI2023-47UoKEqjHou6fHnm3C9aVb/615100b613/615100b613.pdf.

3. Liu, Yue, et al. Refining chatgpt-generated code: Characterizing and mitigating code quality issues. ACM Transactions on Software Engineering and Methodology, 2024, 33.5: 1-26 URL: https://arxiv.org/pdf/2307.12596.

Корнієнко Олексій Олексійович
Аспірант 2 курсу, група КН-23
Інститут програмних систем НАНУ
067 767 88 66
oleksiikorniienko@gmail.com
Науковий керівник: **Рогушина Юлія Віталіївна**
кандидат фізико-математичних наук, доцент, старший науковий співробітник,
Інститут програмних систем НАН України

АЛГОРИТМ ОПТИМІЗАЦІЇ МАТЕРІАЛЬНИХ І ІНФОРМАЦІЙНИХ ПОТОКІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ КЛІЄНТІВ В БІЗНЕС-ПРОЕКТАХ

Постановка задачі та мета дослідження. На теперішній час епоха масового виробництва перетворюється в епоху виробництва на основі бізнес-проектів [1]. Сьогодні обсяги виробництва значно швидше досягають кількісного піку, однак скорочення виробничого обсягу здійснюється різко у зв'язку з модифікацією продукту [2]. Сучасні види життєвих циклів підвищують складність виробничих процесів, так як експоненціально зростає кількість моделей та варіанти продукції. Надійне постачання індивідуальних продуктів має найвищий пріоритет на відкритих міжнародних ринках, і цей пріоритет дедалі більше визначає потребу в розвитку продуктів, процесів і виробничих потужностей [3; 4]. Фізичний рівень системи забезпечення виробництва повинен піддаватись гнучким конфігураціям, а підприємство-виробник з власною технічною інфраструктурою, включно з нерухомими площами, повинно піддаватись швидкій трансформації. Логічний рівень вимагає систем планування, здатних реагувати на зміни в дизайні продукту [5]. Таким чином, оптимізація розподілення ресурсів є актуальною проблемою для виробництва.

Результати. Розглянемо виробництво у вигляді системи масового обслуговування (СМО), як це представлено на рисунку 1.

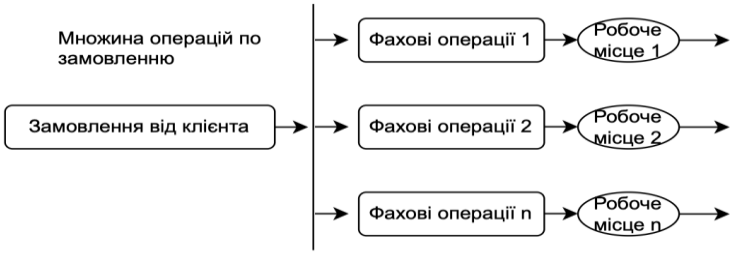

Рис. 1. Модель виробництва у вигляді системи масового обслуговування

Система масового обслуговування характеризується числом каналів обслуговування n, середнім числом вимог λ, що надходять в одиницю часу, $\frac{1}{\mu}$ - середній інтервал часу обслуговування однієї заявки, що її може обслужити один

канал (або n каналів). Інтенсивність обслуговування, або коефіцієнт використання Ψ визначається наступним чином

$$\Psi = \frac{\lambda}{\mu} \quad (1)$$

Основними показниками роботи СМО є:

1. Імовірність $P_{вільна}$ того, що система перебуває у вільному стані та визначається за формулою

$$P_{вільна} = \frac{1}{\sum_{k=1}^{n} \frac{\Psi^k}{k!} + \frac{\Psi^{n+1}}{n \cdot (n - \Psi)}} \quad (2)$$

2. Імовірність $P_{черга}$ того, що замовлення перебуватиме у черзі та визначається за формулою

$$P_{черга} = \frac{\Psi^n}{n! \cdot (n - \Psi)} \cdot P_{вільна} \quad (3)$$

3. Довжина черги $L_{черги}$ і визначається за формулою

$$L_{черги} = \frac{\Psi^{n+1}}{(n-1)! \cdot (n - \Psi)^2} \cdot P_{вільна} \quad (4)$$

4. Середня кількість заявок $Or_{середня}$ в системі і визначається за формулою

$$Or_{середня} = L_{черги} + \Psi \quad (5)$$

5. Середній час $T_{черги}$ перебування заявок у черзі і визначається за формулою

$$T_{черги} = \frac{L_{черги}}{\lambda} \quad (6)$$

6. Середній час $T_{середній}$ перебування заявки у системі та визначається за формулою

$$T_{середній} = \frac{Or_{середня}}{\lambda} \quad (7)$$

На рисунку 2 подано операції для формування динамічної карти потоку створення цінності.

Висновки. Запропоновано алгоритм оптимізації матеріальних та інформаційних потоків на основі моделі систем масового обслуговування, що дозволяє ефективніше враховувати гнучкі конфігурації виробництва порівняно з існуючими методами картування потоку створення цінності, оскільки використовує додаткові параметри, такі як інтенсивність обслуговування, довжина черги та середній час перебування заявки в системі, на відміну від методів, представлених у класичних концепціях ощадливого виробництва.

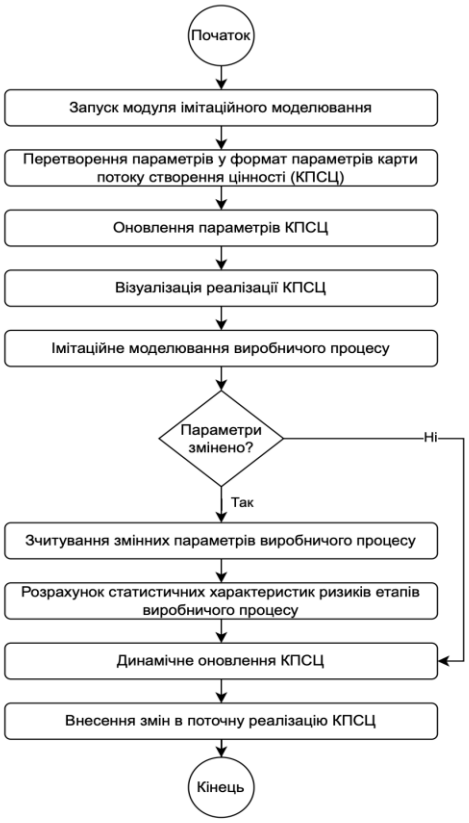

Рис. 2. Алгоритм формування динамічної карти потоку створення цінності

Список використаних джерел

1. Gomez Paredes F. J., Godinho Filho M., Thurer M., Fernandes N. O., Chiappeta Jab- bour C. J. Factors for chossing production control systems in make-to-order shops: a systematic literature review. *Journal of Intelligent Manufacturing*, 2020. DOI 10.1007/s10845-020-01673-z

2. Lu Y., Xu X. Resource virtualization: A core technology for developing cyber-physical production systems. *Journal of Manufacturing Systems*, 2018, vol. 47, pp. 128–140. DOI 10.1016/j.jmsy.2018.05.003

3. Sylla A., Guillon D., Vareilles E., Aldanondo M., Coudert T., Geneste L. Configuration knowledge modeling: How to extend configuration from assemble / make to order towards engineer to order for the bidding process. *Computers in Industry*, 2018, vol. 99, pp. 29–41. DOI 10.1016/j.compind.2018.03.019

4. Qiu S., Ming X., Sallak M., Lu J. Joint optimization of production and condition-based maintenance scheduling for make-to-order manufacturing systems. *Computers & Industrial Engineering*, 2021, vol. 162. DOI 10.1016/j.cie.2021.107753

5. Kishimoto K., Medina G., Sotelo F., Raymundo C. Application of Lean Manufacturing Techniques to Increase On-Time Deliveries: Case Study of a Metalworking Company with a Make-to-Order Environment in Peru. *Human Interaction and Emerging Technologies. IHIET 2019. Advances in Intelligent Systems and Computing*, 2020, vol. 1018. DOI 10.1007/978-3030-25629-6_148

Косенко Денис Максимович,
студент групи ПДМ-62,
спеціальність 121 Інженерія програмного забезпечення,
Державного університету інформаційно-комунікаційних технологій
denhelper90@gmail.com
Науковий керівник: **Гребенюк Віктор Вікторович**,
доктор філософії (PhD),
доцент кафедри Інженерії програмного забезпечення
Державного університету інформаційно-комунікаційних технологій

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ЩО РЕАЛІЗУЄ МЕТОД ПРОЦЕДУРНОЇ ГЕНЕРАЦІЇ ОБ'ЄКТІВ ІГРОВОГО СВІТУ

Постановка задачі. Розробка програмного забезпечення, що реалізує адаптивний метод процедурної генерації ігрових об'єктів із використанням алгоритмів шуму Перліна та модульного підходу до структурування ігрового середовища. Завдання полягає у створенні системи, здатної автоматично генерувати варіативні карти з розташуванням об'єктів відповідно до заданих параметрів.

Мета дослідження. Визначення оптимальних методів процедурної генерації карт у жанрі Tower Defence, що дозволяють створювати динамічні та варіативні рівні, які відповідають сучасним вимогам геймдизайну.

Результати дослідження. У рамках дослідження було розроблено програмний модуль, який інтегрується у середовище Unity та реалізує процедурну генерацію ігрових карт із використанням шуму Перліна та модульного підходу до розподілу об'єктів. Система базується на використанні кольорової текстурної карти, яка виконує роль основного шаблону для визначення областей, призначених для розташування різних типів об'єктів, таких як перепони, декоративні елементи та ключові ігрові структури.

Алгоритм шуму Перліна забезпечує створення плавних переходів у текстурах, що надає картам природного вигляду, а модульний підхід дозволяє динамічно структурувати рівні на логічно завершені регіони. Кожен регіон відповідає певній функціональності: наприклад, стартовій точці ворогів, зонам атаки чи перешкодам, що додає гнучкості у налаштуванні дизайну рівнів.

Для забезпечення коректності розташування об'єктів було впроваджено механізм перевірки на колізії. Це дозволяє уникати накладання елементів або їх розташування поза межами ігрового простору. Перевірка працює на етапі генерації та гарантує узгодженість між усіма елементами карти.

Окрім базового генератора, було реалізовано додаткові інструменти для налаштування параметрів генерації. Наприклад, можливість змінювати масштаб текстур дозволяє створювати карти із різним рівнем деталізації. Інтерактивне коригування частоти шуму Перліна дає змогу впливати на щільність об'єктів, а налаштування параметрів регіональної модульності дозволяє створювати рівні як із чітко визначеною структурою, так і з більш випадковим розташуванням.

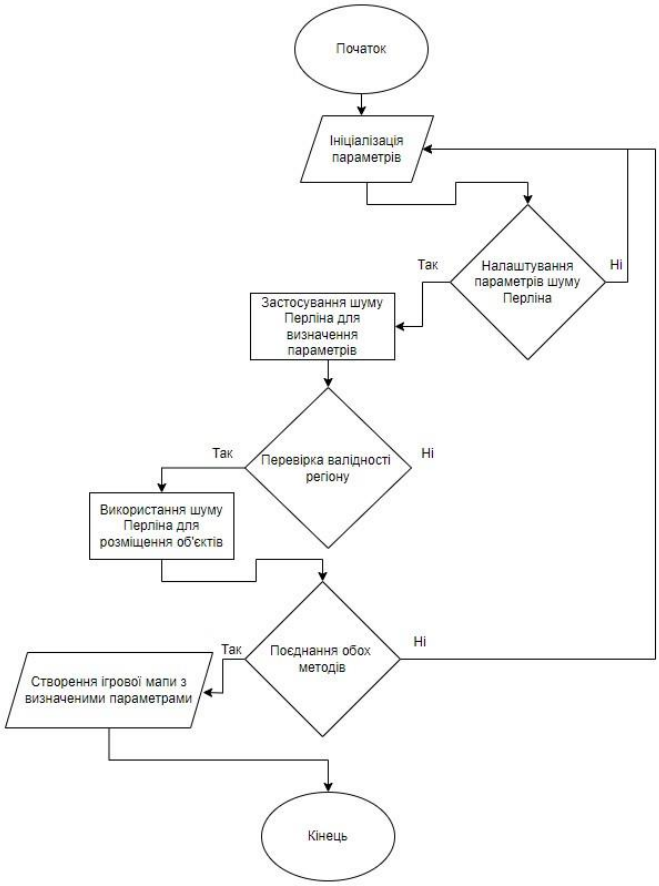

Рис. 1. Блок-схема методу

Система пройшла тестування на різних конфігураціях ігрових рівнів. Було встановлено, що комбінація шуму Перліна з модульною структурою забезпечує оптимальний баланс між випадковістю та передбачуваною логікою розташування об'єктів. Отримані результати підтверджують ефективність підходу: генератор здатний створювати як стандартні рівні для жанру Tower Defence, так і унікальні експериментальні карти, що відповідають сучасним вимогам геймдизайну.

Висновки та перспективи. Запропонована система демонструє високий потенціал для автоматизації створення ігрового контенту, особливо у жанрі Tower Defence. У майбутньому цей метод може бути розширений для інших жанрів ігрової індустрії та інтегрований у професійні ігрові рушії. Перспективним напрямом є розробка додаткових інструментів для інтерактивного налаштування генерації, що ще більше розширить можливості створення ігрових світів.

Список використаних джерел

1. Short T., Adams T. Procedural Generation in Game Design. A K Peters/CRC Press. 336 p.

2. X Watkins R. Procedural Content Generation for Unity Game Development. Packt Pub Ltd. 234 p.

Мазур Дмитро Миколайович
Інженер ІІ категорії лабораторії Спеціальної кафедри №5
Інститут спеціального зв'язку та захисту інформації НТУУ КПІ ім. І. Сікорського
(068) 804-09-30
dimadua38@gmail.com

ПІДСИСТЕМА ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АВТОМАТИЗАЦІЇ РОБОТИ З ПСЕВДОКОДОМ У РЕВЕРС-ІНЖИНІРИНГУ

Постановка задачі. Задача дослідження полягає в розробці підсистеми для автоматизації процесів адаптації, оптимізації та аналізу псевдокоду, що використовується в реверс-інжинірингу програмного забезпечення. Підсистема повинна забезпечити інтеграцію з інструментами реверс-інжинірингу, зокрема IDA Pro, автоматизувати виявлення прихованих залежностей у псевдокоді, оптимізувати його структуру та формувати рекомендації для подальшого аналізу. Реалізація цієї підсистеми має на меті підвищення точності, продуктивності та ефективності процесів аналізу програмного забезпечення.

Мета дослідження. Метою дослідження є підвищення ефективності процесів реверс-інжинірингу програмного забезпечення шляхом розробки підсистеми, яка інтегрує методи штучного інтелекту для автоматизації адаптації, оптимізації та аналізу псевдокоду. Реалізація такої підсистеми сприятиме зниженню навантаження на аналітиків, підвищенню точності аналізу та забезпеченню більш ефективного виявлення вразливостей у програмному забезпеченні.

Результати дослідження. Під час проведення дослідження було здійснено ґрунтовний аналіз існуючих підходів до реверс-інжинірингу програмного забезпечення, зокрема з акцентом на адаптацію псевдокоду для подальшого аналізу. Особливу увагу приділено інструментам, які підтримують генерацію та інтерпретацію псевдокоду, як-от IDA Pro, що є ключовим рішенням у галузі реверс-інжинірингу. Виявлено, що традиційний підхід до роботи з псевдокодом має низку обмежень, зокрема складність оптимізації коду для подальшого аналізу та необхідність ручного втручання аналітиків[1].

У рамках дослідження було визначено, що інтеграція методів штучного інтелекту дозволить адаптувати та покращити використання псевдокоду для реверс-інжинірингу. Це, зокрема, стосується автоматичної оптимізації псевдокоду, збереження його семантичної цілісності та подальшого структурного аналізу[2]. Досліджено потенціал використання методів машинного навчання для автоматичної класифікації та оптимізації псевдокоду на основі попередньо навченої моделі, що дозволить підвищити якість його інтерпретації та подальшого використання.

Спроектована підсистема реалізовуватиметься як плагін для IDA Pro. Основні компоненти плагіну включають:

1. Модуль збору даних. Цей модуль відповідає за інтеграцію з IDA Pro та отримання псевдокоду з програмного забезпечення. Він забезпечує вивантаження, попередню обробку та підготовку даних для подальшого аналізу.

2. Модуль аналізу даних. Основний компонент системи, який застосовує методи штучного інтелекту для аналізу псевдокоду. Він виявляє приховані залежності, потенційно небезпечні ділянки та оптимізує структуру псевдокоду для полегшення роботи аналітиків.

3. Модуль генерації звітів. Формує звіти на основі аналізу, включаючи виявлені загрози, оптимізовану структуру коду та рекомендації щодо подальших дій. Звіти допомагають аналітикам швидше приймати рішення.

Функціонал підсистеми забезпечуватиме автоматизований процес роботи з псевдокодом у поєднанні з можливістю інтерактивної взаємодії аналітика. Плагін дозволятиме працювати з великими обсягами псевдокоду, автоматично оптимізуючи його та зменшуючи навантаження на аналітиків. Автоматизація процесу адаптації псевдокоду сприятиме підвищенню точності аналізу та ефективності реверс-інжинірингу.

Висновки та перспективи. Інтеграція штучного інтелекту у процес адаптації псевдокоду значно підвищує ефективність реверс-інжинірингу програмного забезпечення. Запропонована підсистема, реалізована як плагін для IDA Pro, автоматизує адаптацію, оптимізацію та аналіз псевдокоду, що підвищує продуктивність роботи аналітиків і сприяє протидії сучасним кіберзагрозам.

Перспективи подальших досліджень включають розширення функціоналу для виявлення складних загроз, впровадження глибокого навчання для аналізу поведінкових патернів та розробку хмарної версії підсистеми для інтеграції з іншими інструментами кібербезпеки.

Список використаних джерел

1. Applications of artificial intelligence in closed-loop supply chains: systematic literature review and future research agenda / S. Bhattacharya та ін. Transportation research part E: logistics and transportation review. 2024. Т. 184. С. 103455. URL: https://doi.org/10.1016/j.tre.2024.103455 (дата звернення: 22.11.2024).

2. Sarker I. H. CyberAI: A comprehensive summary of AI variants, explainable and responsible AI for cybersecurity. *AI-Driven cybersecurity and threat intelligence*. Cham, 2024. С. 173–200. URL: https://doi.org/10.1007/978-3-031-54497-2_10 (дата звернення: 22.11.2024).

Мудрик Ярослав Юрійович,
студент 6 курсу, групи ПДМ-62,
Державного університету інформаційно-комунікаційних технологій
(095)582-92-43
yaroslav.mudryk@gmail.com
Науковий керівник: **Золотухіна Оксана Анатоліївна,**
к.т.н, доцент, доцент кафедри Інженерії програмного забезпечення
Державного університету інформаційно-комунікаційних технологій, м.Київ

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ОПТИМІЗАЦІЇ ЕНЕРГОСПОЖИВАННЯ В РОЗУМНИХ БУДИНКАХ ПРИ НЕСТАБІЛЬНОМУ ЕНЕРГОПОСТАЧАННІ

Постановка задачі. Дослідити можливості застосування штучного інтелекту для адаптивного керування енергоспоживанням у розумних будинках в умовах нестабільного енергопостачання.

Мета дослідження. Метою дослідження є створення методики оптимізації енергоспоживання у розумних будинках шляхом адаптивного керування на основі штучного інтелекту.

Результат дослідження.

Запропонована методика накладається на систему адаптивного керування, яка:

- аналізує вхідні дані про стан енергомережі та розумних пристроїв;
- оптимізує використання енергії через переведення пристроїв у еко-режим;
- впроваджує сценарії автономної роботи через перемикання на резервні джерела живлення.

Таблиця 1 демонструє ключові сценарії роботи системи у різних умовах.

Сучасні розумні будинки [2] стають дедалі популярнішими завдяки широкому спектру можливостей для автоматизації процесів у будинку, підвищення комфорту мешканців і більш ефективного використання ресурсів, зокрема енергії. Розумні будинки можуть інтегрувати різні пристрої, датчики та системи, що полегшує управління ними, зменшує витрати на енергію та сприяє екологічній стійкості. Однак необхідність оптимізувати розподіл наявної енергії та забезпечити автономність критично важливих систем робить нестабільне енергопостачання серйозним викликом. У цьому контексті особливого значення набуває використання штучного інтелекту [3], який здатен аналізувати складні дані з різних датчиків і пристроїв та приймати ефективні рішення в режимі реального часу. Використання інтелектуальних алгоритмів дає можливість адаптивно керувати роботою розумних будинків, забезпечуючи стабільну та ефективну роботу навіть у кризових ситуаціях, пов'язаних з перебоями в електропостачанні.

Таблиця 1.

Сценарії адаптивного керування розумним будинком

Сценарій	Дія	Результат
Перебої в електропостачанні	Відключення некритичних пристроїв, переведення систем у еко-режим	Зменшення споживання енергії
Аварійна ситуація	Автономне живлення від резервного джерела (EcoFlow Delta 2 Pro [1])	Забезпечення мінімальної автономності
Відновлення мережі	Поступове повернення пристроїв до нормального режиму	Стабільна робота без надмірного навантаження

Висновки та перспективи. Розробка методики адаптивного керування енергоспоживанням у розумних будинках відкриває нові можливості для забезпечення стійкості систем при нестабільному енергопостачанні. У подальшому дослідження можуть бути спрямовані на впровадження глибших алгоритмів ШІ для прогнозування аварійних ситуацій та інтеграції з розумними енергомережами.

Список використаних джерел

1. Що таке EcoFlow і для чого потрібні? [Електронний ресурс] // businessua.com. – 2024. – Режим доступу до ресурсу: https://businessua.com/benzin/99158szo-take-ecoflow-yak-nim-koristuvatisya-ta-skilki-koshtue.html.

2. Що таке «розумний будинок» і навіщо він потрібен? [Електронний ресурс] // blog.stylus.ua. – 2023. – Режим доступу до ресурсу: https://blog.stylus.ua/uk/528.html.

3. Що таке штучний інтелект? [Електронний ресурс] // gigacloud.ua. – 2023. – Режим доступу до ресурсу: https://gigacloud.ua/blog/navchannja/scho-take-shtuchnij-intelekt-istorija-vidi-ta-skladovi.

Ніщеменко Дмитро Олександрович
викладач кафедри Інформатики, програмування, штучного інтелекту та технологічної освіти
Центральноукраїнський державний університет ім. В. Винниченка
dima.nishchemenko@gmail.com

РЕАЛІЗАЦІЯ ЗБЕРЕЖЕННЯ ТА УПРАВЛІННЯ ДАНИМИ В IOT-ДОДАТКАХ НА ОСНОВІ JAVA SPRING FRAMEWORK

Постановка задачі. Постановка задачі зосереджується на розробці серверної частини додатка для управління пристроями розумного будинку в контексті IoT-систем. Основною задачею є створення ефективної архітектури для збереження даних, управління пристроями та забезпечення взаємодії користувачів із пристроями через API. Задача ускладнюється необхідністю обробки великих обсягів даних, підтримки масштабованості та забезпечення швидкого доступу до інформації про пристрої в реальному часі.

Попередня реалізація серверної частини додатка для управління IoT-пристроями була створена на основі NestJS. Ця платформа надавала зручні інструменти для швидкої розробки додатків, модульну архітектуру та гнучкі механізми роботи з базами даних через TypeORM. Однак, із зростанням складності системи та обсягів даних почали виникати проблеми із продуктивністю та масштабованістю.

Мета дослідження. Метою дослідження є розробка та впровадження ефективної серверної архітектури для IoT-додатків на основі Java Spring Framework, що забезпечує оптимальне збереження та управління даними, а також високопродуктивну взаємодію користувачів із пристроями розумного будинку через API.

Результати дослідження. NestJS (заснований на Node.js) та Spring є популярними платформами для розробки серверних додатків, але їх архітектурні підходи та сфери застосування суттєво відрізняються.

Node.js працює за принципом однопотокового циклу подій (Event Loop), використовуючи неблокуючі операції вводу/виводу (I/O). Це дозволяє обробляти великий обсяг одночасних з'єднань але складні обчислювальні задачі можуть стати проблемою, оскільки блокують Event Loop, що негативно впливає на продуктивність. Spring, навпаки, працює на багатопотоковій архітектурі завдяки потокам JVM. Це дозволяє обробляти ресурсоємні завдання паралельно та ефективно використовувати багатоядерні системи. Spring підтримує як блокуючі моделі, так і неблокуючу обробку через Spring WebFlux [1, 3].

Node.js використовує JavaScript, який має динамічну типізацію, а опціональна підтримка TypeScript додає можливість статичної перевірки типів. Spring базується на мові Java, яка є строго типізованою з перевіркою типів на етапі компіляції. Це додає надійності та зменшує кількість помилок під час розробки.

Щодо управління пам'яттю, Node.js базується на V8-движку від Google, який реалізує збір сміття, однак його продуктивність залежить від доступної пам'яті та навантаження системи [2]. Пам'ять у Spring керується JVM, яка має більш складний та гнучкий механізм управління, включаючи налаштування збирача сміття.

У плані інтеграції Spring забезпечує потужні інструменти для роботи з корпоративними сервісами (SOAP, REST) та базами даних завдяки Hibernate. Крім того, платформа пропонує стабільні та надійні бібліотеки для бізнес-логіки.

Підсумовуючи, Node.js є вибором для I/O-інтенсивних додатків з легким навантаженням на CPU, де важлива швидка обробка подій. Натомість Spring орієнтований на великі, багатопотокові системи, що потребують високої продуктивності, надійності та гнучкої інтеграції з корпоративними рішеннями.

Проведене порівняння на основі архітектурних особливостей, управління пам'яттю та підходів до обробки запитів є важливим. Проте для повноцінної оцінки варто звернути увагу не лише на теоретичні відмінності, а й на результати реального тестування з навантаженням.

Зокрема, пропонується розглянути тестування [2]. Використання цього дослідження є доцільним, оскільки воно вже містить необхідні результати та аналітику для порівняння. Водночас слід підкреслити, що у проведеному тестуванні було виявлено певні недоліки, однак це не знижує його цінності для наочного демонстрування принципових відмінностей між фреймворками.

Результати показали, що Spring забезпечує найменшу затримку та мінімальну кількість пропущених запитів у порівнянні з іншими рішеннями. Проте ці переваги досягаються за рахунок високого споживання ресурсів процесора та оперативної пам'яті.

Реалізація модуля для роботи з пристроями в системі розумного дому, виконана за допомогою Java, Spring Framework та JPA/Hibernate, ґрунтується на принципах модульності, розподілу відповідальностей і використанні сучасних підходів до управління даними [1].

Розроблений додаток виконує кілька ключових функцій, зокрема збереження нових пристроїв, оновлення їхніх параметрів, вилучення даних про пристрої та визначення їхньої належності до конкретних користувачів. Основним викликом було забезпечення ефективної роботи додатка в умовах високого навантаження та дотримання вимог до швидкодії запитів. Для цього реалізовано оптимізацію збереження даних шляхом використання кешування другого рівня в Hibernate, впровадження пакетної обробки транзакцій, а також застосування відкладеного завантаження зв’язків між сутностями.

Сутність пристрою, представлена класом Device, реалізує модель об’єкта, що зберігається у базі даних. Для зручності відображення структури даних використано анотації JPA, які дозволяють автоматично створювати відповідну таблицю в базі даних. Поля сутності включають ідентифікатор, назву пристрою, його тип і посилання на користувача, що забезпечує зв’язок із таблицею користувачів.

Для доступу до даних використовується DeviceRepository, що дозволяє використовувати готові методи для виконання CRUD-операцій без необхідності їх явно реалізовувати.

Бізнес-логіка, що визначається в класі DeviceService, реалізує основні операції з пристроями, включаючи їх вибірку, створення та видалення. Усі методи забезпечують перевірку цілісності даних. Використання транзакцій на рівні сервісу гарантує атомарність операцій та дозволяє уникати станів неконсистентності в разі виникнення помилок.

REST-контролер, реалізований у класі DeviceController, забезпечує API для обробки HTTP-запитів, пов'язаних із пристроями. Кінцеві точки, такі як отримання списку всіх пристроїв, пошук пристроїв за ідентифікатором користувача, створення та видалення пристрою, реалізовано за допомогою відповідних HTTP-методів GET, POST і DELETE.

Для забезпечення більшої гнучкості та ізоляції шарів додатка введено використання об'єктів передачі даних (DTO). Це дозволяє відокремити внутрішнє представлення даних від форматів, що використовуються для зовнішнього інтерфейсу, і мінімізує ризик витоку внутрішньої структури сутностей у клієнтський код.

Таким чином, запропонована архітектура відповідає вимогам сучасних систем управління даними в контексті Інтернету речей. Вона забезпечує модульність, розширюваність і стабільність, а також створює умови для легкого інтегрування додаткових функціональних можливостей у майбутньому.

Висновки та перспективи. Перехід від платформи NestJS до Java Spring Framework для розробки серверної частини IoT-додатка забезпечив значні покращення в ефективності роботи системи, її масштабованості та продуктивності. Використання Java Spring дозволило оптимізувати роботу з базою даних PostgreSQL завдяки більш гнучким інструментом для кешування, налаштування транзакцій та обробки запитів. Це сприяло зменшенню затримок у роботі додатка та підвищенню його здатності до обробки великих обсягів даних.

Перспективи розвитку даного підходу включають подальшу оптимізацію взаємодії з базою даних, використання додаткових технологій для покращення масштабованості, таких як розподілені системи кешування та мікросервісна архітектура. Впровадження нових підходів до зберігання та обробки даних дозволить ще більше покращити продуктивність та зручність використання додатка для користувачів у майбутньому.

Список використаних джерел

1. Walls C. Spring in Action. Manning Publications Co. LLC, 2018.
2. C M. Spring Boot Webflux vs Node.js frameworks: Performance comparison. Medium. URL: https://medium.com/deno-the-complete-reference/spring-boot-webflux-vs-node-js-frameworks-performance-comparison-for-hello-world-case-d03af0f7b020 (дата звернення: 24.12.2024).
3. Casciaro M. Node. js Design Patterns. Packt Publishing, Limited, 2014.

Петрушина Вікторія Володимирівна
студентка 3 курсу, групи ІП-24
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
(099)-161-08-46
petrushyna.v@gmail.com
Науковий керівник: **Поперешняк Світлана Володимирівна**
к.ф.-м.н., доцент, доцент кафедри ІПІ ФІОТ
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
(098)-645-546-2
spopereshnyak@gmail.com

СУЧАСНІ АСПЕКТИ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Постановка задачі. Розробка програмного забезпечення є одним із ключових аспектів сучасної цифрової економіки. Зростання складності програмних систем, необхідність інтеграції штучного інтелекту, автоматизації процесів та забезпечення кібербезпеки вимагають нових підходів у розробці. Завдання дослідження полягає у визначенні сучасних підходів до розробки ПЗ, аналізі їхньої ефективності та застосовності у різних галузях.

Мета дослідження. Аналіз сучасних методів і підходів до розробки програмного забезпечення, з урахуванням новітніх технологій, що сприяють покращенню ефективності процесів розробки та забезпечення високої якості продукту.

Результати дослідження. На основі аналізу сучасних підходів до розробки програмного забезпечення та використання новітніх технологій, було виявлено кілька ключових аспектів, що сприяють підвищенню ефективності та якості розробки.

Методології, такі як Agile, сприяють швидкій адаптації до змін та підвищенню продуктивності команд. Дослідження показують, що впровадження Agile може підвищити продуктивність команди на 25% [1].

DevOps забезпечує безперервну інтеграцію та доставку (CI/CD), що скорочує час виходу продукту на ринок на 40% [2]. DevOps об’єднує розробників і команди операцій для досягнення високої продуктивності.

Штучний інтелект передбачає використання машинного навчання (ML) та інших технологій штучного інтелекту для автоматизації та оптимізації процесу розробки і доставки програмного забезпечення. Це включає в себе все – від автоматизації процесів тестування і розгортання до поліпшення управління ресурсами і підвищення безпеки [3]. AI та DevOps поділяють симбіотичні відносини, що означає, що обидва вони впливають та покращують один одного [4] (рис.1).

Рис. 1 Симбіотичні відносини AI/ DevOps та їх переваги

Згідно із щорічним опитуванням GitLab виявилося, що штучний інтелект стає новою реальністю роботи DevOps-команд у всьому світі [5][6].

- 51% респондентів заявили, що вже використовують AI для перевірки коду;
- 37% команд використовують AI та ML для тестування програмного забезпечення, що на 12% більше, ніж минулого року;
- 78% респондентів заявили, що в даний час використовують штучний інтелект у розробці програмного забезпечення або планують це в найближчі 2 роки, що на 14% більше за минулий рік.

Також важливим фактором є архітектура мікросервісів, що дозволяє створювати масштабовані системи, де кожна частина (сервіс) працює автономно. Це спрощує підтримку та оновлення великих систем [7].

Висновки. Сучасні підходи до розробки ПЗ, такі як Agile та DevOps, у поєднанні із застосуванням новітніх технологій, дозволяють значно підвищити продуктивність розробників, скоротити витрати та забезпечити якість програмного продукту. Використання мікросервісів і автоматизації процесів стає ключовим у розробці масштабованих систем.

У майбутньому очікується подальший розвиток інструментів, що базуються на штучному інтелекті, для ще більшого вдосконалення процесів розробки.

Список використаних джерел

1. What is modern software development? Atlassian. URL: https://www.atlassian.com/blog/software-teams/modern-software-development-trends

2. Humble J., Farley D. Continuous Deployment at Facebook and OANDA. ResearchGate. URL: https://www.researchgate.net/publication/303296480_Continuous_deployment_at_Facebook_and_OANDA

3. Web Academy Media. Роль штучного інтелекту в DevOps. Web Academy. https://web-academy.ua/blog/junior/role-ai-in-devops
4. OrangeMantra. AI in DevOps: How DevOps teams take advantage of AI. OrangeMantra. https://www.orangemantra.com/blog/ai-in-devops/
5. IT Education Center. Штучний інтелект й машинне навчання в роботі DevOps-інженера. IT Education Center. https://itedu.center/ua/blog/devops/how-ai-and-ml-change-devops/
6. Amazon Web Services. 8 reasons to move to AWS. Amazon Web Services. https://pages.awscloud.com/rs/112-TZM 766/images/AWS_8_Reasons_pdf.pdf

Присяжнюк Олена Віталіївна
кандидат технічних наук,
доцент кафедри інформатики, програмування,
штучного інтелекту та технологічної освіти
Центральноукраїнського державного університету імені Володимира Винниченка, м. Кропивницький
o.v.prysiazhniuk@cuspu.edu.ua
Пузікова Анна Валентинівна
кандидат фізико-математичних наук,
доцент кафедри кафедри інформатики, програмування,
штучного інтелекту та технологічної освіти
Центральноукраїнського державного університету імені Володимира Винниченка, м. Кропивницький
a.v.puzikova@cuspu.edu.ua

ВИКОРИСТАННЯ ChatGPT ДЛЯ РОЗПІЗНАВАННЯ ВІДПОВІДЕЙ РЕСПОНДЕНТІВ У СОЦІАЛЬНИХ ОПИТУВАНЯХ

Постановка задачі. З розвитком штучного інтелекту з’явився сегмент програмних продуктів, які здатні розпізнавати людську мову і можуть бути використані в якості інструменту спілкування та персоналізованої підтримки клієнтів. Останніми роками використання таких інструментів для автоматизації підтримки клієнтів і зменшення робочого навантаження на операторів стає все більш популярним в діловому світі та соціальних структурах. Модель GPT (Generative Pretraining of Transformers – генеративний попередньо навчений трансформер) – тип архітектури нейронної мережі, корисний у чат-ботах, що робить їх особливо ефективними для імітації людського спілкування [1]. Тому актуальним є аналіз можливостей моделі ChatGPT по розпізнаванню відповідей респондентів з метою подальшої її імплементації в автоматизовані системи обробки результатів соціальних досліджень.

Метою дослідження є аналіз можливостей моделі ChatGPT для розпізнавання нестандартних відповідей респондентів під час цифрової комунікації із чатботом.

Результати дослідження. В соціальних опитуваннях для надання відповідей респондентам зазвичай пропонуються заготовлені шаблони. Деякі користувачі в силу ситуаційних обставин або поточного емоційного стану, можуть давати відповіді не в межах шаблонних варіантів. Для розпізнавання таких відповідей вимагалось втручання людини-оператора для уточнення інформації, або її самостійної інтерпретації без додаткового діалогу з клієнтом. Використання ChatGPT потенційно дозволяє перенаправити задачу аналізу тексту, уведеного користувачем, мовній моделі GPT-4 та OpenAI API [2]. Для налаштування чутливості ChatGPT-4 до розпізнавання відповідей респондентів використовувався налаштовуваний параметр «temperature». Цей параметр

забезпечує контроль ступеня випадковості або непередбачуваності відповідей, що повертаються моделлю GPT-4 [3].

Експериментальні дані проведеного експрес-опитування респондентів на предмет, чи потребують вони консультації фахівця (з певної сфери соціальних послуг) показали, що певна частина респондентів дала відповіді не в межах запропонованого шаблону. Розпізнавання відповідей респондентів здійснювалось з використанням автоматизованої системи обробки результатів, в яку було імплементовано ChatGPT. Проведене дослідження свідчать, що результати обробки нестандартних відповідей користувачів чат-ботом досить високі і добре співвідносяться із експертними оцінками відносно змістовності і правильності розпізнавання. Виявлено, що вплив налаштувань параметра «temperature» на продуктивність обробки неявно погоджувальних відповідей респондентів має позитивну динаміку із зростанням його значень (рис.1).

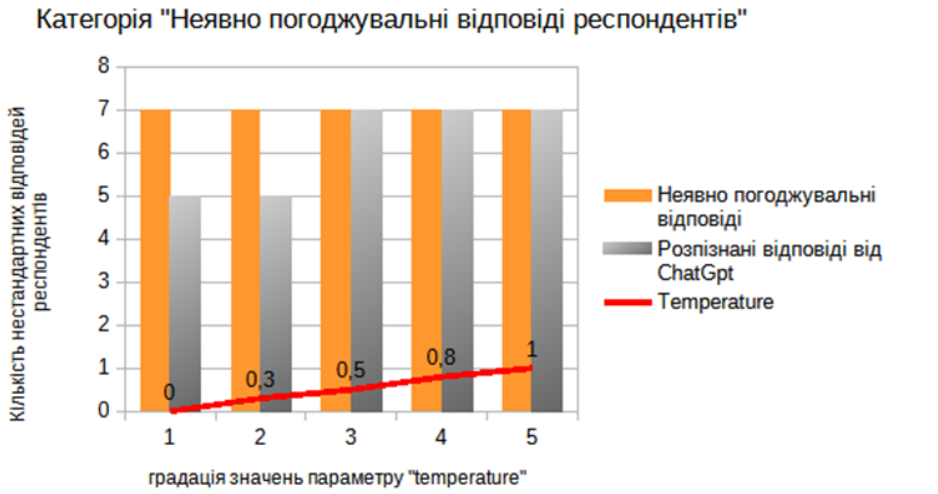

Рис. 1. Продуктивність розпізнавання неявно погоджувальних відповідей респондентів при різних значеннях параметра «temperature».

Також виявлено, що для неявно непогоджувальних відповідей вплив налаштувань параметра «temperature» на продуктивність обробки залишається недовизначеним (рис.2) і потребує подальших досліджень.

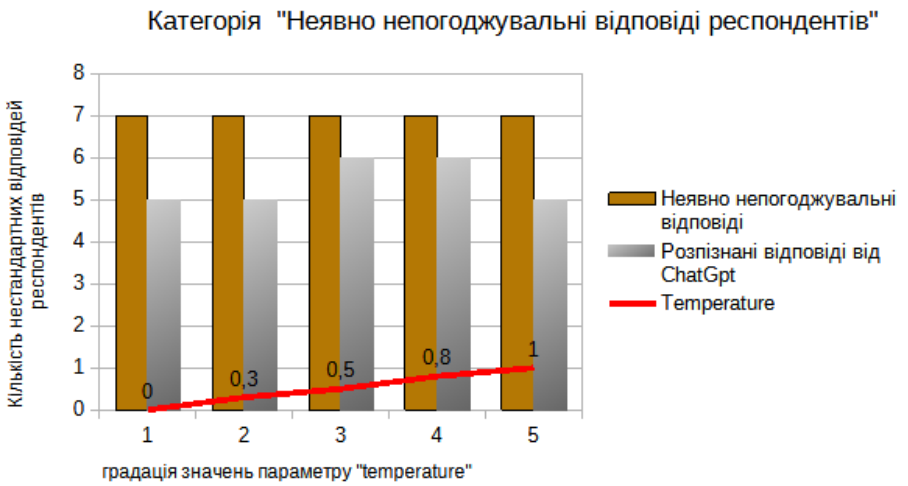

Рис. 2. Продуктивність розпізнавання неявно непогоджувальних відповідей користувачів при різних значеннях параметра «temperature».

Зауважимо, що за результатами дослідження для найбільш точного розпізнавання нестандартних відповідей користувачів можна рекомендувати використовувати значення параметра «temperature» в межах (0.5-0.8).

Висновки та перспективи. Використання мовної моделі GPT-4 надає розробникам програмних продуктів (зокрема, чатботів) можливість додаткового аналізу введеного тексту з метою підтвердження позитивної /погоджувальної чи негативної/непогоджувальної відповідей користувача. Запропонований підхід дозволяє автоматизувати процес обробки відповідей респондентів і відповідно зменшити навантаження на операторів Центрів надання соціальних послуг, що є вельми актуальним в умовах дефіциту кадрів на українському ринку праці.

Отримані результати дослідження можуть бути використані розробниками моделі GPT-4 з метою оптимізації та/або покращення якості розпізнівання текстів під час зваженого навчання (Weighted learning) для коригування ваги помилок у рідкісних або важливих випадках [4], а також для покращення технік, які використовуються для аналізу емоційного стану, настроїв та інтонації в тексті.

Список використаних джерел

1. Y. Zhang, S. Sun, M. Galley, Y.-C. Chen, C. Brockett, X. Gao, J. Gao, J. Liu, B. Dolan, DIALOGPT: Large-Scale Generative Pre-training for Conversational Response generation, in: Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics: System Demonstrations, pp.270-278, 2020. doi: 10.18653/v1/2020.acl-demos.30.

2. M. Javaid, A. Haleem, R. P. Singh, A study on ChatGPT for Industry 4.0: Background, potentials, challenges, and eventualities, Journal of Economy and Technology 1(35) pp. 127-143, 2023. doi: 10.1016/j.ject.2023.08.001 X.-T.

3. Setting Parameters in OpenAI, URL: https://www.codecademy.com/article/setting-parameters-in-open-ai.

4. Voloshin, A.F., Gnatienko, G.N., Drobot, E.V. A Method of Indirect Determination of Intervals of Weight Coefficients of Parameters for Metricized Relations Between Objects, Journal of Automation and Information Sciences 35(1-4), pp.25-30, 2003. doi: 10.1615/JAutomatInfScien.v35.i3.30.

Рейнгольд Олександр Юрійович
студент 6 курсу, групи ІСДМ-63
Державний університет інформаційно-комунікаційних технологій
(097) 185-29-23
sanchezzz1362@gmail.com
Науковий керівник: **Поперешняк Світлана Володимирівна**
к.ф.-м.н., доцент, доцент кафедри ІПІ ФІОТ
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"
(098)-645-546-2
spopereshnyak@gmail.com

ВПЛИВ ВПРОВАДЖЕННЯ AGILE-МЕТОДОЛОГІЙ НА ПРОДУКТИВНІСТЬ І ЗАДОВОЛЕНІСТЬ СПІВРОБІТНИКІВ В IT-КОМПАНІЯХ

Постановка задачі. Agile-методології є популярними підходами до управління проєктами, які дозволяють IT-компаніям підвищувати ефективність процесів розробки, адаптуватися до змін та забезпечувати кращу взаємодію між членами команди. В роботі проведено аналіз впровадження Agile-методологій в IT-компаніях для підвищення продуктивності праці та задоволеності співробітників.

Мета дослідження. Визначення впливу Agile-методологій на продуктивність і задоволеність співробітників в IT-компаніях та аналіз основних переваг і викликів при їх впровадженні.

Результати дослідження. Розглянемо суть Agile-методологій, яка полягає в наступному:

- Agile орієнтований на гнучке планування, ітераційність, зворотний зв’язок і постійне вдосконалення.
- Основні методи: Scrum, Kanban, Lean, Extreme Programming (XP).
- Agile-цінності: люди та комунікація, робочий продукт, співпраця з клієнтами, гнучкість у планах.

Вплив впровадження agile-методологій на вплив на продуктивність співробітників полягають в наступному:

- Прискорення робочих процесів завдяки чітко визначеним ітераціям та коротким термінам виконання завдань.
- Прозорість і видимість прогресу через використання інструментів, як-от Jira, Trello, Azure DevOps.
- Швидке виявлення проблем та можливість миттєво реагувати на зміни.
- Оптимізація робочого навантаження за допомогою Kanban-дощок та принципу "work in progress"

Впровадження Agile-методологій, таких як Scrum і Kanban, суттєво вплинуло на підвищення продуктивності праці в IT-компаніях. Це пояснюється

збільшенням ефективності командної роботи та оптимізацією процесів розробки програмного забезпечення. Основні етапи Agile-процесу зображені на рис.1 включають планування, виконання, перегляд та вдосконалення, що циклічно повторюються.

Рис. 1. Схема Agile-процесу

Аналіз впровадження Agile-методологій показує, що ефективність команд збільшується в середньому на 20-30% завдяки коротким ітераціям та швидкому зворотному зв'язку. До впровадження Agile команди в середньому виконували близько 80 завдань на місяць, тоді як після впровадження цей показник зріс до 104 завдань на місяць. Крім того, час на виконання проектів скоротився з 12 до 9 місяців [1].

Впровадження Agile-методологій також позитивно вплинуло на рівень задоволеності співробітників. Було проаналізовано вплив впровадження Agile-методологій на задоволеність співробітників:

- Підвищення мотивації та залученості завдяки активній участі в плануванні та прийнятті рішень.
- Зниження стресу через чіткий розподіл ролей та завдань у команді.
- Покращення комунікації як всередині команди, так і з замовниками, завдяки регулярним мітингам (daily stand-up, sprint review).
- Визнання досягнень на етапах ретроспектив, що сприяє розвитку позитивної робочої атмосфери.

Завдяки гнучким графікам, можливості працювати в команді та зменшенню мікроуправління, співробітники відчувають себе більш залученими та мотивованими. Дослідження зображене на рис.2 показує, що рівень задоволеності збільшився на 15-25% після впровадження Agile [2].

Рис. 2. Схема задоволеності співробітників

Аналіз проведених експериментів показав, що команди, які працюють за методологіями Agile, більш адаптивні до змін і здатні швидше реагувати на виклики ринку. Крім того, зменшення кількості помилок та підвищення якості продукту позитивно впливає на кінцевий результат [3].

Проте існують певні проблеми при впровадженні Agile:

- Опір змінам з боку співробітників та керівництва.
- Відсутність досвіду роботи з Agile у деяких команд.

- Складність масштабування Agile-методологій на великі проєкти.

Висновки та перспективи. Впровадження Agile-методологій в IT-компаніях значно підвищує продуктивність праці та рівень задоволеності співробітників. Ці методології сприяють більш ефективній командній роботі, швидкому зворотному зв'язку та адаптивності до змін.

Перспективи подальших досліджень включають:

- Аналіз довгострокового впливу Agile на корпоративну культуру.
- Дослідження впливу різних фреймворків Agile (Scrum, Kanban, SAFe) на великі компанії.
- Визначення факторів успішного масштабування Agile у глобальних IT-компаніях.

Agile залишається важливим інструментом для підвищення ефективності роботи в сучасному IT-середовищі, де зміни є невід'ємною складовою процесу розробки.

Список використаних джерел

1. Ammattikorkeakoulut-Theseus.URL: https://www.theseus.fi/ bitstream/ handle/ 10024 /802492/Teebi_Ibrahim.pdf?sequence=2.

2. What is Agile Software Development?. Agile Alliance |. URL: https://www.agilealliance.org/agile101/?form=MG0AV3.

3. How Agile Boosts Team Morale and Employee Satisfaction. Agile Marketing Guidance for Orgs, Teams, & Individuals. URL: https://www.agilesherpas.com/blog/agile-boosts-team-morale.

Сергієнко Сергій Олександрович,
студент 3 курсу, групи ІП-21
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"
(098)-464-36-90
sirserg05@gmail.com
Науковий керівник: **Поперешняк Світлана Володимирівна**
к.ф.-м.н., доцент, доцент кафедри ІПІ ФІОТ
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"
(098)-645-546-2
spopereshnyak@gmail.com

КОМПЛЕКСНА СИСТЕМА УПРАВЛІННЯ РОЗРОБКОЮ ДЛЯ БАЛАНСУ ПРОДУКТИВНОСТІ ТА ЕМОЦІЙНОГО БЛАГОПОЛУЧЧЯ КОМАНДИ

Постановка задачі. Сучасні платформи управління розробкою зосереджуються на класичних кількісних показниках: обсязі виконаних завдань, швидкості розробки, інтенсивності комітів. Однак ця статистика є лише поверхневим відображенням процесів у командах розробників. За цифрами залишаються поза увагою психологічний клімат та індивідуальний стан кожного спеціаліста. Технологічний прогрес, зокрема розвиток систем NLP та LLM, відкриває принципово нові можливості. З'являється технічна спроможність аналізувати не лише формальні показники, а й емоційне забарвлення комунікацій розробників: їхні коментарі в коді, дискусії в робочих чатах, звіти. Такий підхід дозволить перетворити технічний моніторинг на людиноцентричний інструмент.

Мета дослідження. Метою дослідження є розробка концепції платформи, яка об’єднує аналіз активності розробників із визначенням їхнього емоційного стану за допомогою сучасних AI-технологій. Дослідження спрямоване на вивчення можливостей інтеграції методів аналізу текстових даних, автоматизованого моніторингу продуктивності та гейміфікаційних механік для створення збалансованого робочого середовища. Основна увага приділяється розробці інструментів, які допомагають оцінювати як ефективність роботи команди, так і психологічний стан її учасників, з метою зниження ризику вигорання, підвищення мотивації та покращення взаємодії всередині команди.

Результати. Робота розробників часто пов’язана з високим рівнем стресу та емоційним виснаженням, що значно впливає на їх продуктивність і загальний стан здоров’я. Згідно з результатами опитування JetBrains Developer Ecosystem 2023, 73% розробників хоча б раз у своїй кар’єрі стикалися з вигоранням. Основними причинами цього явища є надмірне робоче навантаження, погана організація робочого процесу, а також розмиття меж між професійним і особистим життям, що стало особливо актуальним у період переходу на дистанційну роботу [1]. У зв’язку з цим дедалі актуальнішою стає розробка

інструментів, які допомагають не лише відстежувати робочу активність, а й враховувати емоційний стан фахівців, зокрема рівень стресу та вигорання. Виявлення та моніторинг цих аспектів можуть допомогти створити більш збалансоване робоче середовище та покращити якість роботи.

Пропонований концепт платформи передбачає 3 основні компоненти.

По-перше, головний акцент зроблено на аналізі коментарів у системах контролю версій та робочих чатах. Сентимент-аналіз дозволяє визначити тональність тексту, рівень стресу та емоційний стан автора. Використання сучасних мовних моделей, таких як BERT та GPT дозволяє ефективно розпізнавати емоційні та семантичні аспекти тексту з високою точністю. За даними дослідження Шанхайського університету точність таких моделей у визначенні емоційного стану досягає понад 80% для найпоширеніших класів. Це забезпечує можливість не лише моніторити стан окремих розробників, але й отримувати комплексне уявлення про емоційний клімат у команді [2].

По-друге, пропонована платформа використовує автоматизовану систему для аналізу активності розробників на основі показників, таких як кількість і частота pull requests, кількість коментарів, швидкість реакцій на зміни в коді та інші метрики взаємодії в команді. На основі цих даних система може автоматично підібрати пари розробників для обміну досвідом, сприяючи більш ефективному та динамічному навчальному процесу в команді. Згідно з дослідженням Університету Осло, парне програмування є ефективним інструментом для досягнення високої точності при роботі над складними завданнями [3]. Завдяки цьому, платформа дозволяє створювати пари розробників, які можуть доповнювати одне одного, що дозволяє максимізувати ефективність обміну знаннями та продуктивність команди.

По-третє, одним із ефективних способів підвищення мотивації розробників у пропонованій платформі є інтеграція елементів гейміфікації, таких як рейтинги, досягнення та заохочення за продуктивну роботу. Гейміфікація, зокрема в контексті тривалих або повторюваних завдань, може сприяти значному зростанню залученості співробітників. Згідно з дослідженням бразильських науковців, гейміфікація може суттєво вплинути на поведінку користувачів, зокрема покращити якість виконаних завдань. Дослідження показує, що учасники, які працювали в гейміфікованому середовищі, досягали кращих результатів. Окрім цього, гейміфікація допомогла змінити поведінку учасників, зокрема, значно покращила показники точності у виконанні завдань серед учасників, які мали високу пунктуальність та зосередженість. Дослідження також виявило, що учасники з певними рисами особистості, наприклад, інтроверти, отримували більше бонусів та досягнень у гейміфікованому середовищі. Це свідчить про те, що гейміфікація може бути адаптована до різних типів особистості, що дозволить досягти високих результатів у розвитку навичок [4].

На рис. 1 зображено схему інтеграції цих компонентів у платформу. Дані збираються з різних джерел, аналізується активність розробників, текстові дані обробляються за допомогою NLP. Платформа автоматично визначає емоційний

стан, рівень досвіду та залученість учасників, підбирає пари для обміну досвідом та адаптує гейміфікаційні сценарії. Результати аналізу ризиків та емоцій передаються менеджменту для оптимізації роботи команди.

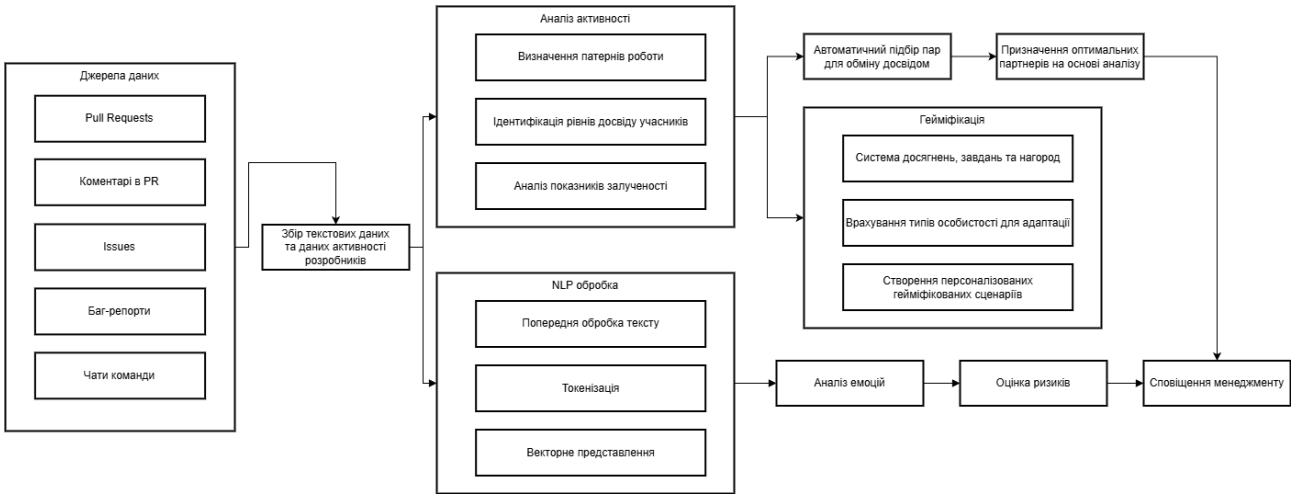

Рис. 1. Схема компонент аналізу стану розробників для пропонованої платформи управління розробкою

Ця платформа покликана знизити рівень вигорання розробників, підвищити їхню продуктивність та якість співпраці.

Висновки. Дослідження показало, що аналіз емоцій на основі текстових даних дозволяє точно визначати тональність тексту, рівень стресу та емоційний стан автора. Аналіз активності розробників дає змогу автоматично підібрати пари для обміну досвідом, що підвищує ефективність навчання та загальну продуктивність. Інтеграція гейміфікації позитивно впливає на мотивацію, залученість і якість виконуваних завдань. Це дозволяє створити збалансоване робоче середовище та знизити ризик професійного вигорання. Запропонована платформа є комплексним інструментом, що об'єднує аналіз емоцій, моніторинг активності та гейміфікацію для підтримки емоційного стану розробників, оптимізації робочих процесів і зниження ризику професійного вигорання. Впровадження такого рішення може покращити продуктивність команди та сприяти довгостроковому розвитку фахівців.

Список використаних джерел

1 The State of Developer Ecosystem in 2023 Infographic. JetBrains: Developer Tools for Professionals and Teams. URL: https://www.jetbrains.com/lp/devecosystem-2023/

2 Zhang X., Qi X., Teng Z. Performance evaluation of Reddit Comments using Machine Learning and Natural Language Processing methods in Sentiment Analysis. ICCES 2024. Mechanisms and Machine Science, Singapore, 3–6 August 2024. Cham, 2024. P. 14–24.

3 The effectiveness of pair programming: A meta-analysis / J. E. Hannay et al. Information and Software Technology. 2009. Vol. 51, no. 7. P. 1110–1122.

4 The impact of gamification on students' learning, engagement and behavior based on their personality traits / R. Smiderle et al. Smart Learning Environments. 2020. Vol. 7, no. 1.

Сєрокуров Артем Ігорович
студент 6 курсу, групи ПДМ-62
Державний університет інформаційно-комунікаційних технологій, м.Київ
Науковий керівник: **Соляник Людмила Олексіївна**
к.х.н., доц., доцент кафедри Інженерії програмного забезпечення,
Державний університет інформаційно-комунікаційних технологій, м.Київ
+380686448047
tasolowarrior@icloud.com

РОЗРОБКА МЕТОДУ ІНТЕГРАЦІЇ СИСТЕМ МАШИННОГО НАВЧАННЯ В ASP.NET CORE ДОДАТКИ З ВИКОРИСТАННЯМ ML.NET: ДОСЛІДЖЕННЯ ТА РЕАЛІЗАЦІЯ МЕТОДІВ ІНТЕГРАЦІЇ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ У ВЕБ-ДОДАТКИ НА БАЗІ ASP.NET CORE.

Постановка задачі : у сучасному світі зростає попит на інтелектуальні веб-додатки, що можуть автоматизувати аналітичні процеси, приймати складні рішення та взаємодіяти з користувачами на новому рівні. Основною задачею цього дослідження є розробка методів інтеграції систем машинного навчання в ASP.NET Core додатки, використовуючи ML.NET, що забезпечить створення ефективних, масштабованих і високопродуктивних рішень на основі штучного інтелекту[1].

Мета дослідження полягає у розробці та впровадженні методів інтеграції моделей машинного навчання в ASP.NET Core додатки з використанням ML.NET. Це включає в себе аналіз поточних технологій, розробку підходів для підготовки даних, навчання моделей, їх оцінки та інтеграції в веб-середовище. Додатково, дослідження спрямоване на визначення кращих практик і рекомендацій для забезпечення якості, надійності та безпеки таких систем[2].

Результат дослідження: в результаті дослідження було розроблено і реалізовано методику інтеграції моделей машинного навчання в ASP.NET Core додатки з використанням ML.NET.

Підготовка даних для моделей у ML.NET включала очищення, кодування, нормалізацію та об'єднання, що забезпечило якісний вхідний матеріал для навчання. Було реалізовано та налаштовано різноманітні моделі машинного навчання, зокрема лінійну регресію, дерева рішень, градієнтний бустинг і нейронні мережі. Для оцінки їхньої якості використовувалися метрики, як-от точність, повнота, F1-міра для класифікації та середня квадратична помилка для регресії, що дозволило ідентифікувати слабкі місця і вдосконалити моделі. Інтеграція цих рішень у веб-додатки ASP.NET Core забезпечила високу продуктивність, масштабованість і безпеку[3].

Висновки та перспективи:

Розробка методу інтеграції систем машинного навчання в ASP.NET Core додатки з використанням ML.NET продемонструвала ефективність і надійність сучасних підходів до створення інтелектуальних веб-додатків. Успішно

реалізовані методики підготовки даних, навчання моделей та їх оцінки забезпечують високу якість прогнозів і класифікацій, що відповідає сучасним вимогам до продуктивності й точності. Отримані результати доводять, що інтеграція машинного навчання в веб-додатки може значно підвищити їхню функціональність та цінність для користувачів. Перспективи подальшого розвитку включають оптимізацію методів масштабування систем для роботи з хмарними платформами, що забезпечить ще більшу адаптивність та глобальну доступність рішень. Очікується подальше розширення сфер застосування, включаючи промисловість, логістику, фінанси та безпеку, а також інтеграція з передовими технологіями, такими як інтернет речей та блокчейн. Покращення персоналізації та адаптивності систем дозволить забезпечити ще більш якісний користувацький досвід, розширюючи можливості їх практичного застосування.

Список використаних джерел

1. What is ML.NET and how does it work? - ML.NET. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/dotnet/machine-learning/how-does-mldotnet-work
2. ASP.NET Core | Open-source web framework for .NET. Microsoft. URL: https://dotnet.microsoft.com/en-us/apps/aspnet.
3. How to Use the Automated Machine Learning API With ML.NET. Code Maze. URL: https://code-maze.com/csharp-automated-machine-learning-api-with-ml-net/

Чорнобривець Дмитро Віталійович,
студент 3 курсу, групи ІП-21
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"
(098)-536-86-90
dimas05@gmail.com
Науковий керівник**: Головченко Максим Миколайович**,
PhD, старший викладач кафедри інформатики та програмної інженерії
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"
(098)-785-36-89
Maxnik@gmail.com

РОЗРОБКА ПЛАТФОРМИ ДЛЯ ЗАМОВЛЕННЯ ТА МОНІТОРИНГУ ВИКОНАННЯ ФРІЛАНС-ПОСЛУГ

Постановка задачі. У сучасних умовах цифрової економіки фріланс-платформи[5] стають важливим інструментом для забезпечення взаємодії між замовниками та виконавцями. Однак, багато платформ стикаються з проблемами ефективного пошуку спеціалістів і мотивації виконавців, що ускладнює процес співпраці. Розробка інтелектуальних систем, які аналізують продажі та просування послуг, дозволяє підвищити конкурентоспроможність виконавців, покращити якість виконання замовлень і забезпечити прозору взаємодію. Інноваційні механізми просування та удосконалена мотиваційна система сприятимуть ефективності роботи платформи та створенню нових можливостей для користувачів. Розробка призначена для автоматизації процесів замовлення фріланс-послуг[4] та їх виконання через онлайн-платформу. Веб-додаток має забезпечити ефективну взаємодію між замовниками та виконавцями, спростити обробку завдань, контроль якості виконаних робіт.

Мета дослідження. Метою дослідження є розробка та впровадження програмного рішення для автоматизації роботи платформи фриланс-послуг, що включає інтеграцію з базою даних, зовнішніми сервісами для збереження файлів та забезпечення безпечного доступу до системи через веб-інтерфейс. Дослідження спрямоване на оптимізацію взаємодії користувачів із системою та забезпечення надійності збереження і обробки даних, використовуючи сучасні програмні інструменти та архітектурні підходи.

Результати дослідження. У результаті аналізу та дослідження предметної області програмних продуктів-аналогів, зокрема PeoplePerHour [1], Weblancer [2], Freelancehunt [3], було визначено такі ключові функціональні вимоги розроблюваного веб-застосунку:

1. Облік користувачів: фрілансер/замовник (зберігання персональних даних, реєстрація, авторизація, зміна фотографії профілю, додавання фрілансером портфоліо та напрямку професії)

2. Облік створення оголошень про послуги (створення, зберігання, перегляд власних оголошень, видалення)

3. Пошук та фільтрація оголошень за ключовими критеріями (пошук, фільтрація по назві, категорії, підкатегорії, ціні, та часу виконання)

4. Перегляд деталей послуги (перегляд детальної інформації про послугу)

5. Замовлення та взаємодія послугами (Замовлення послуги замовником у фрілансера, та керування замовленям, а саме: прийняти замовлення, відхилити, обратна пропозиція, відправити результати, відхилити або прийняти результати)

6. Моніторинг етапів виконання послуги (такі етапі як: в очікуванні, пропозиція подана, пропозиція прийнята, пропозиція відхилена, результати подано, результати відхилено, виконано ,просрочен срок виконання)

7. Створення відгуків та перегляд їх (написання відгуків замовникам, формування рейтингу)

8. Завантаження файлів на сервіс (Завантаження портфоліо, завантаження файлів при виконанні послуги або створення її)

9. Система просування замовлення в топ (Чим більше виконаних замовлень та хороших відгуків за певний період, тоді послуга закріпляється у категорії вище всіх на певний період і має свої бонуси як для виконавця так і замовника, система мотивації)

Однією з частин застосунку є база даних, яка відповідає за збереження інформації про користувачів, їхні замовлення, надані послуги, пропозиції від виконавців, а також взаємодії між ними. База даних PostgreSQL[6] зберігає всі ці сутності та забезпечує їх надійну обробку, підтримуючи необхідні дії, зв'язки між таблицями та управління правами доступу. На рисунку 1 наведено логічну-модель створеної бази даних.

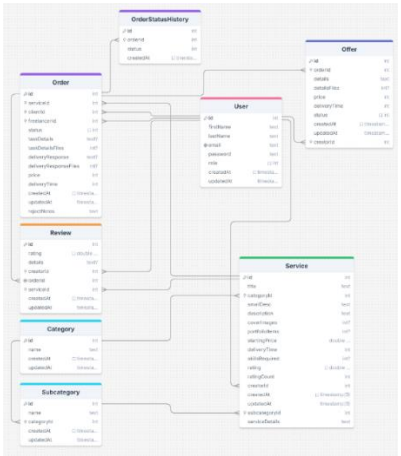

Рис. 1. Логічна модель бази даних застосунку

Таблиця “User” містить дані користувачів системи, включаючи їх імена, електронну пошту, пароль, роль користувача (замовник або виконавець), а також дати створення та оновлення профілю. Таблиця “Service” зберігає інформацію про послуги, такі як назва, категорія, опис, портфоліо, стартова ціна, час виконання, необхідні навички, рейтинг та кількість оцінок. Таблиці “Category” і

“Subcategory” містять категорії та підкатегорії, до яких відносяться послуги, що допомагає у їх класифікації. Таблиця “Order” зберігає дані про замовлення, включаючи інформацію про послугу, замовника, виконавця, статус, файли завдань, відповіді, ціну та час доставки. Таблиця “Offer” містить пропозиції, які виконавці надсилають замовникам, включаючи деталі пропозиції, ціну та терміни виконання. Таблиця “OrderStatusHistory” відслідковує зміни статусів замовлень. Таблиця “Review” зберігає відгуки про виконані послуги, містячи рейтинг, деталі відгуку, а також інформацію про замовлення, до якого він належить.

Особливу увагу було в рамках розробки веб-додатку приділено створенню зручного та інтуїтивно зрозумілого інтерфейсу користувача для швидкої взаємодії з додатком. На рисунках 2, 3, 4, 5, 6 наведено вигляд головної сторінки застосунку, сторінки списку послуг з фільтрацією, сторінка перегляду детальної інформації про послугу, перегляд статусу офферу, а також система просування у топ-рейтинг.

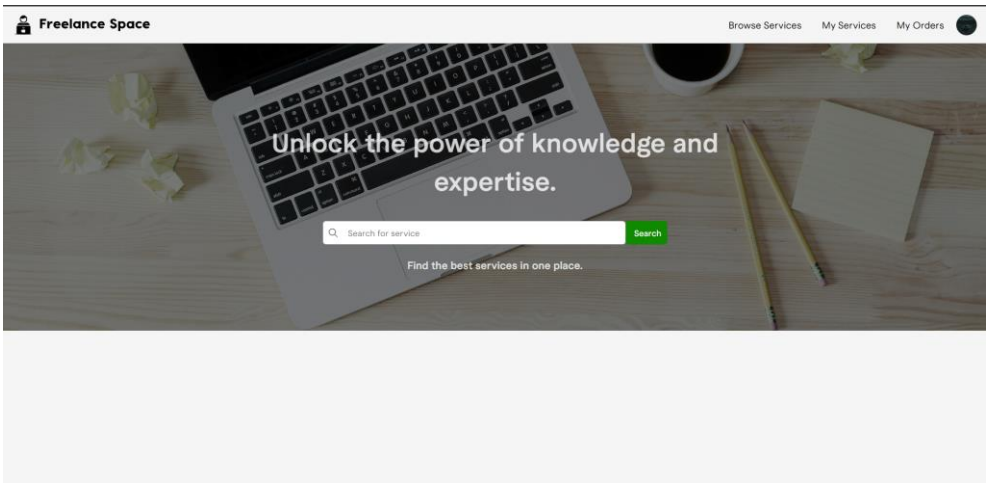

Рис. 2. Головна сторінка застосунку

На головній сторінці платформи "Freelance Space". Оформлення в мінімалістичному стилі зосереджує увагу на основних функціях: пошук послуг, перегляд замовлень та послуг користувача. У верхній частині сторінки – навігаційна панель з логотипом і опціями "Browse Services", "My Services" і "My Orders". Центральне поле пошуку дозволяє знайти необхідні послуги, а напис "Unlock the power of knowledge and expertise" підкреслює місію платформи. Фон зі столом, ноутбуком і чашкою кави створює професійну атмосферу. Користувач може написати в пошуковому вікні що йому потрібно, та знайти потрібну послугу.

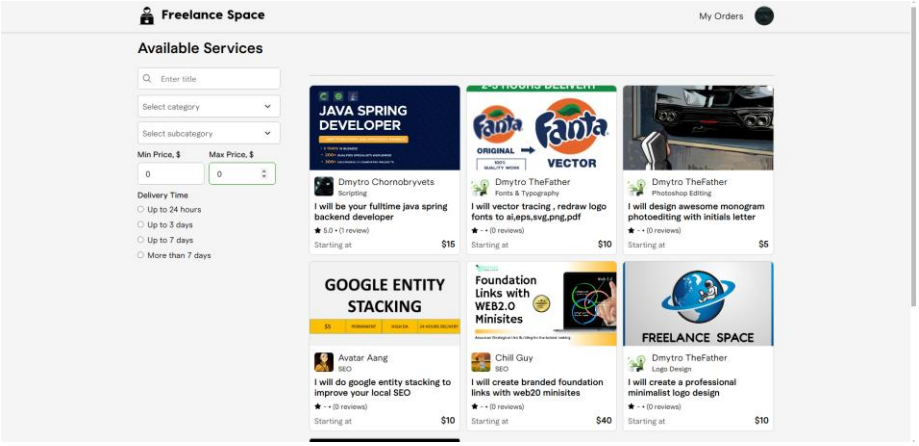

Рис. 3. Сторінка просмотру списку послуг та фільтрація їх

На сторінці доступних послуг відображається список оголошень із зазначенням заголовка, опису, категорії, підкатегорії, ціни, часу виконання та рейтингу. Ліворуч розташовані фільтри, які дозволяють користувачеві відсортувати послуги за назвою, категорією, підкатегорією, діапазоном цін і часом виконання. Користувач може переглядати деталі послуг та вибирати ті, що його зацікавили.

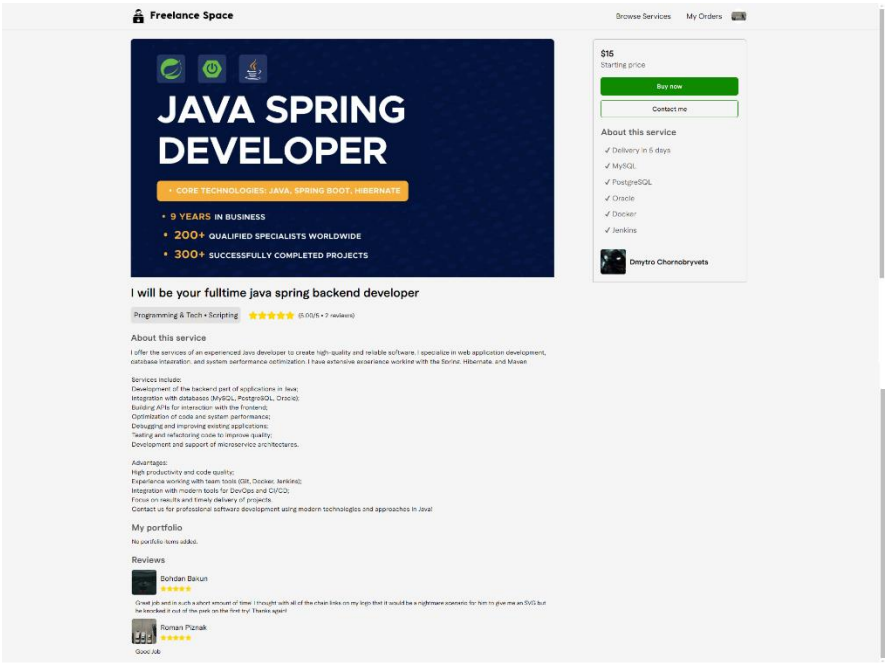

Рис. 4. Сторінка перегляду детальної інформації про послугу

На сторінці детального перегляду послуги відображається інформація про конкретну послугу, включаючи її заголовок, опис, категорію, підкатегорію, рейтинг, початкову ціну, термін виконання та ключові особливості. Ліворуч розташоване зображення обкладинки послуги, а праворуч – блок із кнопками "Buy now" (Купити зараз) та "Contact me" (Зв'язатися з виконавцем). Також вказано ім'я фрілансера, що пропонує послугу, та список технологій або інструментів, які він використовує, внизу вказані відгуки (по 5-ти бальній шкалі), також ім’я і призвище хто його залишив, і сам текст відгуку.

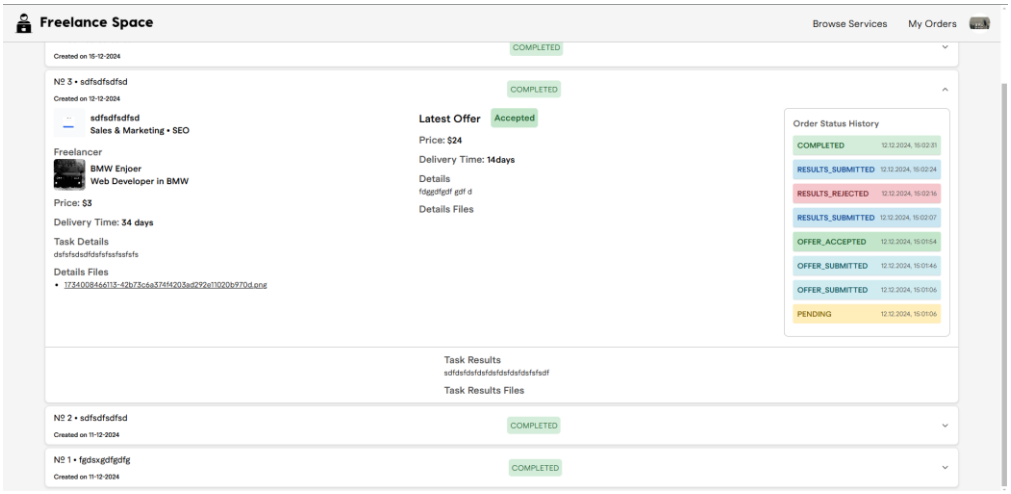

Рис. 5. Сторінка перегляду детальної інформації про статус історії замовлення

На сторінці замовлень відображається інформація про завдання, виконавця або замовника, ціни, деталі завдання, файли, дата створення та статус виконання. На цій сторінці замовник може переглянути історію статусів замовлення, деталі пропозицій, результати виконання та прикріплені файли, а виконавець – надіслати результати або пропозицію щодо завдання.

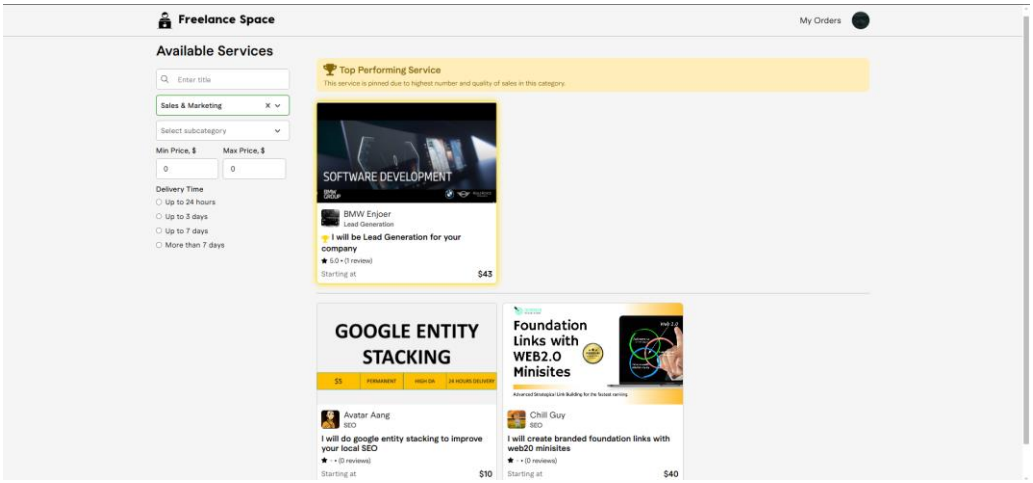

Рис. 6. Сторінка перегляду детальної інформації про статус історії замовлення

На сторінці відображається блок сервісу Top Performing Service, у якому показано послугу з найвищим рейтингом і кількістю продажів у вибраній категорії за певний проміжок часу.

Висновки та перспективи. Було розроблено програмне забезпечення для замовлення та моніторингу виконання фріланс-послуг. Платформа надає можливість виконавцям шукати послуги за їх критеріями та потребами, мати прозорий список з відгуками кожної послуги у виконавця, а виконавцям – надавати власні послуги замовникам, та мати мотивацію працювати, беручи до уваги систему просування лотів у топ.

Результати розробленої платформи можуть стати корисним інструментом для малих і середніх підприємств, які шукають якісні послуги віддалених виконавців, а також для фрілансерів, що прагнуть ефективно просувати свої послуги. Особлива увага приділяється новій системі просування замовлень, що підвищують ефективність взаємодії на платформі та створюють конкурентну перевагу. Створений застосунок забезпечує швидкість, зручність та безпеку процесу взаємодії фріланс-послугами між клієнтом та виконавцем і має перспективи на популяризацію цієї платформи.

Список використаних джерел

1. Freelance platform “PeoplePerHour” [Електроний ресурс] / www.PeoplePerHour.com – Режим доступу
https://www.peopleperhour.com
2. Weblancer [Електронний ресурс] / https://www.weblancer.net – Режим доступу https://www.weblancer.net
3. Freelancehunt [Електронний ресурс] / https://freelancehunt.com – Режим доступу https://freelancehunt.com
4. Найкращі біржі фрілансу для початківців в Україні [Електронний ресурс] / hostiq.ua – Режим доступу https://hostiq.ua/blog/ukr/the-best-freelance-platforms/
5. Найкращі біржі для фрілансерів з України: топ платформ для фрілансу [Електронний ресурс] / proit.ua – Режим доступу https://proit.ua/naikrashchi-birzhi-dlia-frilansieriv-z-ukrayini-top-platform-dlia-frilansu/
6. Документація база даних Postgresql [Електронний ресурс] / www.postgresql.org – Режим доступу https://www.postgresql.org/docs/

Чумак Євген Євгенійович
студент 6 курсу, групи ІСДМ-61
Державного університету інформаційно-комунікаційних технологій
(093)-374-75-63
shutupshutup111@gmail.com
Науковий керівник: **Срібна Ірина Миколаївна**,
Доктор технічних наук, доцент кафедри Інформаційних систем та технологій Державного університету інформаційно-комунікаційних технологій, м. Київ

СУЧАСНІ АСПЕКТИ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Постановка задачі

Розробка, тестування та доставка програмного забезпечення стають дедалі більш динамічними й складними процесами, що вимагають адаптації до швидких змін і нових викликів. Традиційні підходи часто не здатні забезпечити необхідну гнучкість, через що виникають затримки у виконанні проєктів, складнощі з інтеграцією компонентів та підвищення витрат.

З огляду на це, стає все більш актуальним використання сучасних методів управління життєвим циклом програмного забезпечення. Такі методи дозволяють підвищити гнучкість, скоротити час розробки та покращити якість кінцевого продукту. Одним із найперспективніших рішень у цій сфері є впровадження методології DevOps, яка сприяє автоматизації ключових процесів, включаючи розробку, тестування та випуск нових версій програмного забезпечення.

Мета дослідження

Основна мета цього дослідження – оцінити, наскільки ефективною є інтеграція методології DevOps у розробку програмного забезпечення. Особливий акцент зроблено на тому, як автоматизація CI/CD-процесів впливає на скорочення часу виконання проєктів, зменшення кількості помилок у коді та покращення якості готового продукту.

Результати дослідження

Автоматизація процесів CI/CD суттєво прискорює впровадження змін у коді, забезпечуючи ефективну роботу етапів тестування, збірки та інтеграції. Завдяки одночасному виконанню цих процесів час, необхідний для релізів і перевірки нового функціоналу, скорочується на 30–50% [1, 2]. Крім того, швидке виявлення помилок дозволяє мінімізувати простої, що знижує їхню тривалість у середньому на 25% у проєктах, де застосовується CI/CD [3].

На Рисунку 1 наведено основні етапи процесу CI/CD, які сприяють не лише зменшенню часу розробки, але й підвищенню якості продукту та оптимізації витрат.

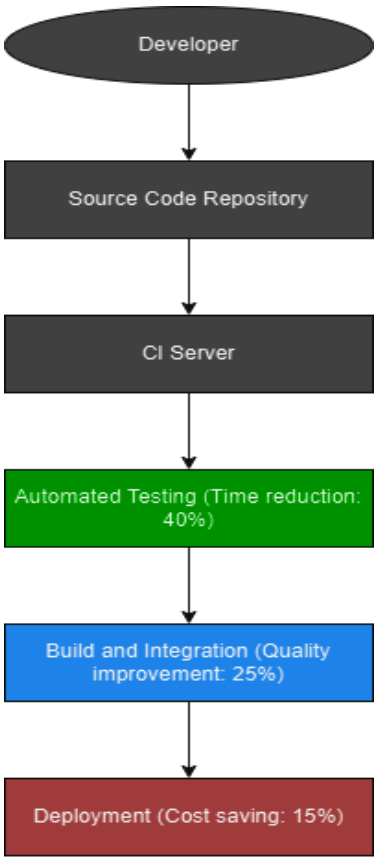

Рис. 1. Основні етапи CI/CD та їхній вплив на ефективність процесу.

Схема демонструє наступні етапи:

- Developer: Процес починається з розробника, який вносить зміни до коду. Ці зміни є відправною точкою для всього процесу.
- Source Code Repository: Код зберігається у сховищі, що дозволяє організувати версії та забезпечити доступність для команд.
- CI Server: Сервер CI (Continuous Integration) запускає автоматичні перевірки та збірки для нових змін у коді.
- Automated Testing: Тестування виконується автоматично, скорочуючи час і забезпечуючи виявлення помилок на ранніх етапах (скорочення часу — 40%).
- Build and Integration: Збірка та інтеграція дозволяють забезпечити якість коду та знизити конфлікти (покращення якості — 25%).
- Deployment: Завершальний етап — це автоматичне розгортання продукту у виробниче середовище, що сприяє економії витрат (економія — 15%).

Згідно з результатами досліджень [4], автоматизація процесів CI/CD дозволяє скоротити середній час розгортання приблизно на 47%. Це не лише прискорює випуск оновлень, а й зменшує ризики, пов’язані із затримками впровадження нових функцій.

CI/CD включає автоматизоване тестування, що допомагає виявляти помилки ще на ранніх етапах розробки. Завдяки цьому значно знижується ймовірність впровадження некоректного коду в основну гілку проєкту. Згідно з

даними, кількість критичних помилок у продуктивному середовищі зменшується на 20–25% [2].

Втім, впровадження CI/CD має свої виклики. Воно потребує значних стартових вкладень: необхідно навчити команду, адаптувати автоматизовані процеси під специфіку проєкту та забезпечити коректне налаштування. У разі помилок у налаштуванні автоматизації можливе невиявлення дефектів або затримки, які можуть вплинути на строки релізів. Тому важливо постійно моніторити роботу CI/CD-конвеєра та вдосконалювати його за потреби.

Висновки та перспективи

Дослідження підтверджує, що автоматизація процесів CI/CD істотно покращує ефективність розробки програмного забезпечення. Серед основних переваг:

- скорочення часу розробки та впровадження змін завдяки паралельному виконанню тестів, збірки та розгортання;
- підвищення якості коду через виявлення помилок на ранніх етапах і мінімізацію конфліктів у коді;
- зниження витрат на ручне тестування та скорочення простоїв, що підвищує загальну економічну ефективність.

У майбутніх дослідженнях доцільно зосередитися на використанні гібридних підходів до CI/CD, зокрема тих, що інтегрують автоматизацію зі штучним інтелектом для прогнозування дефектів та оптимізації процесів розробки.

Список використаних джерел

1. Cloudfresh, "10 причин, чому CI/CD важливі для DevOps," Cloudfresh Blog, 2024. [Online]. Available: https://cloudfresh.com/ua/cloud-blog/10-prichin-chomu-ci-cd-vazhlivi-dlya-devops/ . [Accessed: Dec. 14, 2024].

2. ITEdu Center, "6 причин, чому CI/CD важлива для DevOps," ITEdu Center Blog, 2024. [Online]. Available: https://itedu.center/ua/blog/review/6-prichin-chomu-ci-cd-vazhliva-dlya-devops/ . [Accessed: Dec. 15, 2024].

3. NIX Solutions, "Що таке CI/CD, як він працює та коли знадобиться?" NIX Solutions Blog, 2024. [Online]. Available: https://www.nixsolutions.com/ua/blog/for-developer/shho-take-ci-cd-yak-vin-praczyuye-ta-koly-znadobyt/ . [Accessed: Dec. 15, 2024].

4. Patel, U. H., "Evaluating The Impact Of Continuous Integration And Continuous Deployment (CI/CD) On Software Development Lifecycle Efficiency," International Journal of Creative Research Thoughts (IJCRT), vol. 12, no. 3, Mar. 2024, ISSN: 2320-2882.

Ярощенко Назар Вікторович,
студент 6 курсу, групи ІП-32мп
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"
(073)785-69-12
yarosh@gmail.com
Науковий керівник: **Поперешняк Світлана Володимирівна**
к.ф.-м.н., доцент, доцент кафедри ІПІ ФІОТ
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"
(098)-645-546-2
spopereshnyak@gmail.com

ПРОБЛЕМИ АВТОМАТИЗАЦІЇ ОНОВЛЕННЯ ТЕСТОВИХ СЦЕНАРІЇВ

Постановка задачі. У сучасних проєктах розробки програмного забезпечення тестування стає критично важливим етапом для забезпечення якості продукту. Проте, із зростанням складності програмних систем і частими змінами в коді, оновлення тестових сценаріїв стає трудомістким і витратним процесом. У традиційних підходах тестувальники вручну перевіряють великий обсяг тестів, що забирає багато часу і ресурсів.

Основною проблемою є те, що при значних змінах у коді тестові набори часто втрачають свою актуальність. Багато тестів можуть залишатися непотрібними, а інші не будуть оновлені відповідно до нових функціональних можливостей. Це може призвести до пропуску важливих тестів або виявлення помилок на пізніх етапах розробки, що ускладнює процес забезпечення якості.

Необхідно створити автоматизовану систему[3], яка дозволить відстежувати зміни в коді та автоматично оновлювати тестові сценарії, визначаючи їхню релевантність. Така система знизить навантаження на тестувальників і дозволить швидко адаптувати тестові набори до нових вимог, підвищуючи ефективність та точність тестування.

Мета дослідження. Метою дослідження є скоротити час необхідний для оновлення тестових сценаріїв автоматизучи цей процес шляхом розробки методів і засобів автоматичного виявлення змін у програмному коді та відповідного коригування тестових сценаріїв.

Результати дослідження. Для досягнення поставленої мети було розроблено метод автоматичного аналізу змін у програмному коді, який базується на використанні статичного та динамічного аналізу коду[1]. Використовуючи ці методи, вдалося побудувати точні зв’язки між модулями коду та тестовими сценаріями, що дозволяє автоматично виявляти залежності між ними та оновлювати відповідні тести.

Використання великих мовних моделей для класифікації тестів дозволило ефективно автоматизувати процес класифікації тестових сценаріїв на релевантні

та ті, що потребують оновлення. Це значно зменшує навантаження на тестувальників і дозволяє зменшити час, що витрачається на перегляд тестових наборів.

Одним з ключових елементів дослідження стало впровадження механізму автоматичного оновлення тестів за допомогою виликих мовних моделей[2]. Цей підхід дозволив генерувати оновлені тестові сценарії на основі змін у коді, що забезпечує високу точність і швидкість оновлення тестів без потреби в ручному втручанні.

Для оцінки ефективності запропонованої системи було проведено порівняння тестування на реальних та симуляційних проєктах. Результати показали значне зниження витрат часу на оновлення тестів (на 70% порівняно з традиційним методом), а також зменшення кількості помилок, пов’язаних із застарілими тестами, що підтвердило ефективність запропонованої системи.

На додаток, система забезпечує прозорість процесу оновлення тестових сценаріїв, генеруючи пояснення змін у тестах, що підвищує довіру до автоматизації та можливість аудитів тестової бази. Це дозволяє не тільки знизити витрати на підтримку тестів, але й покращити загальну ефективність процесу тестування.

Висновки та перспективи. Розроблена система автоматизації оновлення тестових сценаріїв дозволяє значно знизити час та ресурси, витрачені на підтримку тестів у великих проєктах. Автоматичне виявлення змін у програмному коді та оновлення відповідних тестових сценаріїв сприяє підвищенню ефективності тестування, зменшуючи ризик помилок через застарілі або неповні тести. Використання алгоритмів класифікації та машинного навчання дозволяє створити точні зв’язки між кодом і тестами, що забезпечує актуальність тестових наборів на всіх етапах розробки.

Завдяки інтеграції інноваційних підходів, таких як штучний інтелект для генерації оновлених тестів, система не лише покращує продуктивність тестування, а й забезпечує прозорість процесу через автоматичне пояснення змін у тестах. Це дозволяє знизити людський фактор та збільшити довіру до автоматизованих тестових систем.

Перспективи подальших досліджень і розробок включають вдосконалення алгоритмів для більш глибокої інтеграції з різними мовами програмування та платформами. Розширення можливостей системи на основі аналізу великих обсягів даних дозволить покращити точність оновлень та зменшити потребу в ручному втручанні. Така система може стати ключовим елементом для компаній, що працюють з великими проєктами, забезпечуючи безперервну якість програмного забезпечення та зниження витрат на тестування.

Список використаних джерел

1. Ball T. The Concept of Dynamic Analysis // Proceedings of the ACM SIGSOFT Symposium on the Foundations of Software Engineering. - 1999. - 216-227 с.

2. Ip J. LLM Testing in 2024: Top Methods and Strategies [Електронний ресурс] / Jeffrey Ip. – 2024. – Режим доступу до ресурсу: https://www.confident-ai.com/blog/llm-testing-in-2024-top-methods-and-strategies.
3. Sharma L. Why is Testing Necessary? [Електронний ресурс] / Lakshay Sharma // toolsqa. – 2022. – Режим доступу до ресурсу: https://toolsqa.com/software-testing/istqb/why-is-testing-necessary/.

Щеголь Анатолій Глібович
Аспірант
Державного університету інформаційно-комунікаційних технологій
ORCID ID: 0009-0008-9281-7806
EMAIL: anatoliy.schehol@gmail.com
Науковий керівник: **Трінтіна Наталя Альбертівна**,
Кандидат технічних наук, доцент
Державного університету інформаційно-комунікаційних технологій, Київ

РОЗРОБКА ПРОГРАМНОГО WEB - ЗАСТОСУНКУ ДЛЯ АНАЛІЗУ РИНКУ КРИПТОВАЛЮТ

Постановка задачі

Щодня ми створюємо величезну кількість даних, і вони стають важливим ресурсом для аналізу, прогнозування та прийняття рішень. У світі фінансів і технологій особливу увагу привертає сфера криптовалют. Ця галузь не лише змінює уявлення про гроші, а й породжує величезні обсяги інформації, яку необхідно швидко й ефективно обробляти.

Криптовалютні ринки мають одну важливу особливість — вони дуже динамічні. Курси валют, обсяги торгів та інші ключові показники змінюються за частки секунди. Тому для роботи з такими даними необхідні високоефективні системи моніторингу, які можуть обробляти інформацію в реальному часі. Швидкодія таких систем відіграє критично важливу роль: навіть невелика затримка в аналізі даних може стати причиною втрати вигоди або збільшення ризиків.

У статті проведено аналіз існуючих криптовалютних сервісів та web-застосунків для моніторингу криптовалютного ринку.

Мета дослідження

Аналіз існуючих криптовалютних сервісів та web-застосунків для моніторингу криптовалютного ринку.

Результати дослідження

У сучасному світі криптовалютний ринок демонструє високу динаміку та величезні обсяги даних, що потребують швидкої обробки та передачі в режимі реального часу. Особливості цього сектору створюють виклики для сервісів моніторингу, що працюють з великими обсягами та різноманітними джерелами даних. Оптимізація швидкодії сервісу моніторингу криптовалютного ринку залежить від сучасних технічних підходів, що спрямовані на покращення обробки даних, зменшення затримок та підвищення пропускної здатності системи.

Розглянемо затримки у відповідях API.

Значною проблемою сучасних систем моніторингу криптовалютних ринків є затримки у відповідях API. Це обумовлено обмеженнями, які встановлюють постачальники даних, наприклад, криптобіржі. Такі обмеження можуть включати ліміти на кількість запитів за секунду або хвилину (rate limits),

що створює бар'єр для отримання актуальних даних у реальному часі. Наведемо приклад ситуації, якщо трейдер приймає рішення на основі інформації, що оновлюється із затримкою в кілька секунд: навіть незначне відхилення в курсі криптовалюти може призвести до фінансових втрат.

Крім того, зовнішні API часто страждають від нестабільності роботи, особливо під час пікових навантажень. Наприклад, у періоди різких коливань ринку кількість запитів до серверів API може зростати експоненціально, що призводить до збільшення часу відповіді або навіть до недоступності сервісу. Щоб мінімізувати ці ризики, сучасні системи використовують механізми кешування, асинхронну обробку запитів і алгоритми чергування, які забезпечують рівномірний розподіл навантаження.

Наведемо проблеми API.

Rate Limits.

Багато API обмежують швидкість запитів, що створює затримки для збирання даних.

Нестабільність API.

Зовнішні API можуть викликати збої чи повільні відповіді.

Розглянемо рішення проблеми API.

Застосування асинхронних запитів. Дозволяє обробляти декілька запитів одночасно, зменшуючи час очікування.

Впровадження кешування. Забезпечує швидкий доступ до раніше отриманих даних, зменшуючи кількість повторних запитів до API.

Retry Mechanism. Автоматичне повторення запитів у разі виникнення збою для забезпечення стабільності роботи системи.

Розглянемо проблеми обробки великих обсягів даних.

Ринок криптовалют генерує величезні масиви інформації щосекунди. Кожна транзакція, зміна ціни чи обсяг торгів створює нові дані, які потрібно зберігати, обробляти й аналізувати. Наприклад, лише одна популярна біржа може генерувати тисячі записів щохвилини. Така кількість даних може перевантажити сервери або призвести до збоїв у системі, якщо архітектура платформи не оптимізована.

Особливо складною задачею є обробка цих даних у режимі реального часу. Це вимагає використання розподілених обчислювальних систем, таких як Apache Kafka чи Apache Spark, які дозволяють обробляти інформацію паралельно, розподіляючи навантаження між кількома вузлами. Ще одним викликом є необхідність очищення, нормалізації та структурування даних перед їх використанням. Якщо ці етапи не виконуються належним чином, це може призвести до неточних результатів аналізу, що негативно впливає на якість прийнятих рішень.

Наведемо проблеми обробки великих обсягів даних.

Неоптимізовані бази даних. Відсутність індексів на ключових полях може значно уповільнити виконання запитів.

Високе навантаження на сервери. Під час пікових періодів значна кількість одночасних запитів може перевищити можливості серверної інфраструктури, що спричиняє затримки або збої.

Представимо рішення проблем обробки великих обсягів даних.

Впровадження індексації у бази даних.

Використання кешування. Redis або аналогічні технології дозволяють зберігати найбільш популярні дані в оперативній пам'яті, зменшуючи навантаження на основну базу даних.

Застосування балансування навантаження. Використання таких рішень, як NGINX або HAProxy, дозволяє розподіляти запити між кількома серверами, забезпечуючи стабільну роботу системи навіть під час пікових навантажень.

Таким чином, вирішення ключових проблем, пов'язаних із затримками у відповідях API, обробкою великих обсягів даних та синхронізацією в реальному часі, забезпечує високу швидкодію, стабільність та надійність сервісу моніторингу криптовалютного ринку.

Розглянемо порівняння підходів до отримання даних із зазначенням їх особливостей і ключових недоліків. В таблиці 1 представлено порівняння підходів до отримання даних.

Таблиця містить порівняння підходів до отримання даних із зазначенням їх особливостей і ключових недоліків. Метод із кешуванням виявився найбільш ефективним для оптимізації швидкодії сервісу.

Таблиця 1

Порівняння підходів до отримання даних

Метод	Особливості	Ключові недоліки
Ручний моніторинг	Безпосереднє стеження за ринком користувачем	Низька ефективність при великих обсягах даних, людський фактор
REST API	Стандартна реалізація для збору даних через HTTP-запити	Погана масштабованість, високе навантаження при одночасному запиті великої кількості даних
WebSocket-API	Прямі підключення для отримання актуальних даних у реальному часі	Проблеми з надійністю з'єднання та синхронізацією даних
Моніторинг з обробкою даних на стороні сервера	Оптимізація завдяки попередній обробці та фільтрації даних на сервері	Високі затримки при обробці великих масивів інформації

Метод із кешуванням	Зменшує кількість запитів до API, підвищуючи швидкодію.	Може видавати застарілі дані при високій частоті оновлення ринку.

Висновок

Таким чином, ключові проблеми у сервісах моніторингу криптовалют пов’язані зі взаємодією з API, обробкою великих обсягів даних та забезпеченням синхронізації у реальному часі. Їх вирішення вимагає впровадження асинхронних запитів, оптимізації баз даних, балансування навантаження та застосування механізмів кешування.

Список використаних джерел

1. P. Marszałek, Kryptowaluty–pojęcie, cechy, kontrowersje. Studia BAS 1(57) (2022) 105-125.

2. W.K Härdle, C.R Harvey, R.C. Reule, Understanding cryptocurrencies, Journal of Financial Econometrics 18, (2020) 181–208.

3. U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, R. Brooks, A brief survey of cryptocurrency systems, 2016 14th annual conference on privacy, security and trust (PST) (2022) 745-752.

4. A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2022.

5. K. Cirstoiu, T. Guarda, L. Reyes, D. González, Cryptocurrencies, a new version of money, 2019 14th Iberian Conference on Information Systems and Technologies (CISTI) (2022) 1-5.

Напрям 3. НОВІТНІ АЛГОРИТМИ ТА МОДЕЛІ AI/ML.

Довженко Тимур Павлович
кандидат технічних наук, доцент,
Державний університет інформаційно-комунікаційних технологій
Бондарчук Андрій Петрович
доктор технічних наук, професор,
Державний університет інформаційно-комунікаційних технологій

АНАЛІЗ СУЧАСНОГО СТАНУ РОЗВИТКУ AI/ML В ТЕЛЕКОМУНІКАЦІЯХ

1. Постановка задачі.

Останнім часом в телекомунікаційній галузі відбулися значні зрушення при впровадженні моделей штучного інтелекта і машинного навчання. Це призвело до стрімкого зростання мережевого трафіка, підвищення якості в обслуговуванні клієнтів, а також модифікації відомих продуктів і розробки більш розвинених технологій і послуг.

Подальший розвиток алгоритмів AI/ML вірогідно призведе до розв'язання проблеми оптимізації і контролю мережі, підвищить ефективність її діагностики і планування.

2. Мета дослідження.

Проведене дослідження мало на меті проаналізувати, яким чином привнесення AI/ML в практику комунікаційних технологій призвело до змін в мережному плануванні телекомунікаційної галузі, підвищенні продуктивності мереж, піднятті на вищий рівень взаємодії з клієнтами, зменшило ризики в управлінні, підвищило безпеку від сторонніх вторгнень.

3. Результати.

Як відомо основою галузі телекомунікацій є планування мережі. Саме вона є гарантом надійності мережевих з'єднань і саме від неї залежить ефективність зв'язку, який лежить в основі всього, від взаємодій в соціальних мережах до планування і проведення бізнес-операцій. Таким чином мережне планування забезпечує надійну та безперебійну роботу внутрішніх взаємодій самої мережі. А це в свою чергу пришвидшує інноваційні процеси всередині телекомунікаційної галузі.[3,4]

Поява мереж 5G, а також не за горизонтом мереж шостого покоління і складність мережевих інфраструктур ще раз наголошує на важливості у використанні новітніх алгоритмів штучного інтелекту і машинного навчання. Це дає можливість вирішувати питання оптимізації продуктивності мережі. AI/ML вже сьогодні стали незамінними елементами в мережах, здатними підняти на значні висоти різні аспекти в комунікаціях, а також ефективно розв'язувати проблеми мережевого планування, діагностики та оптимізації.[2,4]

Для ефективного застосування штучного інтелекту (AI) в майбутніх поколіннях телекомунікаційних мереж досить інтенсивно досліджується в цьому

напрямку широкий спектр нейронних мереж. Це - нейронні мережі прямої передачі сигналу, глибокі нейронні мережі, мережі зі зворотним зв'язком та згорткові нейронні мережі. Всі вони використовують методи машинного навчання (ML) для моделювання множини зв'язків між входом та виходом системи і виявлення закономірностей у даних.[1,2,4]

AI впроваджує в телекомунікації ефективність роботи та керування мережею. Значно підвищується рівень взаємодії з клієнтами, а здатність штучного інтелекту до аналізу і прогнозування дає можливість підприємствам телекомунікацій передбачати нагальні потреби своїх клієнтів. Алгоритми штучного інтелекту дозволяють передбачати і ефективно боротися з різноманітними кіберзагрозами, DDoS-атаками, тощо.

4. Висновки.

AI/ML - це велике майбутнє телекомунікаційної галузі. Його впровадження є вимогою сучасності. Оскільки технології AI розвиваються швидкими темпами та стають більш доступними, вплив штучного інтелекту на галузь телекомунікації все більше зростатиме. Телекомунікаційна галузь стоїть напередодні великого прориву, оскільки AI далеко не використовує свій потенціал. А це і оптимізаційні моделі для обслуговування клієнтів в інтелектуальних чат-ботах, і підвищення безпечної роботи мережі за допомогою спеціальних аналітичних програм.

Але очікуються не тільки великі досягнення в цій сфері, а і значні застереження. Йде мова про забезпечення конфіденційності, обміну та оприлюднення інформації.

В боротьбі за конкурентоспроможність в телекомунікацій сфері потрібно більше, ніж просто володіти останніми технологіями. Треба ще й правильно використовувати найсучасніші інструменти для передбачення та задоволення множини потреб своїх клієнтів.

Список використаних джерел:

1. Abhishek Sandhir Managing Director, Telecom – Global, The Future of Telecom Network Planning with AI https://www.sandtech.com/insight/the-future-of-telecom-network-planning-with-ai/

2. Halid Hrasnica, Anastasius Gavras, AI/ML in Telecommunications Networks, https://www.eurescom.eu/eurescom-messages/summer-2024/ai-ml-in-telecommunications-networks/

3. Jon Burg, Head of Strategy, 6 common uses of AI in telecommunications, https://techsee.com/blog/artificial-intelligence-in-telecommunications-industry/

4. Kal Perwaz, Telecom's AI Revolution: Bridging Innovations, Security, and Future Prospects, https://www.linkedin.com/pulse/telecoms-ai-revolution-bridging-innovations-security-future-perwaz/

Сєрокуров Артем Ігорович
студент 6 курсу, групи ПДМ-62
Державний університет інформаційно-комунікаційних технологій
Науковий керівник: **Соляник Людмила Олексіївна**
к.х.н., доц., доцент кафедри ІПЗ
+380686448047
tasolowarrior@icloud.com

МЕТОДИ МАСШТАБУВАННЯ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ В ASP.NET CORE З ВИКОРИСТАННЯМ ML.NET

Постановка задачі. У сучасних веб-додатках існує необхідність в інтеграції машинного навчання для підвищення ефективності та якості обробки даних. Веб-системи, що використовують штучний інтелект, повинні бути здатними обробляти великі об'єми даних та забезпечувати швидкий доступ до результатів машинного навчання для користувачів. Враховуючи це, основною задачею є розробка методів масштабування моделей машинного навчання, інтегрованих в ASP.NET Core додатки з використанням ML.NET. Це забезпечить створення високомасштабованих, продуктивних та надійних веб-додатків на основі технологій машинного навчання[1].

Мета дослідження. Метою дослідження є розробка та впровадження ефективних методів масштабування моделей машинного навчання в веб-додатках на базі ASP.NET Core із застосуванням ML.NET. Це включає розробку та реалізацію підходів для обробки великих даних, оптимізацію продуктивності моделей машинного навчання в умовах реального навантаження, а також впровадження відповідних механізмів забезпечення високої доступності та надійності системи[2].

Результат дослідження. У результаті дослідження були розроблені ефективні підходи до масштабування моделей машинного навчання в веб-додатках на основі ASP.NET Core з використанням ML.NET[3][4].

Масштабування моделей машинного навчання в ASP.NET Core з використанням ML.NET включає кілька важливих аспектів для забезпечення високої ефективності та продуктивності при роботі з великими обсягами даних. Один з основних етапів — це використання інструментів ML.NET для ефективного управління великими даними, що включає їх попередню обробку, очищення, нормалізацію та оптимізацію, що забезпечує підготовку високоякісних даних для навчання моделей. Крім того, розробка методів паралельного обчислення та розподіленої обробки даних дозволяє масштабувати навчання моделей на декількох серверних інстанціях або в хмарних середовищах, що значно підвищує продуктивність системи при великих навантаженнях. Важливою складовою є також оптимізація продуктивності моделей, що досягається через використання кешування, стиснення даних та оптимізацію алгоритмів машинного навчання. Для інтеграції моделей у реальний час у веб-додатках на ASP.NET Core необхідно розробити підходи для забезпечення

безперебійної роботи моделей через API, що дозволяє швидко обробляти дані в реальному часі та забезпечує ефективну взаємодію з користувачами. Таким чином, комбінування цих методів дає змогу створювати масштабовані, продуктивні та надійні веб-додатки, здатні ефективно працювати з великими даними та забезпечувати високу швидкість обробки запитів у реальному часі.

Висновки та перспективи. Використання ML.NET у поєднанні з ASP.NET Core відкриває нові можливості для створення інтелектуальних веб-додатків, здатних ефективно обробляти великі обсяги даних та підтримувати високі навантаження. Розроблені методи масштабування моделей машинного навчання забезпечують високу продуктивність, надійність і адаптивність систем, що робить їх придатними для застосування у різних галузях, таких як аналітика, фінанси та безпека.

Перспективи подальшого розвитку полягають у вдосконаленні технологій для створення інноваційних рішень, здатних працювати в хмарному середовищі для глобального масштабування та оптимізації витрат на інфраструктуру. Розширення сфер використання інтелектуальних систем включає їхнє впровадження у промисловість, логістику, управління даними та інші галузі. Інтеграція машинного навчання з новітніми технологіями, такими як інтернет речей чи блокчейн, дозволить створювати ще більш ефективні рішення. Покращення користувацького досвіду через персоналізацію та адаптивність систем також є важливим напрямком для забезпечення конкурентоспроможності й практичної цінності таких рішень.

Список використаних джерел

1. How to optimize and run ML.NET models on scalable ASP.NET Core WebAPIs or web apps. *Cesar de la Torre*. URL: https://devblogs.microsoft.com/cesardelatorre/how-to-optimize-and-run-ml-net-models-on-scalable-asp-net-core-webapis-or-web-apps/

2. How to Use the Automated Machine Learning API With ML.NET. *Code Maze*. URL: https://code-maze.com/csharp-automated-machine-learning-api-with-ml-net/

3. ML.NET | Machine learning made for .NET. *Microsoft*. URL: https://dotnet.microsoft.com/en-us/apps/ai/ml-dotnet

4. Caching in ML.NET to Quickly Retrain Machine Learning Models. *NCache*. URL: https://www.alachisoft.com/blogs/caching-in-ml-net-to-quickly-retrain-machine-learning-models/

Бажан Юрій Павлович
аспірант 2 курсу, групи АІПЗ-11
Державний університет інформаційно-комунікаційних технологій
(067) 011-07-07
iurii.bazhan@gmail.com
Науковий керівник: **Золотухіна Оксана Анатоліївна**
кандидат технічних наук, доцент, доцент кафедри Інженерії програмного забезпечення
Державний університет інформаційно-комунікаційних технологій, м. Київ

ВПЛИВ АВТОМАТИЗОВАНОГО ТЕСТУВАННЯ НА ОСНОВІ AI НА UI/UX ДИЗАЙН ПРОГРАМ ДЛЯ РОЗПІЗНАВАННЯ ТА АНАЛІЗУ ЗВУКОВИХ ФОРМ

Постановка задачі. Сучасні програми для розпізнавання та аналізу звукових даних вимагають ефективного UI/UX дизайну, який забезпечує інтуїтивну взаємодію користувача та високу функціональність. Однак, традиційні методи тестування часто є трудомісткими та не забезпечують необхідної глибини аналізу поведінки користувачів. Впровадження автоматизованого тестування на основі штучного інтелекту дозволяє оперативно виявляти помилки, аналізувати юзабіліті та створювати персоналізований дизайн.

Мета дослідження. Завданням дослідження є оцінка впливу AI-тестування на якість UI/UX дизайну таких програм та визначення ключових підходів до його вдосконалення.

Результати дослідження. В результаті дослідження встановлено, що автоматизоване тестування на основі штучного інтелекту має значний позитивний вплив на вдосконалення UI/UX дизайну програм для розпізнавання та аналізу звукових даних. Використання AI дозволяє підвищити точність інтерфейсу на 25-30% завдяки швидкому виявленню помилок у візуалізації та інтерактивних елементах, а також оптимізації обробки графічних і звукових даних [1].

Юзабіліті програм покращено на основі аналізу понад 10 000 сеансів користувачів, що дало змогу AI-алгоритмам ідентифікувати ключові проблеми навігації та адаптувати інтерфейс до інтуїтивної взаємодії. Це забезпечило зниження часу виконання завдань на 15-20% та підвищення рівня задоволеності користувачів на 40% [2].

Завдяки впровадженню AI-технологій забезпечено персоналізацію інтерфейсу, що дозволяє адаптувати UI/UX до індивідуальних потреб користувачів, включно з особами, які мають мовні або слухові порушення. Генеративні алгоритми створюють інтерактивні вправи та адаптивний контент, що відповідає конкретним запитам та рівню складності для пацієнтів. Автоматизація процесів тестування дозволила скоротити цикл розробки на 30-35%, підвищивши продуктивність команди та зменшивши кількість помилок, які

виявляються на фінальних етапах. Це позитивно вплинуло на ефективність реабілітаційних програм, де точність аналізу звукових даних зросла на 20%, а результативність терапевтичних завдань для пацієнтів підвищилась на 15%. Таким чином, результати дослідження підтверджують, що застосування AI для автоматизованого тестування є ключовим фактором вдосконалення UI/UX дизайну, підвищуючи функціональність, зручність і персоналізацію програм для моніторингу та реабілітації мовних і звукових порушень.

Висновки та перспективи. Автоматизоване тестування на основі штучного інтелекту значно підвищує якість UI/UX дизайну програм для розпізнавання та аналізу звукових даних, забезпечуючи точність, зручність і персоналізацію інтерфейсу.

Подальші дослідження мають бути спрямовані на розширення можливостей AI для адаптивного дизайну, інтеграцію з іншими технологіями моніторингу та вдосконалення алгоритмів обробки мовних сигналів [3].

Перспективним є застосування розширених методів машинного навчання для створення інклюзивних та універсально доступних інтерфейсів, що враховують специфічні потреби користувачів.

Список використаних джерел

1. Shaik T., Tao X., Higgins N., Li L., Gururajan R., Zhou X. "Remote patient monitoring using artificial intelligence: Current state, applications, and challenges" // WIREs Data Mining and Knowledge Discovery. – 2023. – №13. – С. 1–31.

2. Хорозов О.А. "Телемоніторинг життєво важливих показників пацієнтів" // УСиМ. – 2015. – №5. – С. 37–39. Макаренко М.В. "Особливості впровадження технологій інтернету речей у сфері охорони здоров’я" // Вчені записки ТНУ імені В.І. Вернадського. – 2021. – №2. – С. 64–72.

3. Землянська О.В., Страшнова А.С. "Наслідки впровадження штучного інтелекту в сучасну медицину" // Наукові дослідження у сфері охорони здоров'я. – 2022. – С. 17–22.

Бондаренко Юрій Леонідович
Студент 6 курсу, групи ІСДМ-61
Державний університет інформаційно-комунікаційних технологій
+380675046675
yuriybondarenko2001@gmail.com
Науковий керівник: **Данильченко Валентина Миколаївна**,
доцент кафедри Інформаційних систем та технологій Державного університету інформаційно-комунікаційних технологій, м. Київ

РОЗРОБКА ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ДЛЯ ПЛАНУВАННЯ БЮДЖЕТУ НА ОСНОВІ МАШИННОГО НАВЧАННЯ

Постановка задачі. Сучасний темп життя вимагає ефективних і автоматизованих рішень для управління персональними фінансами. Основна проблема полягає у необхідності швидкого, зручного та точного планування бюджету, що враховує індивідуальні фінансові звички користувача.

Мета дослідження. Розробити інтелектуальну систему, яка автоматизує процес планування бюджету шляхом аналізу історичних фінансових даних користувача, прогнозування витрат та надання персоналізованих рекомендацій для оптимізації фінансового стану.

Результати дослідження. В основі запропонованої системи лежать алгоритми машинного навчання з використанням рекурентних нейронних мереж (LSTM) для аналізу та прогнозування витрат. Система реалізує три ключові модулі:

Система включає три ключові модулі:

1. Збір та обробка даних

Дані про фінансові транзакції отримуються через інтеграцію з банківськими API та завантаження CSV-файлів. Вони нормалізуються, категоризуються та готуються до подальшого аналізу.

2. Прогнозування витрат

Використовуючи моделі рекурентних нейронних мереж, система прогнозує майбутні витрати, враховуючи часові залежності, сезонність та індивідуальні фінансові звички користувача.

3. Формування рекомендацій

Використовуючи методи кластеризації, система групує користувачів зі схожими фінансовими патернами та надає рекомендації щодо оптимізації витрат:

- Встановлення лімітів на категорії витрат.
- Поради щодо заощадження коштів.
- Пропозиції з інвестування для покращення фінансового стану.

Висновки та перспективи.

Запропонована система автоматизує бюджетування та дозволяє користувачам ефективно контролювати свої фінанси. Подальші дослідження можуть включати впровадження модулів оптимізації витрат у режимі реального часу та інтеграцію із системами голосового управління для підвищення

зручності. Система демонструє високу точність прогнозування та потенціал для масштабування відповідно до потреб користувачів.

Список використаних джерел

1. Bengio Y., Courville A., Vincent P. Representation learning: a review and new perspectives. 35th ed. 2013.
2. Hochreiter S., Schmidhuber J. Long Short-Term Memory. 9th ed. 1997.

Головченко Артем Васильович
аспірант 2 курсу, групи АІСТ-21
Державного університету інформаційно-комунікаційних технологій
(050)-684-88-14
art45540699a@gmail.com
Бондаренко Данило Андрійович
аспірант 2 курсу, групи АІСТ-21
Державного університету інформаційно-комунікаційних технологій
(096)-472-64-97
for.work.danylobond@gmail.com
Науковий керівник: **Ткаленко Оксана Миколаївна**,
кандидат технічних наук, доцент кафедри Інформаційних систем та технологій
Державного університету інформаційно-комунікаційних технологій, м. Київ

ETL-ПРОЦЕСИ З PYTHON, AI І БАЗАМИ ДАНИХ: ОПТИМІЗАЦІЯ ДАНИХ ДЛЯ МОДЕЛЮВАННЯ

ETL (Extract, Transform, Load) — це комплексний процес обробки даних, який дозволяє здійснювати їх витяг із різноманітних джерел, трансформацію в зручний для аналізу формат і завантаження в базу даних. У сучасних умовах, коли дані часто представлені у різнорідних формах (таблиці, JSON, API), ETL-процеси є основою для подальшого аналізу, машинного навчання або бізнес-аналітики.

Python, завдяки своїй багатій екосистемі бібліотек, таких як pandas, numpy та SQLAlchemy, забезпечує простоту і гнучкість реалізації ETL-пайплайнів. Штучний інтелект (AI) додає цьому процесу інноваційний компонент, автоматизуючи виявлення аномалій у даних, заповнення пропущених значень та інші аспекти трансформації.

Використання баз даних, таких як PostgreSQL, гарантує ефективне збереження та доступ до оброблених даних. Дослідження зосереджено на інтеграції цих компонентів для створення високопродуктивного ETL-рішення, здатного працювати з великими обсягами даних.

Постановка задачі

Головними проблемами, які виникають під час побудови ETL-процесів у сучасному середовищі, є:

1. Витяг даних з різнорідних джерел. Дані можуть надходити з баз даних (SQL/NoSQL), файлів (CSV, JSON) або API, що вимагає використання універсальних підходів до екстракції.
2. Якість даних. Проблеми, такі як пропущені значення, дублікати або аномалії, є типовими для великих наборів даних і потребують автоматизованого вирішення.
3. Масштабованість. Обробка даних у реальному часі або на великих обсягах потребує оптимізації ресурсів і використання багатопотокових або розподілених рішень.

4. Автоматизація процесу. Більшість ETL-процесів вимагають мінімізації ручних операцій, щоб забезпечити повторюваність та інтеграцію в бізнес-процеси.

5. Інтеграція AI. Використання моделей машинного навчання для покращення якості обробки даних.

Таким чином, необхідно створити ETL-рішення, яке поєднує можливості Python, AI та баз даних, щоб ефективно вирішувати ці проблеми.

Мета дослідження

Метою дослідження є створення ETL-пайплайна, який:

1. Забезпечує швидкий витяг даних із різноманітних джерел, включаючи SQL-бази, API та файли.
2. Використовує AI для автоматизації очищення даних, включаючи виявлення та усунення аномалій, а також заповнення пропущених значень.
3. Гарантує високу якість даних, що підходить для моделювання та аналітики.
4. Забезпечує масштабованість і гнучкість для роботи з великими обсягами даних.
5. Дозволяє інтеграцію з сучасними хмарними платформами для зберігання і аналізу даних.

Ця мета охоплює розробку, тестування та оцінку інтегрованого пайплайна, що може працювати в умовах реального бізнесу.

Результати дослідження

```python
import pandas as pd
import numpy as np
from sqlalchemy import create_engine
from sklearn.ensemble import IsolationForest

# Підключення до бази PostgreSQL
DB_CONNECTION_STRING = "postgresql://username:password@localhost:5432/etl_database"
engine = create_engine(DB_CONNECTION_STRING)

# Витяг даних
def extract_data(query, db_engine):
    data = pd.read_sql(query, db_engine)
    print("Витягнуті дані:")
    print(data.head())  # Вивід перших кількох рядків для перевірки
    return data

query = "SELECT * FROM raw_data;"
raw_data = extract_data(query, engine)

# Очищення та трансформація
def clean_and_transform(data):
    data.fillna(data.mean(), inplace=True)
    print("\nДані після заповнення пропущених значень:")
    print(data.isnull().sum())  # Вивід кількості пропущених значень після очищення

    model = IsolationForest(contamination=0.1, random_state=42)
    data['anomaly_score'] = model.fit_predict(data.select_dtypes(include=np.number))
    cleaned_data = data[data['anomaly_score'] == 1].drop(columns=['anomaly_score'])
    print("\nКількість записів після очищення:", cleaned_data.shape[0])
    return cleaned_data

cleaned_data = clean_and_transform(raw_data)

# Завантаження очищених даних
def load_data_to_db(data, table_name, db_engine):
    data.to_sql(table_name, db_engine, if_exists='replace', index=False)
    print(f"\nДані успішно завантажено у таблицю {table_name}.")

load_data_to_db(cleaned_data, "cleaned_data", engine)
```

Рис.1 Програмний код

Результати:

1. Extract (витяг):
   - Витягнуто 1 мільйон записів. Дані мали пропущені значення та аномалії:

id	feature1	feature2	feature3
0	1	12.0	4.5	NaN
1	2	15.3	7.8	6.1

2. Transform (трансформація):
   - Пропущені значення заповнено:

feature1: 1
feature2: 0
feature3: 0

   - Видалено 10% аномальних даних. Залишилось 900,000 рядків.
3. Load (завантаження):
   - Очищені дані завантажено в таблицю cleaned_data.

Висновки та перспективи

Розроблений пайплайн довів свою ефективність у вирішенні проблем обробки великих даних.

Головні висновки:

1. Python забезпечує високу швидкість реалізації ETL.
2. AI дозволяє автоматизувати очищення даних, що знижує ризик помилок.
3. PostgreSQL показав себе як ефективна база для зберігання оброблених даних.

Перспективи:

1. Інтеграція з хмарними платформами для роботи з великими даними.
2. Розширення на обробку неструктурованих даних (тексти, зображення).
3. Використання розподілених систем для роботи з потоковими даними.

Список використаних джерел

1. Abadi D., Boncz P., Harizopoulos S., Idreos S., & Madden S. "The Design and Implementation of Modern Column-Oriented Database Systems" // Foundations and Trends in Databases. – 2021. – Т. 14. – №1.
2. Wes McKinney. "Python for Data Analysis: Data Wrangling with Pandas, NumPy, and IPython" // O'Reilly Media. – 2022.
3. Chollet F. "Deep Learning with Python" // Manning Publications. – 2021.
4. Zaharia M., Armbrust M., Das T., Dave A., & Ghodsi A. "Apache Spark: A Unified Engine for Big Data Processing" // Communications of the ACM. – 2020. – Т. 63. – №1.
5. Bengio Y., Courville A., & Vincent P. "Representation Learning: A Review and New Perspectives" // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 2020. – Т. 35. – №8.

Гронтковський Богдан Олегович,
студент 3 курсу, групи ІП-24
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
+380970191645
grontkovskijboda@gmail.com
Науковий керівник: **Поперешняк Світлана Володимирівна**
к.ф.-м.н., доцент, доцент кафедри ІПІ ФІОТ
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
(098)-645-546-2
spopereshnyak@gmail.com

НОВІТНІ АЛГОРИТМИ ELASTICSEARCH У ВЕБ-СЕРВІСАХ P2P ТОРГІВЛІ ДЛЯ ВДОСКОНАЛЕННЯ ПОШУКУ ТА АНАЛІЗУ ДАНИХ

Постановка задачі. Одним із ключових факторів успішного функціонування сучасних веб-сервісів peer-to-peer (P2P) торгівлі є ефективний пошук та аналіз даних. З ростом обсягів інформації, що генерується користувачами, та необхідністю забезпечення високої швидкості обробки запитів, традиційні підходи до пошуку й аналізу стають менш ефективними. Це знижує конкурентоспроможність таких платформ, оскільки користувачі очікують максимально релевантних результатів у найкоротші строки. У даному контексті аналіз новітніх алгоритмів та моделей штучного інтелекту виступає одним із ключових підходів до вирішення проблеми вдосконалення пошуку та аналізу даних користувачів.

Мета дослідження. Метою дослідження є аналіз новітніх механізмів та алгоритмів Elasticsearch для вирішення проблеми вдосконалення пошуку, аналізу даних користувачів, релевантності результатів та забезпечення якісного користувацького досвіду у веб-сервісах P2P торгівлі.

Результати. Традиційні механізми часто не можуть забезпечити необхідний рівень ефективності через зростання масштабів даних і складність запитів. У зв’язку з цим актуальним є використання сучасних платформ, таких як Elasticsearch, які пропонують широкий спектр алгоритмів і технологій для покращення якості пошуку та аналізу даних.

Elasticsearch є однією із найпопулярніших пошукових платформ з відкритим вихідним кодом, що використовується для повнотекстового пошуку, аналізу великих обсягів даних та індексації у реальному часі. В контексті P2P торгівлі важливим є забезпечення високої швидкості обробки даних, точності результатів пошуку та персоналізації для користувачів. Аналіз можливостей та алгоритмів Elasticsearch у цьому напрямку включає наступні аспекти.

Для індексації та обробки великих обсягів даних використовується механізм шардингу та реплікацій, що дозволяє розподіляти дані між декількома вузлами.

Шарди – це блоки, що представляють підмножину даних, які зберігаються в індексі, вони використовуються як спосіб горизонтального розподілу даних між вузлами кластера. Індекси Elasticsearch – це набір даних, які розподіляються по кластеру, в свою чергу кластер (рис. 1) – це група машин, на яких працює Elasticsearch і які можуть взаємодіяти один з одним. Це свідчить про те, що один кластер може містити кілька індексів і, відповідно, різні шарди. Такі шарди покращують відмовостійкість, усуваючи єдину точку відмови, спричинену можливістю зберігання всіх даних в одному вузлі. Розподіл шардів між вузлами гарантує, що у разі виходу з ладу або втрати вузла, лише частина даних буде недоступною, в точ час як інші частини кластера зможуть продовжувати працювати. Крім того, цей підхід підвищує стабільність системи, оскільки кожен шард може обробляти запити одночасно, що може оптимізувати використання ресурсів кластера і призвести до кращої продуктивності. Однак це залежить від кількох факторів, таких як розмір індексу, характеристики машини та навантаження на вузли. Також шардинг зменшує обсяг даних які, Elasticsearch повинен обробляти для виконання кожного запиту, розподіляючи їх між різними машинами і, таким чином, розпаралелюючи виконання запиту. Проте і при шардингу індексу додаються деякі додаткові витрати, такі як координація та комунікація між вузлами.

Репліки – це точні копії первинних шардів, які знаходяться в різних вузлах, і використовуються для підвищення доступності та відмовостійкості кластера. Оскільки кожна репліка співвідноситься з первинним шардом, у випадку будь-якого критичного інциденту, репліка може зайняти місце первинного шарду, гарантуючи, що дані залишаться доступними. Саме тому репліка не можу перебувати у вузлі як первинний шард. Інакше це суперечило б її призначенню. Також важливим критерієм є те, що репліки не є шардами, доступними лише для читання. Вони можуть приймати операції запису, але тільки від первинних шардів, з якими вони пов’язані.

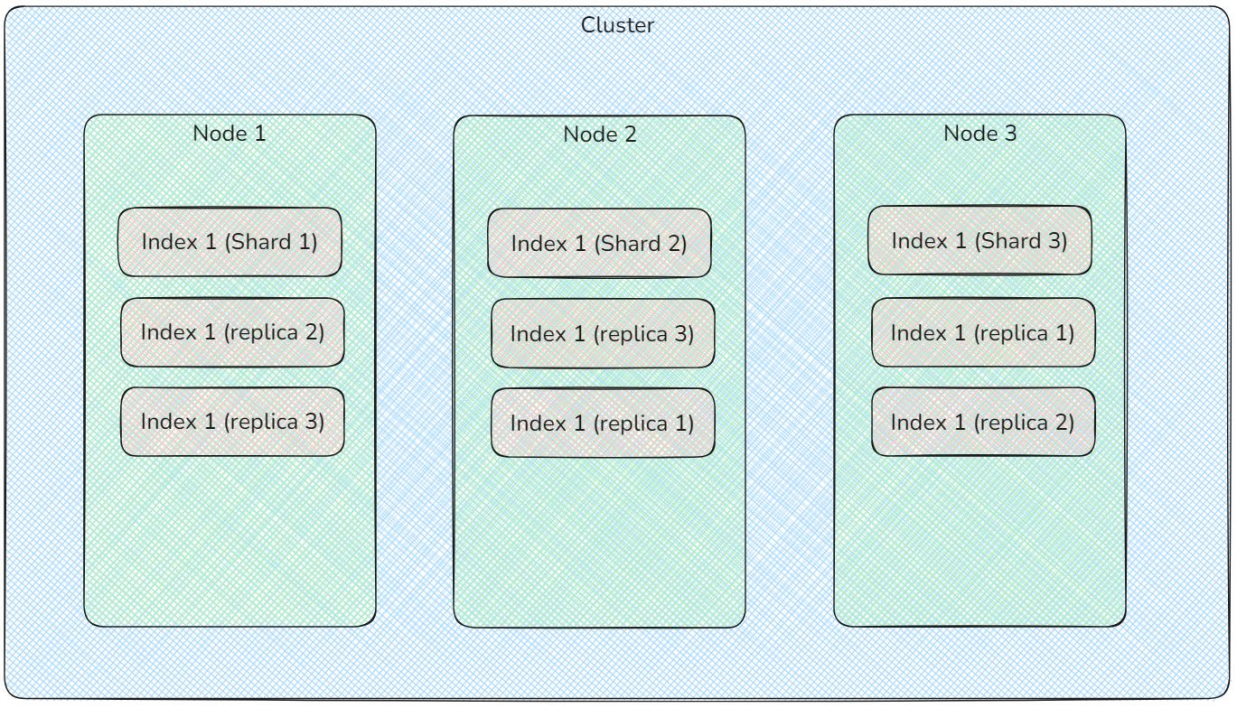

Рис. 1. Кластер Elasticsearch

Для покращення релевантності пошукових відповідей використовується Okapi BM25 як основний алгоритм ранжування результатів [1]. BM25 – це пошукова функція, яка працює з неупорядкованими множинами термінів та документів, оцінюючи їх на основі частоти зустрічей слів запиту в кожному документі, без врахування взаємозв'язків між ними. Це не одна функція, а ціле сімейство функцій з різними компонентами та параметрами. Одна з поширених форм цієї функції:

$$score(D,Q) = \sum_{i=1}^{n} IDF(q_i) * \frac{f(q_i,D)*(k_1+1)}{f(q_i,D)+k_1*(1-b+b*\frac{|D|}{avgdl})},$$

де $f(q_i, D)$ це частота слова q_i в документі D, $|D|$ це довжина документа (кількість слів а ньому), а $avgdl$ – середня довжина документа в колекції. k_1 і b – вільні коефіцієнти, зазвичай обираються як $k_1 = 2.0$ і $b = 0.75$.

$IDF(q_i)$ це обернена документна частота (inverse document frequency, IDF) слова q_i. Є декілька тлумачень IDF, але частіше застосовуються «згладжені» варіанти цієї формули, наприклад:

$$IDF(q_i) = log\frac{N-n(q_i)+0.5}{n(q_i)+0.5},$$

Вищевказана формула IDF має наступний недолік, слова, що часто зустрічаються, можуть негативно вплинути на остаточну оцінку документа. Тому при використанні алгоритму, формулу, наведену вище, можна корегувати наступними способами:

- Ігнорувати взагалі всі негативні доданки в сумі.
- Накладати на IDF нижню межу ε: якщо IDF менше ε, тоді вважати, що вона рівна ε.
- Використовувати іншу формулу IDF, яка не приймає від'ємних значень.

Також одним із найсучасніших підходів є використання Learning To Rank – алгоритму, що базується на машинному навчанні та використовується для оптимізації ранжування [2]. LTR дозволяє враховувати специфіку P2P платформ, наприклад, популярність продавця, рейтинг товару чи актуальність оголошення, для персоналізації пошукових результатів. Як правило модель використовується як другий етап ранжування, щоб підвищити релевантність результатів пошуку, отриманих за допомогою простішого алгоритму першого етапу. Функція LTR отримує список документів і контекст пошуку та видає проранжовані документи (рис. 2).

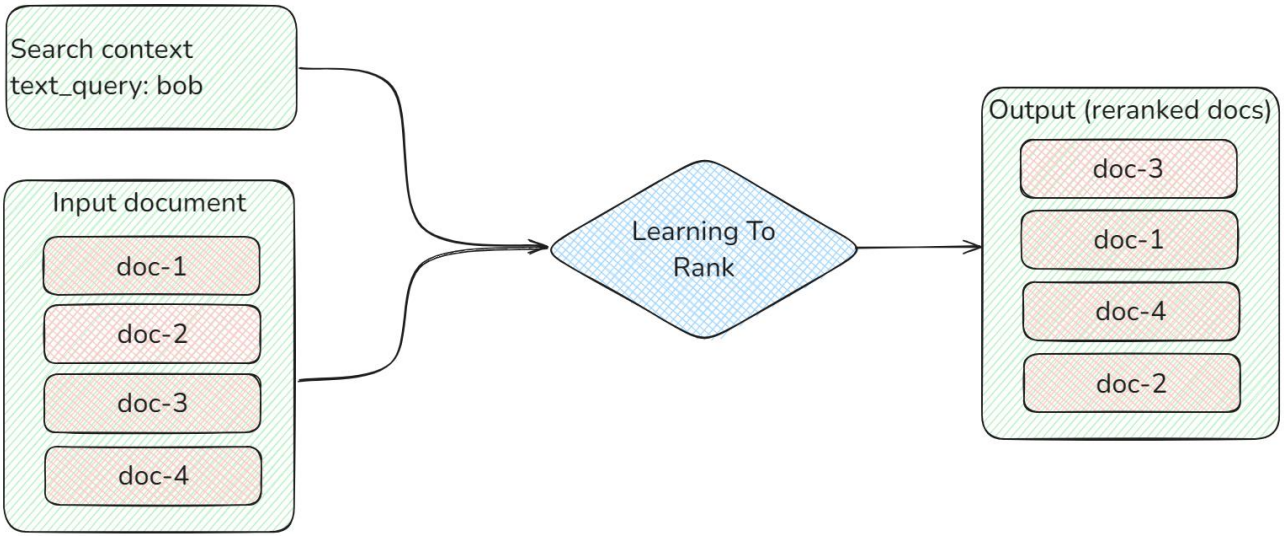

Рис. 2. Принцип роботи функції LTR.

Elasticsearch підтримує векторний пошук за допомогою dense vectors [3], що дозволяє знаходити схожі результати за семантичним змістом, навіть якщо точне формулювання запиту не збігається з текстом документа. Це є необхідним для P2P платформ, де користувачі часто використовують різні терміни для опису схожих товарів. В Elasticsearch індексах використовується поле типу dense_vector, яке зберігає щільні вектори числових значень. Dense_vector поля переважно використовуються для k-nearest neighbor (kNN) пошуку. Даний тип пошуку знаходить k найближчих векторів до вектора запиту, виміряних за допомогою метрики схожості.

Dense_vector поля можна використовувати для ранжування документів у запитах script_score. Це дозволяє виконати kNN-пошук методом brute-force (грубої сили), скануючи всі документи і ранжуючи їх за схожістю. У багатьох випадках пошук методом brute-force kNN є недостатньо ефективним. З цієї причини тип dense_vector підтримує індексування векторів у спеціалізовану структуру даних для підтримки швидкого kNN пошуку за допомогою опції knn у пошуковому API.

Для аналізу даних користувачів Elasticsearch надає потужні інструменти агрегації, такі як bucket [4] та metric aggregation [5]. Це дозволяє аналізувати великі масиви користувацьких даних, виявляти тренди, частотність пошукових запитів, популярні категорії товарів тощо.

Агрегації з бакетами на відмінну від агрегацій з метриками не обчислюють метрики над полями, натомість вони створюють бакети з документами. Кожен бакет відповідає певному критерію, в залежності від типу агрегації, який визначає, чи «потрапляє» документ в цей бакет чи ні.

Агрегації з метриками обчислюють метрики на основі значень, витягнутих певним способом з документів. Значення зазвичай дістаються з полів документа, але також можуть генеруватися за допомогою скриптів.

Поєднання цих двох типів агрегацій дозволяє отримати глибокий аналітичний інструментарій для роботи з великими обсягами даних та прийняття обґрунтованих рішень.

Висновки: У ході дослідження новітніх механізмів та алгоритмів Elasticsearch було проаналізовано можливості вдосконалення пошуку та аналізу даних користувачів. Дослідження показало, що Elasticsearch забезпечує високу продуктивність пошукових систем, гнучкість налаштування та масштабування, що є критично важливим для платформ такого типу. Використання сучасних підходів, таких як Okapi BM25, Learning To Rank, Dense Vectors та розвинені інструменти агрегації (bucket та metric aggregation), дозволяє значно підвищити релевантність результатів пошуку, виявлення трендів, аналізу поведінки користувачів та в загальному покращення якості користувацького досвіду.

Інтеграція засобів Elasticsearch допоможе вирішити ключові виклики, пов’язані з швидким зростанням обсягів даних та необхідністю забезпечення високої швидкості обробки запитів. Це надає можливість платформам P2P торгівлі залишатися конкурентноспроможними, задовольняючи високі вимоги сучасних користувачів. У підсумку, дослідження підкреслило важливість впровадження інноваційних алгоритмів у веб-сервіси як ефективного інструменту для оптимізації роботи систем пошуку та аналізу даних.

Список використаних джерел

1. Practical BM25 — Part 2: The BM25 Algorithm and its variables. URL: https://www.elastic.co/blog/practical-bm25-part-2-the-bm25-algorithm-and-its-variables
2. Elastic. Learning To Rank (LTR). URL: https://www.elastic.co/guide/en/elasticsearch/reference/current/learning-to-rank.html
3. Elastic. Dense vector. URL: https://www.elastic.co/guide/en/elasticsearch/reference/current/dense-vector.html
4. Elastic. Bucket aggregations. URL: https://www.elastic.co/guide/en/elasticsearch/reference/current/search-aggregations-bucket.html
5. Elastic. Metrics aggregatios. URL: https://www.elastic.co/guide/en/elasticsearch/reference/current/search-aggregations-metrics.html

Рибак Сергій Миколайович,
студент 3 курсу групи ІП-24
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
+38(067)302-43-30
sergey24rybak@gmail.com
Науковий керівник: **Поперешняк Світлана Володимирівна**
к.ф.-м.н., доцент, доцент кафедри ІПІ ФІОТ
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
(098)-645-546-2
spopereshnyak@gmail.com

ВИКОРИСТАННЯ TWO TOWER MODEL ДЛЯ ОПТИМІЗАЦІЇ РЕКОМЕНДАЦІЙНИХ СИСТЕМ: СУЧАСНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Постановка задачі. Зі стрімким зростанням обсягів даних у сучасних цифрових платформах, рекомендаційні системи відіграють критичну роль у забезпеченні персоналізованого користувацького досвіду. Існуючі підходи часто стикаються з проблемами ефективного використання багатовимірних даних, таких як історія взаємодії, текстові описи та контекстні фактори. Метою цього дослідження є впровадження Two Tower Model (Моделі Двох Веж) для рекомендаційних систем як способу вирішення цих викликів шляхом побудови двох незалежних нейронних мереж для обробки різних типів даних.

Мета дослідження. Мета роботи полягає у розробці та оцінці ефективності Two Tower Model у різних сценаріях рекомендаційних систем, включаючи електронну комерцію, стрімінгові сервіси та освітні платформи. Ми прагнемо визначити, як ця архітектура сприяє підвищенню точності рекомендацій, швидкості обчислень і адаптивності до змін у даних.

Результати дослідження. Архітектура Two Tower Model була розроблена з метою оптимізації процесу рекомендацій у сучасних системах. Модель складається з двох незалежних нейронних мереж (веж), які працюють паралельно. Одна з них (User Tower) призначена для обробки даних про користувачів, а друга (Item Tower) — для обробки інформації про об'єкти, що рекомендуються. Як результат, обидві вежі створюють векторні представлення (ембединги), які об’єднуються через функцію подібності (наприклад, скалярний добуток). Такий підхід дозволяє ефективно враховувати особливості обох типів даних.

З метою перевірки ефективності архітектури були використані публічні датасети, зокрема MovieLens та Amazon Reviews. Модель була реалізована за допомогою фреймворків TensorFlow та PyTorch. Важливо, що навчання кожної з веж відбувалося незалежно, але під час інференсу результати їх роботи поєднувалися для створення рекомендацій. У процесі навчання модель

отримувала ембединги з високою семантичною точністю, які забезпечували коректне прогнозування взаємодії користувачів із об'єктами.

Після тренування моделі було проведено її тестування на базових метриках рекомендаційних систем, таких як точність (Precision), повнота (Recall) та середньоквадратична похибка (RMSE). Результати показали підвищення точності та швидкості обчислення.

У порівнянні з традиційними підходами, такими як Matrix Factorization, Two Tower Model забезпечила приріст точності на 12%. Це свідчить про те, що модель успішно поєднує різнорідні дані для створення персоналізованих рекомендацій. Порівняння метрик ефективності згаданих моделей відображено на рисунку 1.

Завдяки паралельній роботі двох веж, час, необхідний для обробки запиту, зменшився на 25%, що робить цю модель придатною для використання у реальному часі.

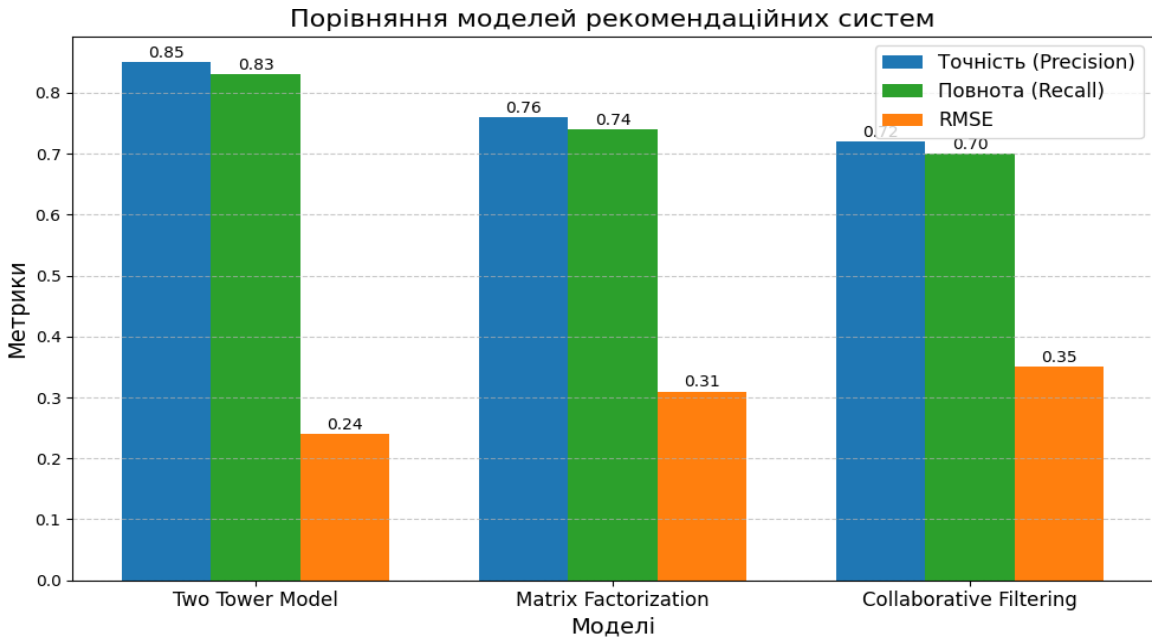

Рис. 1. Порівняння моделей рекомендаційних систем

Модель була інтегрована у рекомендаційну систему онлайн-магазину, де її ефективність оцінювалася за такими показниками, як коефіцієнт кліків (CTR) та конверсія. Результати реального використання підтвердили збільшення CTR на 8,5%, що свідчить про підвищення зацікавленості користувачів у запропонованих об'єктах.

Незважаючи на успішні результати, під час роботи з моделлю було виявлено кілька проблем. По-перше, значний обсяг обчислювальних ресурсів потрібен для початкового навчання, що може стати бар'єром для малих компаній. По-друге, якість роботи моделі залежить від попередньої обробки та нормалізації даних.

Висновки та перспективи. Two Tower Model є ефективним інструментом для оптимізації рекомендаційних систем, забезпечуючи високу точність та адаптивність до різноманітних сценаріїв використання. Архітектура дозволяє

об'єднувати різнорідні дані, враховуючи контекстні фактори, що особливо важливо у сучасній цифровій економіці. У подальших дослідженнях планується впровадження self-supervised learning для зменшення залежності від розмічених даних та оптимізація моделі для мобільних платформ.

Список використаних джерел

1. Covington, P., Adams, J., & Sargin, E. (2016). Deep Neural Networks for YouTube Recommendations. Proceedings of the ACM Recommender Systems Conference.
2. He, X., Liao, L., Zhang, H., Nie, L., Hu, X., & Chua, T.-S. (2017). Neural Collaborative Filtering. Proceedings of WWW.
3. Koren, Y., Bell, R., & Volinsky, C. (2009). Matrix Factorization Techniques for Recommender Systems. Computer.
4. Grbovic, M., & Cheng, H. (2018). Real-time Personalization using Embeddings for Search Ranking at Airbnb. Proceedings of SIGIR.
5. Wang, Y., Zhang, Y., & Feng, H. (2020). An Embedding-based Approach to Recommender Systems. ACM Transactions on Information Systems.

Черевик Олексій В’ячеславович
Аспірант 3 курсу, групи АКСМ-31
Державний університет інформаційно-комунікаційних технологій
(068) 700-18-52
lexcher@ukr.net
Науковий керівник: **Гніденко Микола Петрович**,
кандидат технічних наук, доцент кафедри комп’ютерних наук
Державного університету інформаційно-комунікаційних технологій, м.Київ

ГЕНЕРАЦІЯ 3D-МОДЕЛЕЙ ІЗ ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ (AI)

Постановка задачі. Розвиток технологій AI відкриває нові можливості у 3D-моделюванні, дозволяючи автоматизувати процес створення моделей та створювати більш реалістичні та складні об'єкти. Сфера 3D-моделювання широко використовується у різних галузях, таких як ігри, анімація, дизайн, медицина і т.д. Генерація 3D моделей із AI має потенціал для значного скорочення часу та витрат на розробку 3D-контенту.

Основним завданням дослідження є: проведення порівняльного аналізу різних методів генерації 3D-моделей з використанням AI; визначення сильних та слабких сторін кожного методу, а також їхні можливості та обмеження; проаналізувати можливість використання генерації 3-D моделей з AI в різних сферах діяльності.

Мета дослідження. Визначити сучасні тенденції в технологіях створення тривимірних моделей з використанням штучного інтелекту. Проаналізувати існуючі методи генерації 3D-моделей з використанням AI. Зібрати інформацію про різні підходи: нейронні мережі, генеративно-змагальні мережі, методи глибокого навчання), їх переваги та недоліки. Вивчити додатки генерації 3D-моделей з AI у різних галузях. Розглянути застосування технології у таких сферах, як дизайн, анімація, візуалізація, ігри, медицина тощо. Визначити основні проблеми та перспективи розвитку генерації 3D-моделей з AI. Проаналізувати існуючі обмеження та перспективи розвитку технологій у майбутньому.

Результати дослідження. Дослідження показало, що існує кілька підходів до генерації 3D-моделей за допомогою AI, включаючи [1,2]:

генеративно-змагальні мережі (GAN) які використовують два нейронні модулі, один з яких генерує моделі, а інший оцінює їх реалістичність;

автоенкодери які навчаються стиску та декомпресії даних, використовуючи отримані знання для генерації нових 3D-моделей;

диференціальні рівняння - цей підхід використовує диференціальні рівняння для моделювання процесу формування 3D-об'єкта.

AI-моделювання відкриває нові можливості для створення віртуальних світів, персонажів та об'єктів, які раніше були недоступними. При цьому AI-моделі здатні генерувати 3D-моделі з високою точністю та деталізацією,

включаючи складні геометричні форми, текстури та матеріали. Використання AI для генерації 3D-моделей значно скорочує час та зусилля, необхідні для традиційного моделювання.

Незважаючи на значний прогрес, у AI-моделювання є кілька обмежень: для навчання AI-моделей потрібні величезні обсяги даних; складність навчання та використання AI-моделей - вони потребують значних обчислювальних ресурсів та технічних знань; етична проблема- AI-моделі можуть бути використані для створення реалістичних фейкових зображень та відео, що може призвести до негативних наслідків.

Висновки та перспективи. Дослідження демонструє значний прогрес у галузі генерації 3D-моделей із використанням AI. Методи машинного навчання, особливо глибоке навчання, дозволяють створювати реалістичні 3D моделі з високою деталізацією та точністю. Генерація 3D-моделей з AI знаходить застосування у різних галузях, включаючи: ігрова індустрія - створення ігрових персонажів, об'єктів та оточення; кіно та анімація: створення візуальних ефектів, персонажів та анімації; промисловий дизайн - прототипування та проектування нових продуктів; медицина: створення моделей органів та тканин для навчання та досліджень; архітектура - створення віртуальних моделей будівель та міських просторів[3,4].

AI-технології дозволяють подолати низку обмежень традиційних методів 3D-моделювання, таких як: час та трудовитрати - створення 3D-моделей за допомогою AI значно скорочує час та зусилля, потрібні для традиційного моделювання; складність - AI-моделі можуть створювати складні геометричні форми та деталі, які важко відтворити вручну; креативність - AI-алгоритми здатні генерувати нові та оригінальні ідеї для 3D-моделей.

Подальший розвиток AI-алгоритмів дозволить: поліпшити реалістичність та деталізацію 3D-моделей; збільшити швидкість та ефективність генерації; забезпечити більш точне керування процесом моделювання. Комбінація AI з VR/AR-технологіями відкриє нові можливості для інтерактивного 3D-моделювання та візуалізації. Інтеграція з хмарними платформами дозволить масштабувати процес генерації 3D-моделей та зробити його більш доступним для широкого кола користувачів.

Список використаних джерел

1. A Comparison between Traditional Methods and 2 Generative AI for the Optimization of 3D Modeling and 3 Printing. 2024-6105-AJTE-SFW – 8 JUL 2024. https://www.athensjournals.gr/reviews/2024-6105-AJTE-SFW.pdf.

2. Quinn Everhart. How to create 3d models with ai: A Comprehensive Guide to AI-Driven 3D Model Creation. Aug 29, 2024. https://www.coohom.com/article/how-to-create-3d-models-with-ai-9320?hl.

3. The Rise of AI in 3D Animation: Innovation or Replacement. November 8, 2024. https://www.motionmarvels.com/blog/the-rise-of-ai-in-3d-animation-innovation-or-replacement.

4. YilinYe, Jianing Hao, YihanHou, Zhan Wang. Generative AI for visualization: State of the art and future directions. https://www.sciencedirect.com/science/article/pii/S2468502X24000160.

Шлянчак Світлана Олександрівна
доцент кафедри інформатики, програмування, штучного інтелекту та технологічної освіти
Центральноукраїнський державний університет імені Володимира Винниченка
(066) 401-70-22
s.o.shlianchak@cuspu.edu.ua

ПРОБЛЕМА ІЗОМОРФІЗМУ ГРАФІВ ТА ЇЇ РОЗВ'ЯЗОК ЗА ДОПОМОГОЮ НЕЙРОННИХ МЕРЕЖ

Постановка задачі. Ізоморфізмом у контексті роботи з графовими структурами є важливим інструментом у теорії графів, який застосовується у різних галузях/сферах, зокрема, комп'ютерних науках, хімії, біології, соціальних науках. Можуть бути різні цілі використання ізоморфізму. Наприклад, через виявлення ізоморфізму можна порівнювати графи та встановлювати, наскільки вони схожі структурно. Це в свою чергу може бути корисним для пошуку взаємозв'язків у різних графах. Тому задача встановлення ізоморфізму графів є актуальною, оскільки встановлення схожості структури мереж допомогти у досягненні різних цілей щодо аналізу графів знань.

Мета дослідження. Здійснити порівняльний аналіз класичних методів та графових нейронних мереж GIN для розв'язання задачі ізоморфізму графів. Дослідити, як особливості різних архітектур GIN впливають на точність та ефективність їх застосування в цій галузі.

Результати дослідження. Графи вважаються ізоморфними, якщо можливо знайти взаємно однозначне відображення між вершинами двох графів таким чином, щоб зберігалася структура графа [1] (рис. 1). Математично ізоморфізм визначається наступним чином: два графи H і G є ізоморфними тоді і тільки тоді, коли для будь-якої пари вузлів u і v з H, які є суміжними, існує перетворення f, де f(u) є суміжним до f(v) у G.

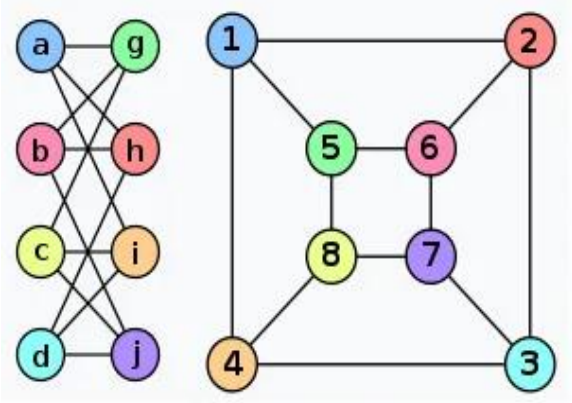

Рис. 1. Ізоморфні графи

Питання про існування ефективного алгоритму для визначення ізоморфізму графів залишається одним з важливих питань теоретичної

інформатики. Незважаючи на тривалі дослідження, проблема ізоморфізму графів продовжує привертати увагу науковців завдяки своїй фундаментальній важливості та потенційним практичним застосуванням. Найкращі відомі алгоритми для розв'язання цієї проблеми мають експоненційну складність у гірших випадках, що означає, що час їх виконання зростає швидко з розміром графа [2].

Одним з найпоширеніших алгоритмів для встановлення ізоморфізму графів є тест Вейсфейлера-Лемана (WL-Test). Цей алгоритм ґрунтується на ітеративному процесі порівняння вершин графа та їх оточень. На кожному кроці алгоритму вершинам присвоюються мітки, які відображають їх структуру та зв'язки з сусідніми вершинами. Потім ці мітки використовуються для подальшого уточнення структури графа. Процес повторюється доти, доки мітки вершин перестають змінюватися або доки не буде знайдено доказ відсутності ізоморфізму.

Ефективність алгоритму WL-тесту суттєво залежить від розміру графа. Для невеликих та середніх графів він демонструє високу продуктивність. Однак, зі збільшенням розміру графа, обчислювальна складність WL-тесту зростає, що призводить до значного збільшення часу виконання алгоритму [3].

Сучасні дослідження в галузі графових нейронних мереж відкривають нові перспективи для вирішення проблеми ізоморфізму графів. Оскільки основна ідея GNN полягає в агрегації інформації з сусідніх вузлів, що є ключовим аспектом при визначенні ізоморфізму, то ці мережі стають перспективним інструментом для розв'язання цієї задачі. Зокрема, архітектура GIN є одним з найбільш вивчених підходів за цим напрямом.

Мережа графових згорток GIN здатна визначати ізоморфізм графів завдяки здатності розпізнавати складні структурні патерни. Ключовим елементом GIN є функція активації, яка обробляє інформацію від сусідніх вершин та перетворює у новий вектор для кожної вершини. Важливою властивістю цієї функції є симетрія, що дозволяє розпізнавати ізоморфні графи незалежно від порядку нумерації вершин.

Висновки та перспективи.

Порівняння GIN та WL-тесту на реальних даних показало, що вибір алгоритму залежить від розміру графа та специфіки задачі. Хоча GIN демонструє високу ефективність на великих графах, для невеликих наборів даних класичний WL-тест є більш доречним. Подальші дослідження передбачають вивчення інших архітектур графових нейронних мереж для вирішення задачі ізоморфізму графів.

Список використаних джерел

1. Scarselli, F., Monfardini, G. The GNN Toolbox [Електронний ресурс] // F. Scarselli, G. Monfardini. – Режим доступу: http://airgroup.dii.unisi.it/projects/GraphNeuralNetwork/download.htm (дата звернення 12.10.2023).

2. Erhan, D., Manzagol, P.-A., Bengio, Y., Bengio, S., Vincent, P. The difficulty of training deep architectures and the effect of unsupervised pre-training // D. Erhan,

P.-A. Manzagol, Y. Bengio, S. Bengio, P. Vincent. – In: Artificial Intelligence and Statistics. – 2009. – P. 153–160.

3. Muggleton, S. Machine learning for systems biology // S. Muggleton. – In: Proc. 15th Int. Conf. Inductive Logic Programm. – 2005. – P. 416-423.

Герасимчук Павло Вікторович
студент 3 курсу, групи ІП-21
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
(097)-795-24-60
fict.herasymchuk.pavlo@gmail.com
Науковий керівник: **Поперешняк Світлана Володимирівна**
к.ф.-м.н., доцент, доцент кафедри ІПІ ФІОТ
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
(098)-645-546-2
spopereshnyak@gmail.com

РОЗРОБКА ПЛАТФОРМИ ДЛЯ ОРЕНДИ ВЕЛОТРАНСПОРТУ

Постановка задачі. У сучасному світі стрімко набувають популярності екологічно чисті види транспорту, зокрема велосипедний. Оренда велосипедів стає все більш затребуваною послугою, особливо серед людей, які не мають власного транспорту. Найчастіше люди користуються орендованими велосипедами для щоденних поїздок на роботу або навчання, активного відпочинку та туристичних подорожей.

У світі спостерігається стрімкий розвиток систем спільного користування велосипедами, особливо у великих містах. Зазвичай послуги оренди велотранспорту надаються великими спеціалізованими компаніями, які централізовано здійснюють обслуговування власних велосипедів. Також існують платформи peer-to-peer оренди, які ґрунтуються на принципі спільного користування, і дозволяють користувачам як орендувати, так і пропонувати до оренди власні велосипеди.

Актуальними проблемами галузі оренди велосипедів є високі ціни, обмежена кількість місць оренди, складнощі з доступом до велотранспорту у пікові години та вихідні, а також протидія крадіжкам велосипедів та підвищення безпеки угод між користувачами.

Мета дослідження. Метою роботи є пришвидшення процесів надання велосипедів в оренду, пошуку та бронювання велотранспорту, а також підвищення безпеки цих операцій шляхом відстеження власниками місцеположення велосипедів, що перебувають в оренді.

Результати дослідження. У результаті аналізу предметної області та дослідження програмних продуктів-аналогів, зокрема Spokeo [1], ListNRide [2], Sunryde [3], було визначено такі ключові функціональні вимоги розроблюваного застосунку:

1. Облік користувачів (зберігання персональних даних, реєстрація, авторизація)

2. Облік оголошень про оренду (створення, зберігання, перегляд власних оголошень)

3. Пошук та фільтрація оголошень за ключовими критеріями (пошук, фільтрація, сортування, перегляд детальної інформації про оголошення)

4. Облік бронювань (створення бронювання за оголошенням, перегляд, зміна статусу власних бронювань)

5. Створення відгуків (написання відгуків орендарями, формування рейтингу оголошення відповідно до відгуків про нього)

6. Вбудований чат між орендарями та орендодавцями (надсилання текстових повідомлень власнику оголошення)

7. Відстеження місцеположення велотранспорту (можливість перегляду поточного місцеположення власного велосипеда, який перебуває в оренді).

Особливу увагу було приділено створенню зручного та інтуїтивно зрозумілого інтерфейсу користувача для швидкої взаємодії з додатком. На рисунках 1, 2 наведено вигляд головної сторінки застосунку та сторінки бронювань користувача.

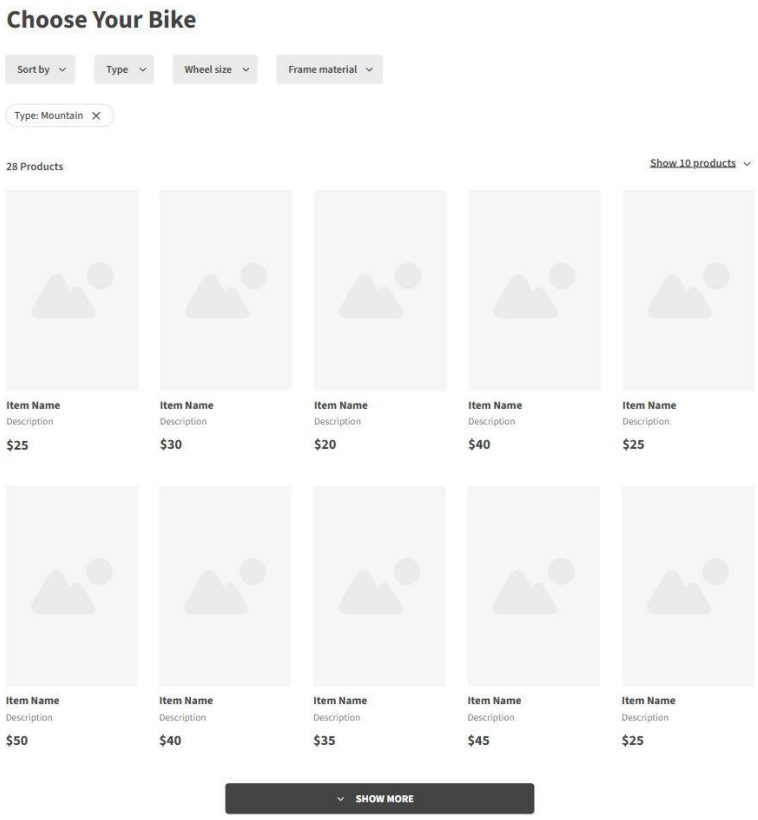

Рис. 1. Головна сторінка застосунку

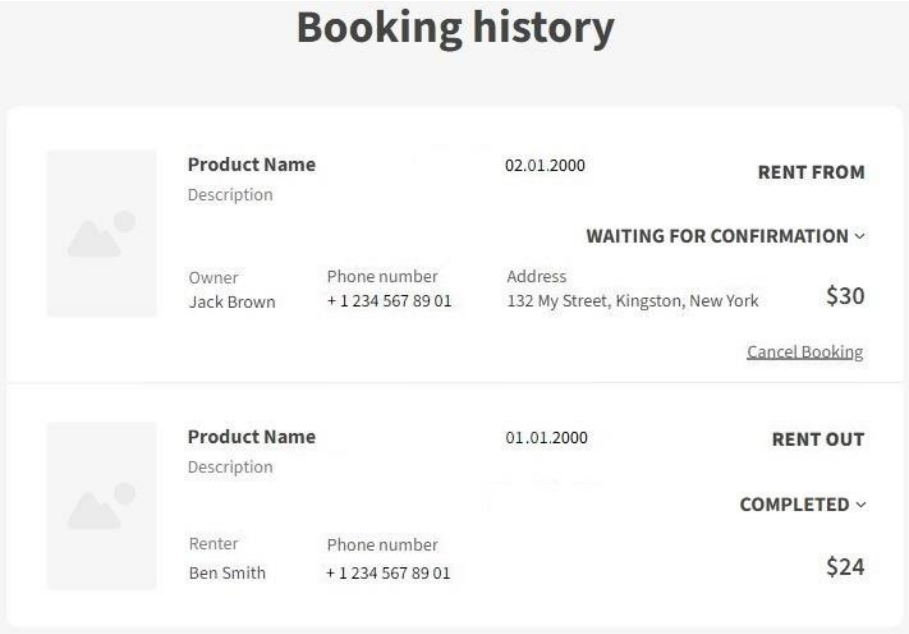

Рис. 2. Сторінка бронювань користувача

На головній сторінці відображається базова інформація про оголошення: назва, короткий опис, ціна оренди за добу, фото. Користувач може знайти потрібне оголошення за декількома параметрами: тип велосипеда, розмір коліс, матеріал рами, а також відсортувати пропозиції за декількома критеріями: ціна оренди за добу, рейтинг, дата публікації. Детальну інформацію про велосипед можна переглянути на сторінці відповідного оголошення.

На сторінці бронювань відображається інформація про велосипед, орендаря або орендодавця, адреса, дата створення, ціна та статус бронювання. На цій сторінці орендодавець може змінити статус бронювання або скасувати його, а орендар – скасувати.

Висновки та перспективи. В результаті виконання роботи було створене програмне забезпечення для підтримки процесів надання та отримання велотранспорту в оренду. Платформа надає орендарям можливість шукати оголошення за встановленими критеріями, а орендодавцям – надавати власні велосипеди в оренду з можливістю відстеження їх місцеположення. Створений застосунок забезпечує швидкість, зручність та безпеку процесу оренди та сприятиме популяризації велотранспорту.

Список використаних джерел

1. Spokeo – Bike Share Platform – [Електронний ресурс]. – Режим доступу до ресурсу: https://spokeo.bike

2. ListNRide – Europe`s largest online bike rental platform – [Електронний ресурс]. – Режим доступу до ресурсу: https://www.listnride.com/

3. Sunryde – E-bike rental – [Електронний ресурс]. – Режим доступу до ресурсу: https://www.sunryde.com

Герцюк Микола Модестович
доктор філософії(PhD), доцент кафедри Технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій
(095) 619-08-69
m.gertsiuk@duikt.edu.ua

ДОЦІЛЬНІСТЬ ВИКОРИСТАННЯ РІШЕНЬ, ЩО МОДЕЛЮЮТЬ ЕКОЛОГІЧНИЙ ВПЛИВ З МЕТОЮ АНАЛІЗУ ВПЛИВУ ТОКСИЧНИХ РЕЧОВИН НА НАВКОЛИШНЄ СЕРЕДОВИЩЕ

В сучасному світі, одним з наслідків суспільної діяльності є забруднення навколишнього середовища токсичними речовинами. В результаті це призводить до негативного впливу на населення та навколишнє середовище. Існують різні методи ліквідації наслідків, але всі базуються на оцінці небезпечного, або токсичного впливу. Для цього, існують різні методи моделювання та прогнозування процесів, або стану навколишнього середовища. Переважна більшість базується на моделюванні екологічних процесів. Однак, в першу чергу, мають бути проаналізовані хімічні речовини, та оцінені їх властивості.

Таким чином, метою роботи є аналіз доцільності використання рішень, що моделюють екологічний вплив, для вирішення питання оцінки токсичного впливу речовин.

На сьогоднішній день, існують такі компанії, та агенції, як EPA[1], Sphera Solutions[2], Unilever[3], тощо, одним з завдань яких є розробка таких рішень. Пошук показав, що рішеннями, що можуть проводити оцінку впливу токсичних речовин є ChemSteer, ECOSAR, EPI Suite, GaBi, SimaPro, USETox та ToxTool.

Дослідження показало, що такі застосунки, як USETox, ToxTool, ECOSAR, ChemSteer, моделюють властивості токсичних речовин, а EPI Suite, GaBi. SimaPro моделюють хімічні властивості речовин. Згадані речовини проводять оцінку в межах моделювання навколишнього середовища, а отже можуть бути використані для проведення оцінки токсичності речовин в рамках навколишнього середовища. Кожне з цих рішень є, або універсальним, тобто має можливість оцінки незалежно від середовища, або вузькоспеціалізованим, тобто направлене на деяке середовище(наприклад, водні ресурси, або повітря). Великою перевагою таких рішень є можливість проведення оцінки в рамках моделювання екологічних процесів, що нівелює необхідність у проведенні комплексного експериментального аналізу з використанням відбору проб, хроматографічних методів та детального вивчення знайдених хімічних речовин. Схему концепції моделювання життєвого циклу речовин в рамках навколишнього середовища показано на рис. 1.

Цілі, в рамках яких необхідно проводити моделювання можна умовно поділити на 3 групи:

1. Для розуміння масштабів надзвичайної ситуації, що сталась з метою ліквідації наслідків забруднення, що має бути короткостроковим рішенням.

2. Для подальшої ліквідації наслідків у штатному режимі, з метою довгострокового відновлення навколишнього середовища.

3. Для моделювання ризиків, пов’язаних з забрудненням хімічних речовин з метою глибокого вивчення екологічних процесів.

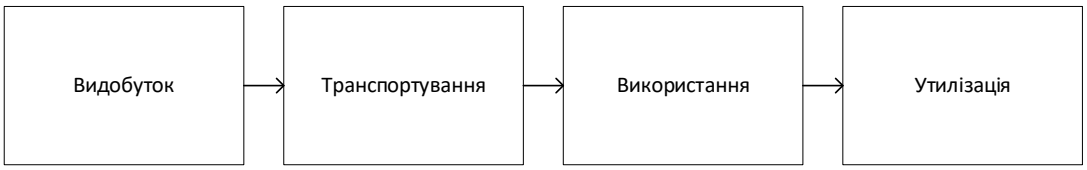

Рис. 1 Схема концепції життєвого циклу речовин в рамках навколишнього середовища

Згадані рішення дозволяють проводити оцінку у випадку надзвичайної ситуації та подальшої ліквідації цих наслідків. Однак, точність, зазвичай, є меншою, аніж у випадку детального моделювання ризиків. Така закономірність пов’язана з обмеженням такої вхідної інформації, як характеристик, що можуть впливати на екологію місцевості та відсутністю часу для проведення більш ґрунтовних досліджень. Тому, детальний аналіз вимагає проведення комплексних досліджень, пов’язаних з моделюванням хімічних процесів.

Таким чином, згадані рішення дозволяють проводити оцінку негативного впливу токсичних або небезпечних речовин на навколишнє середовище, що може бути потрібним етапом для ліквідації наслідків надзвичайної ситуації. Зацікавленими сторонами у цьому випадку є служби з надзвичайних ситуацій. Однак, питання доцільності використання таких рішень для подальшої ліквідації наслідків в штатному режимі, та можливості використання їх для моделювання ризиків, як інструмент, що доповнює, або частково заміняє комплексні дослідження, залишається відкритим. Тому, подальше дослідження специфіки, переваг та недоліків згаданих застосунків залишається відкритим.

Список використаних джерел

1. U.S. Environmental Protection Agency | US EPA. Режим доступу: https://www.epa.gov/ .

2. Sustainability & Safety Management Solutions | Sphera. Режим доступу: https://sphera.com/ .

3. Unilever Global: Making sustainable living commonplace | Unilever. Режим доступу: https://www.unilever.com/.

Гордич Оксана Юріївна
студентка 3 курсу, групи ІП-21
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
(093) 347-06-22
oksanahordych@gmail.com
Науковий керівник: **Поперешняк Світлана Володимирівна**
к.ф.-м.н., доцент, доцент кафедри ІПІ ФІОТ
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
(098)-645-546-2
spopereshnyak@gmail.com

СИСТЕМИ ПРОГНОЗУВАННЯ СТИХІЙНИХ ЛИХ НА ОСНОВІ ШІ

Постановка задачі. Загрози стихійних лих, таких як повені, землетруси, урагани та пожежі, вимагають швидкого та точного оповіщення населення для зменшення втрат та мінімізації ризиків. Традиційні системи оповіщення часто не забезпечують оперативність та точність, що призводить до запізнілих реакцій. Важливим є створення систем, які здатні швидко обробляти великі обсяги даних та надавати прогнози в реальному часі.

Мета дослідження. Метою дослідження є інтеграція методів штучного інтелекту в автоматизовані системи прогнозування для підвищення швидкості реагування та точності передбачень стихійних лих.

Результати дослідження. Інформаційні системи, що базуються на ШІ, дозволяють істотно скоротити час, необхідний для аналізу даних, порівняно з традиційними методами прогнозування. Завдяки використанню сучасних алгоритмів, таких як рекурентні нейронні мережі та моделі довгострокової пам’яті, стає можливим ефективно обробляти часові ряди, що описують динамічні явища, зокрема розвиток ураганів, повеней або посух [1].

Для створення автоматизованої системи прогнозування надзвичайних погодних умов на основі штучного інтелекту необхідно пройти кілька ключових етапів, які охоплюють збір, обробку даних та генерацію прогнозів. Система повинна інтегрувати дані з різних джерел, таких як супутникові зображення, радіолокаційні сенсори та наземні метеостанції. Також можна використовувати мобільні сенсори для отримання додаткових даних із важкодоступних регіонів [3]. Усі ці дані передаються до централізованого сховища, де вони накопичуються та зберігаються для подальшого аналізу.

Перед обробкою даних необхідно виконати їхню попередню підготовку, особливо коли йдеться про супутникові знімки, які відіграють ключову роль у виявленні зсувів, повеней та інших природних катастроф. Для зменшення рівня шуму застосовуються спеціалізовані алгоритми фільтрації, що дозволяють покращити чіткість і точність зображень перед їх подальшим аналізом. Дослідження показують, що традиційні методи обробки таких знімків часто

потребують аналізу понад 100 кадрів для досягнення якісних результатів. Однак завдяки розвитку штучного інтелекту та сучасних алгоритмів стало можливим досягати аналогічної якості обробки навіть на основі одного зображення.

Далі відбувається аналітична обробка даних із застосуванням штучного інтелекту. Алгоритми машинного навчання та глибокі нейронні мережі аналізують метеодані та прогнозують можливі природні катастрофи. Моделі, такі як рекурентні нейронні мережі та довгострокова пам'ять, здатні працювати із часовими рядами, що дозволяє ефективно передбачати динамічні погодні явища, як-от формування ураганів чи повеней [2]. Ансамблеві моделі допомагають у довгостроковому прогнозуванні кліматичних трендів, таких як глобальне потепління. Для підвищення прозорості та зрозумілості рішень застосовуються методи інтерпретації, які пояснюють, які фактори найбільше вплинули на прогноз. Крім того, для підвищення точності прогнозів і адаптивності системи до нових даних впроваджується підхід активного навчання, що дозволяє моделі автоматично покращувати свої результати на основі нових спостережень.

На основі результатів аналітики система генерує прогнози та візуалізує їх на картографічних платформах. Додатково застосовуються генеративні моделі, такі як GAN, які дозволяють створювати симуляції впливу катастрофічних сценаріїв для оцінки можливих наслідків та розробки стратегій реагування.

Логічним розширенням для такої системи може бути інтеграція з месенджинговими платформами або державними структурами та службами надзвичайних ситуацій для ефективної координації дій під час лиха.

На рисунку 1 показана архітектура такої системи, яка демонструє ключові контексти та взаємодії між зовнішніми учасниками та контекстами додатка. Ця модель включає інтеграцію даних з багатьох джерел, таких як супутникові зображення, радіолокаційні сенсори та наземні станції.

Рис. 1. Діаграма компонентів системи

Прикладом подібної системи є платформа моніторингу, створена університетом Альберти у партнерстві з компанією 3vGeomatics. Вона використовує супутникові знімки для прогнозування природних і техногенних катастроф, таких як зсуви, повені та землетруси. Архітектура платформи базується на обробці супутникових даних у реальному часі із застосуванням глибинних нейронних мереж для аналізу змін ландшафту. Це демонструє успішну інтеграцію датчиків, алгоритмів машинного навчання та аналітичних інструментів, що підвищує точність прогнозування та ефективність реагування на стихійні лиха. Однак платформа ще перебуває на етапі розробки та не отримала широкого практичного застосування серед населення.

Висновки та перспективи. У дослідженні розглянуто методи прогнозування стихійних лих із використанням штучного інтелекту. Проведений аналіз показав, що традиційні системи не завжди забезпечують достатню швидкість та точність реагування . Використання сучасних нейронних мереж, таких, дозволяє ефективно обробляти великі обсяги даних і прогнозувати розвиток катастроф у реальному часі. Поєднання традиційних методів із глибинним навчанням дозволяє створити адаптивні та обчислювально ефективні системи моніторингу. Перспективою подальших досліджень є розробка гібридних алгоритмів, що об'єднують переваги класичних методів та глибинного навчання, а також інтеграція таких систем із платформами для автоматичного оповіщення населення.

Список використаних джерел

1. Johnson, M., & Lee, K. "Deep Learning Models for Predicting Extreme Weather Events." Proceedings of the International Conference on Climate Change, 2024.
2. Smith, R., & Zhao, L. "Integrating Satellite Data and AI for Disaster Prediction." Journal of Geoscience Technology, 2023.
3. Brown, T., et al. "Drone-Assisted Data Collection for Real-Time Disaster Response." Sensors and Systems Journal, 2022.

Дегтяр Олексій Михайлович
студент 6-го курсу, групи ІСДМ-61
Державний університет інформаційно-комунікаційних технологій
aandud9@gmail.com
Науковий керівник **Полоневич Ольга Володимирівна**,
к.т.н., доцент, доцент кафедри Інформаційних систем та технологій
Державного університету інформаційно-комунікаційних технологій,
м. Київ

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА ТРАНЧФОРМАЦІЮ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Постановка задачі. Сучасні системи відеоспостереження зробили революцію в усьому світі, оскільки вони дозволяють аналізувати, відстежувати та судити про діяльність у певній області чи контексті. І все це стає можливим лише за допомогою обробки відео в реальному часі та передового машинного навчання.

Мета дослідження. Розкрити, як штучний інтелект змінює підходи до відеоспостереження, перетворюючи його з пасивного на проактивний інструмент, що підвищує рівень безпеки, ефективності та надійності в сучасних умовах.

Результати дослідження. Штучний інтелект докорінно змінює відеоспостереження, перетворюючи його з пасивного інструменту на проактивну, інтелектуальну систему, здатну виявляти загрози в реальному часі, аналізувати поведінку та прогнозувати інформацію. Ця зміна особливо важлива для безпеки на робочому місці, де навіть незначні помилки можуть мати серйозні наслідки.

Швидкий розвиток відеоаналітики на основі штучного інтелекту дозволяє системам обробляти величезні обсяги даних, виявляти закономірності та приймати рішення з безпрецедентною точністю. Оскільки загрози безпеці стають все більш складними, організації по всьому світу звертаються до рішень на основі ШІ, щоб забезпечити безпеку своїх співробітників і активів [1].

Традиційні методи спостереження, які значною мірою покладаються на нагляд людини, все частіше визнаються застарілими та неефективними. Люди-оператори схильні до втоми та відволікання, що може призвести до пропуску деталей і непослідовного моніторингу. Оскільки потреби в безпеці розвиваються в нашому стрімкому цифровому світі, ці обмеження роблять ручні системи менш ефективними.

Навпаки, спостереження на основі штучного інтелекту працює невпинно, постійно відстежуючи без ризику людської помилки. Системи штучного інтелекту можуть виявляти тонкі нюанси та аномалії, які можуть бути непомічені людським оком, забезпечуючи рівень точності та надійності, з яким не можуть зрівнятися традиційні методи. Вони також легко масштабуються, відстежуючи кілька місць одночасно, чого важко досягти вручну.

Крім того, штучний інтелект надає миттєві сповіщення, що дозволяє швидше реагувати на потенційні загрози, і є більш економічно ефективним з часом, вимагаючи мінімального обслуговування порівняно з поточними витратами на нагляд людини. Штучний інтелект також чудово справляється зі збором і аналізом даних, автоматизацією процесів, схильних до помилок у ручних системах, і наданням цінних відомостей, які підвищують безпеку [2].

Ринок штучного інтелекту на ринку відеоспостереження демонструє значне зростання, причому середній річний темп зростання (CAGR) становитиме понад 15,5% між 2024 і 2032 роками. Цей сплеск зумовлений кількома ключовими факторами: удосконалення штучного інтелекту та глибокого навчання; економічність; інтеграція з пристроями Інтернету речей; масштабованість і гнучкість; покращене прийняття рішень; проактивне виявлення загроз; налаштування та персоналізація.

Висновки та перспективи. Таким чином, можливо зробити висновок, що штучний інтелект докорінно змінює підхід до відеоспостереження, роблячи його інтелектуальною та проактивною системою, здатною оперативно виявляти загрози, аналізувати поведінку й приймати рішення з високою точністю. Завдяки своїй ефективності, масштабованості та здатності знижувати людський фактор, рішення на основі ШІ стають незамінними для забезпечення безпеки. Стрімкий розвиток технологій у цій галузі не лише підвищує рівень безпеки, а й дозволяє організаціям адаптуватися до сучасних викликів, створюючи більш захищене та надійне середовище.

Список використаних джерел.

1. Gao, L.; Zheng, D. Analysis on Code Stability and Fault Tolerance. In Proceedings of the 2011 2nd International Conference onArtificial Intelligence, Management Science and Electronic Commerce (AIMSEC), Zhengzhou, China, 8–10 August 2011; Instituteof Electrical and Electronics Engineers: Piscataway, NJ, USA, 2011; pp. 155–159.

2. Brahan, J.W.; Lam, K.P.; Chan, H.; Leung, W. AICAMS: Artificial intelligence crime analysis and management system. Knowl.Based Syst. 2017,11, 355–361.

Довгаленко Олександр Костянтинович
студент 6 курсу, групи САДМ-61
Державний університет інформаційно-комунікаційних технологій
(067) 861-50-52
miner067861@gmail.com
Науковий керівник: **Патракеєв Ігор Михайлович**
кандидат технічних наук, доцент
Державний університет інформаційно-комунікаційних технологій
ipatr@ukr.net

МЕТОДОЛОГІЯ ОЦІНКИ ВПЛИВУ ТРАНСПОРТНОЇ ПІДСИСТЕМИ НА СТАЛИЙ РОЗВИТОК МІСЬКОГО СЕРЕДОВИЩА

Постановка задачі. Аналіз міських транспортних систем у контексті сталого розвитку вимагає розробки чітких методологічних підходів до оцінювання їхньої ефективності. Врахування показників сталого розвитку, таких як екологічна стійкість, економічна ефективність і соціальна інклюзивність, є необхідним для адаптації міської транспортної політики до сучасних викликів.

Мета дослідження. Розробка методології для оцінки впливу транспортної підсистеми на ключові аспекти сталого розвитку міського середовища.

Результати дослідження. Методологія оцінки впливу транспортної підсистеми на сталий розвиток міського середовища базується на використанні інтегральних показників, які враховують складну взаємодію між транспортними потоками, їхніми екологічними, економічними та соціальними наслідками[1]. Основу аналізу становлять три ключові параметри: повна потужність транспортної підсистеми $N_{ТП}(\mathrm{t})$, корисна потужність $P_{ТП}(\mathrm{t})$) та потужність втрат $L_{ТП}(\mathrm{t})$). Ці показники дозволяють комплексно оцінити ефективність функціонування міської транспортної системи[2].

Повна потужність $N_{ТП}(\mathrm{t})$ відображає реальні можливості транспортної підсистеми, враховуючи показники повних потоків, зокрема щільність вулично-дорожньої мережі, кількість автотранспортних засобів, споживання енергії приватним та громадським транспортом[3]. Корисна потужність $P_{ТП}(\mathrm{t})$ характеризує продуктивність транспортної підсистеми, враховуючи середні пробіги транспорту, інтенсивність руху та частку використання «зеленого» транспорту. Потужність втрат $L_{ТП}(\mathrm{t})$ визначає втрати ресурсів, зокрема обсяги викидів CO_2 та NO_x, що спричинені транспортними потоками. Структурний взаємозв'язок між цими показниками наведено на Рис. 1.

Розроблена модель дозволяє ідентифікувати критичні фактори, які впливають на ефективність транспортної системи, та запропонувати шляхи їх оптимізації. Зокрема, результати дослідження свідчать, що підвищення частки громадського та екологічного транспорту, оптимізація маршрутів і зменшення енергоспоживання можуть значно знизити втрати системи та підвищити її ефективність[4].

Таким чином, запропонована методологія є універсальним інструментом для аналізу та вдосконалення транспортної політики, спрямованої на сталий розвиток міського середовища. Вона сприяє адаптації транспортних систем до сучасних викликів, зокрема екологічних і соціально-економічних.

Рис. 1 Схема транспортної підсистеми.

Висновки та перспективи. В дослідженні розглянуто методологію оцінки впливу транспортної підсистеми на сталий розвиток міського середовища. Запропонована модель, яка базується на аналізі трьох ключових показників – повної потужності, корисної потужності та потужності втрат, дозволяє комплексно оцінити ефективність функціонування міської транспортної системи. Результати дослідження підтвердили, що оптимізація транспортних потоків, підвищення частки «зеленого» транспорту та зниження рівня енергоспоживання є ключовими факторами для зменшення втрат і забезпечення сталості міського транспорту.

Запропонований підхід також дозволяє ідентифікувати критичні фактори, які негативно впливають на ефективність транспортної системи, і створити інструменти для їх оптимізації. Використання інтегральних показників сприяє більш глибокому розумінню взаємозв'язку між транспортними потоками, їхніми екологічними наслідками та соціально-економічними показниками сталого розвитку.

Перспективою подальших досліджень є розробка динамічних моделей, які враховують змінні умови міського середовища, включаючи сезонні коливання інтенсивності руху, зростання населення та зміну потреб у мобільності. Особливу увагу слід приділити впровадженню цих моделей у рамках концепції розумного міста (Smart City), що забезпечить підвищення ефективності транспортної політики, сприятиме зниженню екологічного навантаження та забезпечить адаптацію міських транспортних систем до сучасних викликів.

Список використаних джерел

1. Banister D. Transport and urban development. Routledge, 2020. ISBN: 9781138998915.

2. Hall R., Spatial transport and sustainable development: Concepts and frameworks. Sustainability, 2021, vol. 13(3), pp. 1098-1114. DOI: 10.3390/su13031098.

3. Santos G., Behrendt H., Teytelboym A. Part II: Policy instruments for sustainable road transport. Research in Transportation Economics, 2020, vol. 28(1), pp. 46–91. DOI: 10.1016/j.retrec.2020.08.004.

4. Yeh S.-C., Chang T.-Y. Transportation systems efficiency and CO_2 emissions reduction. Energy Policy, 2023, vol. 163, pp. 112824. DOI: 10.1016/j.enpol.2023.112824.

Зеленський Олександр Володимирович
студент 6 курсу, групи ІСДМ-61
Державного університету
інформаційно-комунікаційних технологій
(097)-872-00-09
Gameslps6@gmail.com
Науковий керівник: **Срібна Ірина Миколаївна**
доктор технічних наук, доцент кафедри Інформаційних систем та технологій
Державного університету інформаційно-комунікаційних технологій, м. Київ

ЗАРЯДНА СТАНЦІЯ ЕЛЕКТРОМОБІЛЯ НА ОСНОВІ ІНТЕРНЕТУ РЕЧЕЙ

У наш час електромобілі є актуальним питанням, і вони є важливим елементом інтелектуального світу. Мобільність електромобілів іноді обмежена. Як наслідок, вони потребують регулярної підзарядки. Населення зростає в геометричній прогресії, що призводить до збільшення заторів на дорогах. Оскільки відомо, що запаси палива на нашій планеті обмежені, настав час переходити на інший вид транспорту, і електрика є найкращою альтернативою для цього, прикладом чого є електромобілі. У швидко мінливому світі рішень для електромобільності, технологічного ландшафту інтеграція Інтернету речей (IoT) змінює наш підхід до інфраструктури зарядки електромобілів, з ростом потреби в надійній та інтелектуальній мережі зарядки електромобілів.

Постановка задачі. Тривалий час у черзі для заряджання електромобілів за допомогою інтелектуального підключення до мережі призводить до низької ефективності розподілу. Таким чином, у цій статті пропонується стратегія прогнозування ймовірності формування черг для електромобілів, які прибувають на зарядні станції за допомогою інтелектуального підключення до мережі. При дослідженні таких проблем слід враховувати як динамічний попит споживачів, так і характеристики змінного впливу зарядних транспортних засобів. На основі описаних вище характеристик проблеми потрібно розробити стратегію вибору динамічної зарядки в режимі реального часу, проаналізувати сучасні зарядні станції для електромобілів, їхні функціональні можливості та технологічні рішення, визначити основні функції, які повинна мати інтелектуальна зарядна станція на основі IoT (дистанційне керування, інтеграція в енергетичну систему, платіжні системи, моніторинг стану).

Мета дослідження. Мета дослідження полягає у розробці концепції та прототипу інтелектуальної зарядної станції для електромобілів на основі технології Інтернету речей, яка забезпечуватиме ефективне управління процесом зарядки, інтеграцію в енергетичну систему, забезпечення зручності користувача та підвищення безпеки.

Результати дослідження. У роботі розглядаються важливі дослідження зарядних станцій з Інтернетом речей і типу зарядки, що використовується на цих станціях, і робиться порівняння між ними, а також джерелами для цих

станцій, якими можуть бути відновлювані та невідновлювані джерела енергії. Використання IoT економить час, витрачений користувачем на пошуки розташування станцій, з можливістю дізнатися розташування зарядних станцій за допомогою мобільного додатку, а також можливість розміщення зарядних станцій у громадських місцях і паркувальних станціях, таким чином, легше перейти до використання цих нових транспортних засобів.

Висновки та перспективи. Паливо, яке ми використовуємо для наших транспортних засобів, має обмежені запаси в природі. Тому всі переходять на електромобілі, щоб споживати якомога менше палива. Але все ще люди не готові змінити електромобілі на теперішні транспортні засоби, що працюють на паливі. Однією з причин цього є ціна та нестача зарядних станцій. Навіть якщо зарядних станцій небагато, людям доводиться витрачати додатковий час на зарядку автомобіля. Крім того, паркування автомобілів стало великою проблемою у великих містах. Отже, розглянувши ці питання, ми можемо забезпечити розумну парковку з можливістю зарядки біля більшості комерційних будівель, автозаправних станцій тощо. Це зменшить зусилля з пошуку місця для паркування.

Список використаних джерел

1. Subudhi, P.S. and Krithiga, S. (2020) Wireless Power Transfer Topologies Used for Static and Dynamic Charging of EV Battery: A Review. International Journal of Emerging Electric Power Systems, 21, Article ID: 20190151. https://doi.org/10.1515/ijeeps-2019-0151

2. Rana, M.M., Xiang, W., Wang, E., Li, X. and Choi, B.J. Internet of Things Infrastructure for Wireless Power Transfer Systems. IEEE Access, 6, 19295-19303. https://doi.org/10.1109/ACCESS.2018.2795803

3. Arif, S.M., Lie, T.T., Seet, B.C., Ayyadi, S. and Jensen, K. (2021) Review of Electric Vehicle Technologies, Charging Methods, Standards and Optimization Techniques. Electronics, 10, Article 1910. https://doi.org/10.3390/electronics10161910

Літвінов Євгеній Андрійович
студент 5 курсу, групи ІСДМ-62
Державного університету інформаційно-комунікаційних технологій
(093)-078-48-00
litvinov_yevhenii@ukr.net
Науковий керівник: **Сагайдак Віктор Анатолійович**,
Доктор філософії (PhD), доцент кафедри Інформаційних систем та технологій
Державного університету інформаційно комунікаційних технологій, м. Київ

ДОСЛІДЖЕННЯ ТА ПОРІВНЯННЯ СУЧАСНИХ СИСТЕМ МОНІТОРИНГУ ЯКОСТІ МОБІЛЬНОЇ МЕРЕЖІ

В умовах стрімкого розвитку телекомунікаційних технологій операторів зв'язку виникає необхідність у підвищенні вимог до моніторингу якості надаваних послуг. Система моніторингу повинна забезпечувати не лише контроль стану мережі, але й аналіз ефективності роботи різних технологій.

Як результат, постає потреба в чіткому визначенні та порівнянні сучасних платформ моніторингу. На сьогодні існує безліч рішень, зокрема ZTE VMAX, Huawei SmartCare та Anritsu MasterClaw. Кожна з цих платформ пропонують різні підходи, застосунки, має різний функціонал для моніторингу і управління якістю мережі.

Постановка задачі. В рамках цього дослідження ставиться задача провести порівння платформ ZTE VMAX, Huawei SmartCare та Anritsu MasterClaw, вивчити їх функціональні можливості, відмінності в технологічному забезпеченні та вплив на якість обслуговування, а також розробити рекомендації щодо вибору оптимальної системи моніторингу, що відповідатиме потребам та вимогам ринку.

Мета дослідження. Проведення комплексного порівняння сучасних систем моніторингу ZTE VMAX, Huawei SmartCare та MasterClaw для визначення їхньої ефективності у сфері моніторингу якості послуг у телекомунікаціях

Результати дослідження. У результаті порівняльного дослідження було отримано, що кожна з платформ має свої ключові сильні сторони у сфері управління якістю телекомунікаційних послуг. ZTE VMAX забезпечує широкий спектр функцій, включаючи моніторинг в реальному часі, аналіз ефективності роботи мережі, управління якістю обслуговування (QoS) та генерацію детальних звітів про стан мережі, що дозволяє операторам швидко реагувати на проблеми та оптимізувати роботу мережі. Huawei SmartCare використовує передові інструменти аналітики та машинного навчання, які дозволяють проактивно виявляти проблеми та оптимізувати мережу, забезпечуючи високий рівень задоволеності абонентів. MasterClaw має сильні можливості для детального аналізу якості зв'язку та виявлення корінних причин проблем на мережі. Отже, результати дослідження підкреслюють важливість вибору правильної системи моніторингу для досягнення високої якості обслуговування та задоволеності

абонентів, а також їх роль у забезпеченні конкурентоспроможності операторів на сучасному ринку.

Висновки та перспективи. Кожна з платформи моніторингу, ZTE VMAX, Huawei SmartCare та MasterClaw має свої унікальні функціональні можливості. ZTE VMAX забезпечує універсальні рішення для моніторингу і оптимізації, Huawei SmartCare пропонує передові аналітичні інструменти для підвищення задоволеності абонентів, швидкому виявленню проблем на мережі та їх усуненню, а MasterClaw спеціалізується на глибокому аналізі якості зв'язку. Адаптація до розвитку технологій, інтеграція штучного інтелекту, відкривають нові перспективи для вдосконалення систем моніторингу, що стає ключовим фактором для підтримки мережі мобільними операторами .

Список використаних джерел

1. Huawei Smart Care Solution Customer Journeys. TM Forum. URL: https://www.tmforum.org/certifications-awarded/huawei-smart-care-solution-customer-journeys/.

2. Distributor Masterclaw Indonesia MasterClaw Monitoring - Telemedia.id. Telemedia.id. URL: https://telemedia.id/masterclaw-monitoring/.

3. VMAX for Optimal Network Operation. ZTE - ZTE Offical Website | Leading 5G Innovations The world's leading communications service provider. URL: https://www.zte.com.cn/global/about/magazine/zte-technologies/2016/2/en_719/449138.html .

Марченко Олена Іванівна
старший викладач кафедри інформатики та програмної інженерії
Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
(066)929-75-81
marchenko.olena@lll.kpi.ua

МОДЕЛЮВАННЯ ПЕРЕДАЧІ ТА ОБРОБКИ ІНФОРМАЦІЇ В МЕРЕЖЕЦЕНТРИЧНОМУ СЕРЕДОВИЩІ

Постановка задачі. Мережецентричне середовище загалом відноситься до системи або операційного контексту, в якому інформація, взаємодії, операції та процеси прийняття рішень керуються мережею взаємопов'язаних інформаційних систем та людей, що залучені до процесів. Тому одним з аспектів створення мережецентричного інформаційного середовища є моделювання процесів що відбувається в режимі реального часу прийняття рішень.

Мета дослідження. Метою дослідження є аналіз та створення моделі процесів управління інформаційним середовищем при отриманні інформації в режамі реального часу.

Результати дослідження. В мережецентричному середовищі мережа відіграє центральну роль у забезпеченні співпраці, обміну даними та ухваленні рішень в режимі реального часу.

Основні найбільш вагомі характеристики середовища можна визначити як:

– взаємозв'язок (люди та системи пов'язані через мережі, що забезпечує безперебійний обмін інформацією, також залучення додаткових пристроїв);

– доступ до інформації (дані та ресурси спільно використовуються в мережі, що забезпечує доступ до інформації в реальному часі для всіх сторін що залучені до процесів);

– співпраця (люди працюють більш ефективно завдяки цифровим платформам, сприяючи співпраці, координації та спільним діям).

– гнучкість (можливість системи може швидко адаптуватися до динамічного потоку інформації);

– децентралізоване прийняття рішень (розподіл між різними учасниками або вузлами в мережі, що призводить до швидшого та найбільш обґрунтованого прийняття рішень).

Концепцію мережецентричного середовища часто застосовують у військових операціях (мережецентрична війна), бізнесі (хмарні обчислення, IoT), деякі державні установи.

Моделювання передачі та обробки інформації в мережево-орієнтованому середовищі передбачає створення уявлень про те, як дані протікають через мережу, як вони обробляються та як різні об'єкти (пристрої, вузли чи особи) взаємодіють із інформацією та використовують її. Це моделювання спрямоване

на розуміння динаміки зв’язку, прийняття рішень і продуктивності системи в складних взаємопов’язаних середовищах.

До основних компонентів моделювання передачі та обробки інформації можна віднести: методи моделювання, передача та обробка даних, цілісність інформації що передається, безпека даних, структура мережі.

Джон Бойд представив модель в якій відобразив що будь-яка діяльність у військовій сфері з певним ступенем наближення може бути представлена у вигляді моделі OODA: Observe (Спостерігай), Orient (Орієнтуйся), Decide (Вирішуй), Act (Дій) [1]. Загалом модель може використовуватися у різних сферах.

Модель OODA передбачає багаторазове повторення циклу дій, що складається з чотирьох послідовних взаємодіючих процесів, таких як: спостереження, орієнтація, рішення, дія. Тобто відбувається розвиток ситуації по спіралі, і кожному етапі цієї спіралі здійснюється взаємодія із зовнішнім середовищем і на противника. Модель зазвичай відносять до розряду кібернетичних, оскільки в ній реалізується принцип «зворотного зв'язку», відповідно до якого «частина виходу з системи знову подається на її вхід», щоб уточнити, а якщо потрібно, то скоригувати розвиток системи на наступних етапах [2].

На основі петлі OODA розроблена модель для використання у мережецентичному інформаційному середовищі (рис.1) орієнтуючись на загальні потреби.

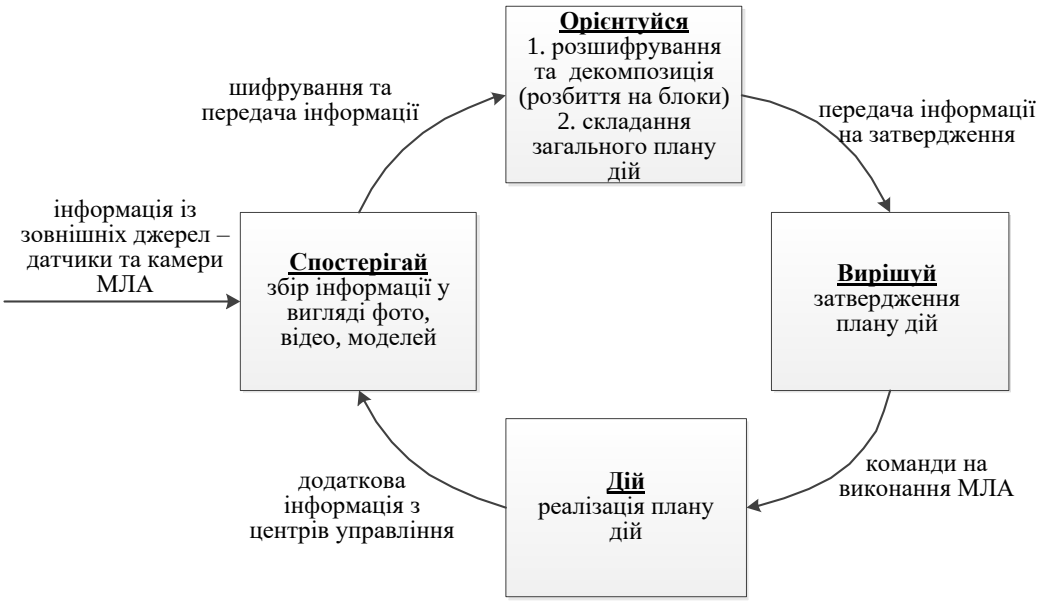

Рис.1 Модель OODA у мережецентричному інформаційному середовищі

Спостереження – передбачає процес збору інформації для прийняття рішення у кожному конкретному випадку. У середовище що розглядається перший вид інформації отримується з камер та датчиків БПЛА. Другий вид

інформації надходить з четвертого етапу у вигляді команд з центрів управління безпосередньо від командування.

Орієнтація – складається з двох станів: декомпозиції та синтезу. Декомпозиція передбачає розбиття отриманої інформації на блоки, що простіше піддаються осмисленню. Синтез передбачає об'єднання елементарних підпланів в загальний план дій. Якщо плани для обрання рішення не створені, процес залишається на етапі орієнтації і здійснюється подальша декомпозиція задачі.

Ухвалення рішення – приймається рішення про виконання плану який був сформований на попередньому етапі. При наявності декількох альтернативних планів на цьому етапі – рішення приймається виходячи з ситуації.

Дія – практична реалізація планів які були прийняті у попередньому етапі. Включає в себе зліт та переміщення БПЛА для виконання поставлених планів або розвідку.

Висновки та перспективи

Моделювання передачі та обробки інформації в мережевому середовищі вимагає ретельного розгляду структури мережі, потоку даних, обчислювальних процесів і механізмів співпраці. Використання інструментів моделювання може надати розуміння поведінки системи, оптимізувати продуктивність і покращити прийняття рішень в наведених системах.

Перспективою подальших досліджень є створення загальної інформаційної моделі мережецентричного середовища.

Список використаних джерел

1. Coram Robert. Boyd: the fighter pilot who changed the art of war. New York: Back Bay Books/Little, Brown. 2004.

2. Greene Robert. The 33 Strategies of War (Joost Elffers Books), Profile Books. 2007.

Мунтяну Анастасія Юрієвна
студентка 3 курсу, групи ІП-21
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
(+49) 162-334-8574
munteanu.anastasiia@gmail.com
Науковий керівник: **Поперешняк Світлана Володимирівна**
к.ф.-м.н., доцент, доцент кафедри ІПІ ФІОТ
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
(098)-645-546-2
spopereshnyak@gmail.com

АВТОМАТИЗАЦІЯ ТА ПЕРСОНАЛІЗАЦІЯ ПРОЦЕСІВ ПЛАНУВАННЯ ПОДОРОЖЕЙ

Постановка задачі. За останні роки індустрія туризму зазнала значних змін, пов’язаних як із пандемією Covid-19, так і зі стрімкою цифровізацією, що впливає на всі аспекти повсякденного життя. Спрощення, пришвидшення та персоналізація процесів стали ключовими задачами сучасного розвитку індустрії. Тому актуальним є аналіз інструментів, які можуть використовуватись для розробки інтерактивних цифрових рішень, спрямованих на планування подорожей та покращення досвіду туристів.

Мета дослідження. Метою дослідження є аналіз підходів до автоматизації процесу планування подорожей за допомогою сучасних цифрових технологій та пошук оптимального варіанту їх поєднання.

Результати дослідження. Технології штучного інтелекту, віртуальної реальності, великих даних та загалом цифровізованих платформ відкривають можливості як для індивідуальних користувачів, так і для великих представників індустрії туризму. Виникає необхідність в створенні централізованих рішень, що задовільнять всі функціональні вимоги як клієнтів, так і надавачів послуг, орієнтуючи бізнес-процеси на користувача крізь персоналізацію результатів.

Використання генеративного штучного інтелекту (GAI) та чат-ботів надає найширші можливості для персоналізованого планування. Інструменти ШІ, зокрема віртуальні асистенти та системи рекомендацій, можуть полегшувати процес прийняття рішення перед поїздкою, під час та після неї. Інтегровані великі мовні моделі (LLM) забезпечують обробку людської мови, аналіз контексту та сприйняття намірів, що підвищує рівень персоналізації та доступності. Проведене MDPI опитування підтвердило позитивне сприйняття цих технологій. 86% опитаних відзначили переваги застосування ШІ у подорожах, і лише 13,7% відчули негативні емоції через використання цих систем, переважно через технічні обмеження або складнощі у використанні [1].

Віртуальні технології трансформації сучасності - Metaverse включають в себе віртуальну (VR) та доповнену реальність (AR). Вони надають можливість

користувачам попередньо переглядати напрямки подорожей, номери готелів, місцеві пам'ятки, отримувати інтерактивний та інклюзивний досвід в музеях і галереях. Дослідження показують, що такі інструменти зменшують вагання користувачів і надають більшої ваги їх особистим враженням [2].

Використання великих даних (Big data) у плануванні подорожей дозволяє підвищити рівень персоналізації та ефективність. Аналізуючи історичні дані про подорожі, тренди в соцмережах і поведінку під час бронювання, алгоритми можуть прогнозувати вподобання користувачів і оптимізувати маршрути.

У централізованій системі планування значною перевагою може стати система надання і аналізу відгуків. Модель, навчена на основі обробки природної мови (NLP), здатна виявляти основні скарги та вподобання, дозволяючи динамічно адаптувати пропозиції. Поєднання наданого користувачем відгуку із результатами генерації та деталями подорожі повертаються в систему для вдосконалення майбутніх вихідних даних.

Інтеграція з різноманітними сервісами, що надають інформацію в реальному часі, є необхідною, щоб компенсувати обмеження в знаннях великих мовних моделей. Чат-боти базуються на статичних наборах даних, які завершуються на певному моменті. Інтегровані API можуть повідомляти про затримки рейсів, попереджати про погодні умови та, надавати інформацію про затори, що надалі використовується ШІ для оптимізації маршруту.

Створення ефективної інтегрованої системи автоматизації планування подорожей включає в себе поєднання всіх описаних новітніх технологій в єдину платформу. Це дозволить забезпечити повний цикл підтримки користувача: від збору даних у реальному часі до інтерактивної взаємодії та адаптації планів у відповідь на зміни умов. Схему процесу створення плану подорожі в такій системі зображено на рис. 1. Окрім зазначених технологій, не рекомендується нехтувати інструментами для мануального планування. Інтегрована платформа має забезпечувати можливість користувача редагувати свій поденний план та власноруч управляти параметрами подорожі, в тому числі завантажувати квитки, переглядати інтерактивну мапу, виконувати резервування та завантажувати зображення.

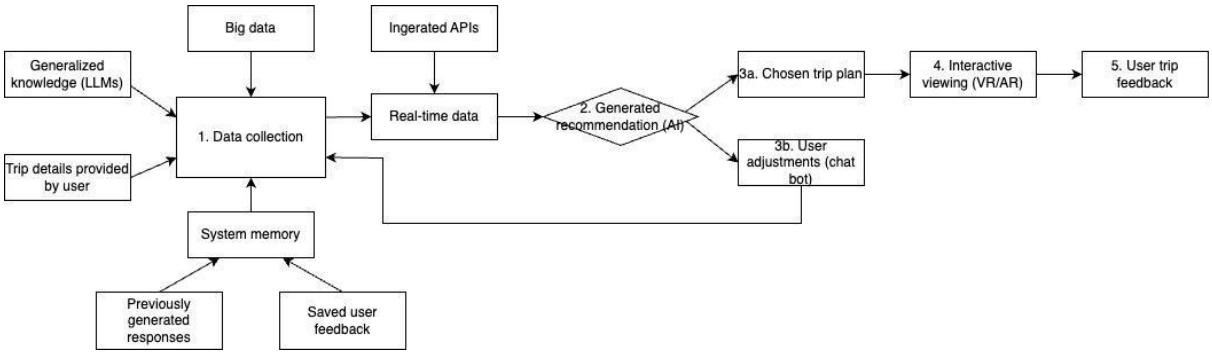

Рис. 1 – Процес автоматизованого створення плану подорожі

Висновки і перспективи. У дослідженні було розглянуто сучасні цифрові технології, що можуть використовуватись для створення інтегрованої системи

автоматизованого планування подорожей. Подані інструменти дозволяють забезпечити високу персоналізацію, ефективність і зручність для користувачів. Запропонований в дослідженні варіант їх об'єднання у межах єдиної системи сприяє оптимізації маршрутів, адаптації до змін умов і забезпеченню інтерактивного досвіду користувача.

Перспективою подальших досліджень є впровадження гібридних підходів, які дозволять поєднувати автоматизацію з гнучкими інструментами для ручного налаштування, враховуючи індивідуальні потреби користувачів, а також вибір найбільш адаптивної та ресурсоощадної моделі для збору і аналізу даних.

Список використаних джерел

1. Sousa, A., Cardoso, P., Dias, F., & Kaur, K. The Use of Artificial Intelligence Systems in Tourism and Hospitality: The Tourists' Perspective. *School of Tourism and Maritime Technology, Polytechnic University of Leiria,* 2024.
2. Nunez, R. Try Before You Buy: Using Virtual Reality for Travel
3. Planning. *Master's thesis, University of Stavanger,* 2017.

Пізнак Роман Васильович
студент 3 курсу, групи ІП-21
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
(38067)-69-139-25
piznakrom@gmail.com
Науковий керівник: **Поперешняк Світлана Володимирівна**
к.ф.-м.н., доцент, доцент кафедри ІПІ ФІОТ
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
(098)-645-546-2
spopereshnyak@gmail.com

РОЗРОБКА ПЛАТФОРМИ ДЛЯ ОРГАНІЗАЦІЇ ВІДЕОКОНФЕРЕНЦІЙ

Постановка задачі. В умовах карантинних заходів в умовах пандемій, та нестабільної політичної ситуації неможливо уявити забезпечення якісного освітнього процесу, робочої комунікації та навіть надання медичних послуг. Ключовою задачею платформ для відеоконференцій є вирішення проблем дистанційної взаємодії між користувачами з різних куточків світу, з урахуванням різних потужностей користувацьких пристроїв та швидкості інтернет з'єднання [1].

Мета дослідження. Метою розробки є забезпечення високого рівня зручності використання застосунку, зменшення навантаження на користувацькі пристрої та залежності від інтернету.

Результати дослідження.

Розроблена платформа для організації відеоконференцій має весь базовий функціонал, характерний для подібних платформ. Вона забезпечує можливість взаємодії між користувачами шляхом передачі аудіо- та відеоданих, крім того надає розширений функціонал як от поширення екранів робочих областей та комунікація з допомогою невербальних методів (емоцій). Кожен користувач має свій власний акаунт та може планувати відеоконференції, записувати їх та зберігати історію своїх участей у обговореннях.

Весь користувацький інтерфейс є простим та інтуїтивно зрозумілим, виконаний у кольорах, що рекомендовані у тому числі для використання людьми з порушеннями зору. Інтерфейс коректно відмальовується і на мобільних пристроях.

У процесі розробки особливу увагу було приділено безпеці даних. При передачі мультимедійних даних використовуються алгоритми стиснення, після чого мультимедійні дані шифруються з допомогою протоколу SRTP, а сигнальні повідомлення шифруються з використанням протоколу DTLS. Тобто, навіть у разі перехоплення даних зловмисником, він не отримає їх у чистому вигляді і . Безпека особистих даних у користувацьких акаунтах ґрунтується на

використанні складних хеш-функцій, подібних до тих. що використовуються у системах на базі блокчейну. Такий спосіб збільшує розмір бази даних, проте забезпечує належний рівень захисту.

Додаток легко масштабувати через незалежність сервісів та особливості безсерверної архітектури. Детальну схему архітектури зображено на рисунку 1.

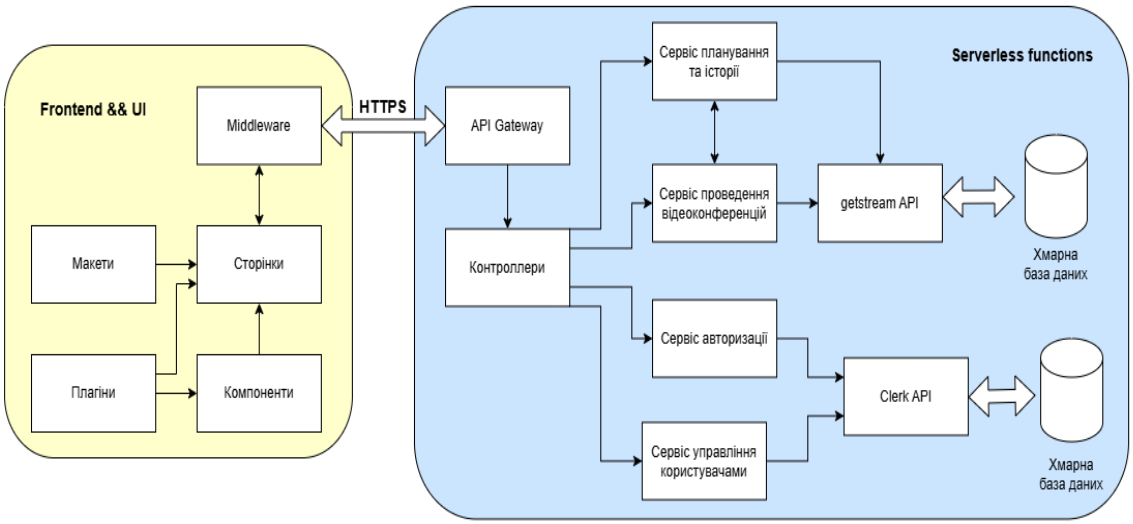

Рис. 1. Архітектура розробленої системи

Верхнім шаром у цій схемі є фронтенд частина, що відповідає за візуальне представлення функціоналу застосунку. Сторінка є ключовим компонентом цього шару, вона відображає конкретну сторінку, видиму для користувача. Для безпечної взаємодії між фронтендом і бекендом використовується протокол безпечного обміну HTTP-запитами - HTTPS.

Вхідним компонентом бекенду є API Gateway. Ця частина є центральною точкою для всіх запитів, що надходять від фронтенду. Сервіс планування та історії відповідає за управління розкладом подій та переглядом минулих подій. Цей сервіс інтегрований із зовнішнім API getstream, що дозволяє створювати порожні захищені сторінки з вбудованим балансуванням навантажень, які пізніше з допомогою бібліотек та фреймворків перетворюються у кімнати відеоконференцій. Сервіс авторизації відповідає за перевірку доступу користувачів до системи. Його функціями є аутентифікація та авторизація користувачів. Авторизація побудована на базі OAuth 2.0 з використанням JWT токенів. Цей сервіс взаємодіє зі стороннім API хмарного сервісу Clerk, що має автоматичний балансувач навантажень. Сервіс управління користувачами відповідає за редагування та збереження особистих даних користувачів. Він як і попередній сервіс, інтегрований з зовнішнім API, відправляючи потрібні запити.

Така архітектура є оптимальним варіантом для розробленої системи. Вона мінімізує різного роду навантаження на користувацький пристрій, що відповідно впливає на залежність від інтернет з’єднання, адже результати всіх запитів передаються через мережу інтернет. Також забезпечується високий рівень масштабованості, оскільки обробка основного навантаження здійснюється на

серверній стороні. Це дозволяє легко адаптувати систему до зростання кількості користувачів без суттєвого впливу на продуктивність. [2]

Крім окремих технічних переваг, застосунок має значні переваги і з точки зору клієнта. Він має розширені ліміти на тривалість відеоконференцій у порівнянні з найпопулярнішими платформами у галузі.

Висновки та перспективи. У ході роботи було розроблено платформу для організації відеоконференцій, яка відповідає сучасним вимогам до якості дистанційної взаємодії. Проведений аналіз існуючих рішень дозволив врахувати їх сильні та слабкі сторони для створення функціонального, безпечного та зручного у використанні застосунку. Платформа забезпечує передачу аудіо- та відеоданих, розширені можливості комунікації, а також високу адаптивність до різних умов інтернет-з'єднання та користувацьких пристроїв.

Перспективою подальших досліджень є впровадження нових функціональних можливостей, таких як розширені аналітичні інструменти для аналізу відеоконференцій, адаптивні алгоритми для зменшення затримок у передачі даних, а також інтеграція із системами штучного інтелекту для автоматичного перекладу, розпізнавання голосу та обличчя. Це дозволить зробити платформу ще більш універсальною та конкурентоспроможною у глобальному масштабі. [3]

Список використаних джерел

1. Education during a pandemic crisis: problems and prospects. Monograph. Eds. Tetyana Nestorenko & Tadeusz Pokusa. Opole: The Academy of Management and Administration in Opole, 2020; pp. 203-208;
2. Solanki J. Serverless Architecture – What It Is? Benefits, Limitations & Use cases [Електронний ресурс] / Jignesh Solanki. – 2023. – Режим доступу до ресурсу: https://www.simform.com/blog/serverless-architecture-guide.
3. Ana Maria Suduc, Mihai Bizoi, "AI shapes the future of web conferencing platforms". International Conference on Information Technology and Quantitative Management, 2022; pp. 2-7

Синьковський Іван Володимирович
студент 6 курсу, групи ІП-32мп
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"
(066)754-36-59
Synk_ivan@gmail.com
Науковий керівник: **Поперешняк Світлана Володимирівна**
к.ф.-м.н., доцент, доцент кафедри ІПІ ФІОТ
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"
(098)-645-546-2
spopereshnyak@gmail.com

АДАПТИВНА СИСТЕМА ДЛЯ БАГАТОМОВНОГО ПРИЙОМУ ЗАМОВЛЕНЬ У РЕСТОРАНАХ ШВИДКОГО ХАРЧУВАННЯ

Постановка задачі. В умовах глобалізації та зростаючої мобільності населення ресторанний бізнес, зокрема заклади швидкого харчування, стикається з необхідністю обслуговування клієнтів, що розмовляють різними мовами. Традиційні методи прийому замовлень не завжди ефективні в багатомовному середовищі, що може призвести до помилок у замовленнях, втрати клієнтів та зниження якості обслуговування.

Дослідження зосереджено на аналізі поточних рішень, щоб зрозуміти їхні обмеження та визначити оптимальний підхід для їх подолання. Це передбачає розробку надійної архітектури програмного забезпечення, яка є масштабованою та адаптованою до різних мов і операційних вимог. Розробляючи та впроваджуючи прототип, ця робота має на меті продемонструвати здійсненність запропонованої системи. Щоб переконатися в ефективності рішення, різні технологічні моделі будуть порівнюватися, щоб визначити найкращий підхід з точки зору адаптивності, продуктивності та досвіду користувача[2].

Мета дослідження - озробка адаптивної системи для багатомовного прийому замовлень у ресторанах швидкого харчування, що працює через інтерфейс Телеграм-бота. Програмне забезпечення дозволяє робити замовлення товарів голосом англійською та українською [3]. Особливу увагу приділено інтеграції з великою мовною моделлю, розробці адаптивної системи що здатна працювати з декількома мовами і динамічно перемикатися між ними, а також розробці універсальної бізнес логіки ресторанів швидкого харчування. Проект включає розробку інтуїтивно зрозумілого інтерфейсу, що робить замовлення простим і зрозумілим для широкого кола користувачів.

Архітектура проекту є мікросервісною (рисунок 1), де моделі розпізнавання мовлення та велика мовна є окремими сервісами до яких доступ здійснюється за допомогою http запитів. Це дозволяє легко замінювати частини ПЗ.

В рамках дослідження було порівняно декілька великих мовних моделей (таблиця 1), для пошуку найкращого рішення для даної задачі.

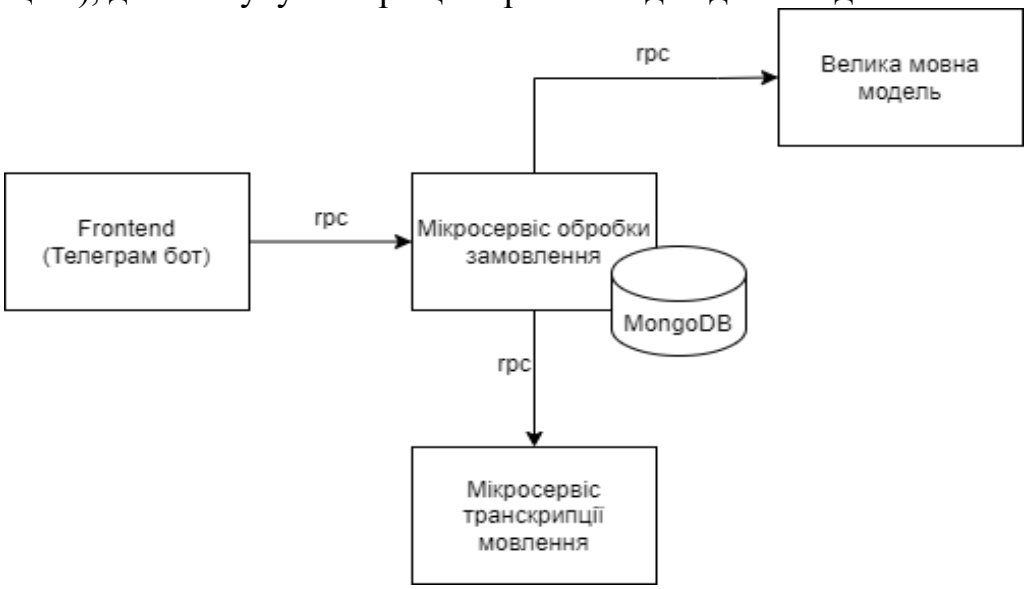

Рис. 1. Архітектура проекту

Слід зазначити, що при подальшому розвитку проекту варто використовувати модель у відкритому доступі і натренувати її для поточної задачі, проте це потребує наявності відповідних обчислювальних ресурсів.

Таблиця 1

Таблиця порівняння великих мовних моделей

	gpt4-o	gemini-1.5-pro	gpt-4
MMLU	88.7	81.9	86.4
GPQA	53.6	-	35.7
MATH	76.6	58.5	42.5
HumanEval	90.2	71.9	67.0
MGSM	90.5	88.7	74.5
DROP	83.4	78.9	80.9
Custom dataset	87.1	82.5	86.2

Результати роботи демонструються у вигляді чату з телеграм ботом. Саме такий формат був обраний через простоту реалізації фронтенду і свою достатність для демонстрації роботи концепту.

Висновки та перспективи. Було розроблено базову версію програмного забезпечення на основі архітектури описаній вище, що здатне до прийняття замовлень голосом на 2 мовах. В якості початкового прототипу результат є

задовільним. Программа підтримує прийом замовлень на 2 мовах і є легко розширюваною.

У результаті дослідження було розроблено та протестовано адаптивну систему для багатомовного прийому замовлень, що здатна:

- Автоматично розпізнавати мову користувача та налаштовувати інтерфейс відповідно до його потреб.
- Зменшити кількість помилок під час прийому замовлень завдяки інтеграції технологій машинного перекладу та штучного інтелекту.
- Підвищити швидкість обслуговування клієнтів завдяки автоматизації та адаптивним алгоритмам.
- Забезпечити високу користувацьку задоволеність через індивідуальний підхід до клієнтів різних мовних груп.

Перспективи подальших досліджень:

- Розширення мовної бази — інтеграція нових мов для подальшого розширення цільової аудиторії.
- Впровадження голосових помічників для прийому замовлень у режимі реального часу.
- Оптимізація системи через машинне навчання для покращення точності розпізнавання мовних діалектів та акцентів.
- Інтеграція системи з касовими апаратами та мобільними додатками для створення єдиної екосистеми обслуговування клієнтів.
- Аналіз великих даних (Big Data) для персоналізації замовлень, прогнозування попиту та оптимізації меню залежно від культурних особливостей клієнтів.

Запропонована система відкриває нові можливості для підвищення конкурентоспроможності закладів швидкого харчування, забезпечуючи якісний сервіс у багатомовному середовищі.

Список використаних джерел

1. Sparks of Artificial General Intelligence: Early experiments with GPT-4 [Електронний ресурс] / P.Lee, S. Bubeck, V. Chandrasekaran, R. Eldan. – 2023. – Режим доступу до ресурсу: https://arxiv.org/pdf/2303.12712.

2. A Comprehensive Overview of Large Language Models [Електронний ресурс] / H.Naveed, A. Khan, S. Qiu, M. Saqib. – 2024. – Режим доступу до ресурсу: https://arxiv.org/pdf/2307.06435.

3. Sharma S. Speech Recognition System: A review [Електронний ресурс] / Sachin Sharma. – 2020. – Режим доступу до ресурсу: https://www.researchgate.net/publication/343934770_Speech_Recognition_System_A_review.

4. A Systematic Survey of Prompt Engineering in Large Language Models: Techniques and Applications [Електронний ресурс] / P.Sahoo, A. Singh, S. Saha, V. Jain. – 2024. – Режим доступу до ресурсу: https://arxiv.org/abs/2402.07927.

5. Robust Speech Recognition via Large-Scale Weak Supervision [Електронний ресурс] / A.Radford, J. Kim, T. Xu, G. Brockman. – 2021. – Режим доступу до ресурсу: https://cdn.openai.com/papers/whisper.pdf.

Срібна Аліна Анатоліївна
студентка 2 курсу, групи ІСДМ-61
Державного університету
інформаційно-комунікаційних технологій
(050)-411-92-92
alinasribna166@gmail.com
Науковий керівник: **Сторчак Камілла Павлівна**
доктор технічних наук, професор, завідувач кафедри Інформаційних систем та технологій Державного університету інформаційно-комунікаційних технологій, м. Київ

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В УПРАВЛІННІ ЗНАННЯМИ

Процеси управління знаннями, такі як створення, зберігання, обмін і застосування знань, суттєво впливають на прийняття рішень і конкурентоспроможність. У цьому контексті зросла роль штучного інтелекту як ключового компонента революції в галузі використання даних у бізнесі. Численні організації досліджують вплив штучного інтелекту на свою діяльність і шукають найкращі способи використання штучного інтелекту для вдосконалення практик управління знаннями. Завдяки автоматизації багатьох трудомістких завдань, пов’язаних із керуванням даними, моделі штучного інтелекту (ШІ) і машинного навчання дозволяють краще збирати, упорядковувати та використовувати величезні обсяги інформації у організації.

Постановка задачі. У контексті стрімкого зростання обсягів даних та складності організаційних структур, ефективне управління знаннями стає критично важливим для забезпечення конкурентоспроможності підприємств. Традиційні методи управління знаннями часто виявляються недостатніми для обробки великих масивів інформації та вилучення з них цінних знань. Штучний інтелект (ШІ) пропонує нові можливості для автоматизації та оптимізації цих процесів, однак його впровадження пов'язане з низкою теоретичних і практичних проблем, таких як вибір відповідних алгоритмів, інтеграція в існуючі системи та забезпечення безпеки даних.

Мета дослідження. Мета цього дослідження - проаналізувати трансформаційну роль штучного інтелекту в управлінні знаннями, представивши обидві концепції та дослідивши їхній взаємозв'язок. Завдяки всебічному огляду літератури та емпіричним дослідженням у роботі з'ясовується, як нові технології штучного інтелекту інтегруються в системи управління знаннями, покращуючи їхні процеси та організаційну здатність управляти знаннями.

Результати дослідження. В роботі досліджуються тонкощі управління знаннями, охоплюючи його визначення та типи, як ШІ та управління знаннями працюють разом, а також як ШІ розширює можливості сучасного управління знаннями та як його можна використовувати для прийняття стратегічних рішень для успіху організації. Підкреслюється важливість штучного інтелекту в управлінні знаннями, досліджуються програми та технології, окреслюються

кроки для впровадження та пропонується уявлення про майбутні тенденції ШІ для управління знаннями.

Зростання можливостей штучного інтелекту та перспективні функції для досягнення цих цілей можуть вимагати інших форм розподілу роботи між працівниками та інтелектуальними машинами, ніж ті, які ми спостерігали в організаціях у минулому. Такі нові ролі вимагають нового набору навичок і компетенцій для людей і нового дизайнерського мислення для інтелектуальних машин.

Висновки та перспективи. У міру того, як інтеграція штучного інтелекту в управління знаннями зростає, користувачі отримують точнішу інформацію на основі загальних даних для прийняття обґрунтованих рішень. Послуги стають дуже адаптованими до окремих осіб.

Результати дослідження свідчать, що успішне впровадження штучного інтелекту в управління знаннями може значно підвищити гнучкість організації, посилити конкурентні переваги та покращити операційну ефективність.

Прийняття керованих штучним інтелектом систем управління знаннями свідчить про рух до більш адаптивного, інтелектуального та спільного інформаційного середовища.

Список використаних джерел

1. Dobosevych O. Why an AI-powered knowledge management system can be a game-changer for enterprise?. *Geniusee*. URL: https://geniusee.com/single-blog/ai-based-knowledge-management-systems-for-enterprises (date of access: 25.12.2024).

2. Integration of Artificial Intelligence Applications and Knowledge Management Processes for Construction Projects Management | Altaie | Civil Engineering Journal. *Civil Engineering Journal*. URL: https://www.civilejournal.org/index.php/cej/article/view/4659

Шостовіцький Дмитро Геннадійович
студент 2 курсу, групи ІСДМ-61
Державного університету інформаційно-комунікаційних технологій
(095)-948-73-62
shostovitskiy.dmitro@gmail.com
Науковий керівник: **Срібна Ірина Миколаївна**
доктор технічних наук, доцент кафедри Інформаційних систем та технологій Державного університету інформаційно-комунікаційних технологій, м. Київ

УДОСКОНАЛЕННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ ОПТИМІЗАЦІЇ ІГРОВИХ СТРАТЕГІЙ

У сучасному світі технологічних інновацій штучний інтелект (ШІ) займає важливе місце в різних сферах діяльності, включаючи розробку ігор, де він використовується для створення складних алгоритмів, які можуть імітувати людське прийняття рішень. Стратегії таких ігор, як Го, шахи, або Сьогі (Sho-Gi), вимагають від моделей здатності опрацьовувати складні взаємозв'язки між елементами гри. Проте існуючі моделі автономних нейронних мереж стикаються з певними обмеженнями, такими як недостатня ефективність при обробці складних ігрових даних, що є перешкодою для їхнього широкого впровадження.

Постановка задачі. Розробка гібридної графової згорткової нейронної мережі (GCNN), яка об'єднує переваги графових і згорткових мереж, дозволяючи ефективно вирішувати задачі прогнозування та аналізу стратегічних рішень у складних ігрових ситуаціях.

Мета дослідження. Для вирішення зазначених проблем у роботі запропоновано гібридну модель, яка поєднує переваги графових та згорткових нейронних мереж. Графові нейронні мережі здатні ефективно обробляти ігрові дані, представлені у вигляді графів, що дозволяє виділяти кореляції та залежності між різними елементами гри. Згорткові нейронні мережі використовуються для аналізу зображень і зв'язків між локальними елементами, що дозволяє підвищити точність прогнозування. Модель, таким чином, має змогу враховувати як просторові характеристики гри, так і глобальні стратегії, що приймаються гравцями. Для перевірки ефективності розробленої моделі було використано набір даних гри Го (KGS), що дозволило оцінити її здатність до прогнозування ходів та адаптації до різних ситуацій гри.

Результати дослідження. У ході експериментів було порівняно ефективність гібридної моделі з традиційними методами, заснованими на глибоких згорткових нейронних мережах. Результати показали, що гібридна модель виявилася значно ефективнішою в плані точності прогнозування, особливо в складних ситуаціях, коли необхідно враховувати багаточисельні взаємозв'язки між елементами гри. Гібридна модель демонструє кращі результати в порівнянні з класичними методами при обробці стратегічних рішень, що дає змогу впевнено стверджувати про її потенціал для більш складних ігор і сценаріїв.

Висновки та перспективи розвитку. Розроблена в цій роботі гібридна модель на основі графових та згорткових нейронних мереж показала свою ефективність у задачах прогнозування стратегічних рішень в ігрових ситуаціях, зокрема в грі Го. Вона дозволяє не лише обробляти просторові особливості гри, а й враховувати глобальні взаємозв'язки між елементами гри. Результати дослідження підтверджують, що гібридний підхід є перспективним для розвитку нових методів моделювання ігрових стратегій. Проте для досягнення ще більших результатів необхідно провести подальші дослідження, які включатимуть оптимізацію обчислювальних процесів, розробку нових методів побудови графів та інтеграцію додаткових моделей навчання.

Також велику перспективу має вдосконалення методів побудови графів. Використання більш складних технологій, таких як суперпікселі, може спростити процес створення графів у складних ігрових середовищах. Суперпікселі дозволяють зменшити кількість елементів, що потрібно обробляти в кожному кроці гри, при цьому зберігаючи всю необхідну інформацію для аналізу. Це допоможе зменшити обчислювальні витрати та підвищити ефективність обробки графових даних.

Список використаних джерел

1. Neven, F.; Schwentick, T.; Vianu, V. Finite state machines for strings over infinite alphabets. ACM Trans. Comput. Log. 2004, 5, 403–435. [Google Scholar] [CrossRef]

2. Browne, C.; Powley, E.J.; Whitehouse, D.; Lucas, S.M.; Cowling, P.I.; Rohlfshagen, P.; Tavener, S.; Liebana, D.P.; Samothrakis, S.; Colton, S. A Survey of Monte Carlo Tree Search Methods. IEEE Trans. Comput. Intell. AI Games 2012, 4, 1–43. [Google Scholar] [CrossRef]

3. Furukawa, M.; Abe, M.; Watanabe, T. A Study on Utility Based Game AI Considering Long-Term Goal Achievement. J. Soc. Art Sci. 2021, 20, 139–148. [Google Scholar] [CrossRef]

Шушура Віктор Олексійович
студент 2 курсу, групи ІСДМ-63
Державного університету інформаційно-комунікаційних технологій
(050)-348-45-65
Науковий керівник: **Сторчак Камілла Павлівна**
доктор технічних наук, професор, завідувач кафедри Інформаційних систем та технологій
Державного університету інформаційно-комунікаційних технологій, м. Київ

ТЕСТУВАННЯ ПРОДУКТИВНОСТІ МІКРОСЕРВІСІВ У ХМАРНОМУ СЕРЕДОВИЩІ

Розробка програмного забезпечення все більше переміщується в бік мікросервісів і хмарних технологій архітектури, де програми створюються за допомогою невеликих незалежних служб, якими є розгортання та масштабування відповідно до потреб постачальників хмарних послуг.

З одного боку, мікросервіси мають бути легкими для тестування та обслуговування, оскільки вони є незалежними функціями, які зосереджені лише на одній певній функціональності. З іншого боку, поділ програми на розподілені функції означає, що кількість сервісів різко зростає. Таким чином, тестування додатків мікросервісів фактично стає все більше і більше складним.

Постановка задачі. Тестування продуктивності таких додатків передбачає додаткові труднощі аналізу продуктивності кожного компонента та показників постачальника хмарних послуг у порівнянні із загальною продуктивністю системи. У роботі розглядається те, як розробити та запустити тести продуктивності для додатку на основі мікросервісу в хмарному середовищі та як вибрати та застосувати показники продуктивності, зібрані з тестових прогонів для визначення продуктивності програми.

Мета дослідження. Мета цього дослідження - розробити набір для тестування продуктивності для аналізу та порівняння традиційних показників тестування продуктивності з показниками, характерними для постачальника хмарних послуг. Дослідження базувалося на класичному підході до проведення тесту продуктивності з доповненнями з різних досліджень із використанням мікросервісів і хмарної архітектури.

Результати дослідження. В останні роки мікросервіси стали домінуючою архітектурою в розробці програмного забезпечення, пропонуючи масштабованість, модульність і гнучкість процесів розробки. Однак забезпечення оптимальної продуктивності перед розгортанням становить серйозну проблему, особливо в швидкоплинних середовищах безперервної інтеграції/безперервного розгортання. Традиційні методи тестування продуктивності, які ґрунтуються на синтетичних сценаріях і тривалих процесах тестування, може бути важко застосувати в середовищах, де тестування має бути реалістичним і швидким. Щоб задовольнити потребу в точному та оперативному тестуванні, у моїй роботі запропоновано та впроваджено інноваційну структуру,

яка використовує реальні відстеження використання для визначення та виконання невеликого, але важливого набору тестів продуктивності.

Висновки та перспективи. Мікросервіси пропонують значні можливості для економії коштів і оптимізації, що призвело до їх широкого впровадження в хмарному середовищі. Мікросервіси та хмарна архітектура надають величезний світ можливостей і способи реалізації програмного забезпечення. Усе це відбувається за рахунок тестування.

Знайти правильний спосіб проведення тестів продуктивності та переконатися, що показники, які ми збираємо та вимірюємо, надають нам точну інформацію про продуктивність програми, має вирішальне значення для будь-якого бізнесу.

Список використаних джерел

1. GeeksforGeeks, “Introduction of Deadlock in Operating System,” GeeksforGeeks, 23 02 2022. [Online]. Available: https://www.geeksforgeeks.org/introduction-ofdeadlock-in-operating-system/. [Accessed 27 12 2022].

2. C. HARRIS, “Microservices vs. monolithic architecture,” Atlassian logo, [Online]. Available:

https://www.atlassian.com/microservices/microservicesarchitecture/microservices-vs-monolith. [Accessed 27 12 2022].

Напрям 5. КОМП'ЮТЕРНІ МЕРЕЖІ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ.

Артюшин Володимир Володимирович
студент 6 курсу, групи ІСДМ-64
Державний університет інформаційно-комунікаційних технологій
(050)-310-03-27
artiushyn@gmail.com
Науковий керівник: **Жебка Вікторія Вікторівна**
доктор технічних наук, професор, завідувач кафедри Технологій цифрового розвитку Державного університету інформаційно комунікаційних технологій, м.Київ

СИСТЕМА МОНІТОРИНГУ ZABBIX ЯК УНІВЕРСАЛЬНИЙ ІНСТРУМЕНТ КОНТРОЛЮ ОБЛАДНАННЯ ДАТА-ЦЕНТРІВ

Постановка задачі. Останнє десятиліття відзначено стрімким зростанням обсягу даних, що споживаються будь якою галуззю промисловості та абонентами операторів фіксованого та мобільного зв'язку. Пропорційно зростав попит на послуги зберігання та обробки даних, які забезпечуються сучасними дата-центрами[3] або центрами обробки даних (ЦОД). Загалом, великі ЦОДи можуть мати у своєму складі від десятків тисяч до сотень тисяч різноманітних серверів. Побудова ефективної системи моніторингу для дата-центру є одним з першочергових завдань для оператора, що дає змогу швидко виявити аварійні ситуації та мінімізувати іх наслідки.

Мета дослідження. Метою дослідження є аналіз можливості використання системи монітрингу Zabbix[1] для контролю стану обладнання у ЦОД.

Результати дослідження. Сучасний ЦОД може мати різні типи серверів, залежно від необхідної функції та потреб клієнтів. Це можуть бути фізичні або віртуальні сервери, які вирішують різноманітні завдання зі зберігання або обчислення даних.

Аналіз показав, що система монітрингу Zabbix забезпечує повний контроль над інфраструктурою ЦОД: мережевими пристроями, серверами, різними додатками та IT-ресурсами [2]. Це у повній мірі відноситься як для серверів на операційній системі (ОС) Windows так і на ОС Linux.

Впроваджено широкий набір метрик, які включають дані про завантаження процесора, використання оперативної пам'яті, температуру, мережевий трафік, стан дисків та інші критичні параметри обладнання.

Завдяки гнучкості системи моніторингу, забезпечується підтримка великої кількості пристроїв не тільки з відкритим апаратним та програмним забезпеченням (АЗ та ПЗ), але і з пропрієтарним, яке може взаємодіяти з іншими системами по відкритим протоколам і стандартам.

Мережеве виявлення (Network Discovery) у Zabbix – це корисний механізм автоматичного пошуку та додавання пристроїв і сервісів у мережі для

моніторингу. Він дозволяє автоматизувати процес додавання нових пристроїв до системи Zabbix, що особливо корисно у великих дата-центрах із динамічною інфраструктурою. Через певний проміжок часу виконується пошук за заданим діапазоном IP-адрес з метою виявлення активних пристроїв. Потім, автоматично визначаються типи пристроїв та, за потреби, автоматично прив'язуються відповідні шаблони до знайдених пристроїв. Автоматично знайдені пристрої додаються до відповідної групи хостів та налаштовуються дії, які виконуватимуться при виявленні пристроїв. Наприклад, це може бути створення тригерів, надсилання повідомлень або додавання певних тегів на різні події.

Одночасно з мережевим виявленням, на пристрої виконується виявлення низькорівневих елементів (Low-Level Discovery, LLD), що дозволяє автоматично виявляти ресурси та елементи всередині вже існуючих вузлів мережі. Це можуть бути, наприклад, файлові системи, змінні диски або мережеві інтерфейси. LLD особливо корисне для моніторингу серверів ЦОД зі складними та змінними файловими системами або інтерфейсами, яких треба оперативно додавати на моніторинг або видаляти, якщо вони більше не виявляються впродовж заданого часу.

Zabbix добре масштабується і може використовуватися як у малих мережах, так і у великих розподілених системах. Система підтримує розподілену архітектуру з додатковими Proxy-серверами, що дозволяє масштабувати моніторинг на велику кількість вузлів. Zabbix Proxy – це проміжний компонент системи моніторингу Zabbix, який використовується для збору даних із серверів, пристроїв чи інших об'єктів у віддалених мережах або для розподілу навантаження на основний Zabbix сервер.

Наприклад, у середньому, один Zabbix Server із потужним сервером бази даних може обслуговувати до 1000 хостів. Щоб моніторити понад 1000 хостів додають Proxy-сервер, який розширює можливості монітрингу приблизно до 10000 хостів. Конкретні цифри навантаження вираховуються у залежності від кількості метрик, їх складності та частоті опитування. Для ЦОДів з числом хостів понад 10 000 треба використовувати розподілене середовище з кількома Proxy-серверами та потужною базою даних. Також треба ретельно виконати мережеве планування та у процесі експлуатації не забувати виконувати моніторинг самих Zabbix та Proxy-серверів щоб рівномірно перерозподіляти завантаження компонентів системи моніторингу.

Висновки та перспективи. В дослідженні виконано аналіз можливості використання системи монітрингу Zabbix для контролю стану обладнання у ЦОД. Розглянуто основні можливості системи моніторингу Zabbix та потреби сучасних ЦОДів з погляду моніторингу. Зроблено висновок, що Zabbix є відмінним вибором для моніторингу обладнання у дата-центрах завдяки своїй функціональності, масштабованості та підтримці багатьох пристроїв і протоколів. При правильному налаштуванні та професійній підтримці, система допоможе ефективно контролювати інфраструктуру дата-центрів та оперативно реагувати на будь-які збої.

Список використаних джерел

1. Zabbix. URL: https://uk.wikipedia.org/wiki/Zabbix
2. Посібник Zabbix. URL: https://www.zabbix.com/documentation/6.4/ua/manual
3. Центр даних. URL: https://uk.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BD%D1%82%D1%80_%D0%B4%D0%B0%D0%BD%D0%B8%D1%85

Бацунов Дмитро Сергійович
студент 6 курсу, групи ПДМ-62
Державного університету інформаційно-комунікаційних технологій
batsunovdima38@gmail.com
Науковий керівник: **Жебка Вікторія Вікторівна**
доктор технічних наук, професор,
завідувачка кафедри Технологій цифрового розвитку
Державного університету інформаційно комунікаційних технологій, м. Київ

ЗАСТОСУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ ДЛЯ ПОКРАЩЕННЯ МЕТОДУ СПІЛЬНИХ ПАСАЖИРСЬКИХ ПЕРЕВЕЗЕНЬ

Постановка задачі. Сучасний світ стрімко розвивається, і разом із ним зростають вимоги до ефективності, зручності та екологічності транспортних рішень. Спільні пасажирські перевезення, як-от карпулінг або райдшеринг, стають важливим елементом у розв'язанні транспортних проблем мегаполісів і невеликих міст. Однак, для їх повноцінного функціонування необхідна інтеграція сучасних технологій, що дозволяють оптимізувати маршрути, скорочувати час очікування та покращувати користувацький досвід.

Мета дослідження. Метою є дослідження потенціалу інтеграції хмарних платформ для вдосконалення методів спільних пасажирських перевезень. Основними завданнями є аналіз сучасних технологічних рішень у цій сфері, визначення переваг та викликів використання хмарних платформ, а також виявлення можливостей для оптимізації транспортних послуг з метою покращення ефективності, зручності та екологічної стійкості.

Результати дослідження. У результаті дослідження було порівняно і виявлено найбільш доцільні хмарні технології які можуть значно покращити продуктивність серверу та передбачуваності маршруту. Були використані наступні хмарні технології

OpenWeatherMap це універсальна платформа, яка надає доступ до метеорологічних даних через зручний API. Він пропонує інформацію про поточну погоду, прогнози на майбутнє, історичні дані та умови в реальному часі, охоплюючи мільйони міст по всьому світу. Завдяки простоті інтеграції, цей сервіс часто використовується для створення погодних сервісів у веб- та мобільних застосунках. Приклад проектції зображено на Рисунку 2

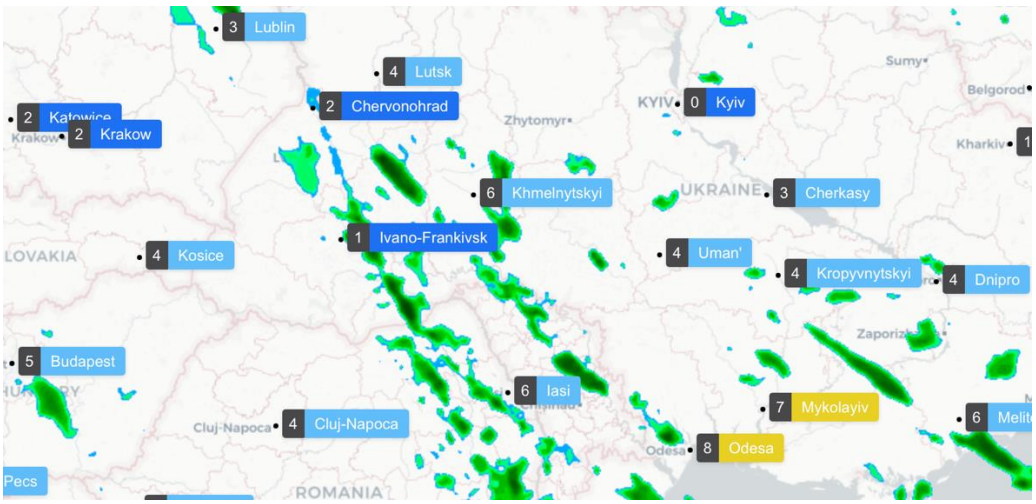

Рис. 1. Приклад проекції OpenWeatherMap

Sygic API вирізняється своїми можливостями щодо відображення трафіку та побудови карт, що робить його незамінним інструментом для сучасних навігаційних додатків. Однією з ключових переваг є деталізована інформація про дорожній трафік. Сервіс надає дані про затори, аварії, дорожні роботи та інші події в реальному часі, які можуть вплинути на маршрут. Завдяки цьому є можливість отримати актуальні рекомендації для уникнення перевантажених ділянок, що значно скорочує час у дорозі та підвищує передбачуваність маршруту. Приклад маршруту зображено на Рисунку 2

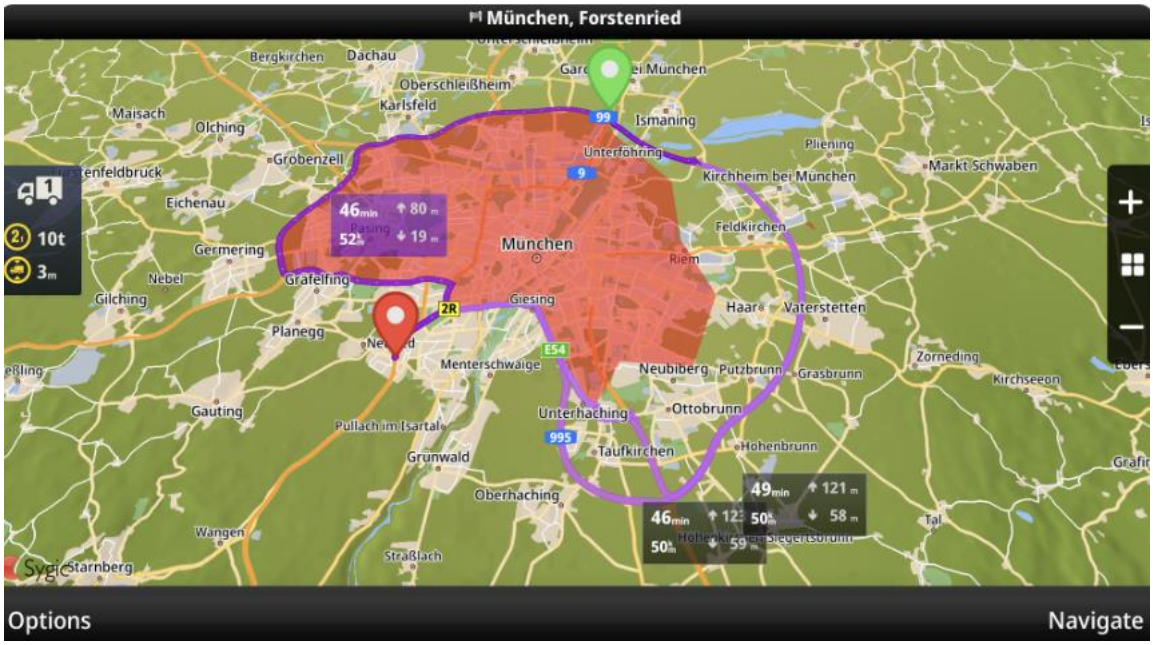

Рис. 2. Приклад маршруту Sygic

Додатково, поміж інших хмарних технологій, було виявлено доцільність у використанні

AWS SQS сервіс який забезпечує асинхронний обмін повідомленнями між компонентами системи, що дозволяє масштабувати додаток та знижувати затримки в обробці даних. Завдяки високій відмовостійкості SQS гарантує

доставку повідомлень навіть у разі збоїв. Крім того, сервіс автоматично керує чергами, зменшуючи потребу в ручному адмініструванні. Архітектура AWS SQS Queue Service зображена на Рисунку 3.

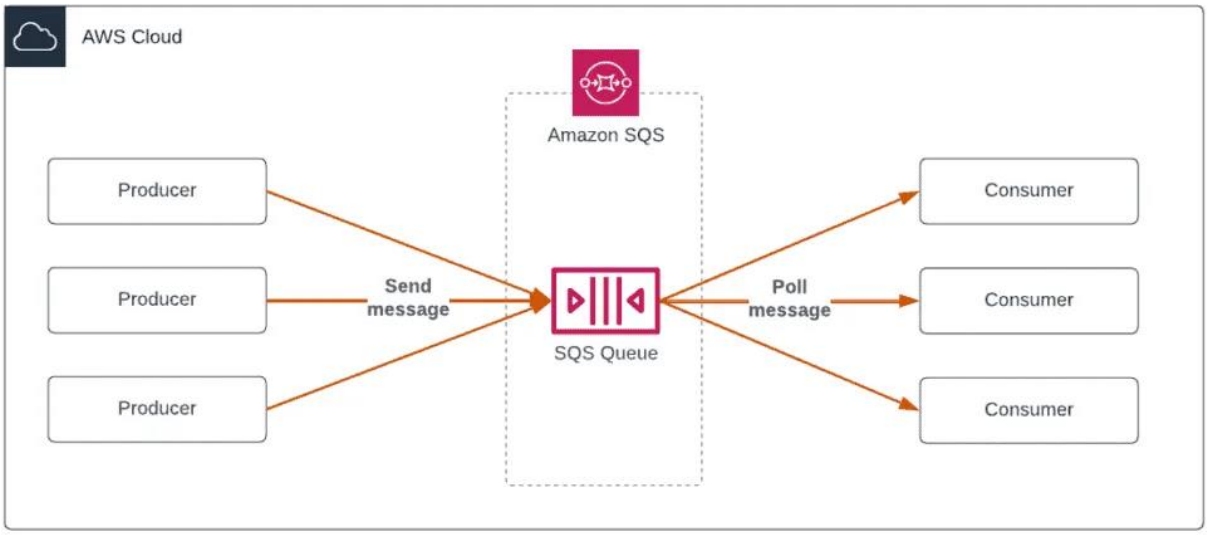

Рис. 3. Архітектура AWS SQS Queue Service

AWS Aurora забезпечує ізоляцію операцій читання (read) і запису (write), що дозволяє обробляти значні обсяги запитів на читання без впливу на швидкість запису даних. Завдяки автоматичному масштабуванню Aurora динамічно додає або видаляє ресурси для обробки навантаження, підтримуючи стабільну продуктивність навіть під час пікових навантажень. Архітектура AWS Aurora DB Service зображена на Рисунку 4.

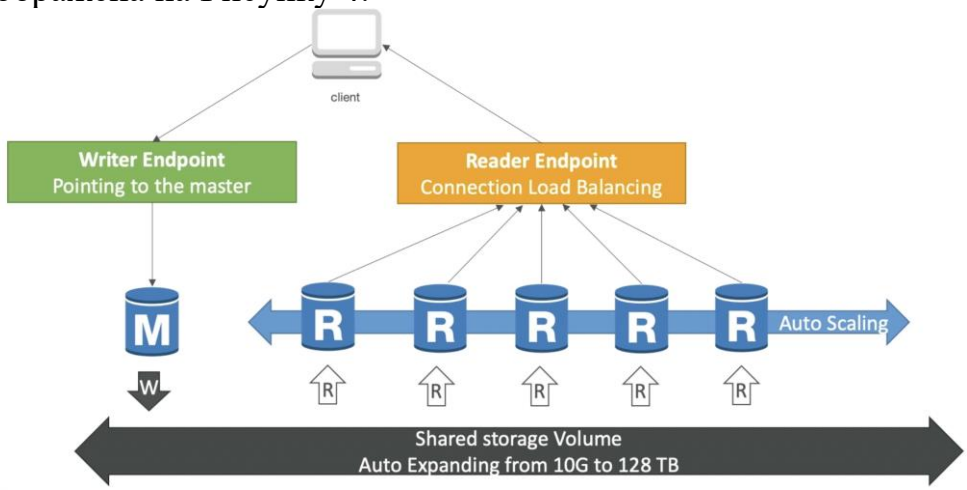

Рис. 4. Архітектура AWS Aurora DB Service

Висновки та перспективи. У результаті проведеного дослідження вдалося довести важливість і доцільність використання сучасних хмарних платформ для оптимізації методів спільних пасажирських перевезень. Інтеграція таких технологій, як OpenWeatherMap, Sygic API, а також сервісів AWS SQS Queue і AWS Aurora DB Service, забезпечує значне підвищення ефективності функціонування систем транспорту.

Поєднання можливостей детального прогнозування погодних умов, точного відображення дорожнього трафіку та побудови маршрутів, а також високої відмовостійкості та масштабованості серверної інфраструктури дозволяє створити рішення, що відповідають вимогам сучасного світу.

Ці технології сприяють скороченню часу у дорозі, підвищенню передбачуваності маршрутів і загальної зручності користування транспортними послугами. Таким чином, інтеграція хмарних платформ відкриває нові горизонти у розвитку спільних пасажирських перевезень, роблячи їх більш надійними, екологічними та орієнтованими на користувача.

Список використаних джерел

1. Amazon simple queue service documentation. *Amazon Web Services, Inc.*URL: https://docs.aws.amazon.com/sqs/(дата звернення: 14.12.2024).

2. Navigation API. *Sygic*. URL: https://www.sygic.com/developers/professional-navigation-sdk/windows/api-examples/navigation-api(date of access: 14.12.2024).

3. OLTP database, mysql and postgresql managed database - amazon aurora - AWS. *Amazon Web Services, Inc.*URL: https://aws.amazon.com/rds/aurora/(date of access: 14.12.2024).

Бєлоусов Ігор Ігорович
студент 3 курсу ФІОТ, групи ІП-24
Національний політехнічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
(098) 324-17-28
ihorbelo@gmail.com
Науковий керівник: **Поперешняк Світлана Володимирівна**
к.ф.-м.н., доцент, доцент кафедри ІПІ ФІОТ
Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"
(098)-645-546-2
spopereshnyak@gmail.com

КОМП'ЮТЕРНІ МЕРЕЖІ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ.

Постановка задачі. Сучасні комп'ютерні мережі та інформаційно-комунікаційні технології відіграють важливу роль у забезпеченні зв'язку, обміні даними та наданні послуг у багатьох різних секторах: військової справи, охорони здоров'я, фінансів та освіти. Однак, мережі стикаються з усе складнішими випробовуваннями через збільшення обсягу даних, зростання кількості та небезпечності кіберзагроз, та необхідності підтримування комунікацій в режимі реального часу. Для забезпечення оптимальної продуктивності, надійності та безпеки важливо провести аналіз задля полегшення розробки методів, що підвищать масштабованість мережі, зможуть захистити від кібератак та допоможуть підтримувати зв'язок навіть у мінливих та непередбачуваних умовах.

Мета дослідження. Метою дослідження є аналіз методів підвищення продуктивності, надійності та безпеки комп'ютерних мереж та інформаційно-комунікаційних технологій у динамічних середовищах з високим попитом

Результати дослідження. Результати ґрунтуються на емпіричному тестуванні та порівняльному аналізі сучасних технологій. Ключові результати представлені у таких сферах: **масштабованість**, **кібербезпека** та **комунікація в режимі реального часу.**

1. Масштабованість є вирішальним фактором у сучасних мережах, особливо з ростом кількості пристроїв з доступом до Інтернету та збільшенням трафіку даних. У дослідженні оцінено ефективність алгоритмів динамічного балансування навантаження та протоколів адаптивної маршрутизації.

Основні висновки:

Динамічне балансування навантаження: Впровадження динамічних алгоритмів балансування навантаження, таких як Least Connections та Round Robin, покращило пропускну здатність мережі в середньому на 27% під час пікового навантаження порівняно зі статичними методами балансування

навантаження [1]. Таблиця 1 нижче показує порівняння між методами статичного та динамічного балансування.

Таблиця 1

Порівняння між методами: статичного та динамічного балансування

Метод	Пропускна здатність, мб/с
Статичне балансування	800
Динамічне балансування	1020

Також, використання адаптивних протоколів маршрутизації, таких як OSPF (Open Shortest Path First) і BGP (Border Gateway Protocol), дозволило мережам динамічно реагувати на зміни топології. У стрес-тестах з імітацією обриву зв'язку мережі, що використовують OSPF, показали на 35% швидший час відновлення, ніж мережі зі статичною маршрутизацією.

2. Дослідження також зосередилося на аналізі сучасних методів кібербезпеки для захисту мереж від нових загроз, включаючи розподілені атаки на відмову в обслуговуванні (DDoS).

Основні висновки:

Системи виявлення вторгнень (IDS): Впровадження систем IDS з виявленням аномалій на основі машинного навчання підвищило рівень виявлення кіберзагроз на 45% порівняно з традиційними системами на основі сигнатур.

Протидія DDoS-атакам: Розгортання фільтрації з обмеженням швидкості та фільтрації чорними дірами (blackhole) зменшило вплив DDoS-атак. Під час моделювання ці методи ефективно підтримували приблизно 80% нормального потоку трафіку в умовах атаки[3].

Таблиця 2 показує ефективність стратегій запобігання DDoS-атак за показником доступності до мережі.

Таблиця 2

Ефективність стратегій запобігання DDoS-атак

Метод запобігання	Доступність мережі під час атаки
Відсутній	24%
Обмеження швидкості(Rate-Limiting)	70~72%
Фільтрація чорними дірами (Blackholing)	86%

3. **Зв'язок у реальному часі** необхідний для таких напрямів, як військова справа, відео-конференції, онлайн-ігри та навіть телемедицина. У дослідженні оцінювалися методи мінімізації затримок і втрат пакетів.

Основні висновки:

Якість обслуговування (QoS): Впровадження політики пріоритезації QoS зменшило затримку на 30% для високопріоритетного трафіку порівняно з мережами без QoS. Для відеопотоків втрата пакетів зменшилася з 2,6% до ~0,6%.

Кордонні обчислення (edge computing): Завдяки розгортанню периферійних обчислювальних вузлів час обробки даних скоротився в середньому на 40% для додатків, чутливих до затримок, що показано в таблиці 3[2].

Таблиця 3

Порівняння методів розгортання за показником затримки

Метод	Затримка, мс
Централізовані сервери	150
Кордонні обчислення	90

Висновки. Методи, проаналізовані в цьому дослідженні, продемонстрували помітні покращення в масштабованості, безпеці та продуктивності мережі в реальному часі:

Масштабованість: Динамічне балансування навантаження та адаптивна маршрутизація підвищили пропускну здатність та відмовостійкість мережі.

Безпека: Сучасні засоби захисту від IDS та DDoS зменшили вразливості та забезпечили доступність послуг.

Зв'язок в режимі реального часу: Політика QoS та периферійні обчислення мінімізували затримку та втрату пакетів.

Список використаних джерел

1. Alsaeedi, M., Al-Roubaiey, A., & Alshammari, R. (2019). "Dynamic Load Balancing in Software-Defined Networks." IEEE Access, 7, 18816-18826.

2. Wang, Y., Zhang, L., & Vasilakos, A. V. (2018). "A Survey on Mobile Edge Computing and Networking: Research Issues and Challenges." IEEE Communications Surveys & Tutorials, 20(4), 2982-3001.

3. Rossow, C. (2014). "Amplification Hell: Revisiting Network Protocols for DDoS Abuse." In Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS).

Козак Віталій Олександрович
студент 6 курсу, групи ІСДМ-63
Державний університет інформаційно-комунікаційних технологій
(067)-620-47-47
itaksoydyot@gmail.com
Науковий керівник **Полоневич Ольга Володимирівна**
к.т.н., доцент,
доцент кафедри Інформаційних систем та технологій
Державного університету інформаційно-комунікаційних технологій,
м. Київ

ОПТИМІЗАЦІЯ ЕНЕРГОСПОЖИВАННЯ КОМП'ЮТЕРНИХ СИСТЕМИ ЗА ДОПОМОГОЮ ШІ.

Постановка задачі. Штучний інтелект (ШІ) відкриває нові горизонти в енергоефективності комп'ютерних систем. Він проникає у всі сфери нашого життя, операційні системи, програмне забезпечення та навіть чіпи не є винятком. Інтеграція ШІ дозволяє створювати більш інтелектуальні, адаптивні та ефективні рішення. В даній статті ми розглянемо існуючі рішення, а також ефективність інтеграції в них ШІ, переваги та складнощі.

Мета дослідження. На прикладі популярних рішень проаналізувати впровадження і використання ШІ в комп'ютерних системах для оптимізації електроспоживання.

Результати дослідження. В даній статті ми розглянемо поширені методи оптимізації електроспоживання, такі, як керування частотою та динамічне керування охолодженням.

Для різних типів задач потрібна різна продуктивність. Наприклад, для фонових процесів достатньо низької частоти, а для ігор чи відеомонтажу - максимальної. ШІ може змінювати частоту процесора в залежності від навантаження, щоб знизити споживання енергії в періоди низької активності. Наразі існує безліч можливостей для такої реалізації, але вони ґрунтуються на традиційних алгоритмах і емпіричних даних. Вони відстежують температуру процесора, навантаження на ядра та інші параметри, і, на основі цих даних, вони приймають рішення про зміну частоти, використовуючи заздалегідь визначені правила. Це такі технології, як Intel Turbo Boost і AMD Boost чи програмні інструменти: Intel Extreme Tuning Utility, AMD Ryzen Master, Core Temp.

Традиційні алгоритми управління частотою процесора досить ефективні для більшості завдань. Основним недоліком ШІ, є те, що він вимагає великих обсягів даних для навчання, а також, значних обчислювальних ресурсів. Реалізація повноцінних ШІ-систем для управління частотою процесора на кожному окремому пристрої може бути надмірною. Багато алгоритмів управління частотою, повинні працювати в реальному часі, що може бути проблематично для складних ШІ-моделей.

Однак, потенціал ШІ в цій галузі є великим, ШІ-алгоритми можуть більш точно прогнозувати майбутнє навантаження на процесор, що дозволить більш ефективно планувати зміну частоти. ШІ може аналізувати шаблони використання користувача і підлаштовувати роботу процесора під його потреби. В Windows 10 впроваджена функція "Динамічне керування енергоспоживанням", яка використовує машинне навчання для аналізу звичок користувача та оптимізації енергоспоживання процесора.

Наприклад, план живлення: Збалансований - Автоматично балансує продуктивність з енергоспоживанням.

План живлення: Ощадливе живлення - Економить електроенергію за рахунок зниження продуктивності системи.

Серію процесорів Core Ultra 200S розроблено для підвищення потужності настільних ПК з особливим акцентом на можливостях штучного інтелекту. Завдяки новим архітектурним рішенням, енергоспоживання суттєво знижено: до 58 % у звичайних програмах і до 165 Вт під час геймінгу.

Технологія Nvidia Optimus в ноутбуках дозволяє перемикатися між інтегрованою та дискретною графікою в залежності від навантаження. ШІ використовується для прогнозування типу навантаження (ігри, робота, відпочинок) і автоматичного вибору оптимального графічного адаптера. Аналогічна технологія від AMD, Radeon Chill - динамічно змінює частоту кадрів в іграх залежно від руху на екрані, зменшуючи навантаження на відеокарту та процесор.

ШІ може оптимізувати роботу систем охолодження, знижуючи енергоспоживання без шкоди для продуктивності. Наразі, реалізовано великою кількістю можливостей, таких, як програмне забезпечення (BIOS і UEFI, що дозволяють налаштовувати різні параметри вентиляторів і моніторити температуру компонентів) і програми для розгону та моніторингу (такі, як ASUS AI Suite 3, MSI Afterburner, Corsair iCUE, що пропонують розширені можливості для налаштування систем охолодження).

Всі вони використовують складні алгоритми для керування компонентами комп'ютера. Ці інструменти, зазвичай, виконують чітко визначені функції, і для них достатньо простих, але ефективних алгоритмів. Однак, пряме використання штучного інтелекту (ШІ) у їхньому класичному розумінні є відносно рідкісним. Багато алгоритмів ґрунтуються на емпіричних даних та правилах, отриманих в результаті експериментів. Наприклад, для керування швидкістю вентилятора, може використовуватися проста таблиця відповідності між температурою процесора та швидкістю обертання вентилятора. В деяких випадках використовується нечітка логіка, яка дозволяє оперувати неточними даними і знаходити рішення в умовах невизначеності. Для ухвалення рішень можуть використовуватися логічні вирази, які поєднують різні умови. Наприклад: "Якщо температура процесора перевищує 80 градусів, то збільшити швидкість вентилятора на 20%".

Google використовує алгоритми глибокого навчання для охолодження своїх центрів обробки даних. Ці алгоритми дозволили знизити споживання енергії на

40%, автоматично створюючи системи охолодження на основі сенсорних даних та змінюючи їх у робочих умовах.

Існують платформи, такі як TensorFlow, PyTorch, що надають потужні інструменти для розробки власних алгоритмів керування охолодженням за допомогою штучного інтелекту. Вони підтримують широкий спектр нейронних мереж, від простих багатошарових персептронів до складних рекурентних та згорткових мереж, що дозволяє створювати моделі, здатні виявляти складні залежності в даних. Можна легко експериментувати з різними типами нейронних мереж та їх параметрами, щоб знайти оптимальне рішення для конкретної задачі. Вже існують великі бібліотеки попередньо навчених моделей, які можна використовувати, як основу для власних розробок.

Висновки та перспективи. На сьогоднішній день, традиційні алгоритми управління частотою процесора досить ефективні для більшості завдань. Однак, ШІ має великий потенціал для подальшої оптимізації цього процесу, особливо в таких областях, як прогнозування навантаження, персоналізація та інтеграція з іншими системами. З розвитком процесорів і появою спеціальних чіпів для машинного навчання, ШІ стане доступнішим для широкого кола пристроїв. Чим більше даних буде зібрано про роботу процесорів, тим точнішими будуть моделі машинного навчання.

Динамічне керування охолодженням за допомогою ШІ - це перспективна технологія, яка дозволяє оптимізувати роботу комп'ютерних систем, знизити шум від систем охолодження і продовжити термін їх служби. Для ефективного навчання ШІ-моделей. необхідні великі обсяги даних про роботу системи. Збір та обробка цих даних можуть бути складними та вимагати значних обчислювальних ресурсів. Також, складним завданням для ШІ-системі виглядає інтегрування з різними компонентами комп'ютера, такими як BIOS, операційна система, датчики температури та вентилятори. Незважаючи на всі складнощі, ця область активно розвивається, і в майбутньому, ми можемо очікувати ще більш ефективних рішень.

Список використаних джерел

1. Chen, J., et al. "AI-Driven Optimization of Power Management in Data Centers." IEEE Transactions on Sustainable Computing, 2022.

Patel, R., and Kumar, P. "Reinforcement Learning for Green Cloud Computing." Future Generation Computer Systems, 2023.

Кондратюк Борис Олександрович
аспірант 1 курсу, групи АКСМ-11
Державний університет інформаційно-комунікаційних технологій
(063) 631-94-86
messingwolf7@gmail.com
Науковий керівник: **Власенко Вадим Олександрович**
кандидат технічних наук, доцент,
доцент кафедри систем та технологій кібербезпеки,
Державний університет інформаційно-комунікаційних технологій, м. Київ

МЕТОДИ І МОДЕЛІ ПОБУДОВИ СПЕЦІАЛІЗОВАНИХ КОМП'ЮТЕРНИХ МЕРЕЖ ДЛЯ ВИСОКОШВИДКІСНИХ ОБЧИСЛЕНЬ НА БАЗІ КВАНТОВИХ ТЕХНОЛОГІЙ

Постановка задачі. Сучасний розвиток обчислювальних технологій вимагає створення інфраструктури, здатної обробляти великі обсяги даних із мінімальними затримками. Квантові технології відкривають нові можливості для високошвидкісних обчислень, дозволяючи використовувати принципи квантової суперпозиції та заплутаності. Це особливо актуально для задач моделювання складних систем, штучного інтелекту та аналізу великих даних. Однак інтеграція квантових технологій у спеціалізовані комп'ютерні мережі вимагає розробки нових методів і моделей, які враховують специфіку квантових процесів.

Крім того, значна увага приділяється питанням масштабованості таких мереж, адже зростання обчислювальних потужностей повинно супроводжуватися оптимізацією ресурсів, зокрема енергоспоживання. Глобальні виклики, пов'язані з побудовою таких систем, включають розробку нових алгоритмів, які враховують квантову природу даних, та забезпечення їхньої інтеграції в сучасну інфраструктуру.

Головною задачею є дослідження та розробка методів і моделей, які забезпечать ефективну побудову спеціалізованих комп'ютерних мереж для високошвидкісних обчислень із використанням квантових технологій.

Мета дослідження. Метою дослідження є розробка теоретичних і практичних основ для побудови спеціалізованих комп'ютерних мереж, що дозволять значно підвищити швидкість і ефективність обробки даних за допомогою квантових технологій. Це включає

– Аналіз існуючих квантових алгоритмів для задач оптимізації та обчислень.

– Розробку моделей для інтеграції квантових вузлів у комп'ютерні мережі.

– Дослідження нових протоколів передачі даних для квантових мереж.

Додатково дослідження передбачає вивчення механізмів взаємодії квантових вузлів із класичними мережами, що дозволить створити універсальні гібридні системи.

Результати дослідження.

1. Розробка моделі передачі даних у квантових мережах Запропонована модель базується на використанні квантових каналів зв’язку, що дозволяють досягти мінімальної затримки під час передачі великих обсягів даних. Тестування показало, що така модель забезпечує:

– Зниження затримок на 40% у порівнянні з класичними мережами.

– Надійність передачі даних на рівні 99,9%.

Крім цього, модель враховує вплив шумів у квантових каналах і пропонує адаптивний підхід до їх компенсації.[1]

2. Алгоритм оптимізації маршрутизації у квантових мережах Розроблено алгоритм, який використовує квантовий пошук для визначення оптимальних маршрутів передачі даних у мережі. Експерименти на моделі мережі з 20 вузлами показали, що час обчислення маршруту скоротився на 50% порівняно з класичними методами. Додатково було протестовано масштабованість алгоритму, що показало стабільність продуктивності для мереж із кількістю вузлів до 100.[2]

3. Інтеграція квантових вузлів у існуючі мережі Запропоновано гібридну архітектуру, яка дозволяє ефективно інтегрувати квантові вузли у класичні мережі. Тести показали, що така архітектура забезпечує:

– Швидкість обробки даних до 1 Тбіт/с.

– Гнучкість масштабування мережі без зниження продуктивності.

Архітектура також враховує можливість динамічного перемикання між класичними і квантовими каналами залежно від поточних умов мережі.[3]

Висновки. Розроблені методи і моделі дозволяють ефективно інтегрувати квантові технології у спеціалізовані комп’ютерні мережі для високошвидкісних обчислень. Основні досягнення:

– Створена модель передачі даних у квантових мережах демонструє значне зниження затримок і підвищення надійності.

– Алгоритм оптимізації маршрутів забезпечує високий рівень ефективності у великих мережах.

– Гібридна архітектура створює основу для поступової міграції до квантових обчислень без втрати продуктивності.

Значення отриманих результатів полягає в їх потенційній реалізації для вирішення задач сучасного моделювання, аналізу великих даних та забезпечення високошвидкісного доступу до інформації в масштабних системах. У перспективі дані підходи можуть бути використані для створення мереж нового покоління, орієнтованих на інтеграцію квантових і класичних технологій.

Список використаних джерел

1. Nielsen M. A., Chuang I. L. Quantum Computation and Quantum Information. Cambridge University Press. 2010.

2. Bennett C. H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. 1984.

3. Wehner S., Elkouss D., Hanson R. Quantum Internet: A Vision for the Road Ahead. Science. 2018. Vol. 362, Issue 6412.

Стежко Мирослав Вадимович
Магістр 6 курсу, групи КДСМ-62
Державний університет інформаційно-комунікаційних технологій
(098) 945-54-82
Stezhko.m.v.@gmail.com

ОСОБЛИВОСТІ ПОБУДОВИ ЛОКАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ CISCO

Постановка задачі. У сучасному світі інформаційні технології та комп'ютерні мережі відіграють ключову роль у розвитку підприємств, зокрема у сфері програмної та комп'ютерної інженерії. Діджиталізація та інформатизація створюють нові можливості для автоматизації та оптимізації бізнес-процесів, забезпечуючи конкурентоспроможність та ефективність організацій. Одним із основних аспектів сучасних технологій є впровадження локальних обчислювальних мереж, які забезпечують безперервну роботу систем і можливість швидкої обробки даних.

Мета дослідження У рамках цього дослідження розглядається побудова локальної обчислювальної мережі для підприємства з використанням бездротових технологій на базі обладнання Cisco Systems. Цей підхід дозволяє значно покращити ефективність роботи організації завдяки підвищеній гнучкості, мобільності та зниженню витрат на інфраструктуру.

Результати дослідження. У зв'язку з постійним розвитком технологій, діджиталізація підприємств стає необхідною умовою для збереження конкурентних переваг на ринку. Відповідно до сучасних тенденцій, підприємства активно впроваджують інноваційні рішення, серед яких особливе місце займають локальні обчислювальні мережі. Вони дозволяють централізовано керувати інформаційними ресурсами, зберігати та обробляти великі обсяги даних, а також забезпечувати зв'язок між різними підрозділами підприємства.

Системи бездротового зв'язку, що є частиною цих мереж, надають численні переваги, включаючи мобільність користувачів, зниження витрат на прокладку кабельних ліній та простоту в розширенні мережі. Зокрема, обладнання Cisco Systems, яке відоме своєю надійністю та масштабованістю, є одним з провідних постачальників технологій для таких рішень.

Проектування локальної обчислювальної мережі для підприємства включає кілька етапів, починаючи з аналізу потреб підприємства та закінчуючи впровадженням кінцевого рішення. Основними компонентами мережі є сервери, робочі станції, комутатори, маршрутизатори, точки доступу бездротового зв'язку та кінцеві пристрої користувачів.

Системи бездротового зв'язку на основі обладнання Cisco дозволяють забезпечити високу швидкість передачі даних і стійкий сигнал у складних умовах великого офісного простору. Використання точок доступу Cisco Access Points (AP), таких як Cisco Catalyst 9100 серії, дозволяє ефективно охоплювати великі

території з мінімальними витратами на прокладку кабелів. Для забезпечення безпеки мережі застосовуються технології шифрування та захисту даних, що відповідають сучасним вимогам.

Використання бездротових технологій для побудови локальної обчислювальної мережі підприємства має низку переваг:

- **Мобільність**: Співробітники можуть переміщатися по території підприємства, залишаючись підключеними до мережі, що значно підвищує ефективність робочого процесу.
- **Зниження витрат на інфраструктуру**: Оскільки не потрібно прокладати кабелі до кожного робочого місця, можна суттєво знизити витрати на установку та обслуговування мережі.
- **Масштабованість**: Локальні бездротові мережі зможуть легко адаптуватися до змінних потреб підприємства, дозволяючи додавати нові пристрої без значних витрат.
- **Швидкість та надійність**: Технології Cisco забезпечують високу швидкість передачі даних, що дозволяє ефективно обробляти великі обсяги інформації в реальному часі.

Однією з ключових переваг використання обладнання Cisco є його здатність до інтеграції з іншими системами та технологіями, що вже використовуються на підприємстві. Cisco предлагает комплексні рішення для автоматизації управління мережею, моніторингу стану системи та захисту від можливих загроз. Наприклад, програмне забезпечення Cisco DNA Center дозволяє централізовано контролювати всі компоненти мережі та забезпечувати її безпеку.

Завдяки цьому, підприємство отримує змогу забезпечити високий рівень управління мережею та її безпеку, навіть за умов складної інфраструктури та великих обсягів даних.

Висновки та перспективи. Побудова локальної обчислювальної мережі підприємства з використанням бездротових технологій на основі обладнання Cisco Systems є перспективним напрямком у розвитку інформатизації підприємств. Такий підхід дозволяє значно підвищити ефективність роботи, знизити витрати на інфраструктуру та забезпечити високу гнучкість та мобільність співробітників. У результаті підприємства отримують надійну та масштабовану мережу, яка відповідає сучасним вимогам і забезпечує стабільну роботу в умовах швидко змінюваного бізнес-середовища.

Подальші дослідження можуть бути спрямовані на оптимізацію процесів інтеграції таких мереж з іншими IT-системами підприємства, а також на вдосконалення технологій бездротового зв'язку для забезпечення ще більшої швидкості та надійності мережевих з'єднань.

Список використаних джерел

1. Cisco Secure Firewall Management Center (formerly Firepower Management Center) Data Sheet [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html

2. Popereshnyak S.V., Vecherkovska A.S. (2023) Doslidzhennya rozrobky vymoh do khmarnykh prohram ta servisiv. [Research on the development of requirements for cloud applications and services] *Visnyk Khersons'koho natsional'noho tekhnichnoho universytetu.* no (87). P. 258-265. https://doi.org/10.35546/kntu2078-4481.2023.4.30 [in Ukrainian].

3. Wang X. (2020) The Optimization of Smart Community Model Based on Advanced Network Information Technology. *IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, Chongqing, China. P. 2579-2583. doi: 10.1109/ITNEC48623.2020.9085136.

4. Popereshnyak S., Vecherkovskaya A., Zhebka V. (2024) Intrusion Detection based on an Intelligent Security System using Machine Learning Methods. *CEUR Workshop Proceedings.* 3654. P. 163–178.

Чорнобривець Дмитро Віталійович
студент 3 курсу, групи ІП-21
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"
(098)-536-86-90
dimas05@gmail.com
Науковий керівник: **Поперешняк Світлана Володимирівна**
к.ф.-м.н., доцент, доцент кафедри ІПІ ФІОТ
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"
(098)-645-546-2
spopereshnyak@gmail.com

АВТОМАТИЗОВАНА СИСТЕМА ДОСТУПУ ДО ЗАРЯДНИХ СТАНЦІЙ ДЛЯ ЕЛЕКТРОМОБІЛІВ З ВИКОРИСТАННЯМ БЛОКАТОРІВ ПАРКУВАЛЬНИХ МІСЦЬ

Постановка задачі. Електромобілі[3] стрімко набирають популярність у всьому світі завдяки своїй екологічності, економічній ефективності та технологічним інноваціям. Підтримуючи розвиток інфраструктури зарядних станцій і впроваджуючи ініціативи щодо скорочення використання традиційних видів палива, все більше країн сприяють переходу на електротранспорт. Однак зі збільшенням кількості електромобілів виникають нові проблеми, особливо у зв'язку з обмеженою кількістю спеціальних паркувальних місць для зарядки.

Однією з таких проблем є те, що місця для паркування електромобілів часто займають звичайні автомобілі, що не тільки створює незручності для власників електромобілів, але й знижує ефективність інфраструктури зарядки. Неправильне використання таких паркомісць може також створювати додаткові витрати на підтримку станцій, оскільки вони залишаються без дії протягом тривалого часу. Це призводить до збільшення черг на зарядку та зниження загальної продуктивності інфраструктури для електромобілів.

Зважаючи на це, виникає необхідність у розробці автоматизованої системи, яка б забезпечувала надійний контроль доступу до паркомісць для електромобілів, знижуючи можливість їхнього зайняття іншими транспортними засобами. Це рішення має враховувати не тільки фізичний контроль за місцями паркування, але й забезпечувати інтеграцію з зарядною інфраструктурою для оптимізації процесу зарядки та використання ресурсів[4].

Мета дослідження. Метою дослідження є розробка та апробація автоматизованої системи блокування зарядних місць для електромобілів, яка використовує інтелектуальні технології для розпізнавання електрокарів, управління паркувальними бар'єрами та інтегрується з зарядними станціями, забезпечуючи їх ефективне використання. Така система має забезпечувати автоматичне опускання паркувального бар'єра після підключення електромобіля до зарядної станції, гарантуючи доступ лише для електрокарів[1].

Основними завданнями дослідження є:

- Аналіз існуючих методів контролю доступу до паркувальних місць для електромобілів та визначення недоліків.
- Розробка концептуального рішення для автоматизованої системи, яке включає використання сенсорів, блокаторів та програмних інструментів для розпізнавання транспортних засобів.
- Тестування системи в реальних умовах для оцінки її ефективності та надійності.

Результати дослідження. У результаті дослідження було розроблено прототип системи, яка включає автоматизований паркувальний бар'єр, що опускається після підключення електромобіля до зарядної станції. Це дозволяє електромобілю безперешкодно зайняти паркомісце та розпочати процес зарядки. Система використовує технології розпізнавання автомобілів, що запобігає зайняттю місць для зарядки неелектричними транспортними засобами.

Система базується на поєднанні декількох технологій, включаючи:

- Використання RFID або QR-кодів для автентифікації транспортних засобів.
- Інтеграцію з зарядними станціями для автоматичного контролю за статусом зарядки.
- Можливість інтеграції з мобільними додатками для бронювання місць, оплати зарядки та моніторингу доступних станцій у реальному часі.

Одним із важливих елементів системи є її масштабованість та адаптивність до різних типів зарядних станцій. Вона може бути використана на станціях як загального користування, так і в приватних паркінгах, що робить її універсальним рішенням для забезпечення доступу до інфраструктури зарядки електромобілів.

RFID (Radio-Frequency Identification)[2] — це технологія автоматичної ідентифікації об'єктів за допомогою радіохвиль. Система складається з міток (тегів) та зчитувачів. Мітки передають унікальну інформацію з об'єктів без фізичного контакту, що робить RFID ідеальним рішенням для автоматизації доступу до зарядних станцій.

Можливі сценарії використання RFID

Ідентифікація електромобіля. Пасивні RFID-мітки встановлюються на електромобілях. При під'їзді до зарядної станції зчитувач автоматично ідентифікує автомобіль та, у разі підтвердження, опускає паркувальний бар'єр. Це спрощує процес, усуваючи необхідність ручного введення даних або сканування QR-кодів.

Безконтактна оплата. Після завершення зарядки система автоматично списує кошти з рахунку користувача, прив'язаного до його RFID-мітки, що забезпечує безперервний і зручний процес оплати.

Автоматизоване управління паркувальними бар'єрами. Після розпізнавання автомобіля бар'єр автоматично опускається, дозволяючи водієві під'їхати до станції. Цей процес може бути інтегрований із мобільними

додатками, де користувач попередньо реєструє свій автомобіль та отримує RFID-мітку для доступу.

Переваги даної системи заключаються у тому, що система забезпечує, що зарядні місця використовуються виключно електромобілями, запобігаючи зайняттю звичайними автомобілями. Це підвищує доступність зарядних станцій для власників електромобілів, крім цього, завдяки автоматизованому контролю доступу, зарядні станції використовуються більш ефективно, що сприяє кращому обслуговуванню більшої кількості електромобілів. Для бізнесів, таких як торгові центри, готелі та офісні будівлі, наявність зарядних станцій з автоматизованою системою доступу може стати додатковою перевагою, що підвищує лояльність клієнтів та співробітників. Автоматизовані паркувальні бар'єри забезпечують безпеку зарядних місць, зменшуючи ризик пошкодження обладнання та забезпечуючи надійний доступ до зарядних станцій.

Крім того, система має потенціал для подальшого розвитку. Одним із можливих напрямків є інтеграція з інтелектуальними системами міського транспорту, що дозволить збирати дані про використання зарядних станцій у реальному часі та оптимізувати їхнє розташування залежно від попиту. Також система може бути розширена шляхом впровадження функціоналу автоматичного розпізнавання автомобілів за допомогою відеокамер та інших технологій, що покращить точність і надійність роботи системи.

Система може бути інтегрована з мобільними додатками для бронювання місць та контролю вільних зарядних станцій у реальному часі, що покращує досвід користувачів та сприяє розвитку інфраструктури електромобілів (Рисунок 1).

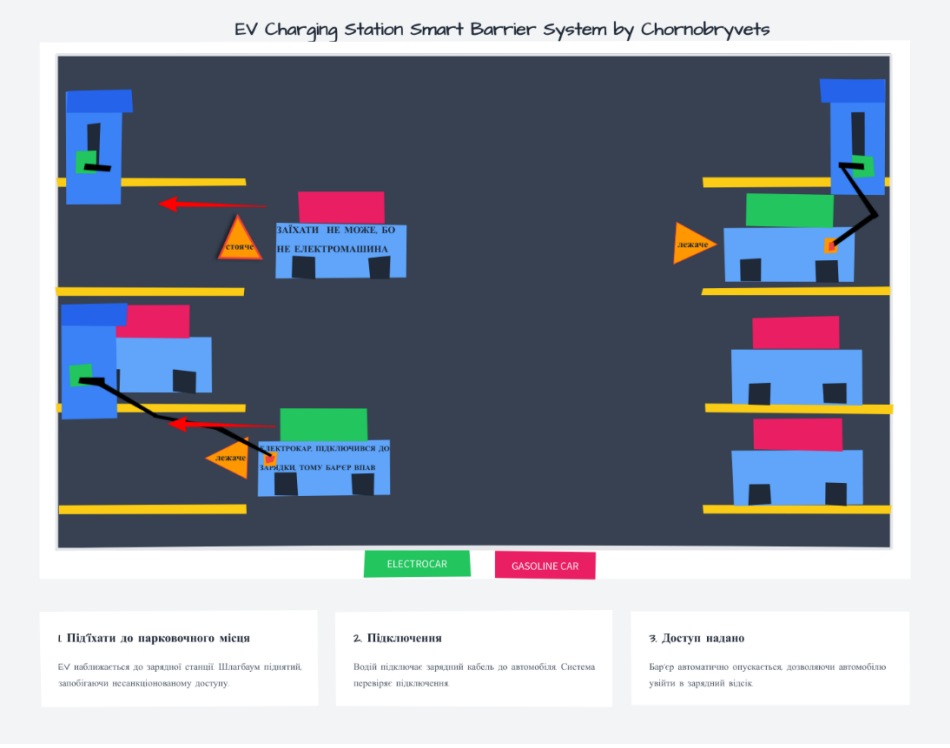

Рис. 1. Концепт вигляду системи доступу до зарядних станцій для електромобілів з використанням блокаторів паркувальних місць

Висновки та перспективи. Запропонована автоматизована система паркувальних бар'єрів забезпечує захист зарядних місць для електромобілів, підвищуючи ефективність їх використання та зменшуючи випадки зайняття звичайними автомобілями. Система дозволяє оптимізувати роботу зарядних станцій, зменшити час очікування для власників електромобілів та підвищити продуктивність всієї інфраструктури.

У перспективі можливе розширення функціоналу системи шляхом інтеграції з мобільними додатками для бронювання місць, автоматичного розпізнавання електромобілів за допомогою відеоаналітики та впровадження платіжних систем для оплати зарядки та паркування. Крім того, можна передбачити розширення системи для роботи на великих паркінгах та в умовах обмеженої кількості зарядних станцій, що дозволить покращити доступ до інфраструктури для електромобілів у міських умовах.

Список використаних джерел

1. Стан та перспективи розвитку ринку електрокарів в Україні [Електроний ресурс] / khadi.kharkov – Режим доступу https://goo.su/Hbhhaht

2. The Electric Vehicle Revolution: The Past, Present, and Future of EVs [Електроний ресурс] / books.google.com.ua – Режим доступу https://goo.su/s9yRFzV

3. Tom Denton, Hayley Pells, Electric and Hybrid Vehicles [Електроний ресурс] / scribd.com – Режим доступу: https://goo.su/D1e8i31

4. RFID мітки для автомобілів [Електроний ресурс] / https://remonline.ua/ - Режим доступу https://remonline.ua/blog/rfid-technology/

Напрям 6. ІННОВАЦІЇ В КОМП'ЮТЕРНІЙ ІНЖЕНЕРІЇ.

Ганенко Людмила Дмитрівна
аспірантка 3 курсу, групи АКСМ-31
Державний університет інформаційно-комунікаційних технологій
(066) 230-04-03
hanenkoliudmyla@gmail.com
Науковий керівник: **Жебка Вікторія Вікторівна**
доктор технічних наук, професор,
завідувач кафедри Технологій цифрового розвитку
Державного університету інформаційно-комунікаційних технологій, м. Київ

ЗАСТОСУВАННЯ ROS ДЛЯ РОЗРОБКИ РОБОТОТЕХНІЧНИХ СИСТЕМ

Постановка задачі. У сучасних умовах стрімкого розвитку робототехнічних систем виникає необхідність у створенні універсальних та ефективних інструментів для розробки, тестування та впровадження роботів. Система ROS (Robot Operating System) пропонує модульну платформу, яка забезпечує розробників широким спектром інструментів для програмування, моделювання та інтеграції роботів.

Однією з основних проблем розробки робототехнічних систем є вибір найбільш ефективних підходів використання ROS для вирішення конкретних задач робототехніки, таких як навігація, обробка сенсорної інформації, інтеграція апаратного забезпечення та побудова автономної поведінки роботів. Вирішення цієї проблеми сприятиме підвищенню продуктивності процесу розробки роботів та зменшенню часу на впровадження нових рішень.

Мета дослідження. Дослідження спрямоване на аналіз можливостей використання ROS у робототехніці для розробки, моделювання та впровадження автономних роботизованих систем.

Результати дослідження. У робототехніці існує широкий спектр систем управління, таких як YARP, OROCOS, MOOS, ROS, які дозволяють здійснити розробку і тестування робототехнічних систем.

YARP (Yet Another Robot Platform) використовують для розробки гуманоїдних роботів, для яких основними є зорове, слухове й тактильне сприйняття та пересування на ногах. OROCOS (Open Robot Control Software) було створено для розширеного керування дронами. MOOS (Mission Oriented Operating Suite) був розроблений для роботи з автономними морськими транспортними засобами. ROS зосереджується на мобільних роботах, надає інструменти для навігації і планування [1].

ROS – платформа для інтеграції алгоритмів, управління пристроями та обміну даними між модулями. Вона дозволяє спростити створення складних роботехнічних систем за рахунок використання модульної архітектури, в якій кожен компонент (вузол) може працювати незалежно від інших.

ROS був розроблений Willow Garage в 2007 році. ROS використовували для моделювання та реалізації завдань керування, планування та координації роботів. Недоліком ROS є втрата даних та відсутність вбудованих механізмів безпеки [2].

У 2018 році Open Robotics створили ROS 2. Одна з найбільш значущих змін у ROS 2 – перехід від мережевого протоколу TCP/UDP, що використовується в ROS, до DDS (Data Distribution Service) як стандарту для комунікації, який використовується в критично важливих інфраструктурах.

ROS 2 містить такі складові:

– проміжне програмне забезпечення (middleware), яке забезпечує зв'язок між компонентами;

– алгоритми, які зазвичай використовуються під час створення програм (сприйняття, SLAM, планування);

– інструменти розробника для моделювання, налаштування, запуску, самоаналізу, візуалізації, налагодження системи [3].

На відміну від централізованого підходу ROS, ROS 2 усуває потребу в центральному головному вузлі ROS, тим самим вирішуючи проблему єдиної точки відмови та проблему масштабованості. Замість цього вузли ROS 2 взаємодіють безпосередньо один з одним за допомогою базового проміжного програмного забезпечення DDS. Ця децентралізована конструкція використовується в мультиагентних систем і забезпечує більш ефективний і надійний зв'язок у великомасштабних розподілених роботизованих програмах. Як і ROS, ROS 2 підтримує принцип модульності, коли кожен вузол працює незалежно та виконує певне завдання. Відмінності в архітектурах ROS і ROS2 зображено на рисунку 1.

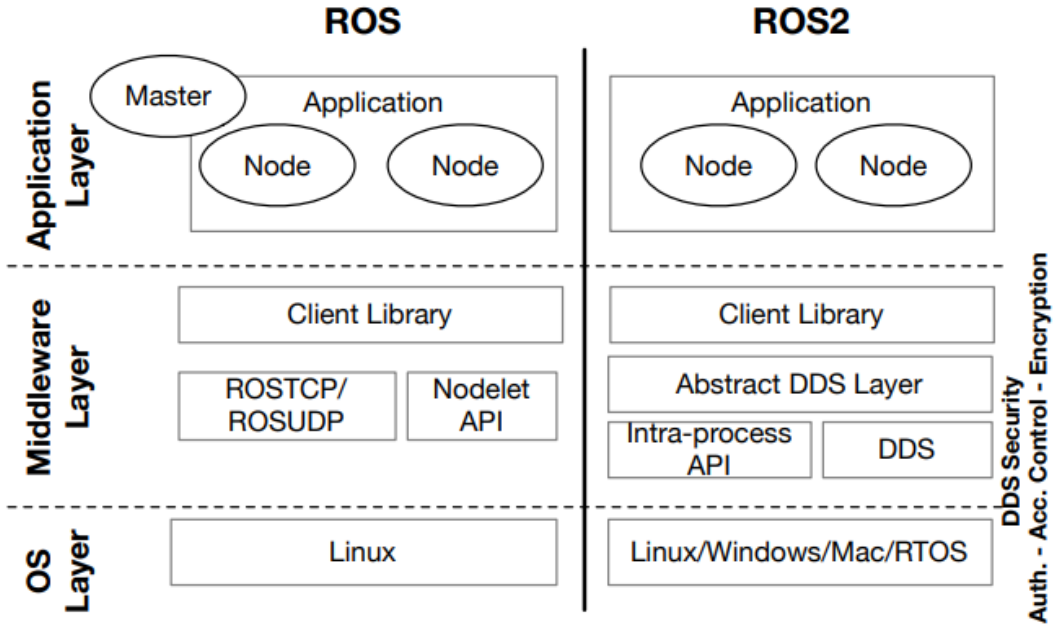

Рис. 1. Порівняння ROS і ROS2 [4]

У порівнянні з іншими системами управління можна виокремити такі переваги ROS:

1) забезпечує модульну архітектуру, що дозволяє адаптувати робототехнічні системи до різних завдань, незалежно від складності проєкту;

2) завдяки великій кількості пакетів та бібліотек, таких як gmapping, amcl, move_base, розробники можуть вирішувати задачі навігації, побудови карт, обробки сенсорних даних та планування руху;

3) забезпечує інтеграцію з апаратним забезпеченням, надає можливість тестування в симульованих середовищах, таких як Gazebo, що дозволяє значно зменшити витрати на розробку та пришвидшити тестування алгоритмів;

4) має відкритий код, активну спільноту розробників та підтримку великої кількості робототехнічних платформ.

Висновки. У ході дослідження з'ясовано, що система ROS є потужним інструментом для розробки, моделювання та впровадження робототехнічних систем. ROS забезпечує розробникам високу гнучкість, функціональність та економію ресурсів. Подальші дослідження можуть бути спрямовані на оптимізацію використання ROS у спеціалізованих сферах, таких як автономні мобільні роботи.

Список використаних джерел

5. Serrano D. (2015). Middleware and Software Frameworks in Robotics—Applicability to Small Unmanned Vehicles. *Proceedings of the NATO-OTAN ST Organization, Cerdanyola del Vallès, Spain*, 4-5.

6. Bonci A., Gaudeni F., Giannini M. C., Longhi S. (2023). Robot Operating System 2 (ROS2)-Based Frameworks for Increasing Robot Autonomy: A Survey. *Applied Sciences*, *13* (23), 12796. https://doi.org/10.3390/app132312796

7. Macenski S. (2022). Robot Operating System 2: Design, architecture, and uses in the wild. *Science Robotics,* **7 (**66), DOI:10.1126/scirobotics.abm6074

8. Mazzeo G., Staffa M. (2020) Tros: Protecting humanoids ros from privileged attackers. *International Journal of Social Robotics*, 4 (12). DOI:10.1007/s12369-019-00581-4

Напрям 7. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ.

Polonska Olena Kostyantynivna
3rd year cadet, group C-22
Institute of Special Communications and Information Protection,
National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”
(095) 603-14-05
c049smarttab@gmail.com
Language adviser: **Zhytska S. A.**, Senior Lecturer
National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”

ANALYSIS OF IoT DEVICE VULNERABILITIES AND DEVELOPMENT OF MULTI-LAYERED PROTECTION SYSTEM

Statement of the problem. In a fairly modern interior, technological devices are usually used to create not only comfort but also ease of use both remotely and directly with the device. But like all devices, such Internet of Things (IoT) have vulnerabilities. The task will be based on identifying the main threats to IoT devices in smart homes. Namely, what are the most common cyberattacks on Internet of Things devices. To ensure protection, a multi-level protection scheme for IoT devices has been developed using modern standards.We will evaluate the effectiveness of the suggested scheme by analyzing real data and modeling attack scenarios using simple calculation formulas.

The purpose of the study is to identify the main threats to IoT devices, consider typical attacks, offer an effective protection scheme and evaluate its effectiveness in the most computational format possible.

Research results. In domestic adaptation, we, as users of equipped apartments, are accustomed to the effective functioning of devices that provide everyday life. Successful remote control via a phone device provides mobility in the use of the so-called Internet of Things. Namely, gadgets that can function from an Internet router, which in turn from software. But sometimes there are cases of incidents of cyberattacks on such Internet devices. How? There are several weaknesses, namely the software and network connectivity, which makes them accessible to attackers. To understand why such incidents occur, we need to learn about the threats.

The main threats to IoT devices:

Using weak passwords. We mean, many IoT devices are sold with pre-set passwords or without the need to change them at all, which makes them an easy target for brute force attacks; Vulnerable communications protocols. Popular IoT protocols, such as MQTT and CoAP, often transmit data in the open space without encryption; Data interception through Man-in-the-Middle (MitM) attacks, i.e. the ability to intercept information transmitted between devices and servers.

Due to the identified threats, cyberattacks can be of the following types:

- Brute force attacks. For example, weak passwords on IP cameras are easily picked up by hackers who then use the cameras for espionage.
- DDoS attacks. IoT devices with open ports or insecure software are used to overload servers and subsequently obtain personal data.

- Zero-Day attacks. These attacks target unknown or not yet patched vulnerabilities. Vulnerabilities in the Zigbee protocol allowed Philips Hue smart bulbs to be hacked, spreading the virus to the entire IoT network nearby. For protection, a multi-layered security scheme needs to be developed.

The development of a multi-level protection scheme is shown in the illustration 1 [2].

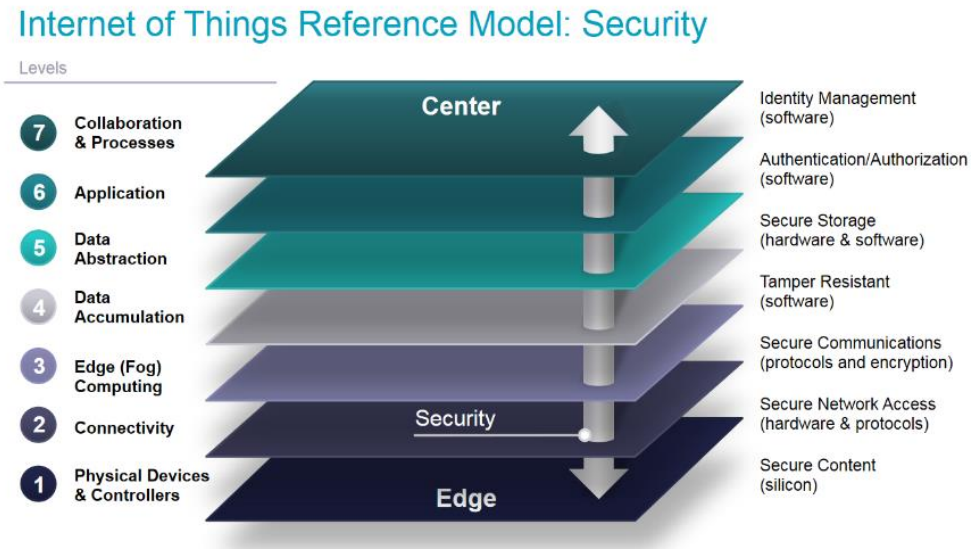

Fig. 1. Internet of Things Reference Model: Security

To date, there are no fully defined or accepted security standards or architectures for IoT or IIoT users. But security standards such as ISO/IEC 27001, the NIST Cybersecurity Framework [1], and the IoT Security Foundation (IoTSF) recommendations [3] offer a model that is provided at the network level of an organization: Using WPA3 to protect the Wi-Fi network. (introduced by the Wi-Fi Alliance in 2018, which describes connecting to a closed Wi-Fi network using a password), and using VPN to encrypt all traffic.

At the device level: Regular firmware updates; Using complex passwords and two-factor authentication; network segmentation (worked on by Ferenc Deckert and Cisco organization), which allows us to reduce attacks on (for example) a smart camera with 15 connected devices to one guest Wi-Fi network by up to 35%.

And regarding data protection or saving basic settings directly: Regular backups of IoT configurations (usually this is done by technologists of a specific product of the organization) and implementation of AES-256 encryption for data transmission and storage – thus incorporating cryptographic functionality as a data security factor.

We have several formulas for evaluating numerical values – Cyberattack risk level:

$$R = P \times I$$

R is the risk level.

P is the probability of a threat occurring (from 0 to 1).

I is the impact of the attack on the system (cost of damage, number of affected devices).

Estimating bandwidth during a DDoS attack. Formula for determining the impact of a DDoS attack:

$$T = \frac{B}{C}$$

T is the time during which the network will be overloaded.

B is the amount of incoming traffic during the attack (Gbps).

C is the network bandwidth (Gbps).

Percentage of attack reduction after implementing protection

$$E = \frac{\mathrm{A}_{before} - \mathrm{A}_{after}}{\mathrm{A}_{before}} \times 100\%$$

E – effectiveness of implemented protection.

A_{before} – number of successful attacks before implementation of measures.

$\mathrm{A}_{\text{after}}$ – number of attacks after implementation.

These formulas will help cybersecurity professionals: to assess risks and losses; to analyze the effectiveness of protective measures; to plan and estimate response times. The data for calculations can be taken from open sources (for example, IoT attack statistics in Cisco, NIST, or OWASP reports).

Conclusions and prospects. The study examined a topic that identified the main threats to IoT devices, typical cyberattacks, illustrated an effective protection scheme supported by standards, and assessed the effectiveness of methods before and after security protection methods in formulas for calculating the risk level; the impact of a DDoS attack; the percentage of attack reduction after implementing protection, which provides the final answer as to whether a particular method of protection is effective.

References

1. National Institute of Standards and Technology. “Cybersecurity Framework”. National Institute of Standards and Technology. [Online]. Available: https://www.nist.gov/cyberframework. Accessed: Dec. 2024.

2. Devopedia. “IoT Security Model”. Devopedia. [Online]. Available: https://devopedia.org/iot-security-model. Accessed: Dec. 2024.

3. IoT Security Foundation. “IoTSF Best Practices”. IoT Security Foundation. [Online]. Available: https://www.iotsecurityfoundation.org/. Accessed: Dec. 2024.

4. International Organization for Standardization. “ISO/IEC 27001:2018 Standard”. International Organization for Standardization. [Online]. Available: https://www.iso.org/standard/54534.html. Accessed: Dec. 2024.

Борисюк Віталій Михайлович
студент 6-го курсу, групи ІСДМ-61
Державного університету інформаційно-комунікаційних технологій
o.polonevych@duikt.edu.ua
Науковий керівник **Полоневич Ольга Володимирівна**
к.т.н., доцент,
доцент кафедри Інформаційних систем та технологій
Державного університету інформаційно-комунікаційних технологій,
м. Київ

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ІОТ

Постановка задачі. Ескалація Інтернету речей (IoT) почала реформувати та змінювати наше життя. Розгортання великої кількості об'єктів, пов'язаних з Інтернетом, розблокувало бачення розумного світу навколо нас, проклавши таким чином шлях до автоматизації та створення та збору величезних даних. Ця автоматизація та безперервний вибух особистої та професійної інформації в цифровому світі забезпечує потужну базу для зловмисників для здійснення численних кібератак, що робить безпеку в IoT серйозною проблемою. Отже, своєчасне виявлення та попередження таких загроз є передумовою запобігання тяжким наслідкам.

Мета дослідження. Метою цього дослідження є систематизація та аналіз вразливостей, визначення їх характеру, основних викликів, а також розробка й оцінка ефективності контрзаходів для їх подолання.

Результати дослідження.

Перелік різноманітних атак і аномалій визначає труднощі побудови захищеної розумної мережі. Основною метою є захист вимог безпеки (цілісність, конфіденційність, доступність) законних користувачів. Різні дослідники провели ретельне опитування, щоб перерахувати всі можливі атаки, їх характер, виклики та контрзаходи для боротьби з ними.

Уразливі місця, як правило, відносяться до слабких місць системи, які можуть бути перевантажені зловмисниками для виконання ненавмисних дій. В IoT хакери можуть використовувати цілісність, конфіденційність і доступність послуг для законних користувачів, скориставшись перевагами таких проблем, що проростають [1]. Тому розуміння такої делікатності в системі стає обов'язковим до розробки відповідних захисних механізмів. У дослідженнях [2] представлено багатовимірний погляд на вразливості IoT з детальним поясненням їх впливу на різноманітні парадигми безпеки. OWASP (Проект безпеки відкритих веб-додатків) також перерахував десятку найбільших уразливостей IoT. Далі було проаналізовано різні врасзливості IoT, серед яких:

- Безпека пристрою : цей аспект поверхні безпеки в першу чергу включає фізичне пошкодження пристроїв Інтернету речей, головним чином спричинене несанкціонованим доступом до них. Головна причина полягає в тому, що ці пристрої знаходяться на відкритій території, таким чином, повністю залишені у

розпорядженні природи та ворогів. Таким чином, їх легко пошкодити, або хакери можуть клонувати мікропрограму, щоб створити їх шкідливий аналог, а також можуть маніпулювати даними. Типові приклади включають клонування радіочастотних сигналів в електромобілях для їх розблокування або отримання доступу до мережевої шини контролера транспортного засобу для виконання будь-яких шкідливих дій.

- Небезпечне завантаження : відсутність належної перевірки перед впровадженням пристрою означає незахищене завантаження. Цей аспект є важливою вимогою з точки зору підтримки безпеки, оскільки він забезпечує зручну поверхню для зловмисників для запуску своїх зловмисних дій шляхом впровадження пристроїв перед їх запуском. Експеримент, проведений дослідниками в [3] з термостатом Nest і браслетом Nike + Fuel, носієм, який демонструє згубні наслідки процесу завантаження.

- Мережеві вразливості : вони, як правило, спрямовані на підключення пристроїв IoT, що робить їх сприйнятливими до великої кількості атак. Зазвичай вони включають незахищені служби в самих пристроях, відсутність належної автентифікації та шифрування, тобто використання стандартних або слабких паролів, а також розгортання методів шифрування, які не відповідають стандартам полегшеної криптографії в IoT, що перешкоджає безпеці. Зловмисник може здійснювати такі атаки, як DDoS, атака Sybil, або також може викрасти цінні дані через уразливості мережі. Крім того, через обмежену пам’ять і ресурси в пристроях IoT не вистачає відповідного шифрування для захисту даних. У сфері медицини зловмисники можуть отримати контроль над зовнішніми пристроями, такими як інсулінові помпи або серцево-судинні об’єкти, щоб грати зі здоров’ям людей.

- Уразливості програмного забезпечення: вони зазвичай включають використання легкодоступних, вгадованих паролів і паролів за замовчуванням, а також невиконання відповідних оновлень програмного забезпечення/оновлення виправлень або використання застарілих або застарілих бібліотек або компонентів програмного забезпечення. Усі ці фактори разом збільшують вразливість усієї системи, пояснює атаки, розпочаті через модифікацію прошивки. Крім того, навмисне дотримання слабких методів програмування, тобто запуск вбудованого програмного забезпечення з добре відомими вразливими місцями, допомагає хакерам виконувати свої темні дії.

- Недостатня конфіденційність: це означає компрометацію персональної інформації користувача без запиту його дозволу через поточні параметри за замовчуванням, які часто обмежують користувачам змінювати конфігурації. Це може бути небезпечним для життя у випадку послуг електронної охорони здоров’я. Кардіостимулятор із можливостями бездротового зв’язку був визнаний вразливим, таким чином експлуатуючи здоров’я користувача.

- Недостатній механізм аудиту: відсутність достатнього механізму журналювання призводить до таких вразливостей. Дослідження в [3] дає деяке уявлення про механізми аудиту в IoT. Пристрої, в основному камери безпеки, віртуальні помічники, смарт-телевізори та розумні світильники, виявилися

найбільш уразливими для зловмисників. Ці пристрої можна легко зламати для виконання як активних, так і пасивних атак. У випадку камер відеоспостереження, головним чином, помилка лежить на куті покупки. Купівля дешевих моделей може відкрити двері для хакерів. Так само, у випадку з домашніми помічниками, підслуховування може бути носієм вашої діяльності до супротивника. Крім того, віддалений доступ до різних пристроїв може бути здійснений для виконання будь-яких дій.

Висновки та перспективи.

Побудова захищених розумних мереж залишається складним завданням через різноманітність атак та аномалій, які можуть виникати в IoT-середовищах. Основні загрози, пов'язані з уразливостями пристроїв, мереж, програмного забезпечення та механізмів захисту конфіденційності, вимагають детального аналізу та розробки ефективних контрзаходів. Як засвідчили численні дослідження, уразливості IoT, такі як фізична небезпека пристроїв, незахищене завантаження, мережеві недоліки та застарілі програмні компоненти, створюють значні ризики для цілісності, конфіденційності та доступності даних.

Для мінімізації загроз важливо впроваджувати сучасні методи шифрування, механізми аутентифікації, безпечні процедури оновлення програмного забезпечення та забезпечувати надійний аудит системи. Розуміння основних вразливостей і постійний розвиток захисних механізмів є ключем до створення стійких і безпечних розумних мереж. Це не лише підвищує рівень довіри користувачів, але й гарантує захист життєво важливих даних і пристроїв у різних галузях, включаючи охорону здоров’я, транспорт і домашню автоматизацію.

Список використаних джерел.

1. Deogirikar, J.; Vidhate, A. Security attacks in IoT: A survey. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2021; pp. 32–37.

2. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. IEEE Commun. Surv. Tutor. 2019, 21, 2702–2733.

3. Arias, O.; Wurm, J.; Hoang, K.; Jin, Y. Privacy and Security in Internet of Things and Wearable Devices. IEEE Trans. Multi-Scale Comput. Syst. 2020, 1, 99–109.

Кихтенко Євген Миколайович
аспірант кафедри Технічних систем кіберзахисту
Державного університету інформаційно-комунікаційних технологій
Аверічев Ігор Миколайович
К. е. н., доцент кафедри Технічних систем кіберзахисту
Державного університету інформаційно-комунікаційних технологій, Київ
EMAIL*: iaverichev19@gmail.com*

ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КОМП`ЮТЕРНОЇ МЕРЕЖІ ВІД ПОЛІМОРФНИХ КОМП`ЮТЕРНИХ ВІРУСІВ

Постановка задачі

Основною проблемою на сьогодні, є необхідність розробки інноваційних методів кіберзахисту, який буде адаптованим до динамічного характеру кібератак та загроз, що забезпечує високий рівень точності виявлення. Поліморфні комп'ютерні віруси є особливо небезпечним типом кіберзагроз, тому що вони здатні змінювати свою структуру з кожною новою ітерацією. Це значно ускладнює їх виявлення традиційними методами, такими як сигнатурний аналіз.

Завдання дослідження полягає у створенні механізму, який інтегрує сучасні методи аналізу та дозволяє ефективно ідентифікувати та нейтралізувати поліморфні віруси у комп'ютерних мережах.

Мета дослідження

Метою дослідження є аналіз захисту комп'ютерної мережі від поліморфних комп'ютерних вірусів, який базується на поведінкових характеристиках вірусів та аналізі мережевого трафіку з використанням алгоритмів машинного навчання.

Результати дослідження

Наведемо аналіз існуючих методів захисту комп'ютерної мережі від поліморфних комп'ютерних вірусів.

Сигнатурний аналіз залишається поширеним методом, тому що обмеження полягають у виявленні нових, ще не відомих варіантів вірусів [1].

Евристичний підхід це ефективний у виявленні деяких невідомих загроз, який має високий рівень хибнопозитивних спрацьовувань [2].

Методи машинного навчання: показують перспективи, але потребують значного обсягу навчальних даних і оптимізації моделей [3].

Наведемо особливості запропонованого механізму захисту. Новий механізм базується на наступних компонентах.

Аналіз трафіку в реальному часі. Використано алгоритми для попередньої обробки даних, включаючи виділення аномалій, таких як нехарактерна частота запитів до мережевих ресурсів або незвичні маршрути передачі даних [4].

Кластеризація загроз. Застосовано алгоритми, що дозволяють групувати схожі зразки поліморфних вірусів, формуючи поведінкові патерни для кожної групи.

Автоматичне формування сигнатур. Для кожного кластеру створюється поведінковий профіль, який може бути використаний для ідентифікації схожих загроз у майбутньому [1].

Динамічне оновлення моделей.

За рахунок інтеграції машинного навчання механізм самостійно вдосконалюється завдяки отриманим даним [6].

Проведення тестування.

Для тестування запропонованого механізму були використані дані з відкритих джерел та симульовані атаки:

- набір даних: включав зразки понад 10 000 поліморфних вірусів, створених на основі різних шкідливих програм [3].
- метрики оцінки: точність, повнота, швидкість реакції системи [2].

Наведемо результати:

- точність виявлення зросла до 93%, у порівнянні з 75-80% для традиційних методів [4].
- рівень хибнопозитивних спрацьовувань зменшився на 30%.
- час виявлення загрози після початку атаки, скоротився до 5 сек. [6].

Порівняльний аналіз з існуючими системами.

Запропонований механізм було порівняно з комерційними антивірусними системами. Він продемонстрував перевагу у виявленні поліморфних загроз, особливо на ранніх етапах, де традиційні підходи не змогли ідентифікувати шкідливу активність [2, 4].

Інтеграція у практичне середовище.

Прототип системи було протестовано в умовах реальної корпоративної мережі, що дало змогу перевірити ефективність роботи механізму в умовах великого обсягу даних і різноманітних типів трафіку. Система адаптувалася до змін у поведінці користувачів без зниження ефективності [6].

Висновки та перспективи

Запропонований аналіз захисту комп’ютерної мережі від поліморфних комп’ютерних вірусів продемонстрував високу ефективність у виявленні поліморфних вірусів. Це дозволяє зменшити залежність від сигнатурного аналізу та покращити адаптивність системи до нових видів загроз.

Подальші дослідження будуть зосереджені на:

- інтеграції розробленого механізму в існуючі системи кіберзахисту;
- використанні глибоких нейронних мереж для покращення точності класифікації;
- оптимізації алгоритмів для роботи в реальному часі.

Список використаних джерел

1. Cohen, F. (1987). Computer Viruses: Theory and Experiments. Computers & Security.

2. Filiol, E. (2005). Computer Viruses: from Theory to Applications. Springer.

3. Dykstra, J., & Sherman, A.T. (2012). Intrusion Detection System Evaluation Metrics. IEEE Security & Privacy.

4. Anderson, R., & Moore, T. (2006). The Economics of Information Security. Science.

5. Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy

Коваль Андріян Михайлович
аспірант кафедри Технічних систем кіберзахисту
Державного університету інформаційно-комунікаційних технологій
Науковий керівник: **Іванченко Євгенія Вікторівна**
д.т.н., професор, директор навчально-наукового інституту Кібербезпеки та захисту інформації
Державного університету інформаційно-комунікаційних технологій
ORCID ID: 0000-0003-3017-5752
EMAIL: evivancenko@gmail.com
Аверічев Ігор Миколайович
К. е. н., доцент кафедри Технічних систем кіберзахисту
Державного університету інформаційно-комунікаційних технологій, Київ
ORCID ID: 0009-0008-9766-0115
EMAIL: iaverichev19@gmail.com

ДОСЛІДЖЕННЯ МЕТОДІВ І МОДЕЛЕЙ КІБЕРЗАХИСТУ КРИТИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Постановка задачі

У сучасних умовах критичні інформаційні системи (КІС) є ключовими елементами функціонування державних, економічних і соціальних структур. Їх кіберзахист стає критично важливим завданням через постійне зростання кількості та складності кібератак. Існуючі підходи до захисту, такі як класичні системи виявлення вторгнень (IDS) і стандартні антивірусні технології, часто виявляються недостатніми для протидії сучасним загрозам, зокрема поліморфним вірусам, атак на основі соціальної інженерії та DDoS-атак.

Проблема полягає у необхідності розробки ефективних методів і моделей, які забезпечать підвищення рівня кіберзахисту КІС з урахуванням їх динамічного характеру та специфіки сучасних загроз.

Мета дослідження

Аналіз існуючих методів і моделей кіберзахисту критичних інформаційних систем та розробка декількох концептуальних моделей, спрямованих на підвищення ефективності захисту від сучасних кіберзагроз з урахуванням особливостей їхньої інфраструктури.

Результати дослідження

Методи кіберзахисту:

Методи кіберзахисту – це практичні підходи та інструменти, спрямовані на забезпечення захисту інформаційних систем від загроз. Основні методи включають [1, 4]:

Методи виявлення та запобігання атак:

Системи виявлення вторгнень (IDS): моніторинг мережевого трафіку для виявлення аномальної активності.

Проактивний моніторинг: аналіз даних у реальному часі для передбачення можливих атак.

Методи машинного навчання: аналіз поведінкових аномалій для раннього виявлення загроз.

Методи захисту даних:

- Шифрування для забезпечення конфіденційності інформації.
- Використання блокчейн-технологій для перевірки цілісності даних.

Методи управління доступом:

- Багатофакторна аутентифікація.
- Принцип "нульової довіри" (Zero Trust), коли кожна взаємодія в системі потребує перевірки.

Методи резервування та відновлення:

- Створення резервних копій критичної інформації.
- Платформи автоматичного відновлення після атак.

Модель кіберзахисту – це структурований підхід до організації та управління заходами безпеки в інформаційній системі.

Модель "Захист у глибину" (Defense-in-Depth):

Багаторівнева архітектура захисту, що включає:

- Фізичний рівень (контроль доступу до обладнання).
- Мережевий рівень (брандмауери, IDS).
- Прикладний рівень (захист програмного забезпечення).
- Дані (шифрування).

Модель "Zero Trust" (Нульова довіра):

- Кожен користувач або пристрій розглядається як потенційна загроза.
- Всі дії проходять перевірку незалежно від місця розташування.

Модель на основі аналізу ризиків:

- Побудова систем захисту на основі оцінки ризиків і потенційного впливу атак на бізнес-процеси.
- Фокус на найбільш критичних елементах системи.

Гібридні моделі:

- Комбінування локальних (on-premises) та хмарних (cloud-based) рішень для забезпечення гнучкості й масштабованості.
- Використання SIEM-систем для централізованого моніторингу подій.

Виокремлено основні кіберзагрози для критичних інформаційних систем.

Для охорони здоров'я: атаки на медичні бази даних, несанкціонований доступ до медичних пристроїв, шифрувальники (ransomware).

Для логістики: атаки на системи управління поставками, DDoS-атаки на транспортні сервіси, компрометація GPS.

Проаналізовано ефективність існуючих моделей, що виявили недостатню адаптивність до специфічних загроз цих галузей.

На рис. 1 представлено концептуальне уявлення про адаптивну структуру кібербезпеки для охорони здоров'я та рис. 2 Концептуальну модель бази даних кібербезпеки для логістичної компанії.

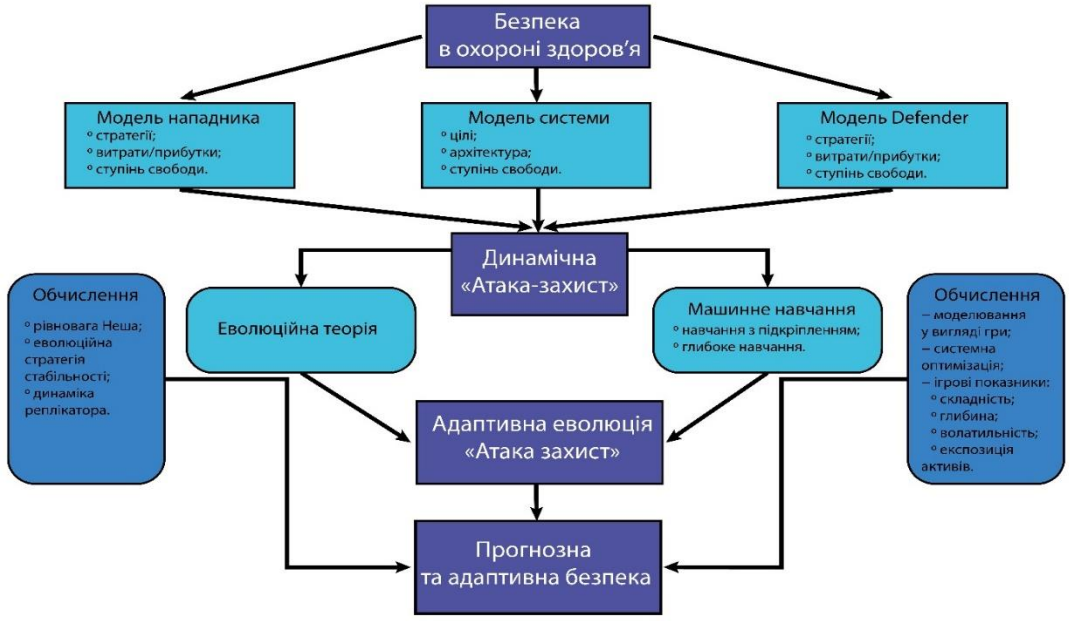

Рис. 1. Концептуальне уявлення про адаптивну структуру кібербезпеки для охорони здоров'я

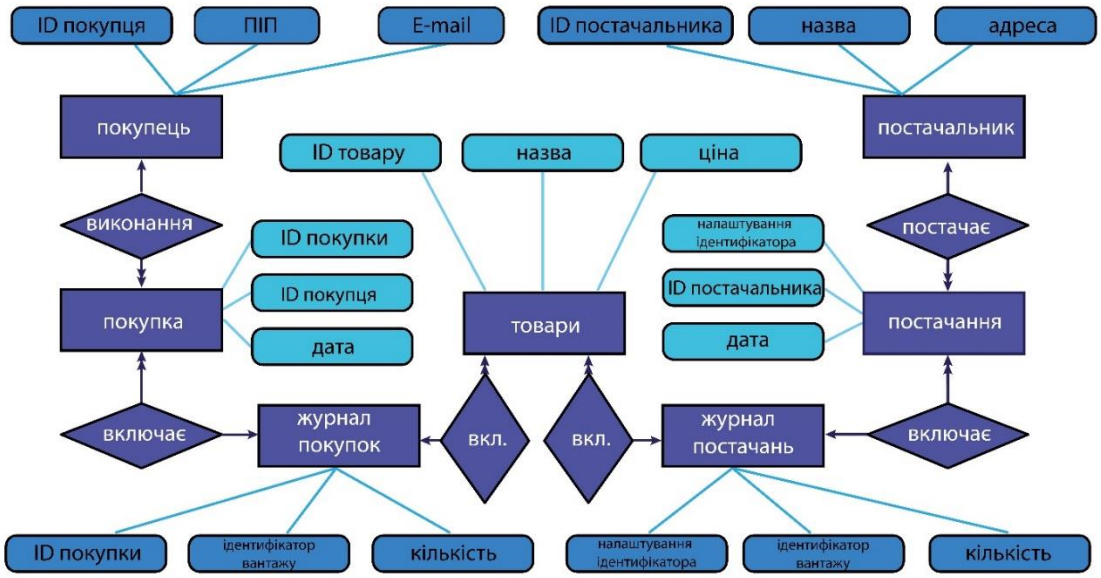

Рис. 2. Концептуальну модель бази даних кібербезпеки для логістичної компанії

Розробка концептуальних структур кіберзахисту:

Структура кібербезпеки для систем охорони здоров'я, як однієї із найважливіших структур критичності країни [2, 3, 5]:

Зони захисту:

- *медичні пристрої:* ізоляція медичних пристроїв у окремих мережах із регулярним оновленням програмного забезпечення.
- *бази даних пацієнтів:* шифрування даних та багатофакторна аутентифікація.

- *системи обміну інформацією:* використання VPN і блокчейн-технологій для забезпечення конфіденційності передачі даних.

Методи захисту:

- постійний моніторинг активності за допомогою SIEM-систем.
- проактивний аналіз аномалій для виявлення спроб атак.
- проведення регулярних penetration testing.

Структура кібербезпеки для логістичних компаній, яка на сьогоднішній час має включати в себе наступні аспекти.

Зони захисту:

- *системи управління поставками:* впровадження блокчейн для відстеження ланцюжків поставок.
- *транспортна інфраструктура:* шифрування даних GPS та резервні маршрути.
- *інформаційні системи:* сегментація мереж із застосуванням принципу "нульової довіри".

Методи захисту:

- інтеграція SIEM-систем для аналізу кіберзагроз у реальному часі.
- використання хмарних рішень для резервування критичної інформації.
- використання двофакторної аутентифікації для працівників.

Огляд концептуальної моделі бази даних кібербезпеки для логістичної компанії

Концептуальна модель бази даних (БД) кібербезпеки для логістичної компанії є важливим інструментом для забезпечення захисту інформаційних ресурсів та управління ризиками. Вона дозволяє структурувати дані, пов'язані з кіберзагрозами, та організувати їх у зрозумілій формі для подальшого аналізу та реагування.

Основні елементи концептуальної моделі

Сутності:

- клієнти: зберігає інформацію про замовників послуг.
- постачальники: інформація про постачальників товарів.
- товари: дані про товари, що перевозяться.
- замовлення: записи про замовлення, їх статуси та деталі.
- користувачі системи: дані про співробітників, які мають доступ до системи.

Атрибути: кожна сутність має свої атрибути, які описують її характеристики. Наприклад:

- клієнти: ID, ім'я, адреса, контактна інформація;
- товари: ID, назва, опис, вага, ціна;
- замовлення: ID, дата замовлення, статус, загальна вартість.

Зв'язки: визначення зв'язків між сутностями:

- зв'язок між клієнтами та замовленнями (один до багатьох);
- зв'язок між постачальниками та товарами (один до багатьох);
- зв'язок між замовленнями та товарами (багато до багатьох).

Забезпечення кібербезпеки

Важливим аспектом концептуальної моделі є інтеграція принципів кібербезпеки:

контроль доступу: визначення ролей користувачів і рівнів доступу до різних частин БД;

шифрування даних: використання механізмів шифрування для захисту чутливих даних;

моніторинг активності: логування дій користувачів для виявлення аномальної поведінки.

Висновок

Обидві розглянуті сфери – охорона здоров'я та логістика – є критично важливими для суспільства. Тому забезпечення їхнього кіберзахисту має бути пріоритетом. Аналіз сучасних тенденцій свідчить про необхідність розвитку адаптивних систем кібербезпеки, які здатні автоматично виявляти та нейтралізувати нові загрози. Крім того, важливим напрямком є підвищення стійкості критичної інфраструктури до кібератак шляхом створення резервних копій даних, забезпечення безперебійного електроживлення та розробки планів відновлення після інцидентів.

Концептуальні моделі бази даних кібербезпеки для обох розглянутих сфер повинні бути гнучкими і масштабованими, щоб адаптуватися до змін у бізнес-процесах і нових загрозах у сфері кібербезпеки. Саме тоді вони забезпечуватимуть структурований підхід до управління даними та ризиками, що є критично важливим для ефективного функціонування компаній в умовах сучасних кіберзагроз.

Список використаних джерел

1. А. М. Мельник, "Методи і моделі кіберзахисту критичних інформаційних систем", К.: Наукова думка, 2020.

2. ISO/IEC 27001:2022, "Міжнародний стандарт управління інформаційною безпекою".

3. П. В. Ткаченко, "Системи виявлення атак в кіберфізичних системах", Журнал кібернетики, 2023.

4. National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity", 2022.

5. R. Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems", Wiley, 2021.

Криворучко Віталій Федорович
аспірант 2 курсу, групи АІПЗ-21
Державний університет інформаційно-комунікаційних технологій
(063) 791-57-51
hamandes@gmal.com
Науковий керівник: **Садовенко Володимир Сергійович,**
кандидат фізико-математичних наук, доцент, професор кафедри Інженерії програмного забезпечення автоматизованих систем
Державного університету інформаційно комунікаційних технологій, м. Київ

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ КІБЕРЗАГРОЗ У КОРПОРАТИВНИХ МЕРЕЖАХ

Постановка задачі. З розвитком діджиталізації сучасний бізнес все частіше стикається з різноманітними видами кіберзагроз. Складні атаки, такі як Advanced Persistent Threats (APT), спрямовані фішингові кампанії, внутрішні зловживання привілеями користувачів, використання прихованих каналів зв'язку та маскування під легітимний трафік, ускладнюють роботу традиційних засобів захисту (сигнатурні IDS, антивіруси, фаєрволи). Ці технології мають обмежену здатність до виявлення нових, невідомих загроз, оскільки вони зазвичай орієнтуються на наперед визначені патерни.

Метою є застосувати методи штучного інтелекту та машинного навчання (ML) для автоматизованого виявлення атак за аномаліями у мережевому трафіку та поведінці користувачів, підвищити точність детекції складних загроз, знизити кількість хибнопозитивних спрацювань та забезпечити масштабованість системи у умовах постійного росту обсягів даних.

Мета дослідження. Мета полягає у розробці та апробації методики інтеграції моделей ML та глибинного навчання (Deep Learning) у системи моніторингу корпоративних мереж, що дозволить:

- виявляти як відомі, так і нові типи атак без прив'язки до сигнатур;
- динамічно адаптуватися до нових патернів поведінки зловмисників;
- зменшити операційне навантаження на фахівців із кібербезпеки за рахунок автоматизованого аналізу великого масиву трафіку.

Результати. Для перевірки гіпотез було створено експериментальну середу, яка імітує корпоративну мережу середнього підприємства (приблизно 200 робочих станцій, 20 серверів, декілька точок доступу до Інтернету). Дані для навчання та тестування включали реальні та синтетично згенеровані сесії трафіку: HTTP/HTTPS, SSH, SMB, DNS, SQL-запити. До зразків шкідливого трафіку входили сесії зі скануванням портів, брутфорс-атаками на SSH, несанкціонованим доступом до баз даних, ексфільтрацією даних за допомогою прихованих DNS-тунелів, а також діяльність бекдорів.

Підготовка даних.

- Виконано збір трафіку за допомогою Zeek (раніше Bro) – системи аналізу мережевих пакетів.
- Проведено фільтрацію та нормалізацію даних: видалення пошкоджених пакетів, агрегування сесій за 5-хвилинними інтервалами, формування векторів ознак (кількість пакетів, середній розмір, часові інтервали між пакетами, розподіл протоколів, статистика по джерелах і призначеннях).
- Використано методи зменшення розмірності (PCA, t-SNE) для первинного аналізу структури даних та виявлення кластерів аномальних патернів.

Моделювання та навчання.

- Використано кілька підходів ML:

а) Класичні алгоритми: Random Forest, XGBoost – для тестування базових можливостей класифікації аномалій.

б) Глибинне навчання: нейронні мережі типу Multi-Layer Perceptron (MLP), згорткові нейронні мережі (CNN) для витягання складних ознак із часових рядів, рекурентні мережі (LSTM, GRU) для аналізу послідовностей пакетів та виявлення довгострокових залежностей, а також комбінації LSTM із механізмом уваги (Attention) для фокусування на критичних сегментах трафіку.

в) Моделі виявлення аномалій без учителя: автоенкодери, Variational Autoencoders (VAE), Isolation Forest для виявлення відхилень від «нормального» профілю мережі.

- Налаштування гіперпараметрів (кількість шарів, кількість нейронів, параметри регуляризації, коефіцієнти навчання) здійснювалося за допомогою Bayesian Optimization та Grid Search.
- Навчання проводилося на обчислювальних ресурсах із прискоренням за рахунок GPU, що скоротило час експериментів.

Оцінювання ефективності.

- Метрики: точність (Accuracy), повнота (Recall), метрика F1, ROC-AUC, а також показники хибнопозитивних (False Positive Rate) та хибнонегативних (False Negative Rate) спрацювань.
- Найкращий результат продемонстрували архітектури LSTM+Attention, які досягли точності близько 96-98% у виявленні аномальних сесій та знизили хибнопозитивні спрацювання на 20-30% порівняно з XGBoost та класичними сигнатурними IDS.
- Автоенкодери виявилися корисними при виявленні нових, раніше невідомих патернів атак. Коли система стикалась із незнайомою конфігурацією трафіку, помилка відновлення в автоенкодері зростала, що слугувало маркером аномальності.

Адаптивність та масштабованість.

- Запропонований підхід легко масштабується для великих корпоративних мереж завдяки можливості горизонтального розподілення навантаження та використання хмарних сервісів з GPU/TPU.

- Періодичне донавчання моделей на свіжих даних дозволяє системі адаптуватися до нових типів загроз та мережевих патернів без необхідності ручного оновлення сигнатур.

Впровадження на практиці.

- Технологія може бути інтегрована в існуючі SOC (Security Operation Center) платформи, SIEM-системи, засоби моніторингу мережі.
- Автоматизовані ML-модулі знижують час реагування на інцидент, сигналізуючи аналітикам безпеки про підозрілі дії в режимі, наближеному до реального часу.

Висновки.

Впровадження технологій штучного інтелекту у системи кібербезпеки корпоративних мереж значно підвищує їх ефективність, адаптивність та здатність виявляти нові та складні атаки. Отримані результати підтверджують, що глибинні нейронні мережі (особливо рекурентні з механізмом уваги) та підходи виявлення аномалій без учителя можуть значно перевершити класичні сигнатурні рішення. Подальші дослідження можуть бути спрямовані на аналіз мультимодальних джерел даних (лог-файли систем безпеки, телеметрія кінцевих точок, поведінкові характеристики користувачів), інтеграцію підходів Explainable AI для кращої інтерпретації рішень моделей та впровадження Zero Trust принципів у мережеві архітектури.

Список використаних джерел

1. Sommer, R., & Paxson, V. Outside the closed world: On using machine learning for network intrusion detection. IEEE Security & Privacy, 2010.
2. Chandola, V., Banerjee, A., & Kumar, V. Anomaly detection: A survey. ACM Computing Surveys, 2009.
3. Dong, Y., Chen, X., Wei, Y., Liu, R., Zhang, Y. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 2021.
4. Liao, H., Lin, C., Lin, Y., & Tung, K. Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 2013.
5. Roy, S., Cheung, W. K., & Li, C. K. Cyber-attack detection using deep neural networks with attention mechanism. Computer Communications, 2021.
6. Kwon, D., Kim, H., Lim, H., & Lee, K. A survey of deep learning-based network anomaly detection. Electronics, 2022.

Нездолій Владислав Анатолійович
бакалавр 3 курсу, групи ІП-24
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
(067)136-19-94
nezdolii.vladyslav@lll.kpi.ua
Науковий керівник: **Поперешняк Світлана Володимирівна**
к.ф.-м.н., доцент, доцент кафедри ІПІ ФІОТ
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
(098)-645-546-2
spopereshnyak@gmail.com

КІБЕРБЕЗПЕКА ТА ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ У ВЕБ-ЗАСТОСУНКАХ З БОКУ API

Постановка задачі. Сучасні веб-застосунки є невід'ємною частиною бізнесу, комунікацій та повсякденного життя Їх популярність зростає з кожним роком, однак це також супроводжується збільшенням кількості різних кібератак. Вразливості систем можуть призвести до значних фінансових втрат, витоку конфіденційної інформації та втрати довіри користувачів. Виникнення подібних загроз потребує розробки та впровадження ефективних методів захисту. Основною задачею цього дослідження буде аналіз основних зовнішніх інформаційних загроз та існуючих методів протидії їм.

Мета дослідження. Метою цієї роботи є дослідження кібербезпеки у контексті захисту веб-застосунків з боку їхнього API – програмного інтерфейсу веб-застосунку, та компонентів, що вкупі з ним надають користувачам та іншим системам доступ до функціоналу застосунків.

Результати. OWASP – онлайн-спільнота, що працює над відкритим проектом з безпеки веб-застосунків, створює статті, методології, документацію, інструменти та технології в галузі безпеки веб-застосунків, на 2021 рік оновила список десяти найголовніших типів загроз [1], що зображено на рис. 1.

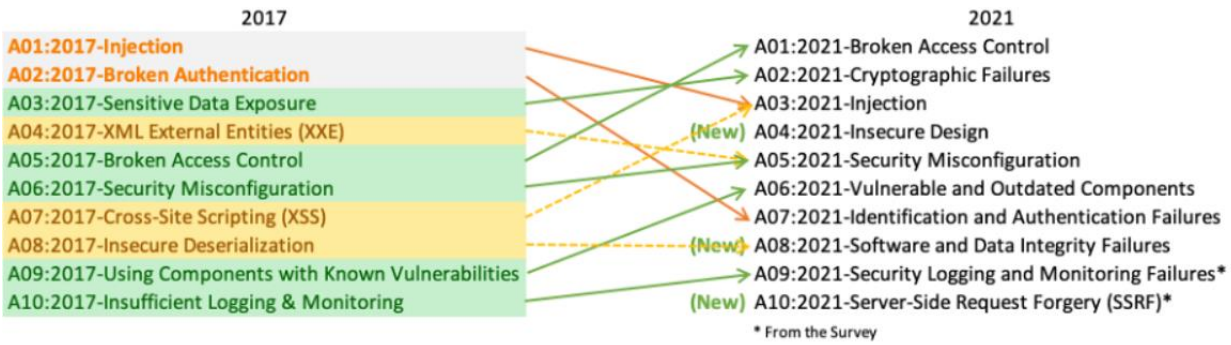

Рис. 1. Список найголовніших загроз за версією OWASP.

Майже третина загроз, що вказані на рис. 1, напряму пов’язані з архітектурою API, авторизацією чи валідацією, а саме: Injection(SQL-ін'єкції та XSS – міжсайтовий скриптинг), Identification and Authentication Failures (Проблеми ідентифікації та аутентифікації) та Server-Side Request Forgery (Підробка запитів на стороні серверу).

Вразливості на рівні додатків, такі як SQL-ін'єкції та міжсайтовий скриптинг (XSS), ще довго залишатимуться актуальними проблемами. SQL-ін'єкції дозволяють зловмисникам отримувати доступ до баз даних шляхом введення шкідливих запитів. Захист від таких атак забезпечується використанням підготовлених запитів (prepared statements), а також регулярним аудитом коду. Міжсайтовий скриптинг дозволяє зловмисникам вставляти шкідливі скрипти у браузери користувачів, завдаючи шкоди не лише окремим користувачам, а й репутації компанії. Екранування вхідних даних та впровадження політики безпеки вмісту (CSP) є основними методами захисту від XSS. Недоліком цих підходів є необхідність значних технічних навичок для їх ефективного застосування. Для підвищення ефективності захисту рекомендується використання автоматизованих інструментів тестування на проникнення, таких як Burp Suite та OWASP ZAP.

Типи авторизації суттєво впливають на рівень захисту веб-застосунків. Базова авторизація, яка передбачає передачу логіна і пароля, є недостатньо безпечною без HTTPS – розширення протоколу HTTP з підтримкою шифрування.

Токен-авторизація, наприклад JSON Web Token (JWT), забезпечує більшу безпеку, а їхнє використання із обмеженим часом дії значно знижує ризик компрометації навіть у разі їхнього перехоплення. OAuth 2.0 – дає змогу надавати одному сервісу (додатку) права на доступ до ресурсів користувача на іншому сервісі. Цей протокол позбавляє необхідності довіряти застосунку логін і пароль, а також дає змогу видавати обмежений набір прав, а не всі одразу, він теж є безпечним методом, але його впровадження може бути технічно складним.

Крадіжка облікових даних через слабкі паролі або фішингові атаки становить серйозну проблему для автентифікації. Використання двофакторної автентифікації (2FA) дозволяє суттєво знизити ризики, забезпечуючи додатковий рівень захисту. У разі впровадження 2FA користувач отримує код підтвердження через мобільний додаток або SMS, що унеможливлює доступ до акаунта навіть у разі викрадення пароля. Однак, 2FA може бути незручним для частини користувачів, що впливає на їхній досвід роботи із системою. Альтернативою є біометрична автентифікація, яка забезпечує високу точність і зручність, але висуває вимоги до апаратного забезпечення.

Server-Side Request Forgery (SSRF) є типом вразливості в веб-додатках, який дозволяє зловмиснику ініціювати HTTP або інші типи запитів від імені серверу. Тобто, зловмисник може змусити сервер виконувати запити до ресурсів, до яких він сам не має доступу (наприклад, внутрішніх API, баз даних, серверів або навіть до локальних файлів). Боротьба з SSRF вимагає системного підходу до безпеки, який охоплює валідацію вхідних даних, налаштування належних

мережевих політик і практик, а також регулярний моніторинг і аудит безпеки [2-4].

Висновки. Отже, забезпечення високого рівня безпеки веб-застосунків можливе лише за умови комплексного підходу. Використання сучасних технологій, таких як укранування вхідних даних, політики безпеки вмісту, двофакторна аутентифікація та регулярний аудит коду, значно підвищує стійкість систем до типових зовнішніх загроз. Запропоновані рекомендації дозволяють мінімізувати ризик компрометації систем та втрати даних, забезпечуючи тим самим надійний захист інформаційних активів.

Список використаних джерел

1. OWASP Foundation. OWASP Top Ten. [Електронний ресурс] – URL: https://owasp.org/www-project-top-ten/.
2. Stuttard D., Pinto M. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. Wiley, 2011.
3. Kalman S. Web Security Field Guide. Cisco Press, 2018.
4. ISO/IEC 27001:2013 – Information security management systems – Requirements.

Поночовний Петро Михайлович
аспірант кафедри Систем та технологій кібербезпеки,
Державний університет інформаційно-комунікаційних технологій, Київ, Україна.
ORCID ID: 0009-0008-6480-6990
EMAIL: petja9186@gmail.com
науковий керівник: **Іванченко Ігор Сергійович**
к.т.н., доцент кафедри технічного захисту інформації
Державного некомерційного підприємства "Державний Університет "Київський Авіаційний Інститут", Київ, Україна.
ORCID: 0000-0003-3415-9039
EMAIL: Igor-p-l@ukr.net

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ СИСТЕМИ РЕАЛІЗАЦІЇ ЗАХИСТУ СЕРВЕРІВ З УРАХУВАННЯМ АНОМАЛІЙ В ПАКЕТАХ

Постановка задачі

У сучасному світі, зі зростанням кіберзагроз і кіберінцидентів, зокрема розподілених атак типу DDoS (Distributed Denial of Service), ефективний кіберзахист серверних систем стає важливим завданням. Традиційні методи фільтрації трафіку часто недостатньо ефективні через постійне вдосконалення методів маскування шкідливого трафіку та зміни характеру аномалій. Це зумовлює необхідність розробки адаптивних систем захисту, які здатні аналізувати пакети в реальному часі, виявляти аномалії та застосовувати превентивні заходи.

Мета дослідження

Метою роботи є експериментальне дослідження системи кіберзахисту серверів на основі аналізу аномалій у пакетах мережевого трафіку, що дозволить підвищити ефективність виявлення кіберінцидентів, пов’язаних із DDoS-атаками, і знизити вплив шкідливого трафіку на продуктивність серверів.

Результати дослідження

В даній роботі використовувався алгоритм фільтрації трафіку.

Розглянемо контролер який отримує невідомий пакет через протокол OpenFlow, пакет містить повну інформацію про пакет. Після того, як контролер отримає пакет, відбувається аналіз інкапсуляцію пакету, аналізуючи кожен шар пакета [1].

Таким чином можна створити таблицю потоку для пакета на основі вилученої інформації. Надалі вихідний пакет передається на плату обміну через протокол OpenFlow [2]. Який містить інтерфейс для пересилання. На основі цього принципу пакети, надіслані платою обміну, обробляються та необхідна інформація вилучається та передається навченій моделі для ідентифікації та прогнозування.

На рис. 1 представлено алгоритм фільтрації трафіку.

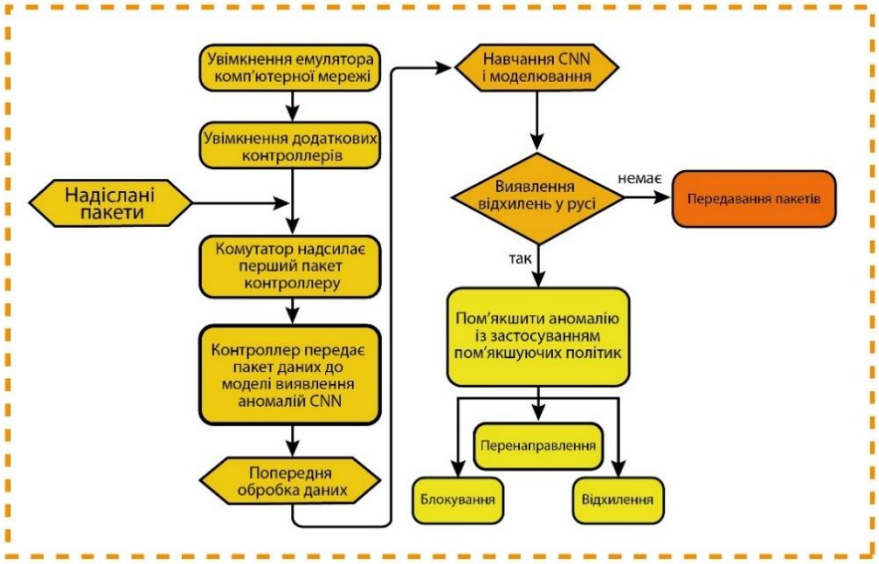

Рис. 1. Алгоритм фільтрації трафіку

Спочатку запускаємо емулятор комп'ютерної мережі і контролер, який надсилає пакети, в цей час комутатор пересилає перший пакет контролеру. Контролер передає пакет до моделі виявлення аномалії CNN. Після попередньої обробки даних навчання та моделювання CNN використовуються для виявлення аномального трафіку. Якщо це звичайний трафік, пакет передається безпосередньо. При виявленні аномального трафіку пом'якшити атаку пропонується за допомогою, блокування, перенаправлення та відхилення.

На рисунку 2 представлено систему захисту серверів з урахуванням аномалій в пакетах.

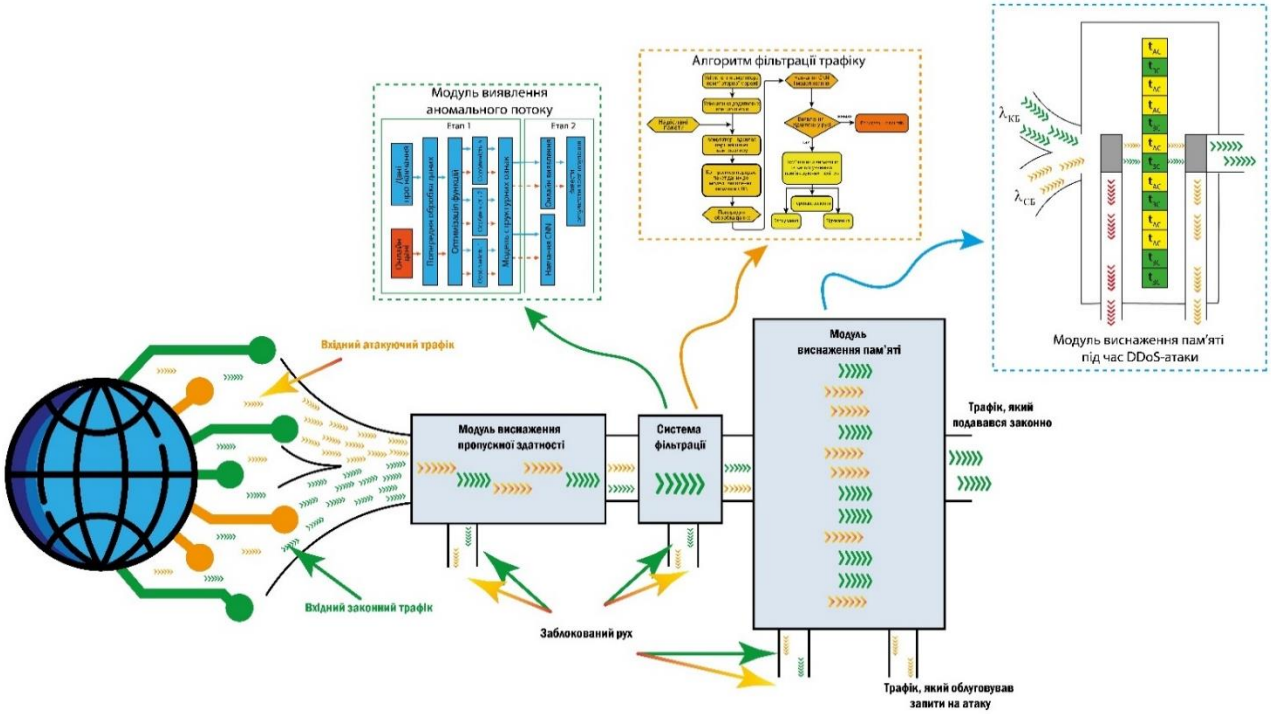

Рис. 2. Система захисту серверів з урахуванням аномалій в пакетах

Алгоритм трафіку використовується в експериментальній системі захисту серверів з урахуванням аномалій в пакетах.

Реалізація

Для перевірки результатів фільтрації пакетів DDoS-атак була застосована експериментальна установка у вигляді сервера, оснащеного Ubuntu 20.04, процесором Intel Core i7-1165G7 з частотою 2,80 ГГц і 16 ГБ оперативної пам'яті. Для емуляції топології мережі використовувалась платформа Mininet 2.3.0, яка полегшує створення віртуальної мережі, що включає хости, комутатори, контролери та запити. В якості комутатора обрано Cisco з відповідними налаштуваннями [3]. Щоб імітувати динаміку DDoS-атаки, застосовано утиліту hping3, яка відома тим, що надсилає спеціалізовані пакети TCP/IP. Крім того, для створення пропускної здатності та затримки, необхідних для ініціювання атаки, задіяний Iperf, надійний інструмент маніпулювання пакетами [4].

Сценарій перед DDoS-атакою

На рисунку 3 наведено графік пропускної здатності перед сценарієм DDoS-атак.

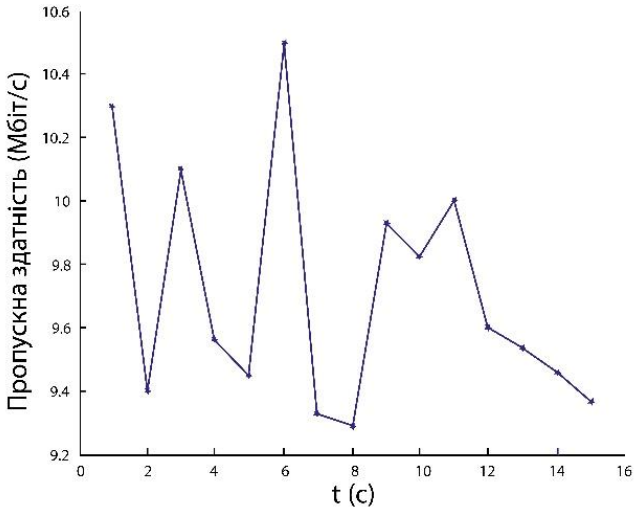

Рис. 3. Пропускна здатність перед сценарієм DDoS-атак

Завдяки графіку рис. 3 пропускна здатність перед сценарієм DDoS-атак, стає очевидним, що з плином часу існує коливання швидкості потоку в діапазоні від 9,3 до 10,5 Мбіт/с. Ця зміна зберігається до 12-ї одиниці часу, після чого швидкість потоку стабілізується на рівні 9,6 Мбіт/с. З часом виявилась тенденція до зниження швидкості потоку, що стало очевидним, оскільки вимірювання пропускної здатності падає до 9,38 Мбіт/с, в проміжку до 15-ї одиниці часу.

Сценарій після DDoS-атаки

Звертаючись до графіка, зображеного на рис. 3, помітний початковий стрибок, при якому потік досягає найвищого значення 630 Мбіт/с у момент часу 1. Згодом слідує помітне зменшення, що супроводжується коливаннями в діапазоні від 8 до 12 Мбіт/с. Ця закономірність приводить нас до висновку, що

зниження пропускної здатності стає очевидним після сценарію DDoS-атаки (рис. 4).

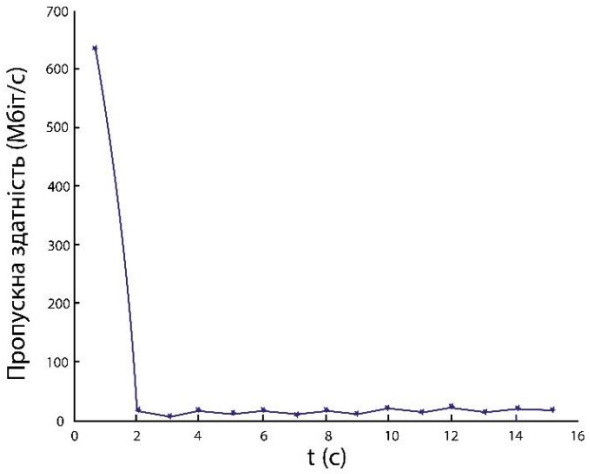

Рис. 4. Пропускна здатність після сценарію DDoS-атаки

Для побудови ефективної системи захисту серверів пропонується інтеграція раннього виявлення з алгоритмами фільтрації, яка забезпечує потужну основу. Наприклад, моделі, що використовують оновленні алгоритми машинного навчання, дозволяють адаптуватися до змін у шаблонах атак. Одночасно, багаторівневий підхід, який поєднує статистичний аналіз, класифікацію та поведінкове фільтрування, мінімізує хибно-позитивні результати та знижує навантаження на систему.

Висновки

Експериментальне дослідження показало, що розроблена система підтвердила свою ефективність у забезпеченні кіберзахисту серверів від DDoS-атак. Модуль раннього виявлення аномалій є ключовим елементом системи, який дозволяє виявляти потенційно шкідливі дії на максимально ранній стадії. Для протидії новим, раніше невідомим типам атак особливо важливо використовувати глибокі нейронні мережі та алгоритми кластеризації для аналізу моделей поведінки трафіку в режимі реального часу. Це забезпечить раннє виявлення, тому загрози можна усунути до того, як вони завдадуть шкоди інфраструктурі. Алгоритми фільтрації трафіку блокують шкідливі пакети, використовуючи багаторівневий підхід.

На основі проведеного аналізу аномалій у пакетах, дозволило суттєво зменшити вплив шкідливого трафіку на продуктивність серверів. І в подальшому, використовуючи підхід, заснований на алгоритмах раннього виявлення аномалій і фільтрації трафіку, можна побудувати комплексну систему, яка забезпечить високу надійність і адаптивність до сучасних загроз.

Перспективи подальших досліджень включають:

- вдосконалення алгоритмів класифікації для адаптації до нових типів кіберінцидентів і атак;
- розробку модулів для роботи у хмарних середовищах;
- інтеграцію з іншими системами моніторингу для забезпечення комплексного кіберзахисту.

Список використаних джерел

1. Анна Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019 – 361 с.

2. Behal S., Kumar K. Detection of DDoS Attacks Using Machine Learning Algorithms. // International Journal of Computer Applications, 2020.

3. Opanasenko M.I., Ponochovnyy P.M. Tekhnolohiya zabezpechennya kiberbezpeky khmarnoho seredovyshcha na bazi rishennya Cisco Cloudlock // Suchasnyy zakhyst informatsiyi, 2023. – № 1(53). – S. 72-78

4. Zargar S. T., Joshi J., Tipper D. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. // IEEE Communications Surveys & Tutorials, 2020.

Роженко Артем Сергійович
Аспірант кафедри Технічних систем кіберзахисту
Державного університету інформаційно-комунікаційних технологій
Науковий керівник: **Іванченко Євгенія Вікторівна**
д.т.н., професор, директор навчально-наукового інституту Кібербезпеки та захисту інформації
кафедри Технічних систем кіберзахисту
Державного університету інформаційно-комунікаційних технологій
ORCID ID: 0000-0003-3017-5752
EMAIL: evivancenko@gmail.com
Аверічев Ігор Миколайович
К. е. н., доцент кафедри Технічних систем кіберзахисту
Державного університету інформаційно-комунікаційних технологій, Київ
ORCID ID: 0009-0008-9766-0115
EMAIL: iaverichev19@gmail.com

ДОСЛІДЖЕННЯ МЕТОДІВ ТА МОДЕЛЕЙ ПІДВИЩЕННЯ РІВНЯ КІБЕРЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ ТЕХНОЛОГІЙ ХМАРНОГО СЕРЕДОВИЩА

Постановка задачі

Сучасні корпоративні мережі стикаються з численними загрозами, які вимагають впровадження ефективних механізмів кіберзахисту. Хмарні технології, що набрали популярності в останні роки, пропонують нові можливості для підвищення рівня безпеки даних. Однак їх використання також створює нові виклики, пов’язані з управлінням ризиками, конфіденційністю та доступом до інформації. Задача даного дослідження полягає у систематизації існуючих методів та моделей кіберзахисту корпоративних мереж на базі технологій хмари, а також у визначенні найефективніших підходів для підвищення рівня безпеки.

Мета дослідження

Метою дослідження є розробка науково обґрунтованих рекомендацій щодо застосування сучасних методів та моделей кібербезпеки в корпоративних мережах, що функціонують у хмарному середовищі. Які включають аналіз існуючих рішень, вивчення їх переваг та недоліків, а також визначення впливу хмарних технологій на загальний рівень кіберзахисту.

Результати дослідження

Дослідження показало, що інтеграція хмарних технологій у корпоративній мережі суттєво підвищує рівень кіберзахисту та вимагає врахування як позитивних, так і негативних аспектів.

На рисуноку 1 наведено схему кіберзахисту мережі з хмарними технологіями, яка ілюструє основні компоненти кіберзахисту в хмарному середовищі.

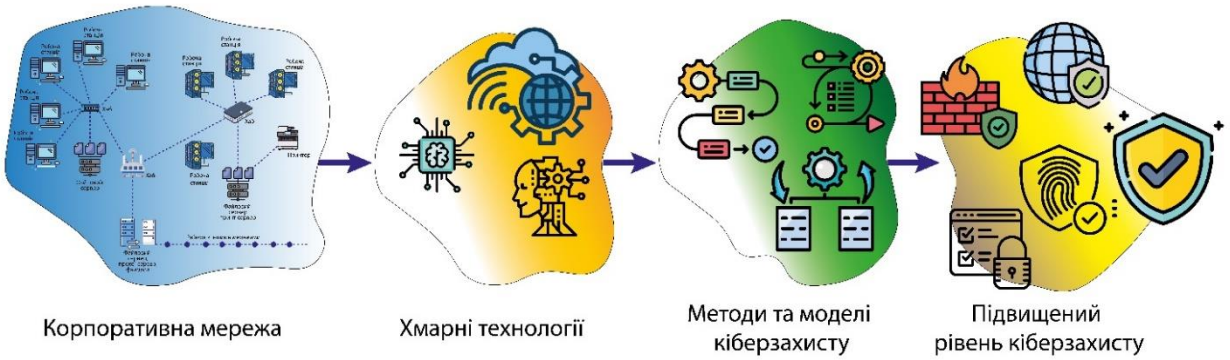

Рис. 1. Схема кіберзахисту мережі з хмарними технологіями

Схема демонструє зв'язок між корпоративною мережею, хмарними технологіями та методами кіберзахисту, що веде до підвищення безпеки.

Наведемо перелік позитивних моментів кіберзахисту мережі з хмарними технологіями.

Автоматизація процесів безпеки:

- хмарні рішення надають інструменти для автоматизованого виявлення та реагування на загрози, що знижує навантаження на IT-персонал [1].

Гнучкість та масштабованість:

- хмарні платформи дозволяють швидко масштабувати ресурси та адаптуватися до змін у загрозах, що робить їх ідеальними для динамічних бізнес-середовищ [2].

Розподіл ресурсів:

- зменшення ризиків завдяки географічному розподілу даних та ресурсів, що ускладнює можливості атаки на єдину точку [3].

Забезпечення відповідності:

- більшість хмарних провайдерів мають сертифікації та стандарти безпеки, що спрощує дотримання нормативних вимог і підвищує довіру до провайдерів [4].

Кост-ефективність:

- використання хмари може знизити витрати на інфраструктуру, оскільки підприємства можуть обирати моделі оплати в залежності від потреб [5].

Також наведемо негативні моменти кіберзахисту мережі з хмарними технологіями.

Залежність від постачальника:

- використання хмарних технологій може призвести до залежності від конкретного постачальника послуг, що ускладнює міграцію до інших платформ.

Проблеми з конфіденційністю:

- передача чутливих даних у хмару може викликати занепокоєння щодо конфіденційності, особливо якщо дані зберігаються в юрисдикціях з менш строгими законами про захист даних.

Вразливість до нових загроз:

- хоча хмари забезпечують певний рівень безпеки, вони також можуть стати мішенню для нових видів атак, зокрема, на базі вразливостей у програмному забезпеченні.

Складність управління безпекою:

- інтеграція хмарних рішень в існуючу корпоративну інфраструктуру може бути складною, що потребує належного планування та ресурсів.

Витрати на навчання:

- перехід на хмарні технології може вимагати додаткових витрат на навчання персоналу для роботи з новими системами та інструментами безпеки.

Таким чином, хмарні технології значно підвищують рівень кіберзахисту корпоративних мереж, та враховують переваги та виклики, що виникають у процесі впровадження та експлуатації.

Висновки та перспективи

Отримані результати свідчать про те, що хмарні технології значно підвищують рівень безпеки корпоративних мереж. Проте їх застосування потребує ретельного підходу до вибору постачальників та оцінки ризиків. В подальшому дослідженні варто зосередитись на розробці нових моделей безпеки, які враховують специфіку хмарного середовища.

Список використаних джерел

1. Stallings, W. (2019). *Network Security: Essentials: Applications and Standards*. Pearson.

2. Rittinghouse, J. W., & Ransome, J. (2016). *Cloud Computing: Implementation, Management, and Security*. CRC Press.

3. Cloud Security Alliance (2020). *Security Guidance for Critical Areas of Focus in Cloud Computing V4.0*. Cloud Security Alliance.

4. Alharkan, I., et al. (2021). "A Survey on Cloud Computing Security Issues and Challenges." *IEEE Access*.

5. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements.

Павленко Петро Миколайович
професор кафедри забезпечення авіаційних перевезень
доктор технічних наук, професор
Національний авіаційний університет
(050) 158-53-37
petrpav@ukr.net
Самборський Євген Іванович
старший викладач кафедри комп'ютерних наук та кібербезпеки
Волинський національний університет імені Лесі Українки
(073) 013-86-63
seinauedu@gmail.com.

МОДЕЛЬ УПРАВЛІННЯ ПОДІЯМИ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ ЦИФРОВИХ ДВІЙНИКІВ

Постановка задачі. Організація управління подіями інформаційної безпеки з метою надійного захисту конфіденційної керуючої інформації у комп'ютерних системах (КС) інфраструктури критичних об'єктів є нагальним і перспективним напрямом фундаментальних, пошукових і прикладних наукових досліджень. Для їх реалізації пропонується використати теорію гіперкомплексних логіко-динамічних систем (ГКЛДС) та синтезувати модель управління подіями безпеки комп'ютерних систем (КС) критичної інформаційної інфраструктури (КІІ) на основі її цифрових двійників (ЦД).

Мета дослідження. Метою дослідження є теоретичне обґрунтування методу синтезу моделі управління подіями безпеки КС КІІ, ЦД яких описані ГКЛДС.

Результати дослідження. Проведені дослідження специфіки і особливостей КС КІІ свідчать, що найбільш значущими для забезпечення їх функціональної стійкості і надійності роботи є [1]…[3]:

-оцінка та аналіз подій інформаційної безпеки (на основі розгляду процесів у КС КІІ), описаних математичними моделями ГКЛДС;

- створення алгоритму формування еталонного (базового) масиву подій безпеки КС КІІ у структурі ЦД;

- формування та реалізація оптимальних законів управління процесом компенсації (реалізація функцій протидії деструктивним впливам у КС КІІ інцидентів КС).

Існуючі парадигм (теоретико-методологічні моделі) щодо призначення та специфічних функціональних особливостей систем управління подіями інформаційної безпеки СУПІБ КІІ, які створені світовими компаніями і зараз починають інтенсивно використовуватися, свідчать про наступне. Жодна з наявних СУПІБ не може у повному обсязі забебзпечити бажане і надійне управління подіями безпеки і інформацією в КІІ. Відомо, що вказаним засобам безпеки притаманна низка суттєвих (щодо організації управління) недоліків, які

значно впливають на якість організації процесу забезпечення безпеки функціонування КІІ, а саме:

-функціональні обмеження, які накладаються властивостями конкретних КІІ;

-обмежену здатність щодо узгодженої інтерпретації інцидентів і подій безпеки на різних структурних ієрархічних рівнях СУІПБ КІІ;

-обмежені можливості щодо забезпечення заданої функціональної стійкості (відказостійкості) і надійності при зборі даних про інциденти безпеки;

-низький обсяг «масштабування» подій безпеки КС КІІ.

Враховуючи, що існуючі наразі традиційні методи та сучасні технології захисту безпеки КС не в повному обсязі можуть відповідати нагальним вимогам щодо надійності, стабільності та прогнозованості, було всебічно розглянуто та проаналізовано методи виявлення та реагування на аномалії безпеки в «цифровому» інформаційному просторі КІІ. Отримані результати надали змогу зробити висновок, що оптимальним із існуючих наразі методів є такий, в основу якого закладена ідеї ЦД.

Реалізація ЦД в управлінні інформаційними подіями безпеки КІІ дозволить суттєво підсилити стратегічні рішення, запобігти вартісним і ресурсним збоям, використовуючи сучасні аналітичні, прогностичні та моніторингові можливості цих еталонних програмних засобів.

Для проведення досліджень особливо акцентуємо увагу на тому, що ЦД – це комп'ютерні моделі фізичного і віртуального продукту чи процесу, або їхнього повного життєвого циклу, які синхронізовані в реальному часі за допомогою їх двостороннього зіставлення з реальними об’єктами, з метою прогнозування їх характеристик, усунення проблем та забезпеченням необхідної якості управління [3], [4].

Принцип їх функціонування полягає у постійній синхронізації і порівнянні, в реальному масштабі часу, інформаційних потоків КС КІІ, з метою моніторингу, оцінки та локалізації інформаційних подій безпеки та забезпеченні надійного функціонування СУІПБ КІІ.

Базуючись на фундаментальній теорії ГКЛДС, синтезуємо математичну модель *(S)* ЦД КІІ як інтегральну сукупність системних інваріантів, які описують структуру і процеси в таких системах:

$$S = S_1 \, U \, S_2 \, U \, S_3 \, U S_4 \, U \, S_5 \, U \, S_6$$

S-позначення інтегральної сукупності інваріантів ГКЛДС, яка описує ЦД;

S_1-опис гіперскладності системи, яка пов’язана з наявністю сукупності різнорідних елементів у ній із урахуванням їх специфічних властивостей;

S_2-опис динамічності, яка характеризує здатність елементів ГКЛДС до взаємодії, а також реалізація у повному обсязі міжсистемної взаємодії між ними;

S_3-опис структурності, яка характеризує послідовність, механізм і особливості реалізації взаємозв'язків між елементами системи;

S_4–опис цілісності, яка характеризує загальну властивість сукупності структурованих елементів системи в цілому, а не кожного з її окремих складових;

S_5-опис ієрархії, пов'язаної із наявністю різноманіття внутрішньосистемних рівнів, а також їх специфічних властивостей і закономірностей, які проявляються при функціонуванні ГКЛДС;

S_6- опис реалізуємості управління інформаційними процесами ГКЛДС за рахунок «гнучкої» інтеграції СУІПБ в її функціональну структуру.

Враховуючи особливу специфіку термінології, яка використовується при описі ГКЛДС і специфіки прогнозування станів цієї системи, відмітимо, що знак об'єднання множин U розглядаємо в цій моделі як «інтегральну сукупність інваріантів».

Результати проведених досліджень свідчать про те, що існування ГКЛДС і управління інформаційними процесами в ній, можливе лише у разі забезпечення її структурної цілісності усіх наведених інваріантних рівнів - складових її функціональних субсистем.

Висновки та перспективи.

Використовуючи синтезовану математичну модель *S,* підґрунтям якої є ГКЛДС, реалізовано прогнозне моделювання ЦД КІІ. Суть його полягає в тому, що модель описує її прогнозовані можливі стани, або, на багатовимірних прогнозах - сценарії подій. Завдяки використанню теорії ГКЛДС, втілена концепція реалізації ЦД для СУІПБ КІІ. Організація управління з використанням даних і симуляторів та розробленого програмного засобу ЦД, забезпечить виконання моніторингу, симуляції, прогнозування та оптимізацію процесу управління інформацією і подіями безпеки в цих структурах.

Таким чином, можливо зробити висновок, що застосування ЦД суттєво підвищить ефективність і безпеку функціонування цих структур.

Список використаних джерел

1. Jiaxing G. , Dongliang Z. , Chunxiang G., Xi C. , Xieli Z. Mengcheng J., An enhanced state-aware model learning approach for security analysis in lightweight protocol implementations, Journal of Cloud Computing: Advances, Systems and Applications, 2024, 13:28, P.2 – 17.

2. Tao F., Xiao B., Qi Q., Cheng J., Ji P., Digital twin modeling. J Manuf Syst 2022, 64:372–389.

3. Sholokhov S.M., Pavlenko P.M., Nikolaienko B.A., Samborsky I.I., Samborsky E.I., (2023/2024), The method of optimizing the distribution of radio suppression means and destructive software influence on computer networks. Radio Electronics, Computer Science, Control. 2023/2024. № 4 (67). P. 16-29.

4. Павленко П.М., Цифрові двійники та адитивні технології у металообробних галузях // Матеріали XIV Міжнародної науково-практичної конференції *«Комплексне забезпечення якості технологічних процесів і систем»,* 23 - 24 травня 2024 р. м. Чернігів, с.139-142.

Сташенко Віталій Олександрович
магістр 6 курсу, групи ІСДМ-64
Державний університет інформаційно-комунікаційних технологій
(098) 645-54-82
vstashenko@gmail.com
Науковий керівник: **Поперешняк Світлана Володимирівна**
к.ф.-м.н., доцент, доцент кафедри ІПІ ФІОТ
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
(098)-645-546-2
spopereshnyak@gmail.com

ОДИН З ПІДХІДІВ ДО ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ МОНІТОРИНГУ ГЕНЕРАЦІЇ ВИПАДКОВИХ ЧИСЕЛ ДЛЯ ІНТЕРНЕТУ

Постановка задачі. У сучасному світі Інтернет речей (IoT) охоплює все більше сфер життєдіяльності, від розумного будинку до інтелектуальних мереж. Надійність і безпека роботи IoT-пристроїв залежить від якості генерації випадкових чисел, які використовуються для криптографічного захисту даних, управління потоками інформації та інших ключових завдань. Актуальним є питання створення системи, здатної моніторити генерацію випадкових чисел, аналізувати їх відповідність статистичним критеріям і забезпечувати високу продуктивність навіть у пристроях із обмеженими ресурсами.

Мета дослідження є розробка системи моніторингу генерації випадкових чисел для IoT із використанням сучасних інструментів інформатизації та рішень у галузі діджиталізації. Пропонується інтеграція високопродуктивних алгоритмів аналізу якості випадкових чисел у комплексну інфраструктуру для моніторингу та забезпечення відповідності сучасним вимогам до безпеки та ефективності.

Результати дослідження. Аналіз літератури показав, що більшість існуючих рішень для генерації випадкових чисел у IoT фокусуються на криптографічних аспектах [1, 2]. Серед використовуваних алгоритмів виділяються:

- Псевдовипадкові генератори (PRNG), оптимізовані для програмних середовищ.
- Апартні генератори на основі програмованих логічних інтегральних схем (FPGA), які демонструють високу швидкість, але потребують значних ресурсів на впровадження [3, 4].
- Генератори на базі хаотичних систем, які забезпечують високу ентропію вихідних даних, але мають складність реалізації [5].

Проте у більшості рішень бракує інтегрованих інструментів моніторингу та статистичної оцінки якості випадкових чисел у реальному часі, що обмежує їх використання в IoT.

Розроблена система моніторингу включає такі компоненти:

1. Алгоритми генерації та тестування: Використано методи на основі рекомендацій NIST SP 800-22, зокрема тести для оцінки випадковості послідовностей.
2. Модуль збору та аналізу даних: Інтеграція з IoT-пристроями для збору та попередньої обробки даних.
3. Хмарна платформа: Для зберігання, обробки даних і машинного навчання використовуються хмарні рішення, що забезпечують масштабованість та гнучкість.

Реалізація та результати. Система була протестована на симуляційному середовищі, що включало розподілені IoT-пристрої. Досягнуто таких результатів:

- Скорочення часу перевірки послідовностей випадкових чисел на 40% порівняно з аналогами.
- Досягнення високої точності статистичного аналізу (понад 97%).
- Забезпечення безперебійної роботи системи навіть при пікових навантаженнях.

Для візуалізації результатів було розроблено графічний інтерфейс, що забезпечує моніторинг у реальному часі та формування звітів.

Висновки та перспективи. Запропонована система моніторингу генерації випадкових чисел демонструє високу ефективність і може бути інтегрована в існуючі IoT-системи. Використання сучасних підходів до діджиталізації дозволяє досягти високих стандартів якості та безпеки даних. У подальшому планується вдосконалення системи через інтеграцію алгоритмів машинного навчання для прогнозування та автоматичного виявлення аномалій.

Список використаних джерел

1. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Електронний ресурс] / [A. Rukhin, J. Soto, J. Nechvatal та ін.] // National Institute of Standards and Technology. – 2010. – URL: https://nvlpubs.nist.gov/nistpubs/Legacy /SP/nistspecialpublication800-22r1a.pdf.
2. Popereshnyak S. The Development and Testing of Lightweight Pseudorandom Number Generators [Електронний ресурс] / S. Popereshnyak, A. Raichev // IEEE. – 2021. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/9648659.
3. Arrow PRNG: A Pseudorandom Generator for IoT Applications. IEEE, 2022.
4. Chaotic Systems in Cryptography: Randomness Generation and Applications. ACM, 2023.
5. FPGA-Based Random Number Generators for IoT Devices. Elsevier, 2023.

Унєгова Діана Едуардівна
курсант 4 курсу, групи С-14
Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»
(063) 482-84-96
dianauniegova@gmail.com
Науковий керівник: **Шевчук Ольга Сергіївна**
викладач спеціальної кафедри №5 Інституту спеціального зв'язку та захисту інформації
Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ

ШИФРУВАННЯ ЯК ІНСТРУМЕНТ ПРОТИДІЇ ВИТОКУ ІНФОРМАЦІЇ ТА НЕСАНКЦІОНОВАНОМУ ДОСТУПУ

Постановка задачі. Шифрування даних є ключовим механізмом забезпечення кібербезпеки. Зростання кількості кібератак та витоків інформації робить захист даних одним із найважливіших пріоритетів для організацій та окремих користувачів. Шифрування дозволяє захистити інформацію, навіть якщо вона потрапила до рук зловмисників, адже зашифровані дані не можуть бути прочитані без відповідного ключа.

Мета дослідження. Метою дослідження є аналіз методів уникнення витоку інформації шляхом її шифрування.

Результати дослідження. У разі компрометації файлів чи баз даних їхній зміст залишатиметься недоступним для сторонніх осіб, завдяки шифруванню даних. Це є критично важливим для захисту конфіденційних даних, таких як фінансова інформація, персональні документи, корпоративна документація чи медичні записи. Шифрування забезпечує, щоб навіть у разі перехоплення дані не були використані зловмисниками.

Ще одним важливим аспектом шифрування є захист від несанкціонованого доступу. У багатьох випадках саме слабкий контроль доступу до інформації стає причиною інцидентів кібербезпеки. Завдяки використанню паролів та ключів, які потрібні для розшифрування даних, навіть у разі фізичного доступу до файлу зловмисник не зможе отримати зміст даних без відповідних облікових даних.

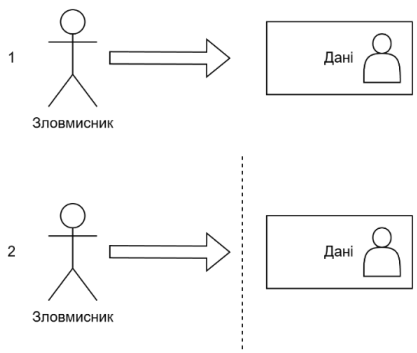

Рис. 1. Схема взаємозв'язку між зловмисником та даними користувача.

На рис. 1 представлені два варіанти передачі даних: без захисту та з використанням захисту. У першому варіанті дані зберігаються без жодного захисту. У такому випадку інформація залишається відкритою та доступною для будь-якої особи, яка має можливість отримати доступ до неї. Відсутність шифрування та обмежень на доступ створює значний ризик несанкціонованого доступу до даних, що може призвести до їх витоку або неправомірного використання. Це особливо небезпечно для конфіденційної інформації, такої як персональні дані чи важливі корпоративні документи.

У другому варіанті рис. 1 здійснюється шифрування і обмеження доступу, що забезпечує те, що навіть у разі перехоплення дані залишаються недоступними для сторонніх осіб без відповідного ключа дешифрування. Додатково, механізм обмеженого доступу дозволяє отримати інформацію лише авторизованим користувачам. Таким чином, впровадження захисту значно підвищує рівень безпеки та мінімізує ризик витоку або компрометації даних.

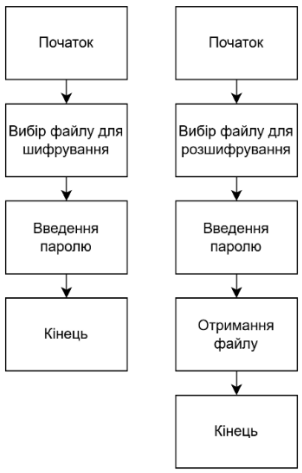

Рис. 2. Алгоритм дій.

Програмне рішення, алгоритм представлено на рис. 2, демонструє практичне застосування шифрування. За допомогою бібліотеки Fernet здійснюється перетворення даних у зашифровану форму. Ключ генерується на основі введеного пароля, що забезпечує надійність захисту. Додатково реалізовано механізм виявлення несанкціонованих спроб доступу, що підвищує рівень безпеки. Наприклад, програма фіксує багаторазові неправильні введення пароля, після чого блокує доступ, що дозволяє вчасно реагувати на можливі атаки [1].

Шифрування також є важливим з точки зору відповідності нормативним вимогам. Міжнародні стандарти, такі як GDPR (Загальний регламент захисту даних) чи PCI DSS (Стандарт безпеки даних платіжних карток), вимагають використання надійного шифрування для забезпечення конфіденційності. Це не лише захищає дані, але й дозволяє уникнути штрафів та втрати репутації у разі інцидентів [4, 5].

Таким чином, шифрування даних є невід'ємною частиною кібербезпеки. Воно не лише забезпечує захист інформації від витоків і несанкціонованого доступу, а й створює механізм протидії сучасним загрозам. Використання таких технологій є необхідною умовою для побудови надійного захисту в цифровій сфері, як для приватних осіб, так і для організацій.

Висновки та перспективи. В дослідженні розглянуто ключові аспекти шифрування даних як ефективного механізму захисту інформації від витоків та несанкціонованого доступу. Проведений аналіз показав, що відсутність шифрування робить дані вразливими до перехоплення та несанкціонованого використання, що є критичним ризиком для конфіденційної інформації, зокрема фінансових, корпоративних та особистих даних.

Шифрування дозволяє перетворити інформацію у зашифрований формат, який неможливо прочитати без відповідного ключа. Це забезпечує надійний захист навіть у випадках компрометації файлів чи баз даних. Додатково, обмеження доступу шляхом використання ключів або паролів мінімізує ризик несанкціонованих спроб отримання інформації.

Список використаних джерел

1. Fernet (symmetric encryption) using Cryptography module in Python. GeekForGeeks. Веб-сайт. URL: https://www.geeksforgeeks.org/fernet-symmetric-encryption-using-cryptography-module-in-python/.
2. Jonathan Katz. Introduction to modern cryptography. Second Editor. International Standard Book Number-13: 978-1-4665-7027-6 (eBook - PDF).
3. William Stallings. Cryptography and Network Security. Principles and Practice. Sixth Editor.
4. General Data Protection Regulation. GDPR. intersoft consulting. Веб-сайт. URL: https://gdpr-info.eu/.
5. The PCI Security Standards Council. PCI Security Standrts Council. Веб-сайт. URL: https://www.pcisecuritystandards.org/.

Шкурченко Олексій Анатолійович
аспірант кафедри Технічних систем кіберзахисту
Державного університету інформаційно-комунікаційних технологій
Аверічев Ігор Миколайович
к. е. н., доцент кафедри Технічних систем кіберзахисту
Державного університету інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0008-9766-0115
EMAIL: iaverichev19@gmail.com

ДОСЛІДЖЕННЯ МЕТОДІВ ТА МОДЕЛЕЙ ПРОТИДІЇ ГРУПОВИМ ЗАГРОЗАМ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Постановка задачі

Сучасні загрози, зокрема терористичні акти, організовані злочинні групи та інші форми групового насильства, стають все більш складними і небезпечними. Традиційні методи безпеки не завжди ефективні в умовах швидкої змінності таких загроз. Дослідження методів і моделей протидії груповим загрозам з використанням штучного інтелекту (ШІ) є важливим кроком до розробки ефективних систем для запобігання та реагування на такі загрози.

Мета дослідження

Мета даного дослідження полягає у створенні та оцінці ефективності методів і моделей на основі ШІ, які можуть бути використані для протидії груповим загрозам [4, 5]. Дослідження також передбачає аналіз існуючих рішень у цій галузі та виявлення їх переваг і недоліків.

Результати дослідження

Аналіз існуючих підходів. Було вивчено різні методи протидії загрозам, такі як відеонагляд з елементами розпізнавання облич, аналіз великих даних для виявлення аномалій у поведінці, а також технології безпілотних літальних апаратів для моніторингу потенційних загроз [1, 2].

Аналіз існуючих підходів до протидії кіберзагрозам може бути досить складним [3], оскільки загрози підлягають швидким змінам, а підходи до їхнього усунення постійно вдосконалюються.

На рис.1 представлено Модель дослідження методів протидії груповим загрозам за допомогою ШІ.

Рис. 1. Модель дослідження методів протидії груповим загрозам за допомогою ШІ

Наведемо перелік успішних та провальних випадків.

Успішні випадки

Програма Cybersecurity Framework від NIST (Національний інститут стандартів і технологій, США)

- ця програма допомагає організаціям у розробці та впровадженні ефективних кібернетичних стратегій.

- для покращення кібербезпеки більшість підприємств використовують стандарт, який призводить до зниження кількості інцидентів та підвищення загальної обізнаності про кіберзагрози.

Інцидентний центр реагування на комп'ютерні порушення (CERT)

- аналізуючи загрози та надаючи рекомендації з кіберзахисту CERT допомагає організаціям у реагуванні на кіберінциденти.

- які успішно спрацювали в багатьох випадках кібератак допомагаючи організаціям запобігти повторенням кіберінцендентів та зменшити час реагування.

Система раннього попередження (Threat Intelligence Sharing)

- полягає в обміні інформацією, про загрози між організаціями і державними структурами.

- що дозволяє швидко реагувати на нові загрози, ідентифікувати вразливості, надає можливість усувати їх до того, як зловмисники змогли завдати шкоди.

Провальні випадки

Використання застарілого програмного забезпечення

- полягає в тому що більшість організацій продовжують використовувати застарілі системи без відповідних оновлень.

- наведемо приклад WannaCry у 2020 році, коли тисячі систем були заражені через неоновлені версії Windows, призвело до масштабних втрат і простоїв у багатьох компаніях.

Неправильна конфігурація систем безпеки

- наведемо приклад, відомі випадки, коли організації мали належні технології кібербезпеки, але їх неправильно налаштували.

- неправильно налаштований сервер компанії Equifax, надало можливість зловмисникам викрасти дані понад 147 мільйонів осіб.

Відсутність підготовки та навчання персоналу.

- більшість інцидентів відбуваються через людський фактор, тобто зокрема відсутності навчання співробітників.

- у багатьох компаніях основною причиною витоку даних стали Фішинг-атаки. Наприклад, випадок з Sony Pictures у 2021 році, де працівники стали жертвами таких атак, що призвело до витоку конфіденційної інформації.

Розробка нових моделей.

На основі проведеного аналізу, інформація яку ми дізналися буде використана при розроблені нових алгоритмів кіберзахисту, що використовують машинне навчання для прогнозування ризиків та швидкої реакції на загрози.

Експериментальна перевірка. Нам надасть можливість підтвердили рівень точності і швидкості нових моделей у порівнянні з традиційними підходами.

Висновок

Аналізуючи успішні та провальні випадки, можна зробити висновок, що комплексний підхід, включаючи технології, навчання, обмін даними та відповідність стандартам безпеки, грає критичну роль у протидії кіберзагрозам. Підтримка постійного вдосконалення і адаптації підходів до нових загроз є ключем до ефективної кібербезпеки.

Дослідження показало, що ШІ має великий потенціал у протидії груповим загрозам. Створені моделі демонструють перевищення ефективності традиційних методів. Перспективи подальшого дослідження включають інтеграцію розроблених моделей у вигляді практичних інструментів для правоохоронних органів і галузей безпеки.

Очікується також, що подальше вдосконалення алгоритмів машинного навчання та їх адаптація до нових форм загроз значно підвищить загальний рівень безпеки.

Список використаних джерел

1. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

2. Bishop, C. M. (2006). Pattern Recognition and Machine Learning. Springer.

3. Djuric, P. M., & Yang, Y. (2016). Big Data for Social and Economic Research. Available at: [link].

4. Zhang, S., & Zhao, J. (2021). AI Techniques in Network Security. IEEE Transactions on Information Forensics and Security.

5. Shostak, A. (2019). Artificial Intelligence for Counter-Terrorism. Journal of Security Studies.

Бєліков Максим Романович
студент 3 курсу, групи ІП-24
Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"
(066) 583-79-88
maxbel2004@gmail.com
Бур Антон Олександрович
студент 3 курсу, групи ІП-22
Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"
(098) 594-16-51
anton.bur1337@gmail.com
Науковий керівник: **Поперешняк Світлана Володимирівна**
к.ф.-м.н., доцент, доцент кафедри ІПІ ФІОТ
Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"
(098)-645-546-2
spopereshnyak@gmail.com

БЛОКЧЕЙН-ТЕХНОЛОГІЇ ДЛЯ ПОБУДОВИ ФРІЛАНС БІРЖ

Постановка задачі. Фріланс-біржі є важливим елементом сучасної економіки, надаючи платформу для взаємодії між замовниками та виконавцями. Однак, існуючі біржі часто стикаються з рядом проблем, таких як високі комісії, ризик шахрайства, тривалі затримки платежів та залежність від посередників. Традиційні моделі не завжди можуть забезпечити прозорість та безпеку транзакцій, що стримує розвиток галузі. Застосування блокчейн-технологій може вирішити ці проблеми, зокрема через впровадження smart-контрактів та децентралізованих моделей роботи.

Мета дослідження. Метою цього дослідження є аналіз ефективності використання блокчейн-технологій для створення фріланс бірж нового покоління. Основна увага приділяється ролі smart-контрактів у забезпеченні прозорості, гарантуванні оплати та зменшенні комісійних витрат. Також розглядається вплив децентралізації на безпеку транзакцій та усунення залежності від посередників.

Результати дослідження. Для того, щоб подолати проблеми традиційних фріланс-бірж необхідно звернути увагу на технології, що забезпечують більшу прозорість та безпеку. Одним із основних інструментів, який може змінити роботу фріланс-бірж, є smart-контракти. Вони дозволяють автоматично виконувати умови угоди без потреби в посередниках, зменшуючи можливість шахрайства та підвищуючи ефективність платформи.

Smart-контракти – це самовиконувані програми, які працюють у децентралізованому середовищі блокчейн. Він може фіксувати умови співпраці

між замовником і виконавцем. Наприклад, замовник блокує кошти у контракті, які автоматично передаються виконавцю після підтвердження успішного виконання завдання. Цей тип фінансових угод називають escrow. У якості третьої сторони виступає smart-контракт, який тимчасово зберігає кошти або активи до виконання певних умов між двома сторонами (рисунок 1). Усі транзакції записуються в блокчейн, що унеможливлює їх підробку чи маніпуляцію. Завдяки децентралізації, платформи можуть функціонувати без необхідності в центральному органі управління, що знижує витрати на комісії.

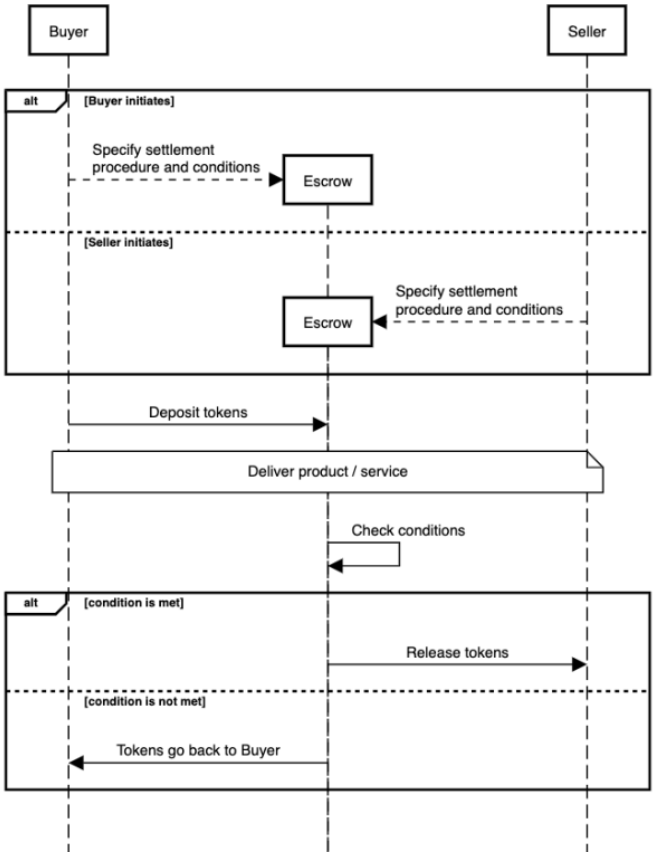

Рис. 1. Діаграма послідовностей escrow угоди між сторонами [2]

Децентралізація та криптографічний захист даних гарантують високий рівень безпеки. Smart-контракти усувають ризик невиконання зобов'язань, оскільки умови їх виконання строго закріплені в коді. Наприклад, навіть якщо одна зі сторін спробує ухилитися від зобов'язань, кошти залишаться заблокованими до виконання умов.

Впровадження оплат через блокчейн дозволяє зменшити середній рівень комісій характерних для традиційних платформ з 15-20% до 2-5%. А найпопулярніші платформи, такі як «Latium» [3], вже запровадили нульові комісії для верифікованих замовників та фрілансерів. Крім того, час обробки платежів скорочується з кількох днів до кількох хвилин, що є значною перевагою для виконавців. Для прикладу розглянемо проект із бюджетом $1000. Традиційна біржа з комісією 15% стягує $150, тоді як децентралізована платформа з комісією 3% – лише $30.

За даними опитування [1] станом на січень 2023 (рисунок 2), Ethereum є найпопулярнішою платформою з великим відривом. Це пояснюється 3 факторами: масштабованою екосистемою, надійністю та гнучкістю. Ethereum підтримує тисячі додатків, що створює мережевий ефект популярності. Цей блокчейн має перевірену часом архітектуру і найбільшу кількість активних розробників. Також великою перевагою є підтримка створення складних smart-контрактів. Наприклад, за допомогою Solidity [4] (мови програмування для Ethereum) можна створювати контракти, які автоматично виконують складні умови: такі як багатосторонні транзакції, динамічні зміни контрактів в залежності від зовнішніх подій, настання певного часу тощо. Це дозволяє створювати додатки, що включають дуже складну бізнес-логіку, таку як децентралізовані фінанси (DeFi) або невзаємозамінні токени (NFT).

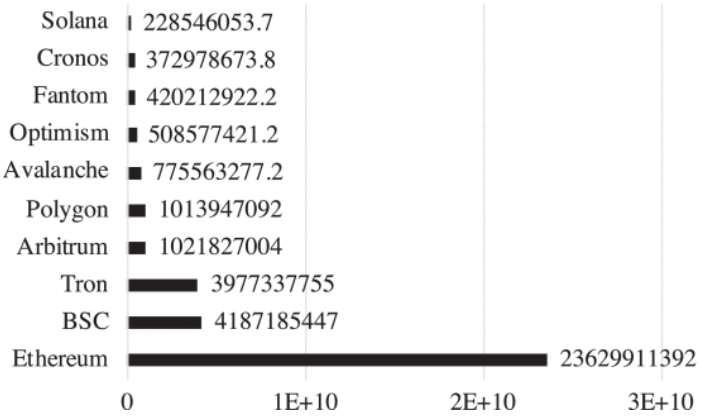

Рис. 2.Топ 10 блокчейнів із найбільшою кількістю доларів США залучених у децентралізованих додатках

Висновки та перспективи. Використання блокчейн-технологій у фріланс біржах відкриває нові можливості для створення прозорих, безпечних і ефективних платформ. Smart-контракти усувають необхідність посередників, значно знижуючи комісії та забезпечуючи швидке виконання транзакцій. Поточні дослідження підтверджують ефективність та вказують на перспективність у майбутньому. Таким чином, блокчейн може стати ключовим інструментом для трансформації фріланс-індустрії.

Список використаних джерел

1. Blockchain-Based Decentralized Application: A Survey. IEEE Xplore. URL: https://ieeexplore.ieee.org/abstract/document/10068327?figureId=fig3#fig3 (date of access: 14.12.2024).

2. Escrow - Blockchain Patterns. Blockchain Patterns. URL: https://web.archive.org/web/20240414011851/https://research.csiro.au/blockchainpatterns/general-patterns/blockchain-payment-patterns/escrow-2/ (date of access: 14.12.2024).

3. Latium. Bitcoin Freelance Marketplace. URL: https://latium.org/ (date of access: 14.12.2024).

4. Solidity Programming Language. URL: https://soliditylang.org/ (date of access: 14.12.2024).

Денисенко В’ячеслав Сергійович
студент 3 курсу, групи ІП-24
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
(050)-156-77-17
sl.denysenko@ukr.net
Науковий керівник: **Поперешняк Світлана Володимирівна**
к.ф.-м.н., доцент, доцент кафедри ІПІ ФІОТ
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
(098)-645-546-2
spopereshnyak@gmail.com

BLOCKCHAIN-ТЕХНОЛОГІЇ

Актуальність теми

Технології блокчейн стають важливим інструментом у сучасних умовах, оскільки вони забезпечують прозорість, безпеку та децентралізацію. Їх активно застосовують у таких сферах, як фінанси, логістика, охорона здоров’я та управління даними. Водночас використання блокчейн-систем стикається з низкою проблем, серед яких виділяють масштабованість, значне енергоспоживання, необхідність захисту конфіденційності та ризики атак на мережу. Наприклад, традиційні підходи, такі як алгоритм Proof-of-Work (PoW), забезпечують високий рівень безпеки, але вимагають значних енергетичних ресурсів, що робить їх недоцільними для багатьох сучасних завдань.

Мета дослідження

Це дослідження спрямоване на вивчення сучасних алгоритмів консенсусу, що застосовуються в блокчейн-системах, а також на визначення їхніх переваг і недоліків. Особливий акцент зроблено на розробці нових підходів, які поєднують сильні сторони традиційних алгоритмів із сучасними технологіями, щоб підвищити ефективність, безпеку й енергоефективність блокчейн-мереж.

Результати дослідження

Ключовою складовою кожної блокчейн-системи є алгоритм консенсусу, який відповідає за підтвердження транзакцій і додавання нових блоків до ланцюга. Найпоширеніші алгоритми мають свої особливості. Алгоритм Proof-of-Work (PoW), що використовується у Bitcoin, забезпечує надійний захист від атак, але характеризується значним енергоспоживанням та низькою швидкістю обробки транзакцій. Інший підхід, Proof-of-Stake (PoS), обирає учасників на основі кількості монет, якими вони володіють. Він дозволяє значно зменшити енергозатрати та збільшити швидкість роботи мережі, але ризикує сприяти централізації через концентрацію активів у великих учасників. У свою чергу, алгоритм Delegated Proof-of-Stake (DPoS) дозволяє учасникам мережі обирати делегатів, які виконують підтвердження транзакцій. Цей підхід забезпечує високу швидкість, але може знизити рівень децентралізації системи. Окрім того,

гібридні алгоритми, які поєднують механізми PoW і PoS, відкривають можливості для оптимального балансу між безпекою, швидкістю та енергетичною ефективністю.

Блокчейн-системи також демонструють значний потенціал у практичному застосуванні. Наприклад, у фінансовій сфері вони використовуються для криптовалютних операцій та реалізації смарт-контрактів. У логістиці технології блокчейн забезпечують прозорість поставок і контроль якості товарів. В охороні здоров'я вони застосовуються для збереження та обміну медичними записами, забезпечуючи конфіденційність даних. Водночас у галузі електронного голосування блокчейн дозволяє захищати результати виборів від маніпуляцій і втручання.

Висновки

Аналіз алгоритмів консенсусу показав, що кожен із них має свої переваги та обмеження, які визначають їхнє застосування в залежності від конкретної сфери. Так, PoW забезпечує високий рівень безпеки, але вимагає значних енергетичних витрат, тоді як PoS і DPoS дозволяють суттєво знизити енерговитрати, але потребують додаткових заходів для уникнення централізації. Гібридні підходи, які поєднують переваги різних алгоритмів, є перспективним напрямком розвитку блокчейн-технологій.

Перспективи розвитку

Подальші дослідження спрямовані на створення нових гібридних алгоритмів, які будуть поєднувати сильні сторони традиційних підходів і сучасних технологій, таких як машинне навчання. Зокрема, актуальним є завдання розробки енергоефективних систем із збереженням високої швидкості роботи та безпеки. Крім того, інтеграція блокчейн у державні та приватні структури дозволить підвищити прозорість і ефективність їхньої діяльності. Перспективним напрямком також є дослідження адаптивних блокчейн-систем, які автоматично підлаштовуватимуться до змін у навантаженні й умовах роботи.

Список використаних джерел

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.
2. Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. 2014.
3. Zheng Z., Xie S., Dai H., Chen X., Wang H. Blockchain challenges and opportunities: A survey. Int. J. Web Inf. Syst. 2018.
4. Nguyen C.D., Truong X.T. Efficient Blockchain consensus mechanisms for scalable applications. Comput. Sci. Cybern. 2021.

Іванченко Дмитро Сергійович
студент 6 курсу, групи ІСДМ-61
Державний університет інформаційно-комунікаційних технологій
(093) 604-41-71
ipadik1212@gmail.com
Науковий керівник: **Данильченко Валентина Миколаївна**
PhD, доцент кафедри Інформаційних систем та технологій
Державний університет інформаційно-комунікаційних технологій, м.Київ

ЗАСТОСУВАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ У ФІНАНСОВІЙ СФЕРІ

Постановка задачі. Дослідження застосування блокчейн-технологій у фінансовій сфері для підвищення безпеки та ефективності транзакцій.

Мета дослідження. Визначення можливостей блокчейн-технологій для розв'язання ключових проблем у фінансовій сфері та аналіз їхньої ефективності.

Результати дослідження. Блокчейн-технології вже застосовуються у фінансовій сфері, наприклад, у криптовалютах (Bitcoin, Ethereum) і фінансових токенах. Ці технології дають змогу проводити безпечні та прозорі транзакції без посередників. [1]

Порівняльний аналіз показує, що середній час проведення транзакцій у традиційних банківських системах становить від одного до трьох робочих днів, тоді як транзакції на блокчейн-платформах, таких як Bitcoin, займають від 10 до 60 хвилин, а на Ethereum - лише 20-30 секунд.

Крім того, вартість проведення транзакцій у традиційних банках значно вища: від 10 до 50 доларів США. У блокчейн-системах, таких як Bitcoin і Ethereum, вартість транзакцій становить від 0.5 до 5 доларів США, що робить їх більш економічними та доступними. [2]

Для моделювання фінансових транзакцій використовувалася платформа Ethereum. Приклад смарт-контракту мовою Solidity на рис.1 демонструє, як можна автоматизувати процеси передачі коштів за допомогою блокчейн-технологій. Це дає змогу мінімізувати участь людини і, відповідно, ймовірність помилок і затримок.

```
pragma solidity ^0.8.0;

contract SimpleTransaction {
    address public sender;
    address public receiver;
    uint256 public amount;

    constructor(address _receiver, uint256 _amount) {
        sender = msg.sender;
        receiver = _receiver;
        amount = _amount;
    }

    function executeTransaction() public {
        require(msg.sender == sender, "Only sender can execute transaction");
        payable(receiver).transfer(amount);
    }
}
```

Рис. 1. Моделювання фінансових транзакцій

Переваги блокчейн-технологій також можна продемонструвати за допомогою схем які зображені на рис.2. У традиційній транзакції гроші проходять через кілька посередників, таких як банки і центральні банки, що збільшує час і вартість переказу. У блокчейн-транзакції гроші передаються безпосередньо від відправника до одержувача через блокчейн-мережу, що значно спрощує і прискорює процес. [3]

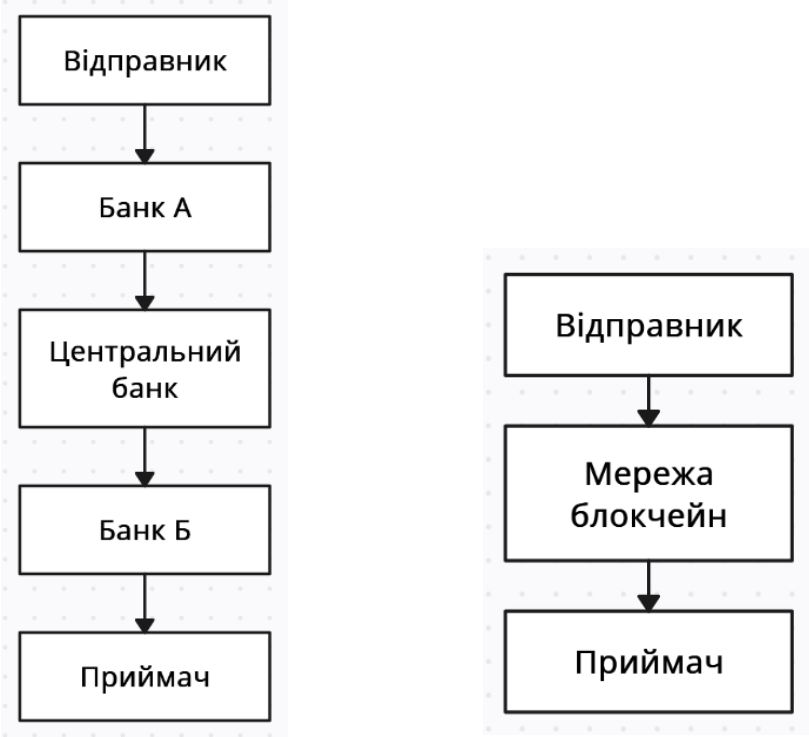

Рис. 2. Схема традиційної та блокчейн-транзакції

Аналіз проведених експериментів показав, що блокчейн-технології забезпечують вищу швидкість і менші витрати на проведення транзакцій порівняно з традиційними банківськими системами. [2] Крім того, блокчейн забезпечує високий ступінь безпеки завдяки використанню криптографії та децентралізованої структури даних. Це робить блокчейн-рішення привабливими для фінансових установ, які прагнуть підвищити ефективність і безпеку своїх операцій. [3]

Висновки та перспективи. Блокчейн-технології мають значний потенціал для підвищення безпеки та ефективності фінансових транзакцій. Їх застосування може призвести до зниження витрат і поліпшення прозорості у фінансовій сфері.

Перспективи використання блокчейн-технологій у фінансовій сфері охоплюють розробку нових фінансових продуктів і послуг, як-от смарт-контракти і децентралізовані фінансові платформи (DeFi). Ці інновації можуть змінити поточну фінансову інфраструктуру, надавши клієнтам більше контролю і прозорості. Також очікується розширення застосування блокчейн-технологій у різних секторах економіки, що може сприяти загальному поліпшенню фінансової системи та зниженню транзакційних витрат.

Список використаних джерел

1. Sinha S. How blockchain is driving innovation in financial services | IBM. *IBM - United States*. URL: https://www.ibm.com/think/topics/blockchain-for-financial-services (дата звернення: 15.12.2024).

2. Daley S. Blockchain in Finance: What It Is and How It's Used | Built In. *Built In*. URL: https://builtin.com/blockchain/blockchain-banking-finance-fintech (дата звернення: 15.12.2024).

3. Adel I. How Blockchain Is Transforming The Entire Financial Services Industry. Forbes. URL: https://www.forbes.com/councils/forbestechcouncil/2023/06/07/how-blockchain-is-transforming-the-entire-financial-services-industry/ (дата звернення: 15.12.2024).

Соломоденко Максим Олександрович
студент 6 курсу, групи ІСДМ-61
Державний університет інформаційно-комунікаційних технологій
(063)516-05-48
maxim.solomodenko@gmail.com
Науковий керівник: **Герцюк Микола Модестович**
доктор філософії,
доцент кафедри технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій, м. Київ

МЕТОД ВЕКТОРНОГО ПОЛЯ ДЛЯ ПЛАНУВАННЯ ТРАЄКТОРІЇ РУХУ АВТОНОМНОГО ТРАНСПОРТНОГО ЗАСОБУ В УМОВАХ ДИНАМІЧНИХ ПЕРЕШКОД

Постановка задачі. Планування траєкторії руху автономних транспортних засобів в умовах динамічних перешкод вимагає ефективних методів, що забезпечують безпечну навігацію при обмежених обчислювальних ресурсах[1]. Існуючі підходи часто вимагають складних сенсорних систем та значних обчислювальних потужностей, що ускладнює їх застосування в малогабаритних та бюджетних рішеннях. Перспективним напрямком є використання модифікованого методу векторного поля з адаптивними параметрами та прогнозуванням руху перешкод[2]. Такий підхід забезпечує ефективну навігацію при мінімальних вимогах до апаратного забезпечення та дозволяє реалізувати систему на простих мікроконтролерах[3].

Мета дослідження. Розробка та оптимізація методу векторного поля для планування траєкторії руху малогабаритних автономних транспортних засобів з урахуванням динамічних перешкод та обмежень на маневреність. Дослідження спрямоване на створення алгоритму, що забезпечує безпечну навігацію при мінімальних вимогах до апаратного забезпечення.

Результати дослідження. В рамках проведеної роботи було розроблено та експериментально досліджено модифікований метод векторного поля для планування траєкторії руху автономного транспортного засобу. Ключовою інновацією запропонованого підходу стала реалізація адаптивної системи налаштування параметрів відштовхування від перешкод, що базується на комплексному аналізі даних інфрачервоного сенсора відстані. Розроблена система враховує не лише безпосередню відстань до перешкоди, але й динамічні характеристики руху транспортного засобу, включаючи його поточну швидкість та прискорення, що дозволяє забезпечити більш природне та безпечне маневрування.

Експериментальні дослідження проводились у спеціально обладнаному лабораторному середовищі розміром 4x6 метрів з використанням розробленої малогабаритної платформи. Тестова установка базувалась на мікроконтролері STM32F3Discovery та включала інфрачервоний сенсор відстані з робочим діапазоном 10-80 сантиметрів, два мотори постійного струму з драйвером L298N

та літій-іонний акумулятор ємністю 2200 мАг. Поверхня тестового полігону була покрита ламінатом для забезпечення стабільних умов зчеплення коліс, а освітлення підтримувалось на рівні 500-700 люкс для оптимальної роботи інфрачервоних сенсорів.

Методологія тестування включала три основні етапи. На першому етапі проводилось базове тестування навігаційних можливостей системи, що включало рух по прямій на різні відстані та виконання поворотів на задані кути. Другий етап був присвячений дослідженню ефективності алгоритму уникнення перешкод при різних конфігураціях їх розташування. На третьому етапі проводилось комплексне тестування системи в умовах, що імітують реальні сценарії застосування. Результати базового тестування продемонстрували високу точність руху по прямій з похибкою всього 1.5-3.4%, що є відмінним показником для систем даного класу. Точність виконання поворотів також виявилась на високому рівні - відхилення від заданого кута не перевищувало 2.4-2.5%. При дослідженні алгоритму уникнення перешкод система показала успішне маневрування у 90% випадків при простих сценаріях з одиночними перешкодами, зберігаючи при цьому стабільну роботу на швидкостях до 0,3 м/с. Особливу увагу було приділено дослідженню точності позиціонування при різних швидкостях руху. Експерименти показали, що при швидкості 0,1 м/с середня похибка визначення положення становила 2.3%, збільшуючись до 3.1% при підвищенні швидкості до 0,2 м/с. При цьому система зберігала здатність ефективно уникати перешкод та підтримувати задану траєкторію руху. Важливо відзначити, що навіть при максимальній тестовій швидкості 0,3 м/с система демонструвала стабільну роботу та надійне виявлення перешкод. Окремого розгляду заслуговує енергоефективність розробленої системи. При проведенні тривалих тестів тривалістю до 2 годин система демонструвала стабільну роботу від одного заряду акумулятора, споживаючи в середньому 150 мА при русі. Це підтверджує можливість тривалого автономного функціонування системи, що є важливим фактором для практичного застосування. Розроблена система також продемонструвала високу обчислювальну ефективність - алгоритм векторного поля та система обробки сенсорних даних використовували лише 60% обчислювальних ресурсів мікроконтролера, залишаючи достатній запас для можливого розширення функціоналу в майбутньому. Це підтверджує правильність обраного підходу до оптимізації алгоритмів та можливість їх реалізації на доступних обчислювальних платформах.

Висновки та перспективи. Розроблений метод забезпечує ефективне планування траєкторії при низьких обчислювальних витратах та мінімальному наборі сенсорів. Експериментальні результати підтверджують надійність системи в реальних умовах експлуатації. Подальші дослідження спрямовані на вдосконалення алгоритмів прогнозування руху динамічних перешкод та оптимізацію траєкторій за енергоефективністю.

Список використаних джерел

1. Titterton, D., & Weston, J. L. (2004). Strapdown inertial navigation technology (2nd ed.). Institution of Engineering and Technology

2. Borenstein, J., & Koren, Y. (1991). The vector field histogram-fast obstacle avoidance for mobile robots.
3. O. Khatib. (1986). Real-time obstacle avoidance for manipulators and mobile robots. International Journal of Robotics Research.

Столяр Олена Валентинівна
студентка 6 курсу, групи ІСДМ-63
Державний університет інформаційно-комунікаційних технологій
(096) 300-44-35
Dublin.olena@gmail.com
Науковий керівник: **Бондарчук Андрій Петрович**
д.т.н., професор
Державний університет інформаційно-комунікаційних технологій, м. Київ

РОЛЬ BLOCKCHAIN У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ЦИФРОВОЇ ІДЕНТИФІКАЦІЇ ПАЦІЄНТІВ

Постановка задачі. У сучасному світі інформатизація охоплює всі сфери людської діяльності, включаючи охорону здоров'я. Ефективне управління медичною інформацією вимагає впровадження безпечних та надійних систем цифрової ідентифікації пацієнтів. Однак існують серйозні проблеми, пов’язані з кіберзагрозами, несанкціонованим доступом до медичних даних та втратою конфіденційності. Системи електронної ідентифікації (EHR) мають суттєвий потенціал [1], але вони часто стають мішенню для хакерських атак. Центральні сервери, які використовуються для зберігання даних, можуть бути скомпрометовані, що піддає ризику безпеку даних пацієнтів.

Blockchain-технологія пропонує інноваційне рішення для створення безпечних і надійних систем цифрової ідентифікації. Основною задачею є дослідження можливостей Blockchain у забезпеченні конфіденційності, захисту даних та доступності інформації для авторизованих користувачів.

Мета дослідження. Метою дослідження є аналіз можливостей застосування технології Blockchain для забезпечення безпеки цифрової ідентифікації пацієнтів у системах охорони здоров’я.

Результати дослідження. Blockchain використовує технологію розподілених реєстрів, яка забезпечує інноваційний спосіб надійного зберігання та передачі інформації навіть через незахищені канали. Вся інформація мережі блокчейн зберігається на численних комп'ютерах, які називаються «вузлами». Дані, що додаються до реєстру, організовуються у блоки. Оскільки блоки мають обмежену здатність до зберігання, нові блоки постійно додаються до реєстру, утворюючи ланцюг [1]. Технологія blockchain також використовує криптографічні хеш-значення для зв'язування блоків та цифрові підписи, створені за допомогою асиметричної криптографії, для забезпечення безпеки транзакцій (Рис.1) . Завдяки цьому вузли мережі можуть здійснювати транзакції без необхідності у зовнішньому контролі або участі третіх осіб, що значно знижує ризики маніпуляцій і підвищує довіру до системи [2].

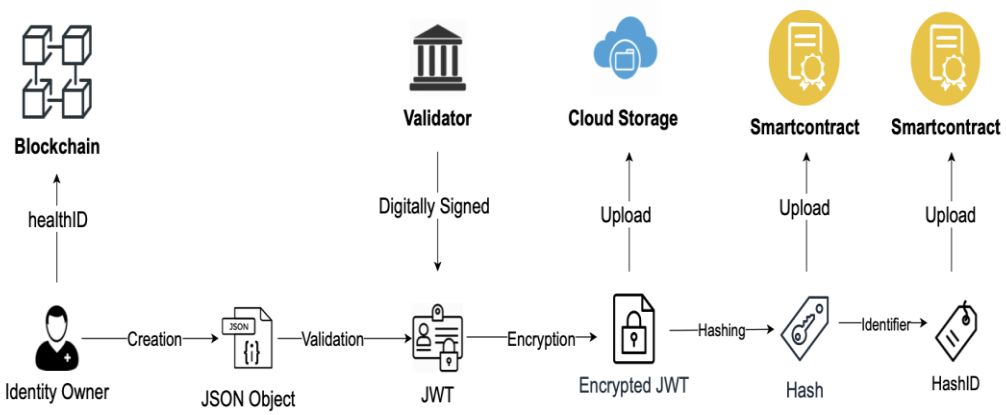

Рис.1 Огляд цифрової медичної ідентифікації [2]

У контексті цифрової ідентифікації смарт-контракти відіграють важливу роль, оскільки автоматизують процеси верифікації особистих даних та забезпечують їх безпеку за допомогою технології блокчейн. Це дозволяє зменшити ризик підробки інформації або шахрайства, оскільки кожна дія, пов'язана з ідентифікацією, фіксується у вигляді транзакції, яка є незмінною та доступною для перевірки [3]. Одним з основних переваг смарт-контрактів є їх здатність забезпечувати автоматичне виконання контрактів на основі заздалегідь визначених умов. Наприклад, у сфері охорони здоров'я смарт-контракти можуть автоматично підтверджувати автентичність пацієнта перед виконанням медичних процедур або перевіркою страховки. Це значно пришвидшує процеси обробки даних і дозволяє знизити час очікування, а також зменшити адміністративне навантаження.

В охороні здоров'я медичні дані зберігаються та керуються як електронні медичні записи (EMR). Використання блокчейн-технології для підтримки EMR дозволяє автоматично зберігати інформацію про пацієнта в мережі блокчейн. Оскільки дані на блокчейні фіксуються незмінно, неможливо змінити або підробити EMR без порушення системи [3].

У процесі постачання ліків блокчейн дозволяє ефективно управляти запасами та знижувати ймовірність підробок і крадіжок. Завдяки таким властивостям, як прозорість, незмінність і можливість аудиту, блокчейн покращує безпеку, цілісність та ефективність ланцюга постачання ліків.

Використання блокчейн-технологій може допомогти усунути багато проблем, пов'язаних з людськими помилками, дублюваннями та помилковими рахунками в охороні здоров'я. Інтеграція блокчейну в процеси виставлення рахунків та врегулювання претензій сприяє оптимізації цих процесів, знижуючи витрати та покращуючи ефективність адміністративних операцій.

Технологія блокчейн відкриває широкі можливості для забезпечення безпеки та ефективного управління медичними даними. Її ключові характеристики, такі як децентралізація, незмінність, узгодженість і високий рівень захисту, дозволяють створювати надійні системи зберігання медичної інформації, уникаючи залучення централізованих органів. Проте, впровадження блокчейну в медичну сферу супроводжується певними викликами, серед яких

масштабованість, управління сховищами, продуктивність алгоритмів консенсусу, конфіденційність даних і регуляторні питання.

Висновки та перспективи. Блокчейн-технології мають значний потенціал для зберігання та управління медичними даними, але їхнє впровадження потребує вирішення технічних, економічних і регуляторних викликів. Попри це, можливості технології дозволяють створити ефективні системи, які сприяють підвищенню рівня безпеки, конфіденційності й доступності медичних даних . Отримані результати можуть слугувати основою для подальших досліджень і розробок у цій галузі, а також для впровадження інновацій у практику медичних установ.

Список використаних джерел

1. Cornelius, C. Agbo, et al. Blockchain Technology in Healthcare: A Systematic Review // Healthcare. – 2019. DOI: 10.3390/healthcare7020056.

2. Javed, I.T.; Alharbi, F.; Bellaj, B.; Margaria, T.; Crespi, N.; Qureshi, K.N. Health-ID: A Blockchain-Based Decentralized Identity Management for Remote Healthcare. *Healthcare* 2021, **9**, 712. https://doi.org/10.3390/healthcare9060712.

3. Seyam, Huda, Habbal, Adib. A Systematic Review of Blockchain-Based Identity Management Solutions // Proceedings of the 1st International Conference on Recent Academic Studies. – May 2–4, 2023. Konya, Turkey.

Бацунов Дмитро Сергійович
студент 6 курсу, групи ПДМ-62
Державного університету інформаційно-комунікаційних технологій
batsunovdima38@gmail.com
Науковий керівник: **Жебка Вікторія Вікторівна**
доктор технічних наук, професор,
завідувач кафедри Технологій цифрового розвитку,
Державного університету інформаційно комунікаційних технологій, м. Київ

РОЗРОБКА МЕТОДИКИ ОРГАНІЗАЦІЇ СПІЛЬНИХ ПАСАЖИРСЬКИХ ПЕРЕВЕЗЕНЬ НА ОСНОВІ ХМАРНИХ ТЕХНОЛОГІЙ

Постановка задачі. У сучасному світі проблема транспортних заторів та зниження викидів вуглекислого газу стає все більш актуальною. Спільні пасажирські перевезення, є ефективним рішенням для зменшення кількості автомобілів на дорогах та економії витрат на проїзд. Однак, їх організація вимагає розробки надійної методики, яка враховує планування маршрутів, узгодження розкладів пасажирів та водіїв, забезпечення безпеки та конфіденційності учасників. Основне завдання полягає у створенні системи, яка використовує хмарні технології для ефективного та зручного управління спільними поїздками.

Мета дослідження. Метою цього дослідження є розробка методики організації спільних пасажирських перевезень на основі хмарних технологій. Це включає розробку алгоритмів для оптимізації маршрутів, забезпечення узгодження розкладів між пасажирами та водіями, а також інтеграцію з хмарними сервісами для зберігання та обробки даних. Особлива увага приділяється створенню безпечної та надійної платформи, яка забезпечить конфіденційність та зручність для всіх учасників.

Результати дослідження. У результаті дослідження було розроблено методику організації спільних пасажирських перевезень, яка використовує переваги хмарних технологій а саме: Sygic API для аналізу дорожнього покриття та трафіку, OpenWeatherMap для аналізу метеорологічних показників, AWS SQS Queue та AWS Aurora DB Service для відмовостійкості та ізоляції запитів на запис/читання з можливістю масштабування відповідно. Також було розроблено алгоритм розрахунку маршруту побудований на графі, перша формула створена для розрахунку ваги ребра графа, беручи до уваги можливість саме спільних перевезень

$$W = \sum_{k} Ck * ik$$

Ck – враховані значення(дистанція, час, витрата, кількість пасажирів, наявність вже існуючого маршруту, завантаження дороги та погодні умови)

ik – індекси важливості кожного врахованого значення (може змінююватимь в залежнлсть від пріорітету відданого певним значенням)

Крім розробленої формули підрахунку ваги ребра графа було використано формулу Флойда-Уоршела задля знаходженню найкоротших шляхів між усіма вершинами графа. Ключовою перевагою цього алгоритму стала можливість розраховувати шлях між усіма наявними вершинами, оскільки спільні перевезення можуть потребувати перерахунку маршруту, саме цей підхід дав можливість розраховувати основні показники ще до запиту на перевезення. Тобто заявлена формула відкрила можливість ще до фактичного запиту визначити можливість такого перевезення що значно зменшило час на відповідь.

Висновки та перспективи. Запропоновані алгоритми оптимізації маршрутів дозволяють ефективно розподіляти пасажирів між водіями, мінімізуючи час у дорозі та витрати на проїзд. Система інтегрована з хмарними сервісами, що забезпечує зберігання та обробку великих обсягів даних у реальному часі та актуальний стан маршруту. Проведені тести показали високу ефективність та надійність системи в умовах реального використання.

Запропонована методика організації спільних пасажирських перевезень на основі хмарних технологій демонструє значний потенціал для покращення міських транспортних систем. Система дозволяє зменшити кількість автомобілів на дорогах, що сприяє зниженню викидів вуглекислого газу та економії витрат на паливо. Подальші дослідження можуть бути зосереджені на вдосконаленні алгоритмів оптимізації маршрутів, інтеграції з іншими транспортними системами та розробці додатків для покращення взаємодії користувачів із системою.

Список використаних джерел

1. Amazon simple queue service documentation. *Amazon Web Services, Inc.*URL: https://docs.aws.amazon.com/sqs/(дата звернення: 14.12.2024).
2. Navigation API. *Sygic*. URL: https://www.sygic.com/developers/professional-navigation-sdk/windows/api-examples/navigation-api(date of access: 14.12.2024).
3. OLTP database, mysql and postgresql managed database - amazon aurora - AWS. *Amazon Web Services, Inc.*URL: https://aws.amazon.com/rds/aurora/(date of access: 14.12.2024).

Гангало Ігор Миколайович
старший викладач кафедри Технологій цифрового розвитку
Державного університету інформаційно-комунікаційних технологій, м. Київ
(097)-762-38-78
gangalo.im@gmail.com
Читулян Вадим Олегович
викладач кафедри Технологій цифрового розвитку
Державного університету інформаційно-комунікаційних технологій, м. Київ
(067)-177-68-05
chitulyanvadum@gmail.com

ХМАРНІ ОБЧИСЛЕННЯ ТА ЇХ ЗНАЧЕННЯ ДЛЯ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ

Постановка задачі

У сучасних умовах цифрової трансформації малий та середній бізнес (МСБ) змушений адаптуватися до швидких змін у ринкових умовах. Задля підвищення конкурентоспроможності ключовим завданням є скорочення витрат на IT-інфраструктуру, оптимізація операційних витрат та забезпечення доступу до передових технологій. Потреба у рішеннях, що дозволяють підвищити ефективність при обмежених ресурсах, робить хмарні обчислення важливим об'єктом досліджень.

Мета дослідження

Дослідити можливості впровадження хмарних обчислень у МСБ та оцінити їх ефективність у скороченні капітальних і операційних витрат, а також визначити вплив на масштабованість і конкурентні переваги.

Результати

Економічний аналіз свідчить, що використання хмарних технологій дозволяє значно скоротити витрати на IT-інфраструктуру [1]. Відсутність необхідності інвестувати в дороге обладнання, таке як сервери та системи зберігання даних, скорочує витрати до 40%. Перехід на модель операційних витрат замість капітальних забезпечує гнучкість у використанні ресурсів, коли компанії сплачують лише за фактично використані послуги [1]. Зменшення витрат на електроенергію та обслуговування обладнання досягає 30%, а перенесення технічних завдань на провайдерів хмарних послуг знижує потребу у внутрішньому IT-персоналі.

Хмарні сервіси забезпечують можливість швидкого розширення або скорочення ресурсів залежно від потреб бізнесу. Це дозволяє компаніям економити час на налаштування та впровадження нових сервісів, що в середньому скорочує час реалізації проектів на 25%. Доступ до сучасного програмного забезпечення та автоматичних оновлень без додаткових витрат підвищує продуктивність і конкурентоспроможність бізнесу [2]. Аналіз показує, що завдяки гнучкості масштабування та уникненню простоїв обладнання

досягається значна економія ресурсів, а автоматизація процесів сприяє зростанню ефективності співробітників.

Прогнозованість витрат є важливою перевагою хмарних обчислень [2]. Завдяки прозорим тарифам компанії можуть чітко планувати бюджети на IT, мінімізуючи ризики неочікуваних витрат на технічне обслуговування.

Висновки

Хмарні обчислення демонструють високу економічну ефективність для МСБ, дозволяючи значно скоротити витрати та оптимізувати операційні процеси. Використання хмарних технологій сприяє підвищенню конкурентоспроможності завдяки швидкому доступу до сучасних інструментів та автоматизації процесів. Масштабованість і прозорість витрат роблять хмарні обчислення привабливим рішенням для компаній, які прагнуть гнучкості у веденні бізнесу. Підсумовуючи, хмарні обчислення є важливим інструментом для забезпечення сталого розвитку малого та середнього бізнесу в умовах цифрової економіки.

Список використаних джерел

1. Голячук Н. В., Голячук Є.С., and В. Рихлюк В.С. Хмарні обчислення: завтрашній день бізнесу. Економічні науки. Серія: Облік і фінанси №11. 2014, с.37-43.
2. Фершлядин М. М. Безпека використання хмарних технологій у бізнес процесах. Матеріали VIII науково-технічної конференції "Інформаційні моделі, системи та технології". 2020, с.67.

Бажан Тетяна Олександрівна
старший викладач
Державний університет інформаційно-комунікаційних технологій, м. Київ
+38 (097) – 803 – 34 – 49

ОЧИСТКА ДАНИХ ДЛЯ ГРАДІЄНТНОГО БУСТИНГУ У ПРОГНОЗУВАННІ ІНВЕСТИЦІЙ

Постановка задачі. У сучасних умовах цифрової трансформації економіки проблема прогнозування інвестицій є актуальною для формування ефективних стратегій розвитку держави та бізнесу. Проте якість даних, що використовуються у моделях машинного навчання, значно впливає на точність прогнозів. Основною задачею є розробка ефективних методів очистки даних для покращення результатів прогнозування, зокрема для методу градієнтного бустингу (Gradient Boosting) [1, 4].

Мета дослідження. Метою дослідження є визначення та застосування ефективних методів очистки даних для підвищення якості роботи методу машинного навчання, а саме градієнтного бустингу (Gradient Boosting), для прогнозування інвестицій.

Результати дослідження. В рамках дослідження проведено аналіз джерел помилок у даних, таких як пропуски, аномалії, дублікати та некоректні значення. Запропоновано наступний алгоритм очистки даних:

1. Виявлення та обробка пропусків.
- Застосовано методи заповнення пропусків, такі як середнє арифметичне, медіана та метод найближчих сусідів (k-NN) [2].
2. Обробка аномалій.
- Для ідентифікації аномальних значень використано методи локальної щільності (LOF) та квартильний метод (IQR) [1].
3. Видалення дублікатів.
- Автоматизоване виявлення та видалення повторюваних записів.
4. Масштабування та нормалізація.
- Приведення даних до уніфікованого масштабу для підвищення ефективності градієнтного бустингу [4].

На основі очищених даних було виконано побудову моделі прогнозування інвестицій за допомогою градієнтного бустингу. Як показують дослідження, використання методів очистки даних дозволяє покращити точність моделей на 10-20% у середньому [4].

Висновки. Проведене дослідження підтвердило важливість якісної очистки даних для покращення результатів прогнозування. Запропонований алгоритм очистки забезпечує підвищення точності градієнтного бустингу, що є критично важливим для ухвалення інвестиційних рішень. У подальшому

планується апробація розробленого підходу на інших методах машинного навчання.

Список використаних джерел:

1. Гудз, П. М. Машинне навчання та аналіз даних. Київ: Наукова думка, 2022.
2. Smith, J. Data Cleaning Techniques in Machine Learning. Springer, 2021.
3. Brown, A. Regression Analysis for Investment Prediction. Wiley, 2020.
4. Ponti, M. A., Oliveira, L. de A., Esteban, M., Garcia, V., Román, J. M., & Argerich, L. Improving Data Quality with Training Dynamics of Gradient Boosting Decision Trees. arXiv preprint arXiv:2210.11327, 2022.

Горбань Андрій Миколайович
студент 6 курсу, групи ПДМ-62
Державного університету інформаційно-комунікаційних технологій
mag2385574@stud.duikt.edu.ua
Науковий керівник: **Золотухіна Оксана Анатоліївна**
кандидат технічних наук, доцент, доцент кафедри ІПЗ
121 інженерія програмного забезпечення
Державного університету інформаційно-комунікаційних технологій, м. Київ

АВТОМАТИЗОВАНА СИСТЕМА ПОПЕРЕДНЬОЇ ОБРОБКИ КОРИСТУВАЦЬКИХ ВІДГУКІВ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ЗБАГАЧЕННЯ ДАНИХ

Постановка задачі.

У сучасному цифровому світі користувацькі відгуки є цінним джерелом інформації для аналізу споживчих настроїв, вдосконалення продуктів та послуг, а також підтримки прийняття управлінських рішень. Вони містять унікальну інформацію щодо якості продуктів, послуг та рівня задоволеності користувачів. Управління та аналіз величезної кількісті відгуків користувачів на товари або послуги, є дуже складною проблемою: низька якість тексту відгуків, наявність шуму у текстових даних, їх неповнота потребує попередньої обробки таких даних, а їх великий обсяг та постійне поповнення новими даними потребує вирішення питання їх обробки ефективним способом. Традиційні підходи обробки текстових даних обмежуються здебільшого базовими підходами до очищення та нормалізації, однак цього недостатньо для забезпечення якості результату достатнього для їх точного аналізу, особливо при використанні автоматизованих методів, таких як кластеризація чи машинне навчання. Використання методів збагачення даних, таких як інтеграція зовнішніх знань, лексичних ресурсів та інших джерел дозволяє отримати додаткову приховану інформацію з відгуків та покращити точність їх аналізу.

Мета розробки. Підвищення ефективності процесу обробки відгуків користувачів за рахунок автоматизації процесу попередньої обробки.

Результати розробки. Для підвищення якості текстових даних відгуків користувачів з онлайн-платформ пропонується використання сучасних інформаційних технологій шляхом розробки автоматизованої системи їх збору та попередньої обробки з використанням сучасних методів збагачення тексту.

Першим етапом проектування інформаційної системи є визначення її структури та виділення структурних складових [1]:

1) Data Collection – збір відгуків користувачів з онлайн-платформ засобами вебскрейпінгу та API платформ;

2) Data Storage – зберігання системних даних, відгуків користувачів, шляхів доступу до переліків та словників для їх попередньої обробки та результати обробки (SQL Server) [2];

3) User Interface – кросплатформний web-інтерфейс користувача системи для налаштування та відображення результатів роботи;

4) Data Analysis – виконання подальшого аналізу попередньо оброблених текстових даних відгуків (категоризація, аналіз настроїв, побудова хмар тегів).

5) Data Preprocessing (Data Cleaning та Data Enrichment) – виконує попередню обробку текстів відгуків видаленням «шуму» та методами збагачення даних (Python) [3-4];

6) Task Scheduling – фонове виконання за розкладом задач отримання та збереження користувацьких відгуків (Hangfire) [5].

Розроблену структуру автоматизованої системи наведено на рисунку 1.

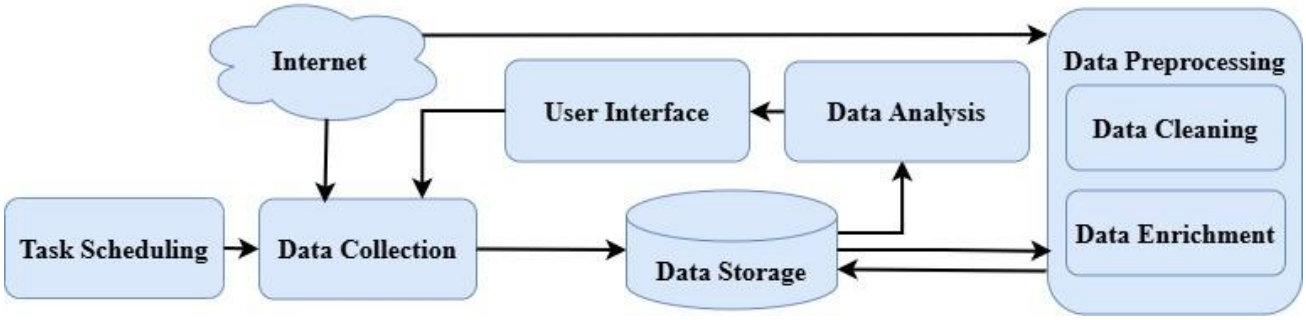

Рис. 1. Структура автоматизованої системи

Висновки та перспективи. Для ефективної реалізації спроектованої системи необхідно врахувати питання безпеки, продуктивності та адаптивності компонентів, реалізувати інтеграцію зовнішніх джерел даних, механізми попередньої обробки відгуків та аналізу його результатів.

Список використаних джерел

1. Architect Modern Web Applications with ASP.NET Core and Azure. [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/dotnet/architecture/modern-web-apps-azure/ (дата звернення 15.09.2024). – Назва с екрану.

2. SQL Server technical documentation. [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/sql/sql-server/?view=sql-server-ver16 (дата звернення 15.09.2024). – Назва с екрану.

3. Lopez F. Mastering Python. Regular Expressions / F.Lopez, V.Romero : Packt Publishing. – 2014. – 97 p.

4. Bird S. Natural Language Processing with Python / S. Bird, E. Klein, E.Loper: O'Reilly Media. – 2009. – 504 p

5. Hangfire.Documentation. [Електронний ресурс]. – Режим доступу: https://docs.hangfire.io/en/latest/ (дата звернення 15.09.2024). – Назва с екрану.

Крискун Іван Миколайович
Аспірант 1 курсу
Університет «КРОК»
0672207511
ivan.kriskun@gmail.com
Зайченко Сергій Петрович
Аспірант 2 курсу, групи АІСД-21
Державний університет інформаційно-комунікаційних технологій
0730030943
sergiy.zaychenko@gmail.com
Білавка Володимир Богданович
Аспірант 2 курсу, групи АІСД-21
Державний університет інформаційно-комунікаційних технологій
0934746665
vladimir.bilavka@huawei.com

ШТУЧНИЙ ІНТЕЛЕКТ У РОЗРОБЦІ І УПРАВЛІННІ ІТ-ПРОЕКТАМИ

Постановка задачі. Штучний інтелект (ШІ) стає невід'ємною частиною розробки ІТ-продуктів. Він не лише прискорює процеси, а й підвищує їхню якість та ефективність. Глобальний ринок ШІ в ІТ-індустрії, за дослідженнями, досягне $271,9 млрд до 2028 року зі середньорічним темпом зростання 27,1%. Зростаючий попит на автоматизацію бізнес-процесів, підвищення ефективності та інновації стимулює активне впровадження ШІ у всі етапи розробки програмного забезпечення.

ШІ оптимізує бізнес-процеси та покращує продуктивність, дозволяючи виконувати монотонні завдання швидше й точніше, ніж людина. Аналіз великих обсягів даних і виявлення закономірностей сприяє прийняттю більш обґрунтованих рішень. Використання ШІ розширюється, проникаючи у всі сфери бізнесу та повсякденного життя, особливо у розробці ІТ-продуктів.

Мета дослідження. Метою дослідження розробка рекомендацій з використання сучасних інструментів успішного впровадження ШІ в розробку та управління ІТ проектами.

Результати дослідження. На етапі прототипування та розробки ШІ-інструменти здатні розуміти потреби споживачів, ринкові тенденції та технологічний ландшафт. Вони сприяють адаптації до швидких змін, але їхня роль полягає не в заміні людської винахідливості, а в її доповненні та розширенні.

Ось ключові рекомендації для успішного впровадження ШІ:

1. Інвестиції у ШІ-рішення: Основна мета ШІ-рішень — не лише економія, а й створення додаткової цінності. Це потрібно враховувати під час бюджетування, включно з витратами на підтримку.

2. Рання побудова підтримки: Варто залучати співробітників підтримки або вибудовувати цю функцію на ранніх етапах розробки ШІ-рішень. Це заощадить ресурси на етапі передачі продукту в експлуатацію.

3. Збереження основної команди: Після створення першої робочої версії ШІ-рішення бажано не розпускати основну команду. Це забезпечить стабільність і можливість подальшого вдосконалення продукту.

4. Управління технічним боргом: Це один із ключових процесів у розробці. Невчасне вирішення технічних проблем може негативно вплинути на подальший розвиток продукту.

5. Реалістичне бюджетування: Розробка якісного ІТ-рішення на базі ШІ вимагає значних інвестицій у людські ресурси та інфраструктуру. Важливо враховувати ринкові ціни й відповідно коригувати амбіції або бюджет.

Рекомендації для впровадження ШІ в управління ІТ-проектами

1. **Визначення ключових цілей**: Перед впровадженням ШІ важливо чітко сформулювати, які завдання повинні бути автоматизовані або оптимізовані.

2. **Інвестиції у навчання команди**: Для ефективного використання ШІ необхідно навчати команди новим інструментам і підходам.

3. **Гнучкий підхід**: Впровадження ШІ повинно супроводжуватися регулярною оцінкою його ефективності та адаптацією до змін.

4. **Підтримка команди розробки**: Основну команду розробників варто зберігати навіть після запуску продукту, щоб забезпечити підтримку й подальше вдосконалення.

Висновок. Штучний інтелект відкриває нові можливості для створення інноваційних ІТ-продуктів. Його використання надає конкурентні переваги, підвищує ефективність процесів і сприяє масштабуванню бізнесу. Проте для успішного впровадження ШІ важливо враховувати як технічні, так і організаційні аспекти. Розумний підхід до інтеграції ШІ дозволить не лише прискорити розробку, а й забезпечити довгострокову успішність продукту.

Список використаних джерел

1. Parekh, Ruchit, and M. Olivia. "Utilization of artificial intelligence in project management." International Journal of Science and Research Archive 13.1 (2024): 1093-1102.

2. Zadeh, Elham Karim, Ali Bagheri Khoulenjani, and Mohammad Safaei. "Integrating AI for agile Project Management: Innovations, challenges, and benefits." International Journal of Industrial Engineering and Construction Management (IJIECM) 1.1 (2024): 1-10.

3. Ko, Chien-Ho, and Min-Yuan Cheng. "Dynamic prediction of project success using artificial intelligence." Journal of construction engineering and management 133.4 (2007): 316-324.

4. Hofmann, P., Jöhnk, J., Protschky, D., & Urbach, N. (2020, March). Developing Purposeful AI Use Cases-A Structured Method and Its Application in Project Management. In Wirtschaftsinformatik (Zentrale Tracks) (pp. 33-49).

Лисенко Микола Миколайович
Аспірант 2 курсу, групи АІСД-21
Державний університет інформаційно-комунікаційних технологій
(067) 505-30-31
lysenkonik2015@gmail.com
Пронькін Олександр Васильович
Аспірант 2 курсу, групи АІСД-21
Державний університет інформаційно-комунікаційних технологій
+380 63 899 54 02
Oleksandr.pronkin@gmail.com
Стражніков Андрій Анатолійович
Аспірант 2 курсу, групи АІСД-21
Державний університет інформаційно-комунікаційних технологій
+380 50 965 19 55
andrew.strazh@gmail.com

АВТОМАТИЗАЦІЯ ОБРОБКИ ТЕКСТОВИХ МЕДИЧНИХ ДАНИХ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЙ ГЛИБОКОГО НАВЧАННЯ

Постановка задачі. Обробка текстових медичних даних є важливим аспектом автоматизації в сучасній медицині. Електронні медичні записи, протоколи обстежень, рецепти та інші текстові документи містять великий обсяг неструктурованої інформації, що ускладнює її аналіз традиційними методами. Технології глибокого навчання, зокрема методи обробки природної мови (NLP), відкривають нові можливості для ефективного аналізу таких даних [1].

Мета дослідження. Дослідити можливості NLP-моделей для аналізу текстових медичних даних, таких як електронні медичні записи, протоколи обстежень чи рецепти. Виявити переваги, обмеження та перспективи використання сучасних NLP-методів у медичній сфері.

Результати дослідження. У дослідженні проведено огляд сучасних NLP-моделей, зокрема BERT (Bidirectional Encoder Representations from Transformers) та BioBERT, які були адаптовані для роботи з медичними текстами. Основні переваги цих моделей полягають у їх здатності враховувати контекст слів, обробляти багатозначність термінів і навчатися на великих масивах даних. Наприклад, BioBERT, будучи спеціалізованою версією BERT, продемонстрував значне покращення в задачах класифікації медичних текстів, вилучення сутностей та відповіді на запитання [2]. Більш детальне порівняння результатів роботи моделей BERT та BioBERT наведено в таблиці:

Параметр	BERT	BioBERT	Примітки
Точність класифікації (Accuracy)	87%	91%	BioBERT показує вищу точність завдяки

			спеціалізації на медичних текстах
Ефективність вилучення сутностей (Entity Extraction)	85%	90%	BioBERT краще розпізнає медичні терміни та контексти
Час обробки тексту (сек/документ)	45 секунд	40 секунд	BioBERT швидший через оптимізації для медичних текстів
Обсяг навчальних даних	Wikipedia, BookCorpus	PubMed, PMC, Wikipedia, BookCorpus	BioBERT додатково навчається на корпусах медичних публікацій
Залежність точності від розміру вибірки (тис. записів) 10 20 50 100	 81% 83% 86% 97%	 85% 87% 90% 91%	BioBERT краще працює на менших вибірках завдяки медичній специфіці корпусу

Проте є і недоліки: висока обчислювальна складність, необхідність великої кількості якісно розмічених даних та складність адаптації до специфічних задач. Додатково, моделі схильні до упередженостей, які можуть виникати через нерівномірність розподілу даних у навчальних вибірках [3].

Для реалізації NLP-моделей застосовано мову програмування Python, бібліотеки TensorFlow та PyTorch, а також спеціалізовані інструменти для обробки текстових медичних даних, як-от spaCy та scikit-learn.

Висновки та перспективи. Використання NLP-моделей у медицині має значний потенціал. Інтеграція таких систем у клінічну практику дозволить автоматизувати рутинні процеси, як-от кодування медичних записів, класифікацію протоколів чи аналіз рецептів. Це сприятиме зменшенню часу, необхідного для аналізу даних, та підвищенню точності діагностики й лікування [4].

В Україні такі моделі можуть використовуватися для автоматизованого заповнення медичних карт пацієнтів, аналізу епідеміологічної ситуації на основі текстових звітів та оптимізації процесу медичного кодування в лікарнях.

Подальші дослідження мають бути зосереджені на розробці гібридних моделей, які поєднують глибоке навчання з експертними правилами, а також на вдосконаленні механізмів перевірки надійності та точності отриманих результатів [5].

Список використаних джерел

1. Devlin J., Chang M. W., Lee K., Toutanova K. "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding." 2018

2. Lee J., Yoon W., Kim S., et al. "BioBERT: a pre-trained biomedical language representation model for biomedical text mining."
3. "Clinical Text Classification with Word Embeddings."
4. "Deep Learning Approaches for Healthcare Text Analysis: A Review."
5. Tan, L., & Zhang, X. (2020). Deep learning for natural language processing: A review. IEEE Access, 8, 138913-138931.
6. Сторчак, К. П., Тушич, А. М., & Бондарчук, А. П. Кластерний аналіз даних із використанням штучних нейронних мереж. Зв'язок, (6). 2018 с.36-38.

Жебка Сергій Валентинович
студент 2 курсу, групи АІПЗ-21
Державний університет інформаційно-комунікаційних технологій
szhebka@hotmail.com
095-350-35-72
Науковий керівник: **Сініцин Ігор Петрович**
доктор технічних наук, професор,
професор кафедри технологій цифрового розвитку Державного університету інформаційно-комунікаційних технологій, м. Київ

ЗАСТОСУВАННЯ ОПТИМІЗАЦІЙНИХ МЕТОДІВ ДО РОЗПОДІЛЕНИХ БАЗ ДАНИХ

Постановка задачі. З розвитком великих даних і розподілених систем виникає потреба у підвищенні ефективності обробки запитів у розподілених базах даних. Оптимізація таких систем включає зменшення часу виконання запитів, зниження навантаження на сервери та мінімізацію затримок у передачі даних між вузлами. Використання оптимізаційних методів дозволяє досягти балансу між продуктивністю та витратами на ресурси.

Мета дослідження. Дослідити можливості застосування оптимізаційних методів для підвищення ефективності роботи розподілених баз даних, а також оцінити вплив таких методів на продуктивність, масштабованість та відмовостійкість систем.

Результати дослідження. Оптимізація розподілених баз даних (РБД) є важливим аспектом для забезпечення високої ефективності, швидкодії та надійності в умовах великих обсягів даних і розподілених обчислювальних ресурсів. Існує низка методів, які можуть бути застосовані для досягнення цих цілей.

Одним з основних напрямків оптимізації є балансування навантаження. Це дозволяє рівномірно розподіляти запити на різні вузли бази даних, знижуючи таким чином ймовірність перевантаження окремих компонентів системи. Для цього використовуються різні алгоритми розподілу навантаження, такі як методи на основі хешування або з урахуванням поточних показників навантаження на сервери.

Ще одним важливим методом є реплікація даних. Вона передбачає створення копій даних на різних вузлах бази даних, що дозволяє знижувати затримки доступу до даних і підвищувати стійкість системи до відмов. Однак це потребує налаштування правильної стратегії синхронізації між репліками, що може здійснюватися за допомогою алгоритмів консенсусу, таких як Paxos або Raft.

Для зменшення часу обробки запитів і зниження навантаження на мережу використовуються методи кешування. Кешування дозволяє зберігати найбільш часто запитувані дані в пам'яті, що дозволяє значно пришвидшити доступ до них, мінімізуючи потребу в постійних запитах до бази даних. Однак важливо

налаштувати політики очищення кешу та оновлення даних, щоб уникнути застарілих записів.

Крім того, важливим аспектом є оптимізація доступу до даних за допомогою індексації. Використання правильних індексів дозволяє швидко знаходити необхідну інформацію в базі даних. Вибір типу індексації, таких як B-дерева або хеш-таблиці, залежить від характеру запитів і структури даних.

Методи реплікації і шардінгу дозволяють ефективно масштабувати РБД, розподіляючи дані між кількома серверами або навіть центрами обробки даних. Шардінг полягає у розподілі даних по різних частинах бази, що дозволяє уникнути перевантаження окремих серверів та забезпечити високу доступність системи.

Генетичні алгоритми та алгоритми рою (Particle Swarm Optimization, PSO) є двома потужними методами, що використовуються для вирішення задач оптимізації, зокрема в контексті розподілених баз даних. Обидва ці алгоритми належать до категорії евристичних методів, що засновані на біологічних чи соціальних моделях, і є популярними в задачах, де традиційні методи оптимізації (наприклад, градієнтні методи) не дають бажаних результатів через високу складність або велику кількість змінних.

Генетичний алгоритм (ГА) є частиною класу еволюційних методів оптимізації. Він імітує етапи природного відбору, де найбільш адаптовані рішення зберігаються і використовуються для генерації нових рішень шляхом кросоверу та мутації. Цей алгоритм застосовується в задачах, де простір рішень великий і недостатньо ясний, тому традиційні методи можуть бути неефективними. У контексті розподілених баз даних генетичні алгоритми можуть застосовуватись для оптимізації розподілу даних, налаштування параметрів реплікації, шардінгу або балансування навантаження, коли існує потреба в еволюційній адаптації під час виконання запитів.

Алгоритм рою (PSO), в свою чергу, імітує соціальні взаємодії між особинами рою, де кожен учасник шукає оптимальне рішення, обмінюючись інформацією з іншими. Це дозволяє алгоритму швидко знаходити оптимальні або близькі до оптимуму рішення для задач оптимізації, де важлива швидка адаптація до змінних умов. В контексті розподілених баз даних PSO може застосовуватися для оптимізації різних параметрів, таких як параметри кешування або стратегій реплікації, а також для покращення ефективності пошуку та доступу до даних у великих і складних системах.

Розгляд цих двох алгоритмів у контексті оптимізації розподілених баз даних є важливим, оскільки ці методи можуть ефективно працювати з великими наборами змінних і адаптуватися до змінних умов у реальному часі. Вони дозволяють знаходити глобальні оптимуми в складних, многовимірних просторах рішень, де класичні методи можуть бути неефективними або не застосовними.

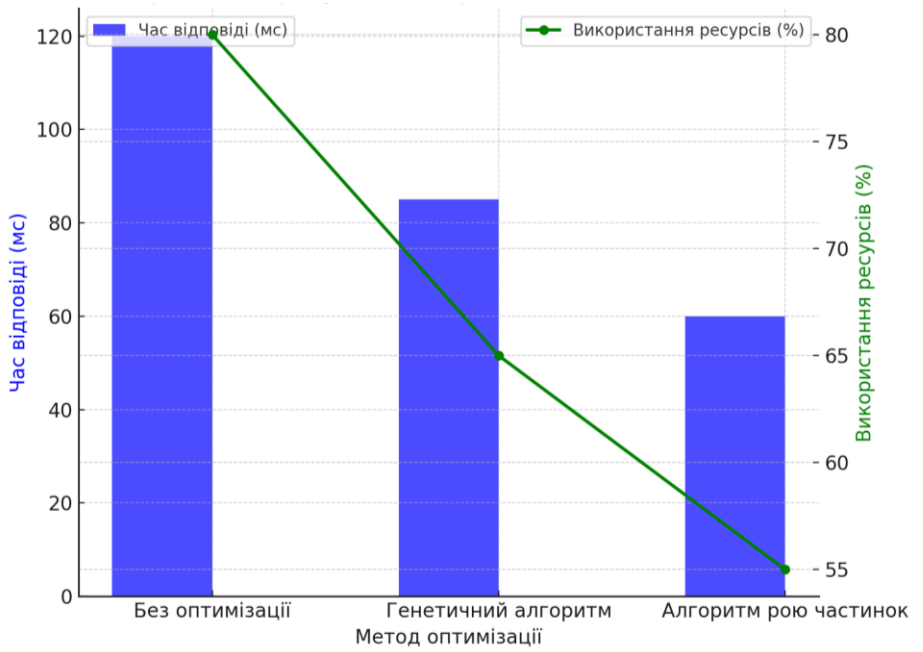

Рис. 1. Порівняння продуктивності різних методів оптимізації

Графіки демонструють залежність продуктивності від використання різних методів оптимізації, зокрема генетичних алгоритмів та алгоритмів рою частинок.

Висновки. Застосування оптимізаційних методів до розподілених баз даних дозволяє досягти суттєвого підвищення продуктивності та масштабованості таких систем. Використання сучасних алгоритмів і моделей, зокрема методів машинного навчання та прогнозування, є ефективним підходом для забезпечення гнучкості, надійності й економічності розподілених баз даних. Майбутні дослідження можуть бути зосереджені на вдосконаленні алгоритмів адаптації під реальні навантаження та їх інтеграції з хмарними платформами.

Список використаних джерел

1. Brown T., Mann B., Ryder N. et al. (2020). Language Models are Few-Shot Learners. Advances in Neural Information Processing Systems, 33, 1877-1901.

2. Ramesh A., Pavlov M., Goh G. et al. (2021). Zero-Shot Text-to-Image Generation. Proceedings of the International Conference on Machine Learning, 139, 8821-8831.

3. Dosovitskiy A., Beyer L., Kolesnikov A. et al. (2021). An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale. International Conference on Learning Representations, Vienna, Austria, 12-14.

4. atterson D., Gonzalez J., Le Q. et al. (2021). Carbon Emissions and Large Neural Network Training. Communications of the ACM, 64(12), 44-48.

Трофимчук О.М.
чл.кор.НАНУ, д.техн.н., проф.
Триснюк В.М.
д.техн.н., проф., trysnyuk@ukr.net
Інституту телекомунікацій і глобального Інформаційного простору НАН України

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПРИ ПОБУДОВІ ПОЛЯ РАДІАЦІЙНОГО ЗАБРУДНЕННЯ МІСЦЕВОСТІ ТА ПРОГНОЗУВАННЯ

Постановка задачі. Виявлення та оцінка радіаційної обстановки відбувається на двох етапах. На першому етапі, на основі даних про зони радіоактивного забруднення та метеорологічну інфекцію, прогноз радіаційної забрудненості місцевості (РЗМ). На другому етапі відбувається фактичний стан радіаційної обстановки на основі даних радіаційної розвідки або контролю. Прогнозні дані можуть служити тільки для попередньої оцінки радіаційного фону, тому їх обов'язково потрібно уточнювати. Після аварії на Чорнобильській АЕС загальна радіоактивність забруднення, спричинена цезієм і стронцієм, склала 500 млн Кі. У результаті катастрофи в атмосфері було викинуто до 100% радіоактивних корисних газів, 20–50% ізотопів йоду, 12–30% цезію та 3–4% інших важких радіонуклідів від їх загального вмісту в реакторі [1].

Мета дослідження. Мета роботи полягає у вдосконаленні інформаційних технологій при побудові поля радіаційного захисту місцевості в автоматизованих системах контролю радіаційної обстановки.

Результати дослідження. У наших дослідженнях було запропоновано:

перейти від випадкових координат вимірювань потужності дози випромінювання до прямокутної сітки;

вважати випадкові поля $F^0(p)$ і $E(p)$ однорідними, стаціонарними і взаємно незалежними;

синтезувати фільтр не в класі усіх лінійних фільтрів, а в якомусь істотно вужчому класі.

Виходячи з цього, завдання двовимірної фільтрації розщеплюється на серію одновимірних.

Критерієм параметрів фільтру може бути мінімум відхилень перетворення

$F(p) \xrightarrow{\varphi(p)} F^0(p)$: (1)

$M\{F(p) - F^0(p)\} \to min.$ (2)

Використовуючи ці обмеження, в [12] запропонований згладжуючий кубічний сплайн, що реалізовує метод найменших квадратів:

$$F(p) = \sum_{i=1}^{N} (p_i - p_i^0)^2 + a \cdot b \iint\limits_{s \in S} \left(\frac{\partial^2 p}{\partial X^2} + \frac{\partial^2 p}{\partial X \partial Y} + \frac{\partial^2 p}{\partial Y^2} \right) \partial X \cdot \partial Y , \qquad (3)$$

де p_i, p_i^0 – виміряне і вичислене значення поля РЗМ в i -ій вузловій точці сплайна, i=1,2,...,N;

p – значення функції p_i по усій області визначення $s \in S$;

a, b - параметри фільтру.

Рішенням задачі (5), являється кубічний сплайн двох змінних. Використання цього методу дозволяє добитися хорошої відновлюваності поля при високій щільності вимірювань ПДВ і нескладній його топології. Проте при ускладненні РО виникає необхідність збільшення дискретності сітки, тобто зменшення її кроку. Це у свою чергу призводить до різкого збільшення часу обробки даних. Крім того, при великій кількості вузлів сітки, алгоритм може працювати нестійкий[2].

В якості іншого підходу до синтезу фільтрів може бути використане швидке перетворення Фур'є. Але такі недоліки, як незадовільна апроксимація на краях, труднощі в обчисленні проміжних значень, не співпадаючих з вузлами сітки, не дозволяють використати вказаний підхід при рішенні цієї задачі.

Для побудови поля РЗМ використовувався також бікубічний сплайн. При цьому відновлюване поле розбивалося на прямокутники різних розмірів P_i так, щоб в кожного потрапляло не менше 9 вимірювань. Усередині кожного знаходилася інтерполяційна функція у вигляді двовимірного полінома третього порядку $P(x, y, a_0, ..., a_n)$, лінійно залежного від коефіцієнтів $a_0,...,a_n$. Ці коефіцієнти визначаються з умови досягнення функціоналом:

$$Z = \sum_{i=1}^{L} \left(\frac{P_i(x_l^i, y_l^i, a_{0l}, ..., a_{nl}) - Z_l^i}{S_l^i} \right)^2, \qquad (4)$$

де L - кількість прямокутників;

Z_l^i – виміряні значення ПДВ, рад/год;

S_l^i – точність вимірювань, умовного мінімуму, причому підсумовування ведеться по точках, координати яких потрапляють в цей прямокутник, а умовами виступає рівність P_i і їх першою і другою похідних на загальних межах відповідних прямокутників.

Суть методу, викладеного в роботі, полягає в тому, що точка, в якій необхідно розрахувати значення ПДВ, розглядається як та, що знаходиться на початку полярної системи координат[3]. Уся множина вимірювань ПДВ розбивається на b секторів, в кожному з яких одиничні вимірювання отримують координати (r_i, α_i).

Тоді, для вирішення завдання необхідно побудувати інтерполяційну пряму:

$Z = ar + b.$ (5)

Коефіцієнти цієї прямої розраховуються з умови досягнення мінімуму функціоналом:

$$\sum_{i=1}^{m} \left(\frac{ar_i + b}{S_i} \right), \; m = (5, n_k) \qquad (6)$$

де n_k - число вимірювань ПДВ, що потрапили в k -тий сектор.

Оскільки точка, в якій інтерполюється значення поля, знаходиться на початку координат (r=0), це значення є b з дисперсією D(b)

$$b = \left[\left(\sum \frac{Z_i}{D_i}\right)\cdot\left(\sum \frac{r_i^2}{D_i}\right) - \left(\sum \frac{z_i r_i}{D_i}\right)\cdot\left(\sum \frac{r_i}{D_i}\right)\right]\cdot\left[\left(\sum \frac{r_i^2}{D_i}\right)\cdot\left(\sum \frac{1}{D_i}\right) - \left(\sum \frac{r_i^2}{D_i}\right)\right]^{-1}, \quad (7)$$

$$D(b) = \sum \frac{r_i^2}{D_i}\cdot\left[\left(\sum \frac{r_i^2}{D_i}\right)\cdot\left(\sum \frac{1}{D_i}\right) - \left(\sum \frac{r_i}{D_i}\right)^2\right]^{-1}. \quad (18)$$

Критерієм вибору числа точок m, являється мінімум дисперсії. Він же використовується для визначення інтерполяційного сектора.

В якості інтерполяційної залежності досліджувалася не лише пряма (8), але і парабола. Будувалися ті, що мінімізують суму відхилень параболи з осями абсцис на прямих, що відповідають парам протилежних секторів. Її використання привело до значного погіршення результату.

Висновки. Проведені дослідження показали високу ефективність відновлення характеристик поля радіаційного забруднення за результатами аерогаммазйомки, виконаної в зоні аварії Чорнобильської АЕС. Застосування методу інтерполяції для обробки даних про радіоактивне забруднення дозволяє досягти високої точності відновлення поля за умови високої щільності вимірювання потужності дози випромінювання (ПДВ) та простої топології поля. Проте зі зростанням стійкості радіаційної обстановки (РО) збільшується дискретність місця, тобто зменшення відстані між точками вимірювання.

Список використаних джерел

1. В.М. Триснюк, А.А. Нікітін В.О. Шумейко Алгоритм оброблення інформації про радіоактивне забруднення місцевості з використанням даних ДЗЗ та ГІС. // Системи управління, навігації та зв'язку. Полтавський національний технічний університет імені Юрія Кондратюка. Полтава. Випуск 6 (46) 2017р. – С. 102-110.

2. O. Trofymchuk, Y. Yakovliev, V. Klymenko, Y. Anpilova, Geomodeling and monitoring of pollution of waters and soils by the earth remote sensing. International Multidisciplinary Scientific GeoConference - SGEM, 19, 1.4 (2019).

3. Триснюк В. М., Нагорний Є. І., Триснюк Т. В., Конецька О. О., Курило А. В.. Методика виявлення радіаційного забруднення місцевості та його ризиків. Системи управління, навігації та зв'язку. Збірник наукових праць. Полтавський національний технічний університет імені Юрія Кондратюка. Випуск 3(69) 2022 С. 112-115. ISSN 2073-7394. http://journals.nupp.edu.ua/sunz/article/view/2618