МАТЕРІАЛИ X ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО: «ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ»

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ОДЕСА
23 травня 2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра інформаційних технологій

ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

МАТЕРІАЛИ X ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

23 травня 2025 року, м. Одеса

Одеса, 2025

УДК 340.12:316.3

Відповідальній редактор:
Н. І. Логінова, завідувачка кафедри інформаційних технологій, канд. пед. наук, доцент
https://orcid.org/0000-0002-9475-6188

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку

Друкується за рішенням кафедри інформаційних технологій Національного університету «Одеська юридична академія» (протокол засідання кафедри № 13 від 26.05.2025 р.)

Інформаційне суспільство : проблеми та перспективи : Матеріали X Всеукраїнської науково-практичної конференції (м. Одеса, 23 травня 2025 р.). Одеса : Національний університет «Одеська юридична академія», 2025. 216 с. URL: https://hdl.handle.net/11300/29842; DOI: https://doi.org/10.32837/11300.29842

Всеукраїнська науково-практична конференція «Інформаційне суспільство: проблеми та перспективи» присвячена розгляду актуальних питань розвитку інформаційного суспільства в Україні та у світі.

До участі у конференції запрошені студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

ПЕРЕДМОВА

Сучасне інформаційне суспільство формує нову парадигму взаємодії людини, цифрових технологій і соціальних інститутів. Інтенсивний розвиток таких технологій, як штучний інтелект, інтернет речей, великі дані, а також цифровізація всіх сфер суспільного життя – від економіки й освіти до державного управління та приватного простору – зумовлює глибокі трансформаційні процеси. Водночас це породжує низку нових викликів, серед яких особливо актуальними є питання кібербезпеки, цифрової нерівності, етичного використання даних і забезпечення інформаційного суверенітету.

В умовах воєнного стану, в яких нині перебуває Україна, зростає потреба в ефективному інформаційному захисті, цифровій трансформації державного управління та стратегіях протидії гібридним загрозам. Ці обставини, поряд із викликами, створюють і нові можливості для розвитку національної цифрової інфраструктури, модернізації системи освіти та стимулювання науково-дослідної діяльності.

Штучний інтелект на сучасному етапі розвитку вже не обмежується суто технічними аспектами – його застосування охоплює також правові, етичні, психологічні, соціальні та творчі сфери. Активно розвивається сфера розробки комп'ютерних ігор (GameDev), яка, крім своєї індустріальної значущості, виконує також освітню та дослідницьку функцію, зокрема в контексті вивчення поведінки користувача. Зростає зацікавленість до веброзробки та створення мобільних застосунків. Кібербезпека розглядається як міждисциплінарне явище, що охоплює технічні, соціальні та етичні аспекти. Значна увага привертається впровадженням інформаційних технологій у систему освіти, а також дослідження соціальних і моральних наслідків цифровізації.

Зазначені напрями стали предметом обговорення під час конференції, що свідчить про міждисциплінарний характер сучасних досліджень у галузі інформаційних технологій. Такий спектр доповідей конференції повністю узгоджується з актуальними світовими IT-трендами й підтверджує значущість та актуальність проведеного наукового заходу.

Сподіваємося, що конференція стане стимулом до подальших наукових досліджень, конструктивного діалогу та обміну досвідом серед молодих учених задля формування ефективної моделі розвитку сучасного інформаційного суспільства.

Секція 1. СУЧАСНІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ЖИТТІ ЛЮДИНИ ТА СУСПІЛЬСТВА

СТВОРЕННЯ ІГОР НА PYGAME ЯК МЕТОД ГЕЙМІФІКАЦІЇ ПРОЦЕСУ ВИВЧЕННЯ PYTHON

Годлевська Марія

студентка 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету "Одеська юридична академія"

Сучасні цифрові технології обумовлюють формування навичок з програмування, що є однією з ключових компетенцій для фахівців IT галузі. Мова Python посідає лідерські позиції у рейтингах найпопулярніших мов програмування [1]. Завдяки простому та зрозумілому синтаксису, високій читабельності та широкому спектру застосувань – від веброзробки та аналізу даних до штучного інтелекту та автоматизації – Python є ідеальним вибором для початківців у програмуванні. Згадані переваги дозволяють швидко опанувати базові концепції та почати створювати власні проєкти.

Попри всі переваги, вивчення великої кількості необхідної базової теорії та монотонність у виконанні типових вправ можуть значно знизити мотивацію та зацікавленість у вивченні програмування. Тому виникає потреба у пошуку захопливих та інтерактивних методів викладання, які б не лише передбачали засвоєння матеріалу, а й підтримували високий рівень ентузіазму. Одним із таких ефективних підходів є гейміфікація освітнього процесу, тобто використання ігрових елементів та механік у неігровому контексті. Це може бути реалізовано, зокрема, завдяки проєктній діяльності, яка передбачає створення не просто консольних застосунків, а візуальних та інтерактивних проєктів, таких як прості 2D-ігри.

Дослідження підтверджують ефективність гейміфікації у покращенні результатів навчання, залученості та мотивації в програмуванні [2]. Дані свідчать про те, що гейміфіковані підходи можуть призвести до кращого засвоєння практичних навичок кодування, формування більш позитивного ставлення до навчання та підвищення впевненості у власних силах.

Зокрема, дослідження показують, що гейміфікація є ефективнішою за традиційні методи у розвитку практичних навичок кодування та поліпшенні ставлення студентів до вивчення програмування [3].

Аналіз популярних ігрових рушіїв та бібліотек з підтримкою Python, серед яких Pygame, Pyglet, Kivy, Delta 3D, Cocos 2D та Panda 3D, свідчить про те, що бібліотека Pygame має низку ключових характеристик, які роблять її особливо вдалим інструментом для опанування основ програмування на Python [4]. Ці характеристики включають, перш за все, низький поріг входження, що є надзвичайно важливим для студентів-початківців, дозволяючи їм швидко перейти від вивчення синтаксису до створення реальних проєктів без необхідності

опановувати складні архітектурні рішення, на відміну від рушіїв, що вимагають середнього чи високого рівня досвіду.

Орієнтація Pygame на 2D-графіку значно спрощує процес візуалізації та управління об'єктами порівняно зі складністю 3D-простору, що дозволяє зосередитися на фундаментальних програмних концепціях та ігровій логіці. Хоча деякі аспекти, як-от вбудовані редактори чи просунута фізика, часто реалізовані у Pygame як розширення, це надає гнучкість та дозволяє додавати складність поступово, відповідно до рівня знань студента. Крім того, підтримка кросплатформенної розробки робить Pygame доступним на більшості операційних систем, що є зручним у навчальному процесі. Таким чином, характеристики Pygame підкреслюють його доступність, відносну простоту та гнучкість, роблячи його відмінним вибором для першого досвіду розробки ігор та ефективного вивчення основ програмування.

Важливим фактором, що робить бібліотеку Pygame особливо привабливою для студентів-початківців, є наявність великої та доступної бази освітніх ресурсів. бібліотека існує вже тривалий час та має вичерпну офіційну документацію, яка детально описує функції, модулі та класи, дозволяючи отримати точну інформацію про роботу бібліотеки [5]. Окрім офіційних джерел, в Інтернеті існує величезна кількість високоякісних посібників, підручників, відеоуроків, онлайн-курсів та прикладів коду, створених спільнотою розробників та ентузіастів. Така розгалужена екосистема навчальних матеріалів значно знижує поріг входження, дозволяючи студентам швидко знаходити відповіді на запитання, долати технічні труднощі та вивчати різні аспекти створення ігор у зручному для себе форматі. Наявність цих ресурсів сприяє самостійному навчанню та дослідженню, що є невід'ємною частиною розвитку навичок програмування.

Окрім вичерпної документації та численних навчальних матеріалів, офіційний вебсайт Pygame (pygame.org) слугує не лише інформаційним порталом, але й галереєю реальних проєктів – ігор та застосунків, створених членами спільноти [6]. Ця демонстрація робіт користувачів є важливим джерелом натхнення для студентів, оскільки вона наочно показує, які саме результати можуть бути досягнуті за допомогою бібліотеки. Перегляд готових ігор, створених такими ж ентузіастами, як і вони, допомагає початківцям оцінити реальний потенціал Pygame та побачити конкретні приклади застосування вивчених концепцій на практиці, що додатково стимулює їх до власної творчості та експериментів.

Як приклад, під час розробки гри на Pygame можна не просто вивчати синтаксис, а й наочно освоювати фундаментальні концепції програмування, бачачи їхнє миттєве візуальне застосування. Створення навіть простої гри вимагає використання циклів для постійного оновлення екрану та ігрового стану, умовних операторів if / elif / else для обробки натискання клавіш та реагування на події, взаємодії зі змінними координат для переміщення спрайтів, а також створення власних функцій для структурування коду та реалізації повторюваних дій (наприклад, малювання об'єктів) тощо.

Цей процес не тільки закріплює теоретичні знання через практику, але й інтенсивно розвиває алгоритмічне мислення, логіку та критично важливу навичку відлагодження коду. Завдяки вивченню цих тем та отриманню практичного досвіду, початківцю вистачить навичок для самостійного створення таких ігор, як: «Змійка», «Пінг-Понг», простий арканоїд або ж вікторину з графічним інтерфейсом, отримуючи при цьому значний стимул для подальшого навчання. Кожен написаний рядок коду або внесена зміна відразу відображається у поведінці або зовнішньому вигляді елементів гри, в той час, як навіть складна консольна програма не буде такою візуально привабливою.

Розробка ігор на Pygame дозволяє студентам не просто вивчати синтаксис та базові конструкції мови (змінні, типи даних, умовні оператори, цикли, функції), але й одразу бачити їхнє практичне застосування та візуалізований результат своєї роботи. Цей проєктний підхід сприяє кращому розумінню абстрактних концепцій програмування, розвитку алгоритмічного та логічного мислення, навичок налагодження коду та самостійного розв'язання проблем.

Найважливіше – це інтерактивність процесу створення гри та можливість отримати робочий продукт значно підвищують рівень ентузіазму та внутрішньої мотивації студентів до подальшого вивчення. Впровадження розробки ігор на Pygame у навчальні програми з Python у вищих та середніх навчальних закладах є перспективним напрямом, що може значно покращити якість засвоєння матеріалу та рівень зацікавленості студентів.

Список використаних джерел

1. TIOBE Index - TIOBE. TIOBE. URL: https://www.tiobe.com/tiobe-index/ (дата звернення: 22.04.2025).
2. Using Game Design to Enhance the Learning Motivation of Programming Courses. URL: https://iaiai.org/letters/index.php/liir/article/download/90/103 (дата звернення: 22.04.2025).
3. Assessing the Role of Python Programming Gamified Course on Students' Knowledge, Skills Performance, Attitude, and Self-Efficacy. Manuel B. Garcia | Licensed Professional Teacher. URL: https://manuelgarcia.info/media/full_paper/python-programming-gamified-course.pdf (дата звернення: 22.04.2025).
4. Koupritzioti E., Xinogalos S. Teaching Game Programming to Novices: Lessons Learned from a High School Educational Intervention. Education and Information Technologies. 2020. Vol. 25, Iss. 4. P. 2747–2764. URL: https://ruomoplus.lib.uom.gr/bitstream/8000/1181/1/EAIT_2020_Koupritzioti_Xinogalos_postprint.pdf (дата звернення: 22.04.2025).
5. Shinners P. Pygame Intro – pygame v2.6.0 documentation. pygame news. URL: https://www.pygame.org/docs/tut/PygameIntro.html (дата звернення: 22.04.2025).
6. Projects. pygame news. URL: https://www.pygame.org/tags/all (дата звернення: 22.04.2025).

Ключові слова: Python, Pygame, розробка ігор, комп'ютерні ігри, програмування, 2D-ігри, мотивація, гейміфікація

Keywords: Python, Pygame, game development, computer games, programming, 2D games, motivation, gamification

Науковий керівник: доцент Задерейко О.

СПЕЦИФІКА ВИКОРИСТАННЯ РУШІЯ UNITY ДЛЯ РОЗРОБКИ 2D-ІГОР

Д'якова Ксенія

студентка 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету "Одеська юридична академія"

Сфера створення комп'ютерних та мобільних ігор через свій стрімкий розвиток демонструє невпинне зростання, супроводжуване появою нових ігрових студій та збільшенням кількості випущених ігрових продуктів. З'являється підвищений попит на кваліфікованих фахівців, здатних втілювати в життя різноманітні ігрові концепції, особливо у галузі двовимірних ігор. При цьому 2D-проєкти продовжують утримувати значну популярність серед гравців різного віку, пропонуючи легкі для сприйняття та зрозумілі ігрові механіки, що є важливим чинником для залучення широкої аудиторії в сучасному динамічному світі, де час та увага користувачів є обмеженими.

Популярним інструментом для розробки 2D-ігор є Unity, завдяки гнучкості, багатофункціональності та підтримці кросплатформності цього рушія. Специфіка розробки 2D-ігор у Unity полягає в тому, що хоча цей рушій спочатку був створений для 3D-проєктів, він має потужний набір інструментів і компонентів саме для 2D-графіки [1]. Серед них – спеціальний 2D-режим редактора, підтримка спрайтів, анімації, фізики та колайдерів, оптимізованих саме під двовимірний простір. Unity також забезпечує розробників можливістю легко інтегрувати зовнішні ресурси, створювати кастомні шейдери для 2D-графіки та використовувати візуальне редагування сцен, що значно пришвидшує процес створення контенту.

В Unity різноманітні компоненти відіграють ключову роль у створенні повноцінної 2D-гри, оскільки кожен з них відповідає за окремий аспект взаємодії гравця зі світом гри. Камера у 2D-проєктах дозволяє налаштовувати видиму область сцени, визначаючи, яка частина рівня буде відображатися на екрані, і часто прив'язується до персонажа для створення динамічного руху. Освітлення, хоч і не завжди критичне в класичних 2D-іграх, використовується для створення атмосферності, візуальних ефектів та глибини сцени. Звук забезпечує емоційне наповнення гри: музика, ефекти та озвучення допомагають занурити гравця в ігровий процес. Робота з колайдерами та фізикою дозволяє створювати реалістичну взаємодію об'єктів, наприклад, зіткнення, гравітацію або стрибки, що

критично важливо для платформерів або головоломок. Компоненти анімації відповідають за візуальні зміни об'єктів у часі – вони дозволяють оживити персонажів, реалізувати цикли руху, атаки чи інші дії. Графічний інтерфейс, своєю чергою, необхідний для виведення інформації, такої як здоров'я, рахунок чи меню, і забезпечує зручну взаємодію гравця з грою. Всі ці компоненти взаємодіють між собою, формуючи цілісну ігрову систему, де кожна деталь має значення для геймплею та враження від гри.

На початкових етапах створення 2D-гри потрібно підготувати всі необхідні налаштування та компоненти. Важливу роль у створенні проєкта відіграють асети (Assets). Файл ASSET – це спеціальний файл, який використовується в Unity, програмі для створення відеоігор. Він містить важливі конфігурації ігрових об'єктів та налаштувань, а саме: текстури та зображення, аудіофайли, шрифти, скрипти, сценарії, анімації, шейдери, матеріали, сцени (Scenes) та інші сторонні ресурси та плагіни [2]. В Unity для цих компонентів використовується спеціальний редактор – Sprite Editor. За його наявності є можливість обробляти імпортовані зображення, особливо спрайт-аркуші, що містять численні кадри анімації або окремі графічні елементи, не виходячи із середовища Unity. Функціональність редактора охоплює нарізку спрайтів (slicing) – автоматичну, на основі прозорості чи сітки, або ручну, для повного контролю над межами кожного елемента. Важливим є точне налаштування опорних точок (pivot points), відносно яких відбуваються трансформації об'єктів. Правильне їх встановлення є вирішальним для коректної анімації та розміщення у сцені [3]. Редактор також надає змогу модифікувати полігональну сітку спрайта (shape editing) для точніших фізичних контурів або створення спрайтів нестандартної геометрії. Одночасно з підготовкою асетів відбувається налаштування ігрової сцени, де головне місце займає положення камери. Для 2D-ігор камеру зазвичай налаштовують на використання ортографічної проєкції (Orthographic projection), що усуває ефект глибини та забезпечує класичний плаский вигляд.

Наступним кроком є встановлення фізики об'єктів у грі. Для цього в Unity є окрема, оптимізована підсистема 2D-фізики. Її основу складають компоненти Rigidbody 2D та Collider 2D. Додавання Rigidbody2D надає спрайту фізичні можливості, тобто враховування сили, гравітації та рухів, а колайдер реагує на зіткнення з іншими об'єктами, окреслює об'єкт для зіткнення з іншими об'єктами [4].

Після налаштування фізики об'єкти анімують. Unity надає вбудовану схему послідовності для створення та контролю двовимірних анімацій. Її елементами є вікно Animation та Animator Controller. Анімація спрайта, що полягає у покадровій зміні спрайтів, створюється у вікні Animation. Тут розробник формує анімаційні кліпи (Animation Clips) з можливостями налаштування тривалості кадрів та додаванням подій анімації. Керування відтворенням цих кліпів та логікою переходів між ними реалізується через Animator Controller [5].

Завершальні етапи розробки стосуються створення користувацького інтерфейсу (UI) та фінальне налаштування візуальної частини. Система UI в 2D-іграх будується на об'єкті Canvas, текст (Text), зображення (Image) та кнопках (Button).

Як приклад практичного застосування описаних інструментів та підходів автором реалізовано двовимірний ігровий проєкт. Специфіка його розробки полягає у послідовному використанні функціоналу Unity для 2D. Програмування ігрової логіки здійснено мовою C#. Керування головним персонажем – його переміщення та взаємодію з оточенням, реалізовано через скрипт, що керує компонентом Rigidbody 2D для фізики стрибків під дією сили, що реагує на натискання вказаної клавіші користувача. Система рахунку та визначення умов завершення гри (наприклад, зіткнення з перешкодою або вихід за межі екрана) застосовані через взаємодію об’єктів, що використовують тригери Collider2D, з увімкненим Is Trigger.

Методи та взаємозв’язки класу гравця, генератора перешкод, самих перешкод, менеджера рахунку, головного менеджера гри та елементів інтерфейсу в реалізованому 2D-ігровому проєкті показують, як взаємодіють основні системи гри для створення цілісного ігрового процесу (рис. 1). Цей приклад показує, як об'єднання стандартних інструментів Unity та власної логіки створюють функціональні 2D-ігри.

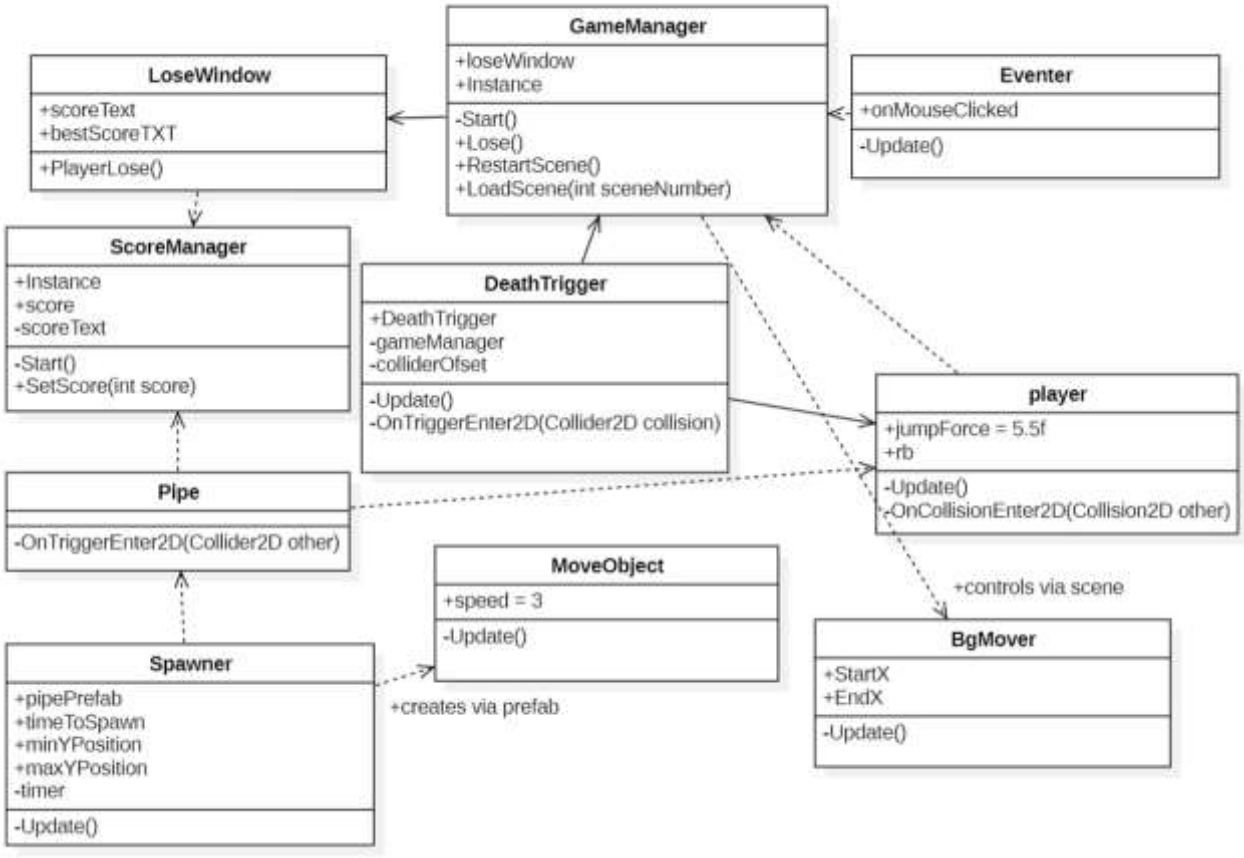

Рисунок 1 – UML-діаграма (діаграма класів) реалізованого 2D-ігрового проєкту

Клас гравця (player) відповідає за обробку вводу користувача, переміщення, анімацію та зіткнення з іншими об’єктами. Він взаємодіє з перешкодами через систему фізики або тригерів, викликаючи, наприклад, події на зіткнення, які обробляє головний менеджер гри. Генератор перешкод працює автономно або за сигналом менеджера, створюючи нові об’єкти з певною частотою, які гравець має уникати.

Менеджер рахунку відповідає за облік ігрових балів, оновлює значення при успішному проходженні перешкод і передає ці дані до інтерфейсу. Елементи інтерфейсу, своєю чергою, реагують на зміни у грі, відображаючи поточний рахунок, статус гравця або повідомлення про завершення гри. Головний менеджер (GameManager) гри координує всі ці компоненти: він запускає гру, ставить її на паузу, скидає при повторному запуску та слідкує за загальним станом, наприклад, чи відбулося зіткнення, і чи потрібно зупинити рух перешкод і змінити інтерфейс. Усі ці класи й елементи пов’язані логічно через виклики методів, події або змінні стану, створюючи керовану та динамічну структуру, яка дозволяє грі функціонувати стабільно й передбачувано.

Важливою перевагою Unity є підтримка розробки ігор для широкої сфери платформ, охоплюючи персональні комп’ютери, мобільні пристрої на Android та iOS, ігрові консолі, веббраузери, а також платформи доповненої (AR) та віртуальної (VR) реальності, що відкриває можливості для максимального охоплення аудиторії.

Немаловажним є велика база користувачів Unity, активна спільнота та доступ до численних навчальних матеріалів, що особливо важливо для інді-розробників або початківців. Крім того, інструменти для монетизації, аналітики та зручна система оновлень також сприяють повноцінному циклу створення ігор. Усе це робить Unity привабливою платформою для розробки 2D-проєктів різної складності.

Список використаних джерел

1. Unity Engine. URL: https://docs.unity.com/
2. ASSET. URL: https://docs.fileformat.com/uk/game/asset/
3. Pivot Point. Blender Manual. Версія 3.1. URL: https://docs.blender.org/manual/uk/3.1/editors/3dview/controls/pivot_point/index.html
4. Using Rigidbody2D in Unity. URL: https://stackoverflow.com/questions/63866216/using-rigidbody2d-in-unity
5. Animator Controller. Unity Technologies. URL: https://docs.unity3d.com/6000.1/Documentation/Manual/class-AnimatorController.html

Ключові слова: Unity, 2D-гра, розробка ігор, анімація

Keywords: Unity, , 2D game, game development, animation

Науковий керівник: доцент Трофименко О.

РОЗРОБКА КОМП'ЮТЕРНИХ ІГОР У СУЧАСНОМУ СВІТІ: ЇЇ РОЛЬ ТА ПРИЗНАЧЕННЯ

Задерейко Олександр

доцент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»
кандидат технічних наук, доцент

Петрушков Костянтин

студент 1-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Індустрія розробки відеоігор за останні десятиліття перетворилася зі звичайного захоплення на одну з найвпливовіших форм цифрового мистецтва та розваг [1]. Сьогодні комп'ютерні ігри - це не лише спосіб дозвілля, а й потужний інструмент соціального впливу, освіти та культури.

До того ж практичний досвід гравців неодноразово рятував багатьом людям життя від самотності та допомагали відволіктися від проблем. Вони ставали своєрідним емоційним притулком, у якому гравець міг знайти розуміння, спокій або навіть сенс. У складні моменти саме комп'ютерна гра надавала відчуття контролю над ситуацією та безпечного простору для самовираження. Такий вплив цифрових розваг вказує, що вони важливі не лише для проведення вільного часу, а й для позитивного емоційного стану людини.

Суспільство по-справжньому недооцінює комп'ютерні ігри, кажучи, що це просто іграшки для дітей. Але нині це одна із найвпливовіших сфер та частина економіки світу, і одна із найсучасніших сфер, яка стрімко розвивалась для створення ігор для комп'ютерних і мобільних пристроїв.

У професійному середовищі сучасні комп'ютерні ігри виходять за рамки звичайної гри - це справжній феномен, що з'єднує технологічний прогрес із людською фантазією, тонко вплітаючись у почуття людей та їх погляди на життя. Хоч процес розробки комп'ютерних ігор і потребує величезних ресурсів та вкладень, їхня унікальність полягає в здатності оживляти задуми, які надихають велику кількість людей.

Розробка комп'ютерних ігор є динамічною сферою сучасного цифрового світу [2]. Вона об'єднує творчий підхід, застосування сучасних технологій та командну взаємодію. Ця галузь також стимулює пошук нестандартних рішень у мистецтві, дизайні та програмуванні. Водночас робота у сфері розробки комп'ютерних ігор пропонує певні переваги, але й ставить перед фахівцями конкретні виклики. Ці фактори важливо враховувати всім, хто розглядає для себе кар'єру у цієї індустрії.

Перший важливий аспект – розробки комп'ютерних ігор є потужним економічним чинником. Це багатомільярдний сектор, що генерує значні прибутки через продаж ігор, внутрішньоігрові покупки та супутні товари. Важливо, що ця

індустрія створює численні робочі місця для фахівців різних профілів: від програмістів та дизайнерів до маркетологів та тестувальників [3]. Крім прямого економічного внеску, розробка комп'ютерних ігор стимулює розвиток суміжних ринків, таких як виробництво комп'ютерного обладнання (відеокарти, процесори) та супутнє обладнання.

Другий важливий аспект – технологічне лідерство. Саме потреби у розробці комп'ютерних ігор часто стають рушієм для розробки нових технологій. Прагнення до реалістичнішої графіки, складніших фізичних симуляцій та переконливіших сцен за використанням штучного інтелекту спонукає до інновацій у комп'ютерній графіці, обчислювальних потужностях, сучасних алгоритмах ШІ, а також у сферах віртуальної (VR) та доповненої (AR) реальності [4]. Ці розробки згодом знаходять застосування в інших галузях: медицині, архітектурі, освіті, військових симуляторах.

Третя ключова роль – культурний вплив. Комп'ютерні ігри давно перестали бути просто розвагою для вузького кола людей і стали невіддільною частиною сучасної масової культури, порівнянною за впливом із кінематографом чи музикою. Вони формують нові наративи, впливають на візуальні тенденції, створюють власні субкультури та глобальні спільноти гравців. Феномени кіберспорту та стрімінгу ігрового процесу також підкреслюють культурну значущість цієї сфери.

Крім того, розробка комп'ютерних ігор знаходить застосування і в менш очевидних напрямках, виконуючи соціальні та освітні ролі. Існують так звані "серйозні ігри" (serious games), розроблені для навчання, тренування певних навичок (наприклад, у медицині чи авіації), підвищення обізнаності щодо соціальних проблем або навіть для терапевтичних цілей [5].

Розробка комп'ютерних ігор це не просто індустрія розваг. Вона є певною частиною економіки країн, рушієм їх технологічного прогресу. Фактично, можна констатувати що розробка комп'ютерних ігор комплексно впливає на суспільство: від можливості цікаво провести час до стимулювання інновацій та формування нових способів спілкування й творчого самовираження у ігровому середовищі.

Список використаних джерел

1. Климентенко П. Професія геймдев: що робить та скільки заробляє розробник ігор? URL: https://happymonday.ua/jak-staty-rozrobnykom-igor 2021.
2. Газіс А., Кацирі Е. Серйозні ігри в цифровому геймінгу: комплексний огляд додатків, ігрових рушіїв та досягнень. URL: https://wseas.com/journals/cr/2023/a045118-001(2023).pdf
3. Немчинський С. Йдемо в геймдев? URL: https://foxminded.ua/jdemo-v-gejmdev/2022
4. Усе що ви хотіли знати про ШІ: вісім переваг та шість недоліків. URL: https://internetua.com/use-sxo-vi-hotili-znati-pro-shi-visim-perevag-i-shist-nedolikiv

5. Задерейко О. В., Толокнов А. А., Струк Н. О. Розробка ігрового застосунку «симулятор оператора надводного дрона». Сучасні технології в енергетиці, електромеханіці, системах управління та машинобудуванні: матер. VI Всеукр. наук.-практ. інтернет-конф. (м. Харків, 06-07 грудня 2023 р.) Харків: ННППІ УІПА, 2023. С. 11-12. URL: https://hdl.handle.net/11300/26945/

Ключові слова: розробка комп'ютерних ігор, роль комп'ютерних ігор, ігрова індустрія, ігрові технології

Keywords: computer game development, role of computer games, game industry, game technologies

СУЧАСНІ МЕТОДИ ФІЗИЧНОГО МОДЕЛЮВАННЯ У КОМП'ЮТЕРНИХ ІГРАХ

Толокнов Анатолій

асистент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»

Фізичне моделювання стало визначальним елементом сучасних комп'ютерних ігор, суттєво впливаючи на реалістичність, механіки та емоційне занурення гравців. За останні двадцять років спостерігається значний прогрес у розробці та впровадженні технологій, які симулюють природні фізичні процеси у віртуальних світах. Ця стаття досліджує ключові методи та підходи до фізичного моделювання в іграх, їхні переваги, обмеження та перспективи розвитку.

Фізичне моделювання (англ. physical simulation) – це комплекс обчислювальних технік для відтворення фізичних законів у цифровому середовищі. У контексті відеоігор воно виконує низку важливих функцій:

- забезпечує правдоподібну взаємодію об'єктів з середовищем;
- підвищує достовірність рухів та анімацій;
- створює інноваційні ігрові механіки;
- посилює емоційне занурення гравця.

Ігрові проєкти з розвиненими фізичними системами, такі як «Half-Life 2», «Red Dead Redemption 2» чи «The Legend of Zelda: Breath of the Wild», здобули визнання критиків і гравців саме завдяки реалістичним і глибоко інтегрованим фізичним симуляціям [1]. Вони не лише підвищують візуальну якість, але й розширюють можливості взаємодії гравця зі світом.

Упродовж 2000-х років індустрія комп'ютерних ігор почала активно впроваджувати спеціалізовані фізичні рушії. Havok, PhysX і Bullet стали стандартними інструментами для розробників. Havok забезпечував надійну симуляцію жорстких тіл, виявлення зіткнень і систему обмежень для управління поведінкою об'єктів [2]. PhysX, розроблений компанією NVIDIA, розширив можливості

фізичного моделювання, додавши підтримку м'яких тіл, рідин і тканин за допомогою GPU-прискорення.

Математичний апарат цих рушіїв спирається на класичну механіку, зокрема: ньютонівські рівняння руху, метод Ейлера, методи Рунге-Кутти для чисельного розв'язання диференціальних рівнянь [3].

Ключовою перевагою сучасних фізичних рушіїв є їхня оптимізація для роботи в реальному часі, що дозволяє застосовувати складні обчислювальні моделі на споживчих пристроях. Водночас це часто вимагає компромісів між точністю фізичних розрахунків і продуктивністю, особливо на платформах з обмеженими ресурсами.

Симуляція рідин залишається одним із найскладніших аспектів фізичного моделювання у реальному часі. Найпоширенішим методом є SPH (Smoothed Particle Hydrodynamics) – метод згладжених частинок, який представляє рідину як систему взаємодіючих частинок. Цей підхід використовується у таких технологіях, як NVIDIA FleX та система Niagara в Unreal Engine [4].

Альтернативою є решіткові методи, зокрема скінченно-різницеві схеми, що моделюють рухи потоків у фіксованому об'ємі. Хоча такі симуляції забезпечують вищу точність, вони менш ефективні для застосування у реальному часі. Для досягнення балансу між реалістичністю та швидкодією розробники часто поєднують фізично коректні та процедурні візуальні ефекти.

У сучасних AAA-проєктах моделювання рідин часто використовується для таких елементів: реалістичні водойми та їх взаємодія з об'єктами; ефекти впливу погодних умов; динамічні руйнування з витіканням рідин; симуляція крові та інших органічних субстанцій.

Симуляція м'яких тіл охоплює широкий клас об'єктів, здатних змінювати форму: тканини, органічні структури, желеподібні субстанції. Основними підходами до моделювання таких об'єктів є:

Масо-пружинні моделі – представляють об'єкт як мережу точок (мас), з'єднаних пружинами. Цей метод вирізняється обчислювальною ефективністю та гнучкістю налаштувань, що робить його популярним у 3D-анімації та ігрових проєктах [5].

Метод скінченних елементів (FEM) – забезпечує вищу фізичну точність, розбиваючи об'єкт на дискретні елементи та розв'язуючи рівняння для кожного з них. Через високі обчислювальні вимоги цей метод переважно застосовується в інженерних симуляціях або у високобюджетних іграх на потужних платформах.

В іграх симуляція м'яких тіл найчастіше застосовується для реалістичних тканин одягу та прапорів, динамічної рослинності, желеподібних субстанцій, хутра і волосся персонажів.

Сучасні графічні процесори (GPU) з їхньою паралельною архітектурою відкрили нові можливості для фізичного моделювання. Технології CUDA (NVIDIA), OpenCL і DirectCompute дозволяють обробляти тисячі частинок або елементів одночасно, що суттєво підвищує продуктивність складних симуляцій [6].

GPU-прискорення стало стандартом у високобюджетних проєктах, уможливлюючи масштабні симуляції руйнувань, реалістичні ефекти вибухів з тисячами частинок, складні моделі тканин з високою деталізацією, об'ємні ефекти диму, вогню та туману.

Інноваційним напрямком у фізичному моделюванні стало застосування нейронних мереж для апроксимації фізичних процесів. Такі моделі здатні «навчатися» фізичним законам на основі даних, отриманих з традиційних симуляцій або реальних спостережень [7].

Перевагами нейромережевого підходу є висока швидкодія після завершення навчання, здатність узагальнювати фізичну поведінку для нових ситуацій, можливість працювати з неповними або зашумленими даними.

У сучасних іграх нейромережі часто застосовуються для керування рухами персонажів. Наприклад, у «Shadow of the Tomb Raider» деякі анімаційні реакції тіла героїні створені за допомогою систем на основі нейромереж із фізичним зворотним зв'язком, що забезпечує природну адаптацію до різноманітних ситуацій та поверхонь [8].

Сучасні ігрові рушії рідко обмежуються одним методом фізичного моделювання. Натомість вони комбінують кілька підходів у гібридній архітектурі, поєднуючи симуляцію жорстких тіл, моделювання м'яких тіл, системи частинок, симуляцію газів і рідин.

Важливою тенденцією є також інтеграція фізичних моделей із системами штучного інтелекту. Це дозволяє створювати неігрових персонажів (NPC), які природно взаємодіють із фізичним середовищем, враховуючи його стан у процесі прийняття рішень [9].

З розвитком обчислювальних технологій і алгоритмів машинного навчання очікується поява нових підходів до фізичного моделювання. Особливо перспективним напрямком є «нейрофізика» – гібридні системи, що поєднують традиційні фізичні симуляції з нейромережевими моделями. Такі системи потенційно зможуть забезпечити баланс між фізичною точністю та обчислювальною ефективністю.

Інші перспективні напрямки включають:

- масштабні симуляції руйнувань з високою деталізацією;
- реалістичне моделювання природних явищ (ерозія, зростання рослин);
- вдосконалені моделі взаємодії матеріалів;
- фізично коректні симуляції звуку на основі геометрії об'єктів.

Фізичне моделювання залишається одним із ключових напрямків розвитку комп'ютерних ігор. Сучасні методи поєднують класичні підходи обчислювальної фізики з інноваційними технологіями машинного навчання, забезпечуючи все вищий рівень реалістичності та інтерактивності віртуальних світів. З подальшим розвитком обчислювальних платформ і алгоритмів ми можемо очікувати ще глибшої інтеграції фізичних симуляцій у ігрові механіки та наративи.

Список використаних джерел

1. Bédard C., Tisserand L., Migneault B. Physics-Based Animation for Game Development. Boca Raton: CRC Press, 2020. 354 p.
2. Havok Physics SDK Documentation [Електронний ресурс]. URL: https://www.havok.com/products/physics/ (дата звернення: 10.05.2025).
3. Eberly D. Game Physics. 2nd Ed. Burlington: Morgan Kaufmann, 2010. 752 p.
4. Müller M., Chentanez N., Macklin M. Fast and Robust Simulation of Cloth with Position Based Dynamics // ACM Transactions on Graphics. 2016. Vol. 36, No. 4. Article 105. P. 105:1–105:10.
5. Baraff D., Witkin A. Large steps in cloth simulation // Proceedings of the 25th Annual Conference on Computer Graphics and Interactive Techniques (SIGGRAPH '98). 1998. P. 43-54.
6. NVIDIA CUDA Toolkit Documentation [Електронний ресурс]. URL: https://developer.nvidia.com/cuda-toolkit (дата звернення: 15.05.2025).
7. Sanchez-Gonzalez A., Godwin J., Pfaff T., et al. Learning to Simulate Complex Physics with Graph Networks // Proceedings of the 37th International Conference on Machine Learning (ICML 2020). 2020. P. 8459–8468.
8. Bergamin K., Beacco A., Komura T., Kaufmann P. DART: Dense Action-aware Retargeting for Character Control // ACM Transactions on Graphics. 2019. Vol. 38, No. 4. Article 144. P. 1-11.
9. Goyal A., Lamb A. M., Hoffmann J., et al. Inductive biases for relational reasoning in physics // Advances in Neural Information Processing Systems 35 (NeurIPS 2022). 2022. P. 16215–16229.

Ключові слова: комп'ютерні ігри, фізичне моделювання, GPU-прискорення, машинне навчання у фізиці, реалістична симуляція, інтерактивність, рідинна динаміка, деформація об'єктів, м'які тіла, фізичний штучний інтелект.

Keywords: video games, physical simulation, GPU acceleration, machine learning in physics, realistic simulation, interactivity, fluid dynamics, object deformation, soft bodies, physical artificial intelligence.

СТВОРЕННЯ АДАПТИВНОГО ІНТЕРФЕЙСУ у відеогрі

Кремішов Данило

студент 5-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У сучасній індустрії відеоігор користувацький інтерфейс відіграє критичну роль у забезпеченні позитивного досвіду гравців. Проте розробка естетично привабливого та функціонального інтерфейсу створює значні труднощі для розробників, які не мають професійної дизайнерської підготовки.

При розробці застосунку однією з проблем може стати створення якісного дизайну інтерфейсу без залучення професійного дизайнера. Розробники з обмеженим досвідом у дизайні, навіть дальтонізмом можуть зіткнутися із

труднощами підбору гармонійних кольорових схем для різних елементів відеогри: динамічні темі, ігрове поле та інші меню як вікно перемоги/поразки.

Традиційний підхід до підбору кольорів передбачає використання колірного кола та суб'єктивну оцінку комбінацій, що для розробників з дальтонізмом створює суттєві перешкоди. Наприклад, інтерфейс з п'ятьма анімованими елементами, кожен з яких потребує підбору 3–4 кольорів для різних станів (базовий, при наведенні, активний, неактивний), вимагає узгодження 15–20 кольорів, що для людини з порушенням кольоросприйняття перетворюється на процес "спроб і помилок". Це збільшує тривалість розробки до 2-3 разів порівняно зі стандартним процесом, знижує якість візуального оформлення та може призвести до відмови від динамічних елементів на користь більш консервативного дизайну, що негативно впливає на користувацький досвід. Ці обмеження особливо критичні для інді-розробників, які працюють самостійно або в невеликих командах без спеціалізованих дизайнерів.

Ефективним рішенням є імплементація систематичного підходу з використанням спеціалізованих інструментів та алгоритмізації процесу підбору кольорів. Замість суб'єктивної оцінки, процес ґрунтується на математичних моделях колірної гармонії та доступності для користувачів з різними типами кольоросприйняття. Сервіс Coolors.co, що пропонує генерацію гармонійних палітр та симуляцію різних типів дальтонізму, використовується як базовий інструмент для створення статичних колірних схем.

Першим кроком потрібно обрати основні кольорі користувацького інтерфейсу для тем, які будуть використовуватися у відеогрі. Це можуть бути такі кольори: бежевий, блакитний, та червоний. Дуже важливо щоб насиченість кольорів була не занадто велика, тому що в такому випадку користувач може втомитися не знаючи причини та покинути відеогру. Отже потрібно обрати кольори (рис. 1), які одночасно не будуть стомлювати і будуть поєднуватися.

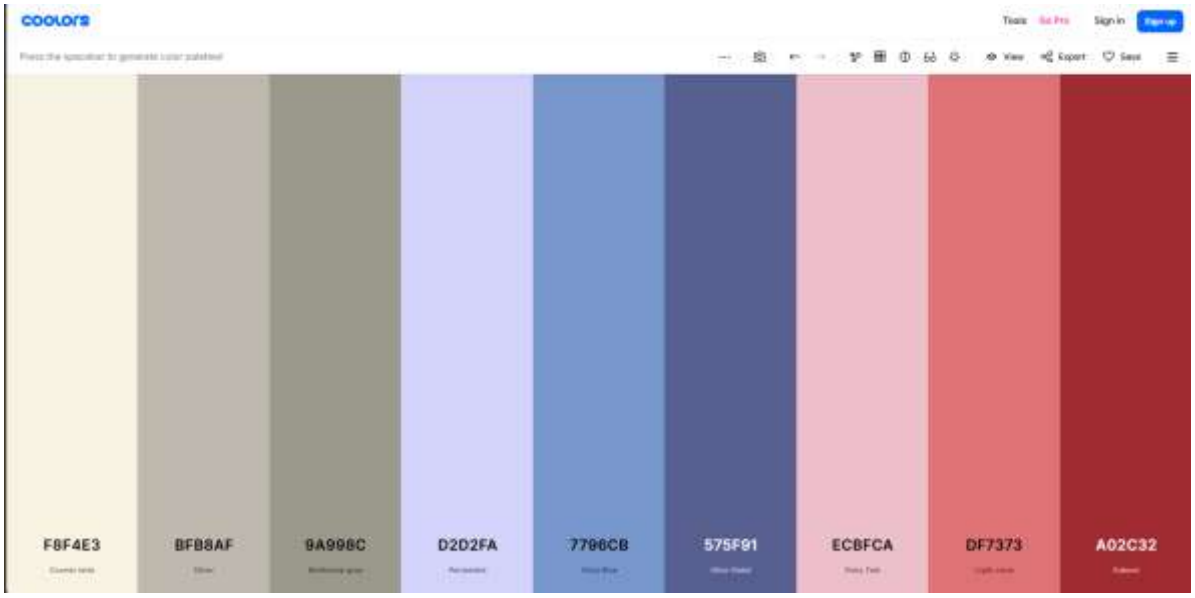

Рисунок 1 – Генератор кольорів Coolors.co

Далі потрібно інтегрувати кольори до проекту. На цьому етапі також створюються анімації переходів між станами з використанням DOTween. Зокрема, для зміни кольору кнопки при наведенні курсору створюється послідовність DOTween.To(). Unity та DOTween (рис. 2) автоматично обчислюють проміжні кольори для плавного переходу між станами, забезпечуючи візуальну привабливість анімацій.

```
95          DOTween.To(
96              getter: () => _backgroundImage.color,
97              setter: color => _backgroundImage.color = color,
98              _currentBackgroundColor,
99              _colorChangeSpeed
100         );
```

Рисунок 2 – DOTween динамічний перехід кольорів

Останній етап полягає у тестуванні створених елементів. За допомоги додаткових скриптів для керування інтерфейсом створюється можливість керувати інтерфейсом та змінювати рівень складності разом із кольорами інтерфейсу (рис. 3).

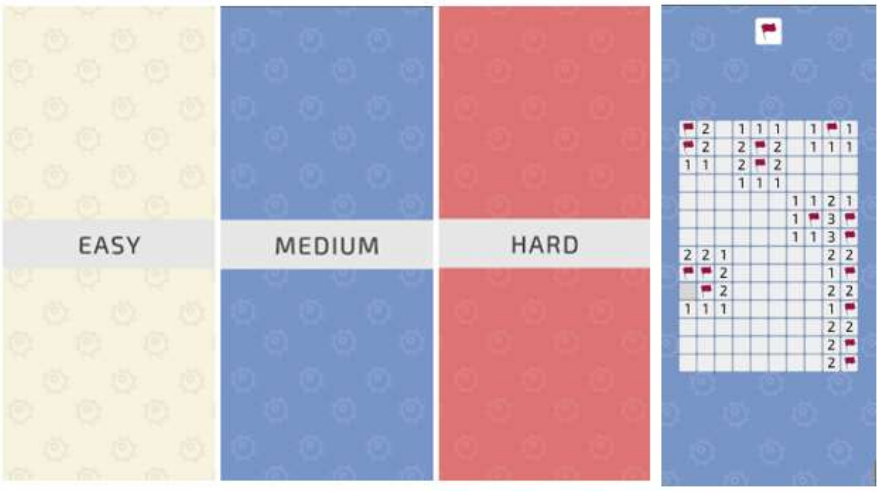

Рисунок 3 – Результат створеного інтерфейсу

Такий підхід до створення дизайну інтерфейсу дозволяє подолати обмеження через дальтонізму та недостатньої кількості навичок у сфері дизайну. Час розробки кольорових схем для динамічних елементів може скоротитися у рази завдяки автоматизації через Coolors.co. Використання DOTween у поєднанні з оптимізованим підбором кольорів забезпечило створення плавних, візуально узгоджених анімацій, що позитивно вплинуло на загальне сприйняття інтерфейсу користувачами.

Список використаних джерел

1. Coolors.co help center URL: https://coolors-help.zendesk.com/hc/en-us
2. Unity Manual. URL: https://docs.unity3d.com/Manual/index.html
3. DOTween documentation. URL: https://dotween.demigiant.com/documentation.php

4. Color Theory. URL: https://careerfoundry.com/en/blog/ui-design/introduction-to-color-theory-and-color-palettes/

Ключові слова: розробка ігор, адаптивний інтерфейс, Coolors.co, Unity, DOTween.

Keywords: game development, adaptive interface, Coolors.co, Unity, DOTween.

Науковий керівник: доцент Манаков С.

РОЗРОБКА ОБ'ЄКТІВ З SOFTBODY ФІЗИКОЮ У КОМП'ЮТЕРНИХ ІГРАХ

Федоренко Даніїл

студент 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У наш час комп'ютерні ігри стали дуже різноманітними. Різноманітність їх можливостей показує, наскільки далеко вони можуть зайти за допомогою різноманітних рушіїв, таких як Unity, Unreal Engine тощо. Ця різноманітність проявляється не тільки в програмному коді але і в візуалізації того, що відбувається у гравця або ж глядача на екрані. Така візуалізація може обманювати глядача, симулюючи будь-яку візуалізацію та графіку.

Один із найцікавіших і найвідоміших методів симуляції об'єктів є фізика *softbody* (м'яких тіл) в іграх [**Ошибка! Источник ссылки не найден.**]. Фізика softbody – це симуляція, яка деформує об'єкт при впливі зовнішніх сил, на відміну від *rigidbody* (твердих тіл), які зберігають свою форму. Простішим словами, це об'єкти у виді «желе», які при зштовхуванні з твердим об'єктом змінять свою форму, а потім приймуть початкову. Такий метод дає найреалістичніший вид «желейних» об'єктів який тільки можна зробити, але головне питання: як це реалізувати?

У прикладі буде розглянуто цей метод у межах рушія Unity. Слід зазначити що є *rigidbody* під номером 1 та *rigidbody* під номером 2, якщо тіло 1 та тіло 2 знаходяться дуже близько одне до одного, то вони відштовхуються, а коли дуже далеко – притягуються. Таким чином, можна стверджувати про силу, пропорційну їх відстані, на яку вони перебувають від бажаної позиції один від одного, або простіше можна уявити таку прозору пружину між тілами яка не дає ним відштовхуватися та не дає притягуватися один до одного.

Така формула має назву Spring Force Formula (формула сили пружини): $F = -kx$, де

F – це сила пружини;

k – це пружність;

x – це зміщення від положення рівноваги пружини в метрах.

Для кращої стабільності нашої "пружини" слід підключити силу яка напряму затримує будь-який рух розглядвємих тіл bv, тобто $F = kx-bv$. Частина яку ми добавили частіше за всього називається /damping (демпфування) [2], у якій:

b – це коефіцієнт демпфування;

v – це відносна швидкість кінців пружини.

Разом ці сили в розробці комп'ютерних ігор називаються *Spring Joint*. Можемо розглядати компонент *bv* що протидіє руху, як тертя в системі, поглинаючи енергію, щоб запобігти нескінченним коливанням. Розуміння цих сил у контексті, як вони працюють це дуже важлива частина роботи з фізикою *softbody*, та її структурою.

Softbody не являється лише двома тілами. Щоб створити насправді плавний і цілий об'єкт то треба зробити фігуру. У нашому випадку на прикладі зробимо куб, який буде складатися з 8 тіл які будуть відштовхуватися один від одного на регулярній основі, поставив їх по кутам нашого куба. Щоб наш куб насправді був як "желе" слід з'єднати тіла не тільки по вертикалі, а і по діагоналям один до одного щоб кожен об'єкт мав один і той самий ефект.

Розробка комп'ютерної ігри – це дуже продумана річ, яка має бути розвинена не лише на візуальну частину, а й на оптимізаційну, тож це головна причина чому було встановлено лише 8 тіл по кожному куту, а не наприклад 32 на весь куб, щоб не навантажувати надмірними розрахунками рушій.

Наступне що треба добавити на куб це mesh (сітка), на яку потім буде налаштовуватись текстура куба [3]. Сітка складається з багатьох вершин або точок, які формують трикутники з яких потім виходять сітки. Для розробки сітки слід встановлювати по кожній унікальній частці нашого куба, в даному випадку беремо лише частці котрі знаходяться на кутах нашого основного об'єкту.

Дуже важливо не брати дуже багато тіл, тобто з сіткою не брати дуже багато часток щоб наша текстура не переламалася з іншими текстурами, та дуже важливо також з'єднати усі частинки між собою як на попередньому прикладі. Наступним чином треба зробити та розрахувати точки які знаходяться всередині трикутника.

Слід уявити що у створеному кубі є багато точок, наприклад 32, всі ці точки відповідальні за нашу сітку, та щоб створена текстура не ламалася при колізії куба з якимось сталим об'єктом треба розраховувати скільки точок остається при кожному стиснені куба та його руху до нього самого. Наша текстура лежить на цих точках які залишаються в кубі при тиснені. Ці точки це є за що сітка тримається та відображає потрібну текстуру.

В загалом фізика *softbody* відкриває багато можливостей розробникам у сфері геймдеву та програмного моделювання об'єктів. Softbody надає можливість створювати желейно-подібні тіла, гладкий одяг, імітацію кульок тощо [4]. Навчитися створюванню такого типу речей не найпростіше завдання але воно дає свої найцікавіші результати та показники які можна використовувати у дуже різноманітніших речах.

Список використаних джерел

1. Lem Apperson Beginning Game Development: Soft Body Physics. URL:

https://medium.com/@lemapp09/beginning-game-development-soft-body-physics-03a092b6ca3f
2. LibreTexts Physics: Damped Oscillations. URL: https://phys.libretexts.org/Bookshelves/University_Physics/University_Physics_(OpenStax)/Book%3A_University_Physics_I_-_Mechanics_Sound_Oscillations_and_Waves_(OpenStax)/15%3A_Oscillations/15.06%3A_Damped_Oscillations
3. DayyanSisson: Mesh Deformation. Question on Unity Discussions. URL: https://discussions.unity.com/t/mesh-deformation/45190
4. Swapnil More: Advanced Physics: Soft Bodies, Cloth, and Fluid Simulation. URL: https://swapnilmore03.medium.com/advanced-physics-soft-bodies-cloth-and-fluid-simulation-7b847d7f021e

Ключові слова: м'яке тіло, тверде тіло, Формула Сили Пружини, демпфування, сітка

Keywords: softbody, rigidbody, Spring Force Formula, damping, mesh

Науковий керівник: доцент Задерейко О.

РУШІЙ UNITY: ПОРІВНЯННЯ, АРХІТЕКТУРА ТА ОСОБЛИВОСТІ ЗАСТОСУВАННЯ

Задерейко Олександр

доцент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»
кандидат технічних наук, доцент

Д'якова Ксенія

студентка 1-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету "Одеська юридична академія"

Рушій Unity – це сучасний ігровий рушій зі зручним візуальним редактором і гнучкою підтримкою скриптів, що робить його інструментом для створення ігор різного рівня складності. На відміну від більшості схожих платформ, які звичайно ускладнюють інтеграцію, рушій Unity дає змогу розробникам без зусиль поєднувати написані скрипти з проєктами. Це значно спрощує процес створення та налаштування, зберігаючи при цьому гнучкість і контроль над розробкою комп'ютерних ігор [1].

Однією з сильних сторін рушія Unity є його редактор, який прискорює процес розробки комп'ютерних ігор, дозволяючи швидко вносити зміни і одразу бачити результат. Завдяки цьому інструменту можна легко налаштовувати об'єкти, змінювати їх під час розробки гри, у реальному часі та розширювати функціонал редактора власними скриптами, створюючи нові потрібні функції. Рушій Unity має набір кількох варіантів ліцензій, що визначають вибір доступних інструментів. Безкоштовна ліцензія забезпечує всі необхідні можливості для

розробки ігор для Windows, Mac, Linux, вебплатформ, а також мобільних систем, таких як iOS (iPhone, iPad, iPod Touch), Android і BlackBerry. Ліцензія Pro надає професійні інструменти, зокрема Профайлер чи вбудовану систему контролю версій, що дозволяє використовувати апаратне забезпечення ефективно [2].

Ще однією сильною стороною рушія Unity є його здатність працювати на різних платформах. Рушій дає змогу розробляти на Windows і Mac OS, а також переносити їх на різноманітні системи: ПК, веб, мобільні пристрої, консолі (PS3, PS4, PS Vita, Xbox 360, Xbox One, Wii, Wii U, 3DS) і WebGL [3, С. 105–109].

Професійні студії, які працюють із фірмами Sony, Microsoft та Nintendo, рушій Unity надає можливість використати плагіни для консолей.

У архітектурі Unity лежить модульна система компонентів. Вона дуже полегшує створення ігрових об'єктів, отже за допомогою цього розробники можуть комбінувати вже готові елементи, роблячи процес розробки ігор не лише продуктивним, а й зрозумілим користувачу. Завдяки інтеграції з редактором і підтримці скриптів, Unity балансує між простотою використання та глибиною налаштувань.

Рушій Unity здобув популярність у розробці ігор для різних платформ завдяки своєї універсальності. Стартувавши у 2005 році як інструмент для операційної системи Mac, рушій з часом розширив підтримку різних платформ: у 2006-му з'явився веб-плеєр, у 2008-му – підтримка iPhone, у 2010-му – Android, а пізніше додалися консолі та WebGL [4]. На сьогодні рушій Unity є одним із фаворитів серед ігрових рушіїв, адже мало хто з конкурентів може зрівнятися з ним за кількістю підтримуємих операційних систем і легкістю їхнього опанування. Безкоштовна версія ідеально підходить для початківців, тоді як Pro-версія відкриває додаткові можливості для великих команд.

Одним із популярних прикладів можливостей рушія Unity є розробка простих, але популярних 2D-ігор, таких як «Flappy Bird». Цей проєкт було розроблено Донгом Нгюеном для iOS у 2013 році, а вже у 2014-му захопив увагу користувачів Android завдяки своєї мінімалістичній механіці [5]. Рушій Unity підходить для таких проєктів, адже має вбудовані інструменти для 2D-розробки. До прикладу система Physics 2D, що робить взаємодії у двовимірному світі простими і зрозумілими [6]. Порівнюючи з Unreal Engine, який більше підходить для розробки 3D ігор, рушій Unity дає можливості швидше зануритися в процес розробки і здобути необхідні навички.

Простота рушія Unity частково вирізняється в застосуванні мови C#, що є більш прозорим синтаксисом і автоматичним управлінням пам'яттю в порівнянні з C++, який використовується в Unreal Engine [7]. Саме це робить рушій Unity вдалим рішенням для розробки ігор у будь-яких жанрах.

Unity відрізняється можливістю поєднувати різноманітні аспекти розробки в одну єдину систему. Наприклад, програмісти та дизайнери можуть одночасно працювати над кодом і візуальною частиною гри прямо у редакторі, без потреби перемикатися між зовнішніми програмами або окремими інструментами.

Подивившись на рушій Unity з іншого погляду, стає зрозуміло, що він втілює ідею поєднання зв'язків. Модульна структура рушія Unity дозволяє об'єктам гри, персонажам чи перешкодам, мати окремі компонентів, які взаємодіють спільно, не прив'язуючись до одної бази [8]. Це додає процесу розробки ігор гнучкості і доступності. Рушій Unity дозволяє вносити зміни як в редакторі, так і розвивати його, зберігаючи певний стан проєкту та додаючи можливості з часом. І досвідчені розробники великих проектів, і новачки, які, розробляють невеличку просту гру, дуже цінують саме гнучкість проєкту.

Важливу роль у поширенні рушія Unity грає спільнота, що гуртується навколо нього. Завдяки активному обміну досвідом, кодом і готовими матеріалами розробники мають змогу знаходити підтримку чи ідеї для реалізації. Це дає відчуття тісного зв'язку між розробниками і користувачами [9]. Рушій Unity не просто надає технічні елементи розробки, а й об'єднує людей, які разом створюють ігри. Фахівці мають змогу покращити свої проєкти, користуючись складними інструментами, як ML-Agents (для роботи зі штучним інтелектом).

Рушій Unity збирає до купи різні елементи розробки, від написання коду до створення дизайну. Інструменти для 2D і 3D проєктів, створюються за схожими принципами – використовуються компоненти і скрипти, отже розробники легко перемикаються з 2D і 3D виміру і навпаки. У випадку з рушієм Unity це відображається в його модульній структурі, де різні компоненти – фізичні, візуальні, логічні, перетинаються, формуючи багато можливостей для об'єднання елементів гри.

Рушій Unity – професійний інструмент для створення ігор, завдяки якому можна створювати проєкти для комп'ютерів, телефонів та консолей [10]. Він поєднує простоту використання та можливості безкоштовних версій. Рушій є знахідкою для навчання. Кросплатформеним IDE та активне онлайн ком'юніті допомагає з вирішенням питання будь якої складності. У рушії є вбудована бібліотека Asset Store, де розробники обмінюються готовими скриптами, моделями й матеріалами або беруть їх безкоштовно чи за плату. Отже починаючий користувач матиме більше часу на освоєння, адже правильне використання часу має велике значення у здобуті навичок, а профійльний спеціаліст зможе ефективно проаналізувати розробку ідеї та її реалізацію.

Список використаних джерел

1. Бондаренко М. Р. Ігровий додаток жанру «Аркада» для ОС Android [Електронний ресурс] : кваліфікаційна робота бакалавра / М. Р. Бондаренко ; КПІ ім. Ігоря Сікорського. Київ, 2023. URL: https://ela.kpi.ua/items/bc05b784-1339-4f9f-8175-ff861c923272
2. Лабзенко О. С. Оптимізація ігор на рушії Unity за допомогою алгоритмів Occlusion Culling та Frustrum Culling [Електронний ресурс] : кваліфікаційна робота бакалавра / О. С. Лабзенко ; КПІ ім. Ігоря Сікорського. Київ, 2023. URL: https://ela.kpi.ua/items/ca36521c-d1a6-4285-99b4-c90cc41a7fdf

3. Шабанов-Кушнаренко Ю. П., Клименко І. А., Клименко А. В. Методи та алгоритми портування ігор. Радіоелектроніка та інформатика. 2011. № 3. С. 105–109. URL: https://openarchive.nure.ua/entities/publication/ed7183c4-50a9-4a25-a6eb-00e06c24b22a
4. Чоботар О. О. Розробка комп'ютерної 2D гри на платформі Unity [Електронний ресурс] : кваліфікаційна робота бакалавра / О. О. Чоботар ; ЧНУ ім. Петра Могили. Миколаїв, 2020. URL: https://krs.chmnu.edu.ua/jspui/handle/123456789/3304
5. Flappy Bird [Електронний ресурс] // Вікіпедія : вільна енциклопедія. URL: https://uk.wikipedia.org/wiki/Flappy_bird
6. Shalamov M. E., Belyaeva E. V., Gainutdinova E. V. 2D and 3D virtual interactive laboratories of physics on Unity platform. Journal of Physics: Conference Series. 2017. Vol. 935, iss. 1. P. 012069. URL: https://iopscience.iop.org/article/10.1088/1742-6596/935/1/012069. DOI: https://doi.org/10.1088/1742-6596/935/1/012069.
7. Редакція GameDev DOU. Unity проти Unreal Engine – який рушій обрати для гри та чому. Зважуємо всі за та проти з розробниками. GameDev DOU. 2024. 14 лют. URL: https://gamedev.dou.ua/articles/unity-or-unreal-engine/
8. Макушенко І. М. Оптимізація гри на рушії Unity [Електронний ресурс] : кваліфікаційна робота бакалавра / І. М. Макушенко ; КПІ ім. Ігоря Сікорського. Київ, 2023. URL: https://ela.kpi.ua/items/14d957d8-37e9-41b0-8fcd-5795876044e0
9. Unity Discussions [Електронний ресурс] / Unity Technologies. URL: https://discussions.unity.com/
10. Гальчинський А. С. Розробка гіперказуальної мобільної 3D-гри «Stack Tower» [Електронний ресурс] : кваліфікаційна робота магістра / А. С. Гальчинський ; Державний університет «Житомирська політехніка». Житомир, 2022. URL: https://eztuir.ztu.edu.ua/bitstream/handle/123456789/6657/109.pdf?sequence=1&isAllowed=y

Ключові слова: рушій Unity, ігрові рушії, розробка ігор, кросплатформеність, 2D ігри, 3D ігри

Keywords: Unity engine, game engines, game development, cross-platform, 2D games, 3D games. Unity engine, game engines, game development, cross-platform, 2D games, 3D games

ПСИХОЛОГІЯ ГРАВЦЯ: ІНФОРМАЦІЙНО-ТЕХНОЛОГІЧНИЙ АНАЛІЗ ФАКТОРІВ, ЩО СПРИЯЮТЬ ПОВТОРНОМУ ЗАЛУЧЕННЮ ДО КОМП'ЮТЕРНИХ ІГОР

Черненко Олександра

студентка 2 курсу факультету кібербезпеки та інформаційних технологій
Національний університет «Одеська юридична академія»

Комп'ютерні ігри стали невід'ємною частиною сучасного суспільства, охоплюючи мільйони гравців по всьому світу. Згідно з даними аналітичної компанії Newzoo, у 2024 році глобальна аудиторія геймерів перевищила 3,2 мільярда осіб, а обсяг ринку комп'ютерних ігор склав понад 200 мільярдів доларів США. Така популярність значною мірою зумовлена здатністю ігор викликати повторне

залучення гравців. У цій доповіді ми розглянемо психологічні та інформаційно-технологічні фактори, які сприяють цьому явищу, спираючись на сучасні дослідження та аналіз механізмів, вбудованих у дизайн комп'ютерних ігор.

Психологія гравця у контексті комп'ютерних ігор ґрунтується на фундаментальних принципах людської поведінки, таких як: мотивація, винагорода та соціальна взаємодія, які разом формують потужний механізм повторного залучення. Одним із ключових підходів до розуміння цього процесу є теорія самодетермінації, яка пояснює, як комп'ютерні ігри задовольняють базові психологічні потреби людини: автономію, компетентність і пов'язаність. Наприклад, у грі «The Legend of Zelda: Breath of the Wild» гравці отримують свободу досліджувати відкритий світ, що посилює відчуття автономії, складні виклики та система нагород у «Dark Souls» стимулюють компетентність через подолання труднощів, даючи відчуття прогресу, а взаємодія з іншими гравцями, відвідування островів друзів, обмін предметами та листування в «Animal Crossing: New Horizons» створюють атмосферу спільноти і дозволяють гравцю відчувати себе частиною колективу. А спільне виконання рейдів та участь у гільдіях у «World of Warcraft» створює міцні соціальні зв'язки, шо іноді переходять у дружбу в реальному житті.

Паралельно з цим важливу роль відіграє система дофамінової винагороди, підтверджена дослідженнями нейробіологів, зокрема опублікованими в журналі Nature Neuroscience [1] у 2021 році, які показують, що ігрові механіки, такі як отримання досягнень чи лут-боксів, активують дофамінові шляхи в мозку, створюючи цикл "бажання-винагорода", що мотивує гравців повертатися до гри знову і знову.

Додатковим фактором є ефект Зейгарник, коли незавершені завдання або сюжетні лінії, як-от у «Mass Effect», де гравці прагнуть дізнатися наслідки своїх рішень, спонукають їх продовжувати грати, щоб досягти завершення. Подібний механізм застосовується в «*Detroit: Become Human»*, де багатовекторна структура оповіді з десятками можливих варіантів розвитку подій тримає гравця в напрузі, стимулюючи повертатися до гри, щоб дослідити альтернативні наслідки власного вибору. Таким чином, психологічні основи повторного залучення до комп'ютерних ігор поєднують у собі внутрішню мотивацію, нейрофізіологічні реакції та когнітивні стимули, створюючи комплексний вплив на поведінку гравців.

Сучасні інформаційно-технологічні фактори відіграють ключову роль у підсиленні психологічних тригерів, що сприяють повторному залученню гравців до комп'ютерних ігор, завдяки складним системам, які розробники впроваджують за допомогою передових технологій. Одним із таких інструментів є персоналізація через штучний інтелект (ШІ), який аналізує поведінку гравця і адаптує ігровий досвід, як це реалізовано в «Shadow of Mordor» через систему Nemesis, де унікальні вороги «запам'ятовують» дії гравця, підвищуючи рівень залученості, а аналітика даних у реальному часі дозволяє динамічно коригувати складність гри чи пропонувати персоналізовані винагороди.

Не менш важливими є механіки гейміфікації, які інтегрують рівні, значки та

таблиці лідерів, як у «Call of Duty», стимулюючи конкурентність і соціальний престиж; за даними дослідження Journal of Interactive Marketing [2] 2022 року, такі елементи здатні збільшувати час, проведений у грі, на 30-40%. Соціальна взаємодія також стала потужним фактором завдяки мультиплеєрним іграм, таким як «Fortnite» чи «Among Us», де технології хмарних серверів і потокового мовлення забезпечують об'єднання мільйонів гравців у реальному часі, посилюючи відчуття спільноти та спонукаючи повертатися до гри. Нарешті, системи мікротранзакцій і модель «ігор як сервісів» (Games as a Service), яскравим прикладом якої є «Genshin Impact», використовують лут-бокси та сезонні перепустки з обмеженими за часом пропозиціями, що мотивують регулярне повернення; звіт Statista за 2023 [3] рік підкреслює, що 70% доходів від комп'ютерних ігор генеруються саме за рахунок мікротранзакцій. Таким чином, поєднання ШІ, гейміфікації, соціальних технологій і економічних моделей створює технологічну основу, яка ефективно утримує увагу гравців і сприяє їхньому тривалому залученню.

Аргументи та факти, що підтверджують феномен повторного залучення до комп'ютерних ігор, спираються на об'єктивні дані та наукові дослідження, які демонструють як масштаби явища, так і його технологічні основи. За даними Entertainment Software Association (ESA) [4] за 2024 рік, 65% гравців витрачають на комп'ютерні ігри понад 10 годин на тиждень, що свідчить про значний рівень їхньої залученості, причому 40% із них повертаються до улюблених ігор завдяки регулярним оновленням контенту, які підтримують інтерес і додають нові стимули для гри.

Водночас технологічний прогрес суттєво сприяє цьому процесу: розвиток мереж 5G і хмарних платформ, таких як Google Stadia чи Xbox Cloud Gaming, усуває бар'єри доступу, дозволяючи гравцям занурюватися в ігровий світ із будь-якого пристрою – від смартфонів до ноутбуків, що значно підвищує частоту їхнього залучення.

Крім того, наукові дослідження підтверджують вплив соціальних елементів на психологію гравців: Університет Оксфорда у 2023 році встановив, що ігри з мультиплеєрними та соціальними функціями підвищують рівень задоволеності гравців на 25% порівняно з одиночними іграми, підкреслюючи важливість соціальної взаємодії як фактора, що утримує аудиторію.

Напрями розвитку інформаційних технологій у контексті психології гравця відкривають нові горизонти для створення більш захопливого ігрового досвіду, але водночас ставлять перед розробниками етичні виклики. Технології віртуальної реальності (VR) та доповненої реальності (AR), яскравим прикладом яких є Half-Life: Alyx забезпечують глибше занурення в ігровий світ, підсилюючи емоційний зв'язок гравців із контентом і роблячи кожен сеанс гри незабутнім, що мотивує їх повертатися. Паралельно з цим аналіз великих даних (Big Data) стає невід'ємною частиною стратегій компаній, таких як Epic Games, які використовують зібрану інформацію для прогнозування поведінки гравців і створення цільових оновлень, що відповідають їхнім інтересам і потребам, ще більше закріплюючи залученість. Однак цей прогрес має й зворотний бік: надмірне залучення може призводити до ігрової залежності, що є серйозною проблемою.

Проблема ігрової залежності, зокрема у жанрі гача-ігор, є прикладом того, як психологічні та інформаційно-технологічні механізми можуть мати негативні наслідки. У цих іграх гравці витрачають реальні кошти на внутрішньоігрову валюту для участі в механіці «кручення банерів», що спрямована на отримання рідкісних персонажів чи предметів. Дослідження поведінкової економіки, зокрема концепція «ефекту вкладених ресурсів» (sunk cost fallacy), пояснює, що гравці, інвестуючи значні суми, відчувають мотивацію продовжувати гру, щоб виправдати свої витрати. Така поведінка зумовлена емоційною прив'язаністю до гри, що формується через фінансові вкладення. Обмежені за часом події та персоналізовані пропозиції, підтримувані алгоритмами штучного інтелекту, посилюють тиск на гравців, сприяючи компульсивній поведінці для здійснення додаткових покупок. Наприклад, за даними форумів, таких як GameFAQs, гравці *Honkai: Star Rail* повідомляли про витрати від $500 до $1000 на банери, а у 2021 році, як зазначає The Straits Times [5], 18-річна гравчиня з Сінгапуру витратила $20,000 на внутрішньоігрові покупки у *Genshin Impact*. Таким чином, монетизація гача-ігор, хоча й ефективна для залучення доходів, проте може сприяти розвитку ігрової залежності, що потребує подальшого дослідження її впливу та регулювання реалізації моделей монетизації.

Отже, у висновку слід зазначити, що повторне залучення до комп'ютерних ігор є результатом складної взаємодії психологічних механізмів і передових інформаційних технологій. Такі інструменти як: ШІ, гейміфікація, соціальні елементи та персоналізація - ефективно утримують гравців, одночасно задовольняючи їхні базові потреби, проте їх використання, особливо в моделях монетизації, породжує етичні виклики, пов'язані з ризиком ігрової залежності. Водночас стрімкий розвиток технологій відкриває нові можливості для створення ще більш захопливого досвіду. Подальші дослідження в цій галузі можуть допомогти оптимізувати дизайн ігор, роблячи їх не лише привабливими, але й безпечними для психічного здоров'я гравців.

Список використаних джерел

1. Nature Neuroscience. URL: https://www.nature.com/neuro/articles?year=2021
2. Journal of Interactive Marketing. URL: https://journals.sagepub.com/home/JNM
3. Statista. URL: https://www.statista.com/
4. Entertainment Software Association (ESA). URL: https://www.theesa.com/
5. Dad saddled with $20,000 credit card bill after daughter's in-game spending spree on Genshin Impact. URL:https://www.straitstimes.com/singapore/community/dad-saddled-with-20000-credit-card-bill-after-daughters-in-game-purchase-spree-on-genshin-impact

Ключові слова: психологія гравця, інформаційні технології, гейміфікація, компьютерні ігри.

Keywords: player psychology, information technology, gamification, computer games.

Науковий керівник: PhD Грезіна О.

СКЛАДНОЩІ ТА НЕДОЛІКИ ВИКОРИСТАННЯ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ В РОЗРОБЛЕННІ ТА ТЕСТУВАННІ ІГОР

Трофименко Олена

доцент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»
кандидат технічних наук, доцент

Використання генеративного штучного інтелекту (ШІ) у розробленні та тестуванні ігор відкриває нові горизонти, проте водночас має низку складнощів та недоліків, зумовлених як технічними, так і концептуальними обмеженнями сучасних генеративних моделей, а також природою самого процесу розробки ігор.

В силу специфіки генеративний ШІ добре працює з творчими завданнями, як-от: створення концепт-арту, діалогів або рівнів, проте він не завжди враховує ігрову логіку, баланс та взаємозв'язки в системі гри. Наприклад, модель може згенерувати гарний з естетичної точки зору рівень, але при цьому не забезпечити належного балансу складності чи можливостей для його проходження. Причиною цього є те, що генеративний ШІ працює на основі великих мовних або мультимодальних моделей, які не мають справжнього розуміння контексту та інтуїції. Вони оперують ймовірностями появи слів, зображень або структур на основі великих обсягів даних, на яких вони були натреновані [1]. Це означає, що модель може згенерувати щось, що виглядає правдоподібним, але не є функціональним або логічним у конкретному ігровому середовищі. Наприклад, вона може згенерувати граматично коректний діалог, який не відповідає поведінці персонажа, його мотивації або загальному наративу гри. Це обмеження є наслідком відсутності справжнього розуміння, адже ШІ не знає, що таке гра, сюжет, мотивація, правила чи емоції, а лише моделює ймовірні патерни на основі текстів або зображень з інтернету.

Генеративні ШІ-моделі часто працюють на основі текстових або візуальних підказок, але не завжди розуміють повну картину світу гри, її механіки або сюжет. Це може призвести до створення нелогічного або неузгодженого контенту. Наприклад, у фентезі-грі із суворою внутрішньою логікою може з'явитися NPC, який порушує цю логіку через те, що ШІ просто не врахував всіх деталей і логіки вигаданого світу гри – того, що називається лором (Game Lore). Наприклад, у грі на кшталт «The Elder Scrolls» є цілий всесвіт із расами, богами, законами магії, конфліктами між народами [2]. Якщо дати генеративному ШІ завдання створити нового персонажа для цієї гри, він може придумати щось, що на перший погляд здається цікавим, але суперечить встановленим правилам світу. Наприклад, згенерує ельфа, який вільно володіє забороненим видом магії, або який живе у місті, де його раса ніколи не жила (і навіть ворогувала з місцевими). Адже ШІ не розуміє цих обмежень, бо він не мислить як людина, а просто оперує ймовірностями на основі текстів, які бачив під час навчання. Якщо не надати ШІ повного

опису цього лору в конкретному запиті, він не зможе здогадатись, врахувати контекст та автоматично врахувати все тонкощі і тим самим порушить внутрішню логіку гри. Генеративний ШІ може створювати унікальний ігровий контент, але його якість не завжди відповідає очікуванням. Наприклад, алгоритми ШІ можуть генерувати нерівномірний рівень складності або недопрацьовані сюжетні лінії. Це може спричинити ситуації, коли гра здається незбалансованою або нецікавою.

У тестуванні ігор генеративний ШІ теж має певні обмеження. Хоча він може автоматизувати створення тест-кейсів і навіть виявляти помилки, його складно навчити розуміти складні ситуації, які виникають у грі з багатьма змінними. Автоматизований тест може пропустити баги, які для людини є очевидними, наприклад, злам балансу через певну комбінацію навичок або неприродна поведінка персонажа в конкретному сценарії [3]. Це пов’язано з тим, що генеративний ШІ не має інтуїції чи когнітивного досвіду гравця, який мають тестувальники. Людина, яка тестує гру, орієнтується на емоції, очікування, звички гравців і здатна виявити «тонкі» баги, які ШІ не вважає аномаліями. Крім того, генеративні моделі ШІ, особливо на основі трансформерів або інших подібних архітектур, не мають постійного стану пам’яті чи внутрішньої структури ігрового світу, яка дозволяла б їм повноцінно розуміти зв'язки між різними елементами гри, тому не можуть виявити логічні порушення на великих часових відрізках чи в складних ланцюгах подій.

Ще одна важлива причина – етичні та правові обмеження даних. Моделі навчаються на відкритих джерелах, які далеко не завжди стосуються професійних геймдизайнерських практик, технічних вимог до ігор чи то комерційних стандартів. У підсумку генеративний контент часто виявляється поверхневим, шаблонним або навіть надмірно повторюваним. Це також пояснює проблему авторського права: якщо модель тренується на творах без ліцензії або дозволів, вона може згенерувати результат, подібний до наявного твору, що створює юридичні ризики порушення прав третіх осіб. Крім того, є ризик створення небажаного або токсичного контенту. Це особливо критично в комерційній розробці, де будь-який юридичний спір може обернутись серйозними наслідками.

З іншого боку, надмірне використання генеративного ШІ може призвести до витіснення творчих спеціалістів – художників, сценаристів, дизайнерів ігрових рівнів. Водночас результати ШІ часто потребують доопрацювання, що означає додаткові витрати часу і ресурсів. Наприклад, згенерований сценарій може мати правильну структуру, але бути емоційно порожнім або не відповідати загальному тону гри. Генеративний ШІ не здатен повноцінно замінити цю командну динаміку, бо не володіє емоційною, креативною чи стратегічною гнучкістю людини. Навіть найкращі ШІ-моделі залишаються лише зручними інструментами, а не повноцінними учасниками процесу.

Також варто врахувати високі вимоги до обчислювальних ресурсів, оскільки генеративний ШІ потребує значних обчислювальних потужностей для

створення складного ігрового контенту. Технологія нейронного рендерингу, яку застосовують у сучасних іграх, потребує високопродуктивних серверів, що значно підвищує бюджет на розробку [4]. Це може бути фінансово обтяжливо для інді-студій та малих груп розробників.

Сучасна розробка ігор є складним міждисциплінарним процесом. У ньому взаємодіють програмісти, сценаристи, художники, дизайнери, продюсери, тестувальники, психологи. Якщо студії надто покладаються на автоматичне створення контенту засобами ШІ, унікальність та оригінальність ігрового досвіду можуть постраждати, гра може відчуватися менш "живою", а її рівні й механіки надто одноманітними.

Генеративний ШІ використовується для створення рівнів у багатьох rogue-like іграх, де кожен рівень та сценарій важливий для створення непередбачуваного і захоплюючого досвіду для гравця, але часто вони відчуваються шаблонними та позбавленими "людської" творчості. ШІ, хоч і здатен створювати нескінченну кількість варіацій, все одно залишається в межах визначених алгоритмами патернів, що може призвести до відчуття шаблонної повторюваності. Так, у більшості rogue-like ігор згенеровані рівні часто будуються за допомогою певних стандартних елементів: приміщення, коридори, вороги та предмети, і ці елементи часто розташовуються за принципом випадковості, без урахування загального балансу та атмосфери. Хоча такі рівні можуть бути різними по своїй структурі, вони все одно можуть виглядати схожими через відсутність глибокої людської креативності в їх дизайні. Подекуди це може призвести до відчуття, що, хоча рівні і змінюються, сама структура гри залишається насправді одноманітною. Особливо це відчувається, коли ті самі типи ворогів та пасток зустрічаються знову і знову. Це негативно позначається на оригінальності ігрового досвіду, бо гравці починають помічати схожі патерни при проходженні рівнів. При цьому проблема не стільки у використанні ШІ, а в тому, що він не здатен створити того рівня розмаїття, який можуть запропонувати справжні дизайнери. Саме дизайнери можуть адаптувати ігрові рівні, додавати елементи сюжету разом з відчуттям прогресії та глибини, а також враховувати емоційні реакції гравця на певні ситуації, що є складним для ШІ.

Всі зазначені складнощі й недоліки переважно зумовлені глибинними технічними обмеженнями моделей, відсутністю глибокого контекстного розуміння, обмеженістю навчальних даних і невідповідністю ШІ до багатогранності людської творчої діяльності в ігровій індустрії. Тому з розвитком технологій і можливостей генеративного ШІ, стає важливою роль людського контролю та креативного втручання в процес. Хоча генеративний ШІ дає потужні можливості для швидкого створення великої кількості ігрового контенту, важливо збалансувати його використання з людським дизайном, щоб зберегти унікальність і глибину геймплею. Людська творчість дозволяє внести несподівані елементи, емоційні моменти та складну взаємодію, чого поки що не може досягти ШІ в контексті геймдизайну. Наразі генеративний ШІ у розробці та тестуванні ігор потребує

ретельного контролю, адаптації та тестування. Найкращим рішенням є поєднання можливостей ШІ та творчого підходу розробників, що гарантує якісний контент й унікальний ігровий досвід.

Список використаних джерел

1. Трофименко О.Г., Дика А.І., Лобода Ю.В., Толокнов А.А., Бондаренко М.Є. Штучний інтелект у розробці ігор. Кібербезпека*: освіта, наука, техніка*. 2025. № 3(27). С. 109-119. DOI: https://doi.org/10.28925/2663-4023.2025.27.701.
2. I tried two demos of machine learning AI NPCs, and they didn't convince me AI will lead to anything that immersive sims like Deus Ex haven't already done better. URL: https://www.pcgamer.com/gaming-industry/i-tried-two-demos-of-machine-learning-ai-npcs-and-they-didnt-convince-me-the-ai-will-lead-to-anything-that-immersive-sims-like-deus-ex-havent-already-done-better/
3. Трофименко О.Г., Дика А.І., Лобода Ю.Г. Аналіз інструментів тестування вебзастосунків. *Кібербезпека: освіта, наука, техніка*. 2023. № 4(20). С. 62-71. DOI: https://doi.org/10.28925/2663-4023.2023.20.6271.
4. Inzoi's 'Smart Zoi' AI system sounds great on paper but seeing it in a live demo didn't exactly wow me. URL: https://www.pcgamer.com/games/life-sim/inzois-smart-zoi-ai-system-sounds-great-on-paper-but-seeing-it-in-a-live-demo-didnt-exactly-wow-me/

Ключові слова: штучний інтелект, ШІ, алгоритми ШІ, розробка ігор, тестування.

Keywords: artificial intelligence, AI, AI algorithms, game development, testing.

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ТЕСТУВАННЯ ВІДЕОІГОР

Шевченко Олександр

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сучасні технології штучного інтелекту (ШІ) відкривають нові можливості для тестування відеоігор, що є важливим етапом у забезпеченні якості кінцевого продукту. Традиційні методи тестування часто залежать від ручної перевірки, що вимагає великих часових та людських ресурсів і може бути схильним до людських помилок. Завдяки застосуванню штучного інтелекту розробники можуть автоматизувати виявлення багів та недоліків. Системи, що базуються на глибокому навчанні, здатні аналізувати тисячі сценаріїв у режимі реального часу, що дозволяє швидко знаходити проблеми, навіть ті, які раніше могли залишатися непоміченими. Такі алгоритми можуть симулювати поведінку користувачів, тестуючи різні шляхи проходження гри, що допомагає виявити помилки в логіці геймплею або збої в роботі штучного інтелекту ігрових персонажів.

Один із реальних прикладів використання таких технологій – нова розробка компанії Razer, яка створила платформу для розробників Wyvrn. Ця платформа має інструменти автоматизації, спрямовані на допомогу у забезпеченні якості ігрових продуктів, такі як Razer AI QA Copilot для тестування та автоматичного виявлення помилок, а також AI Gamer Copilot, що надає голосові поради під час гри [1].

Особливо важливим є AI QA Copilot – хмарний плагін для таких ігрових движків, як Unreal Engine та Unity, що допомагає автоматизувати процес тестування. Цей інструмент може спостерігати за процесом гри, виявляти баги та проблеми з продуктивністю, створюючи звіти про тестування, що включають знайдені помилки та теги від тестувальників. Згідно з даними компанії, AI QA Copilot може знаходити на 20-25% більше помилок порівняно з традиційним тестуванням, знижуючи час на тестування на 50% та економлячи до 40% на витратах [2]. Тим самим технології ШІ, які активно інтегруються в сучасний процес розробки відеоігор, значно змінюють підходи до тестування та вдосконалення ігрових продуктів.

Ще одним чудовим використання ШІ для тестування гри є застосування Behavior Tree (поведінкового дерева) – одного з ключових інструментів, який надає Unreal Engine 4 для створення, візуалізації та налагодження логіки поведінки персонажів. Цей інструмент дозволяє розробникам створювати складну поведінку для ботів або NPC без потреби прописування структури поведінки у коді. Натомість використовується візуальний редактор, у якому логіка подається у вигляді дерева. За допомогою такого підходу можна автоматизувати тестування штучного інтелекту у грі, як це було зроблено для боса гри «Labyrinth of Darkness» (рис. 1).

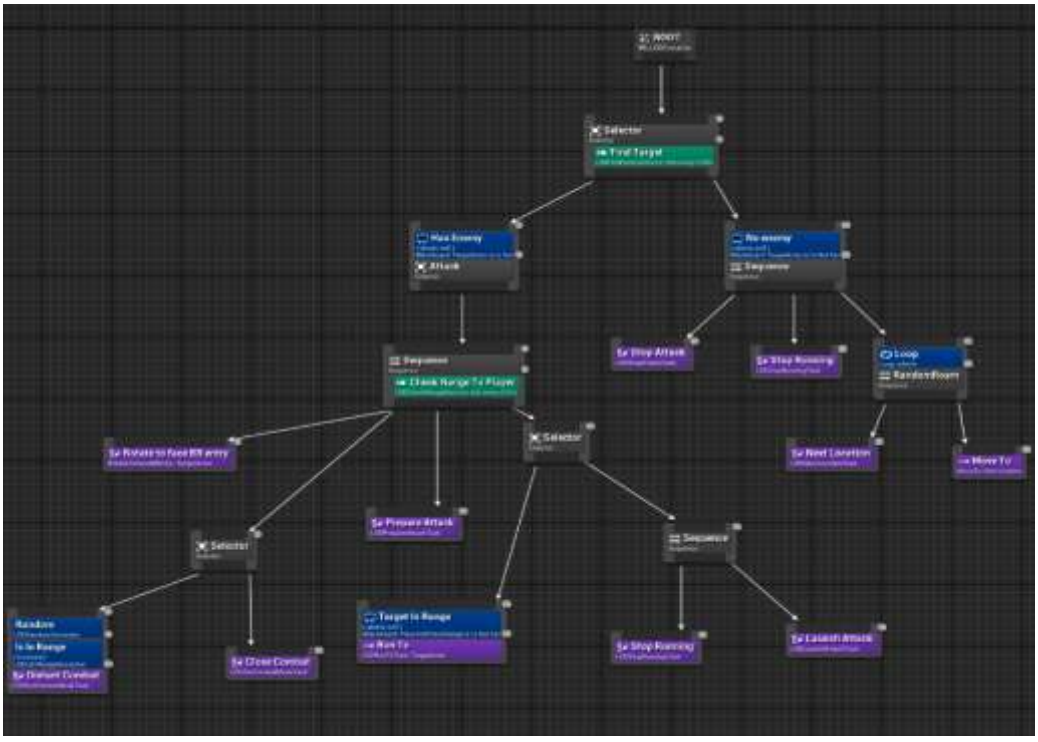

Рисунок 1 – Дерево поведінки для ШІ-персонажу гри «Labyrinth of Darkness»

Система перевіряє, чи є ворог поблизу, як показано у вузлі "Has Enemy", і відповідно до результату виконує або атаку, або перехід у стан патрулювання, як видно з гілки "No enemy". У випадку атаки система далі перевіряє відстань до гравця ("Check Range to Player") та вирішує, чи потрібно підійти ближче, чи вже можна розпочати атаку.

Цей процес дає змогу легко відслідковувати, чи правильно ШІ реагує на різні ігрові ситуації, що критично важливо під час тестування. Наприклад, перевірка роботи вузлів "Run To", "Launch Attack", "Rotate for BB entry" та інших дозволяє виявити недоліки логіки ворога або збої в анімації та навігації.

Завдяки цим інструментам UE4 надає потужні можливості для створення та тестування гнучкої та адаптивної поведінки ворогів. Під час тестування гри «Labyrinth of Darkness» використовувся Behavior Tree для різних персонажів для автоматичної перевірки, як NPC реагують у різних умовах, чи правильно виконують анімації, як обирають дії, і чи немає зависань логіки. Це значно пришвидшує виявлення помилок і дає змогу побудувати більш живу ігрову поведінку.

Список використаних джерел

1. Razer Reveals WYVRN: AI-Powered Gaming Ecosystem Set to Transform Play and Development. Razer Newsroom. URL: https://press.razer.com/company-news/razer-reveals-wyvrn-ai-powered-gaming-ecosystem-for-game-developers/.
2. Razer launches new Wyvrn game dev platform with automated AI bug tester. The Verge. URL: https://www.theverge.com/news/632121/razer-wyvrn-developer-ai-qa-gamer-copilot-sensa-haptics-thx?utm_source=chatgpt.com.

Ключові слова: вебзастосунок, фінансові транзакції, діаграма класів, інтерфейс, PostgreSQL

Keywords: web application, financial transactions, class diagram, interface, PostgreSQL

Науковий керівник: доцент Трофименко О.

ВПРОВАДЖЕННЯ ШТУЧНГО ІНТЕЛЕКТУ ДО СУДОВОЇ СИСТЕМИ УКРАЇНИ

Барабанщікова Євгенія

студентка 1-го курсу факультету судового та міжнародного права Національного університету «Одеська юридична академія»

Судова система України нині стикається з низкою викликів. Серед ключових проблем можна зазначити декілька основних моментів. Нестачу суддів - станом на квітень 2023 року в судах першої та апеляційної інстанцій було 1 903 вакансії з 6 490 посад (29,3%). Це спричиняє перевантаження, особливо в малих містах. Велику кількість нерозглянутих справ - до кінця 2021 року їх було 760 000 із 4,2 млн зареєстрованих, а у 2022 - 2023 роках частка таких справ перевищила 40%. Середній строк розгляду некримінальних справ - у 2020 - 2021 роках строк

розгляду сягав 138 днів. Низький рівень довіри до суддів - близько 70% українців не вірять у справедливість правосуддя через корупцію та політичний вплив [1].

З огляду на глобальні технологічні трансформації, застосування штучного інтелекту (ШІ) у судовій сфері стає одним із перспективних напрямів її модернізації. Світовий досвід доводить ефективність цифрових інструментів для підвищення прозорості, ефективності та доступності правосуддя. Водночас, використання ШІ в судовій практиці викликає низку юридичних, етичних і соціальних питань, що потребують системного аналізу. Штучний інтелект може стати ефективним інструментом підтримки суддів у прийнятті рішень, аналізі судової практики, прогнозуванні результатів справ і автоматизації документообігу. Успішні приклади вже є в Китаї, США та ЄС. Головні виклики при впровадженні ШІ до судової системи України - це забезпечення прозорості алгоритмів, захист даних, уникнення дискримінації, розмежування відповідальності та підтримання довіри до правосуддя. Необхідно також акцентувати увагу на підвищенні цифрової грамотності суддів та створенні нормативного врегулювання. Впровадження ШІ доцільно здійснювати поетапно - через пілотні проекти та їх поступове розширення.

Використання штучного інтелекту у правосудді – це не лише технічне питання, а комплексне завдання, що охоплює юридичні, етичні та соціальні аспекти. В умовах перевантаження українських судів, нестачі кадрів та потреби в уніфікації судової практики, інтелектуальні технології розглядаються як інструмент для підвищення ефективності судочинства. Одним із перших напрямів, у якому потенціал ШІ уже реалізується, є автоматизований аналіз судової практики, що дозволяє швидко виявляти релевантні рішення та правові позиції. Однак, попри значний потенціал ШІ у допоміжних функціях, важливо не втрачати з поля зору фундаментальні принципи правової системи. Зокрема, стаття 127 Конституції України чітко визначає: «Правосуддя здійснюють судді». Це означає, що системи штучного інтелекту не можуть і не повинні замінювати людину-суддю, адже саме вона несе відповідальність за прийняття рішень у судовому процесі, керуючись законом, внутрішнім переконанням і принципами справедливості [2].

Міжнародна практика демонструє зростаючу роль штучного інтелекту у правосудді, зокрема в автоматизації рутинних процесів. В Естонії розробляється «робот-суддя» для розгляду дрібних позовів онлайн, рішення якого можна буде оскаржити у звичайному суді. У Великій Британії та Канаді алгоритми застосовуються у медіації споживчих спорів, що свідчить про поступову довіру до цифрових способів вирішення конфліктів. В Індії створено інструменти SUPACE та SUVAS для аналізу великих обсягів судових даних та перекладу рішень 22 мовами, що значно покращує доступність судової практики. У Китаї система «Smart Court» забезпечує онлайн-засідання та автоматизовану обробку справ, наближаючи судочинство до цифрової епохи. Ці приклади демонструють глобальний тренд делегування технічних функцій судової системи штучному інтелекту [3].

З розвитком цифрових технологій та зростанням потреби в ефективному правосудді Україна також почала активно впроваджувати інновації. У цьому напрямі важливим кроком стало затвердження нової Концепції ЄСІКС із використанням штучного інтелекту.

Державна судова адміністрація України затвердила оновлену Концепцію Єдиної судової інформаційно-комунікаційної системи (ЄСІКС), яка передбачає інтеграцію технологій штучного інтелекту в окремі етапи судового процесу. Згідно з документом, ШІ використовуватиметься для автоматичного розпізнавання та класифікації документів, виявлення юридично значущих елементів у текстах, маскування конфіденційної інформації, створення стенограм засідань, озвучування документів та інтерфейсу для користувачів із порушеннями зору.

Крім того, система зможе здійснювати узагальнення змісту документів, перевіряти їх на граматичні та логічні помилки, оновлювати правові норми, перекладати тексти, здійснювати семантичний пошук судової практики, генерувати проекти процесуальних документів і навіть рекомендувати оптимальну методику розгляду справ. Передбачено також виявлення відхилень у розгляді справ – таких як ігнорування доказів чи відступ від усталеної практики та надання базової правової допомоги користувачам.

Система має функціонувати на основі самонавчання, що дозволить їй поступово вдосконалювати якість результатів та ефективність своєї роботи. Це свідчить про серйозний крок України у напрямі цифровізації судової влади з урахуванням сучасних технологій.

Реалізація проекту впровадження ЄСІКС передбачає два основні етапи:

Перший етап, запланований на 2025–2026 роки, охоплює впровадження ключових функцій підсистеми «Електронний документообіг суду», а також запуск ряду інших підсистем, що підсилюють основну функціональність системи.

Другий етап, який триватиме з 2026 по 2028 рік, зосереджений на розширенні можливостей системи за допомогою технологій штучного інтелекту та аналізу великих даних, включаючи експериментальні та додаткові компоненти ЄСІКС [4].

Показовим прикладом використання штучного інтелекту у судовому процесі стала справа, розглянута Ленінським районним судом міста Запоріжжя в грудні 2024 року. Суд розглядав порушення ПДР водієм автомобіля Mercedes-Benz G350, який смертельно травмував кота і залишив місце події. Адвокат обвинуваченого клопотав про закриття справи, обґрунтовуючи це висновками, сформованими за допомогою ChatGPT.

У відповідь суд зазначив, що хоча Україна є учасником Спеціального комітету Ради Європи з питань ШІ, а в 2020 році було затверджено Концепцію розвитку штучного інтелекту, жодні технології не можуть замінити незалежне й критичне мислення судді та не повинні впливати на прийняття рішень у правосудді [5].

Підсумовуючи, можна зазначити, що впровадження штучного інтелекту до судової системи України має значний потенціал для трансформації правосуддя в бік ефективності, швидкості та доступності. ШІ здатен суттєво пришвидшити розгляд справ, автоматизуючи рутинні процеси - аналіз документів, створення шаблонів рішень, пошук прецедентів, прогнозування результатів та розподіл справ. Його використання може надати суддям доступ до ширшого масиву релевантної інформації, аналітики й прогнозів, що сприятиме ухваленню більш обґрунтованих рішень. Окрім того, ШІ може зробити правосуддя доступнішим для соціально вразливих груп - осіб, які не можуть дозволити собі адвоката чи не володіють юридичною мовою. Разом із тим, існують суттєві ризики: можливі помилки в аналізі, поширення недостовірної інформації, порушення конфіденційності, дискримінаційність алгоритмів, що працюють на основі історичних даних. Тому впровадження ШІ в судову систему потребує виваженого підходу, розробки етичних стандартів, політик безпеки, навчання персоналу й регулярного моніторингу роботи алгоритмів. Ключовим має бути сприйняття ШІ як інструменту підтримки, а не заміни судді. З урахуванням зазначеного, цифрова трансформація правосуддя може відбутися успішно лише за умов правової, технологічної й етичної відповідальності всіх учасників процесу [6].

Список використаних джерел

1. Mykhailo Minakov Functioning of Ukrainian Courts during the War. URL: https://surl.lu/ckoiws.
2. Конституція України - Розділ VIII URL: https://surl.li/mzejwg.
3. Бессонов О.В. Зарубіжний досвід використання штучного інтелекту в правосудді URL: https://surl.lt/ezqmyz.
4. Мамченко Наталя ДСА затвердила концепцію ЄСІКС – у правосудді планують використати штучний інтелект URL: https://surl.li/bjzdzs.
5. Тараненко Віталій Українські суди почали розглядати матеріали, згенеровані штучним інтелектом. Як реагує Феміда? URL: https://surl.li/eahpcy.
6. Петрів Ольга Роль штучного інтелекту в модернізації судової системи: інструменти для суддів URL: https://surl.li/gvnkwz.

Ключові слова: штучний інтелект, судова система України, цифровізація правосуддя, автоматизація судочинства, ЄСІКС, юридична етика, міжнародний досвід, конституційні засади, алгоритми в суді, цифрові інструменти

Keywords: artificial intelligence, judicial system of Ukraine, digitalisation of justice, automation of court proceedings, UCCJ, legal ethics, international experience, constitutional principles, algorithms in court, digital tools

Науковий керівник: доцент Чанишев Р.

ВИКОРИСТАННЯ СИСТЕМНОГО ПІДХОДУ ДЛЯ ПОЯСНЕННЯ РІШЕНЬ МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ У КРИТИЧНИХ IT-СИСТЕМАХ

Богданова Діана

студентка 1-го курсу магістратури
факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Грезіна Олена

PhD, асистент кафедри інформаційних технологій
Національний університет «Одеська юридична академія»

Інтеграція моделей машинного навчання в критичні IT-інфраструктури вимагає забезпечення прозорості та зрозумілості прийнятих рішень. Особливої уваги набуває застосування інтерпретованих моделей у сферах, де наслідки неправильного рішення можуть призвести до збоїв у роботі системи, фінансових втрат або загроз безпеці. При цьому важливо не лише пояснювати результат моделі, а й відстежувати шлях обробки даних, зокрема, як змінювались вектори ознак на кожному етапі трансформації.

Традиційні підходи до інтерпретації нейронних мереж, такі як LIME та SHAP, не враховують системні взаємодії та ієрархічну структуру прийняття рішень у складних IT-системах. LIME (Local Interpretable Model-Agnostic Explanations) [1] створює лінійні аппроксимації моделей у локальному оточенні, що не завжди репрезентативно в умовах багатокомпонентної обробки. SHAP (SHapley Additive exPlanations) базується на концепції теорії ігор, надаючи глобальне пояснення через підсумовування впливу кожної ознаки, проте не фіксує внутрішні залежності між модулями системи, які можуть змінювати значущість ознак залежно від контексту виконання.

Системний підхід дозволяє розглядати модель штучного інтелекту (II-модель) як складову частину більшої технічної системи, що забезпечує контекстуалізацію та структурування процесу пояснення рішень.

Запропонована методологія базується на принципах системної інженерії та включає три основні рівні аналізу. На архітектурному рівні виконується декомпозиція II-моделі на функціональні блоки з визначенням вхідних та вихідних інтерфейсів кожного компонента.

Для цього використовується мова моделювання SysML [2], яка дозволяє формалізувати як логічну, так і фізичну архітектуру системи. Кожен компонент описується через контракти, що визначають допустимі значення вхідних параметрів, час реакції та тип оброблюваних даних.

Алгоритмічний рівень передбачає трасування потоків даних та процесів прийняття рішень усередині кожного блоку з використанням методів структурного аналізу.

Зокрема, застосовується метод зворотного проходу через мережу (backpropagation tracing) для визначення чутливості результату до змін вхідних параметрів, а також автоматичне виявлення «вузьких місць» – елементів системи з найбільш високим впливом на результат.

Операційний рівень забезпечує моніторинг та логування станів системи в реальному часі для подальшого аналізу причинно-наслідкових зв'язків.

Архітектура системи пояснення включає модуль семантичної анотації рішень, компонент побудови графа залежностей та підсистему візуалізації причинно-наслідкових ланцюжків. Модуль семантичної інструкції використовує онтологічні уявлення предметної області зіставлення внутрішніх станів моделі зі зрозумілими користувачеві концепціями. Граф залежностей будується на основі аналізу градієнтів активації нейронів та вагових коефіцієнтів зв'язків між шарами нейронної мережі.

Додатково застосовуються техніки attention-based аналізу (наприклад, із трансформерів), які дозволяють визначити, які входи мали найбільший контекстуальний вплив при формуванні підсумкового рішення.

Візуалізація реалізується через інтерактивні діаграми, що відображають ієрархію факторів впливу та їх кількісні ваги у підсумковому рішенні.

Валідація запропонованого підходу проводилася з прикладу системи автоматизованого управління мережевої безпекою корпоративної IT-інфраструктури. Система включає модулі детекції аномалій трафіку, класифікації загроз та прийняття рішень щодо блокування підозрілих з'єднань. Застосування системного підходу дозволило створити деталізовані пояснення для 94% рішень з тимчасової затримкою не більше 150 мілісекунд. Точність пояснень, оцінена експертами з інформаційної безпеки, склала 87% для критичних інцидентів та 92% для стандартних випадків виявлення загроз.

Запропонована методологія системного підходу до пояснення рішень II моделей демонструє високу ефективність у контексті критичних IT-систем. Ієрархічна структура пояснень та контекстуалізація рішень через системні інтерфейси забезпечують необхідний рівень прозорості для операторів критичних систем. Подальші дослідження спрямовані на розширення методології для роботи з ансамблями моделей та адаптацію до специфічних вимог різних предметних областей критичної IT-інфраструктури.

Список використаних джерел

1. Qian J, Du X, Pan R, Ling M, Ding H. ELIME: Exact Local Interpretable Model-Agnostic Explanation. The European Journal on Artificial Intelligence. 2025. URL: doi:10.1177/30504554251325141
2. Boelsen, K., May, M., Jacobs, G. et al. SysML v2 based modelling guidelines for mechanical system elements. Forsch Ingenieurwes 89, 60 (2025). URL: https://doi.org/10.1007/s10010-025-00827-w

Ключові слова: системний підхід, інтерпретація нейронних мереж, архітектура ІІ-модель, модель штучного інтелекту, критичні ІТ-інфраструктури.

Keywords: systems approach, interpretation of neural networks, architecture of AI model, artificial intelligence model, critical IT infrastructures.

ЧИ ПРАВДА, ЩО ВИКОРИСТАННЯ ШІ РОБИТЬ ЛЮДИНУ БІЛЬШ НЕРОЗУМНОЮ?

Гелета Тетяна

студентка 1-го курсу факультету психології політології та соціології Національного університету «Одеська юридична академія»

Штучний інтелект (ШІ) володіє величезним потенціалом, здатним значно покращити якість життя людей, а також оптимізувати різноманітні процеси в сучасному суспільстві. Цей реферат має на меті розглянути не лише основні переваги, які надає використання ШІ, але й можливі негативні наслідки, що можуть виникнути внаслідок його впровадження в різні сфери діяльності [1].

Штучний інтелект відкриває нові горизонти в автоматизації повсякденних завдань, таких як перевірка правопису, обробка великих обсягів даних, виконання математичних розрахунків та інші рутинні процеси. Це не лише звільняє цінний час для виконання більш важливих і творчих завдань, але й дозволяє зосередитися на саморозвитку та інноваціях. Автоматизація значно підвищує загальну продуктивність, зменшуючи ризик помилок, які можуть виникати при ручному виконанні цих завдань.

Алгоритми штучного інтелекту забезпечують миттєвий доступ до величезних обсягів даних, що суттєво пришвидшує навчальний процес і наукові дослідження. Це особливо корисно для студентів, науковців і професіоналів, які часто потребують швидкого та ефективного пошуку специфічної інформації. ШІ також допомагає структурувати та фільтрувати ці дані, роблячи їх більш доступними та зрозумілими для кінцевого користувача, що підвищує загальний рівень обізнаності.

Завдяки можливостям аналізу великих обсягів даних, які надає штучний інтелект, люди можуть приймати більш обґрунтовані та швидкі рішення. Це має критичне значення в таких сферах, як бізнес, медицина та фінанси, де точність і швидкість прийняття рішень можуть суттєво вплинути на результати. Використання даних для прийняття рішень зменшує ризик помилок, пов'язаних з людським фактором, і підвищує загальну результативність роботи організацій [2].

Інтелектуальні системи, побудовані на основі штучного інтелекту, можуть адаптуватися до індивідуальних потреб кожного користувача, надаючи персоналізовані рекомендації. Це робить навчання більш ефективним, оскільки враховує попередні знання, інтереси та прогрес учнів. Персоналізація навчального

процесу підвищує мотивацію та зацікавленість, що, у свою чергу, сприяє більш глибокому засвоєнню матеріалу.

Незважаючи на численні переваги, надмірне використання штучного інтелекту може мати негативні наслідки для когнітивних здібностей людини. Постійне покладання на технології може зменшити здатність до самостійного мислення, вирішення проблем та критичного аналізу інформації. Важливо усвідомлювати ці ризики та шукати оптимальний баланс у використанні технологій, щоб уникнути можливих негативних наслідків.

Часте використання штучного інтелекту може призвести до залежності, коли людина перестає використовувати свої власні розумові здібності та навички. Наприклад, системи, такі як голосові помічники, можуть знизити здатність до самостійного вирішення завдань і критичного мислення. Ця залежність може негативно вплинути на базові навички, такі як орфографія, математичні розрахунки та аналітичне мислення.

Використання ШІ для виконання завдань може призвести до втрати важливих когнітивних навичок, які необхідні для повсякденного життя. Це особливо стосується молоді, яка, залежачи від технологій, не розвиває базові навички без сторонньої допомоги. Важливо заохочувати дітей і молодь до самостійного мислення, щоб вони могли розвивати свої навички без постійної підтримки технологій.

Звичка покладатися на готові рішення, які пропонує штучний інтелект, може призвести до пасивності у прийнятті рішень. Люди можуть перестати аналізувати інформацію та розглядати альтернативи, що призводить до зниження рівня критичного мислення. Це може стати серйозною проблемою, оскільки критичне мислення є ключовим елементом для успішного функціонування в сучасному світі [3].

Залежність від технологій може призвести до соціальної ізоляції та зменшення взаємодії з реальними людьми. Люди все більше часу проводять за екранами, спілкуючись з машинами, отримуючи інформацію з інтернету, замість того, щоб взаємодіяти з оточуючими.

Це негативно впливає на розвиток емоційного інтелекту та соціальних навичок, необхідних для успішного спілкування та побудови стосунків.

Стереотипи про те, що штучний інтелект робить людину нерозумною, часто є перебільшеннями. Технології можуть бути надзвичайно корисними, якщо їх використовувати правильно та усвідомлено. ШІ може істотно підвищити інтелектуальні здібності, якщо його застосовувати як інструмент для вирішення складних завдань, а не як заміну для людського мислення.

У підсумку, можна з упевненістю стверджувати, що використання штучного інтелекту не призводить до зниження інтелектуальних здібностей людини, якщо технології інтегруються в повсякденне життя належним чином. Важливо знайти баланс між використанням ШІ та активною діяльністю власного розуму, оскільки це є ключовим для збереження інтелектуальної самостійності. Збереження

активності розуму та критичного мислення є надзвичайно важливими для подальшого розвитку навичок і особистісного зростання в епоху стрімкого технологічного прогресу.

Список використаних джерел

1. Russell, S. J., & Norvig, P. (2016). Artificial Intelligence: A Modern Approach. Pearson.
2. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
3. Chui, M., Manyika, J., & Miremadi, M. (2016). Where machines could replace humans–and where they can't (yet). McKinsey Quarterly.

Ключові слова: штучний інтелект (ШІ),технології, інтелектуальні системи, алгоритми, автоматизація, персоналізація, цифровізація

Keywords: artificial intelligence (AI), technologies, intelligent systems, algorithms, automation, personalization, digitalization

Науковий керівник: доцент Чанишев Р.

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА ПОШУКОВИЙ ТРАФІК

Костєва Кароліна

студентка 1-го курсу факультету адвокатури та антикорупційної діяльності Національного університету "Одеська юридична академія"

Штучний інтелект (ШІ) суттєво впливає на трафік пошукових систем у 2025 році, змінюючи, як користувачі взаємодіють із цифровим простором. Дослідження свідчить, що інструменти, такі як AI Overviews від Google та Search Generative Experience (SGE), надають прямі відповіді, зменшуючи потребу у переходах на сайти, що призводить до зниження органічного трафіку. Наприклад, Gartner прогнозує, що до 2026 року обсяг традиційного пошукового трафіку може зменшитися на 25% через зростання популярності AI-чатботів, таких як ChatGPT[1].

Цей тренд, відомий як "zero-click пошук", означає, що користувачі дедалі частіше задовольняються інформацією, представленою безпосередньо на сторінці результатів. Дані показують, що AI Overviews можуть спричинити до 60% зменшення органічного трафіку для певних запитів, а клікрейт (CTR) для платних оголошень падає з 21% до 10%, коли такі огляди присутні. Це створює виклики для бізнесів, які покладаються на пошуковий трафік для залучення аудиторії.

Водночас ШІ сприяє появі нових форматів взаємодії, таких як голосовий пошук та AI-асистенти. Нові платформи, як-от Perplexity, обробляють понад 100 мільйонів запитів на тиждень, що становить близько 9% від запитів, оброблених Google через AI Overviews, що свідчить про зростання конкуренції. Це змінює поведінку користувачів, змушуючи компанії адаптувати свої стратегії, зокрема через оптимізацію контенту для ШІ.

Нарешті, ШІ відкриває можливості для персоналізації пошуку, покращуючи користувацький досвід. Завдяки аналізу поведінки та вподобань, ШІ може надавати більш релевантні результати, що допомагає бізнесам залучати цільову аудиторію. Однак це вимагає від компаній інвестувати в AI-інструменти для SEO, таких як інструменти для дослідження ключових слів та створення контенту, щоб залишатися конкурентоспроможними

У 2025 році штучний інтелект (ШІ) продовжує кардинально трансформувати цифровий ландшафт, зокрема функціонування пошукових систем, що має значний вплив на трафік веб-ресурсів. Інтеграція ШІ, таких як AI Overviews від Google та Search Generative Experience (SGE), призвела до значного зменшення органічного трафіку, що є одним із ключових трендів цього року. Ці інструменти надають користувачам вичерпні відповіді безпосередньо на сторінці результатів пошуку, зменшуючи потребу у переходах на зовнішні сайти. Це явище, відоме як "zero-click пошук", стало поширеним, що, за прогнозами Gartner, може призвести до зменшення традиційного пошукового трафіку на 25% до 2026 року[3].

Цей зсув у поведінці користувачів супроводжується значним зниженням клікрейту (CTR). Дослідження, опубліковані в 2025 році, показують, що присутність AI Overviews може спричинити до 60% зменшення органічного трафіку для певних запитів, а CTR для платних оголошень падає з 21% до 10%, коли такі огляди відображаються. Це створює серйозні виклики для рекламодавців і контент-креаторів, які традиційно покладаються на пошуковий трафік для залучення аудиторії та генерації доходів. Наприклад, компанія Chegg подала позов проти Google, стверджуючи, що AI Overviews негативно вплинули на їхній трафік і доходи, що свідчить про реальні економічні наслідки для бізнесу.

Паралельно з цим, ШІ сприяє появі нових форматів взаємодії з користувачами, зокрема зростанню популярності голосового пошуку та AI-асистентів, таких як ChatGPT. За даними, ChatGPT прогнозується мати 1% частки ринку пошуку у 2025 році, що, хоча й невелике, вказує на зміну парадигми . Це свідчить про те, що ШІ не лише трансформує існуючі пошукові системи, але й відкриває двері для нових гравців, які можуть підірвати домінування Google, яке досі охоплює понад 90% традиційних пошукових запитів.

У відповідь на ці зміни бізнеси та маркетингові агентства активно інтегрують ШІ у свої стратегії. За даними звіту Basis Technologies, 97,7% рекламних агентств використовують генеративний ШІ, із них 38,6% щоденно, а понад 90% – щонайменше щотижнево.

Крім того, ШІ пропонує нові можливості для персоналізації пошуку, що покращує користувацький досвід. Завдяки аналізу поведінки та вподобань, ШІ може надавати більш релевантні та індивідуалізовані результати, що відкриває перспективи для бізнесів, які вміють адаптуватися. Наприклад, за даними ResearchFDI, AI-інструменти дозволяють бізнесам залучати цільовий трафік і ліди, що є критично важливим для інвестиційної привабливості.

Однак не всі регіони однаково відчувають цей вплив. Наприклад, в Україні функції, такі як AI Overviews, ще не повністю доступні в українській версії пошуку, що дає деякий час для підготовки, але в майбутньому очікується подібний вплив, як і в інших регіонах [4].

У перспективі пошукові системи продовжать впроваджувати ШІ, що, ймовірно, спричинить подальше зменшення органічного трафіку на традиційні веб-ресурси. Водночас це стимулюватиме розвиток нових форматів пошуку та контент-маркетингу, орієнтованих на ефективну взаємодію з аудиторією в умовах швидких технологічних змін. Компанії, які зможуть адаптуватися, матимуть можливість не лише зберегти, але й посилити свою позицію на ринку, інвестуючи в AI-інструменти та стратегії, які враховують ці трансформації.

Незважаючи на виклики, ШІ відкриває нові перспективи. Завдяки інтеграції штучного інтелекту в пошукові алгоритми результати стають більш персоналізованими та релевантними, що сприяє вдосконаленню користувацького досвіду. Це може призвести до трансформації моделей монетизації контенту та появи інноваційних каналів взаємодії з аудиторією[2].

Однак компанії стикаються з необхідністю адаптації. Наприклад, Google дедалі більше орієнтується на транзакційні запити, що може зменшити трафік для інформаційного контенту, особливо для некомерційних сайтів . Ефективне використання AI потребує поєднання його можливостей із людською експертизою для забезпечення автентичності та залучення аудиторії [5].

Важливо зазначити, що вплив AI Overviews ще не повністю відчувається в деяких регіонах, таких як Україна, де ці функції поки що недоступні в українській версії пошуку . Це дає деякий час для підготовки, але в майбутньому очікується подібний вплив, як і в інших регіонах [6].

У перспективі пошукові системи продовжать впроваджувати ШІ, що, ймовірно, спричинить подальше зменшення органічного трафіку на традиційні веб-ресурси. Водночас це стимулюватиме розвиток нових форматів пошуку та контент-маркетингу, орієнтованих на ефективну взаємодію з аудиторією в умовах швидких технологічних змін. Компанії, які зможуть адаптуватися, матимуть можливість не лише зберегти, але й посилити свою позицію на ринку.

Штучний інтелект значно трансформує пошукові системи, впливаючи на трафік веб-ресурсів і змушуючи бізнеси адаптуватися до нових реалій. Зменшення органічного трафіку через zero-click пошук, зростання популярності голосового пошуку та AI-асистентів, а також необхідність оптимізації контенту для ШІ – все це ставить нові виклики перед маркетинговими стратегіями. Однак ШІ також відкриває можливості для персоналізації пошуку, вдосконалення користувацького досвіду та розробки нових моделей монетизації. Для успіху у цифровому середовищі майбутнього компаніям необхідно інвестувати в інтеграцію ШІ та розробку стратегій, які враховують змінюючіся тенденції пошукового трафіку.

Список використаних джерел

1. Goodwin D. Чи зменшиться трафік пошукових систем на 25% до 2026 року? Search Engine Land. URL: https://searchengineland.com/search-engine-traffic-2026-prediction-437650.
2. Kurtz R. ШІ та майбутнє маркетингу пошукових систем. Basis Technologies. URL: https://basis.com/blog/artificial-intelligence-and-the-future-of-search-engine-marketing
3. AlixPartners. Майбутнє пошуку: порушення та диверсифікація, спричинені ШІ. AlixPartners. URL: https://www.alixpartners.com/insights/102jze5/the-future-of-search-ai-driven-disruption-and-diversification/
4. ResearchFDI. Майбутнє SEO: як ШІ вже змінює оптимізацію пошукових систем. ResearchFDI. URL: https://researchfdi.com/future-of-seo-ai/
5. Rose-Collins F. SEO у 2024 році: орієнтуємося на майбутні тенденції та стратегії. Ranktracker. URL: https://www.ranktracker.com/uk/blog/seo-in-2024-navigating-future-trends-and-strategies/
6. Edgelab. SEO проти ШІ: хто переможе у боротьбі за пошуковий трафік у 2025 році. Edgelab. URL: https://edgelab.com.ua/blog/seo-proty-shtuchnogo-intelektu-hto-peremozhe-v-bytvi-za-poshukovyj-trafik-u-2025-roczi/.

Ключові слова: штучний інтелект(ші), zero-click пошук, AI Overviews, голосовий пошук, персоналізація пошук, пошукові алгоритми

Keywords: artificial intelligence(AI), zero-click search, AI Overviews, voice search, personalization search, search algorithms

Науковий керівник: доцент Чанишев Р.

ВИКОРИСТАННЯ ГЕНЕРАТИВНОГО ШІ У ТВОРЧИХ ГАЛУЗЯХ: БАЛАНС МІЖ ІННОВАЦІЯМИ ТА ЗАХИСТОМ АВТОРСЬКИХ ПРАВ

Мамедова Захра

студентка 1-го курсу факультету адвокатури та антикорупційної діяльності Національного університету «Одеська юридична академія»

Генеративний штучний інтелект (ГШІ) – це технологія, що здатна створювати нові твори: тексти, зображення, відео, музику, код та інший контент. Серед найвідоміших прикладів – ChatGPT, Midjourney, DALL·E, Copilot, Sora та інші. ГШІ стрімко змінює способи створення контенту, стає доступним навіть для тих, хто не має спеціальної підготовки у сфері мистецтва чи програмування. Водночас, його впровадження в творчі процеси породжує численні юридичні та етичні запитання.

Одним із головних викликів є визначення авторства. Чи може штучний інтелект бути автором твору? Відповідно до чинного українського законодавства (а також більшості міжнародних норм), автором визнається лише фізична особа. Машини не мають юридичної особистості, а отже, не можуть мати авторських

прав. Проте, якщо твір створено повністю за допомогою ШІ без творчого внеску людини, виникає питання, кому належатимуть права на такий продукт. Деякі юристи вважають, що автором є особа, яка ввела інструкцію (prompt), інші – що це продукт без авторського захисту.

Також важливим є аспект навчання нейромереж на великих масивах даних, які можуть містити захищені авторським правом твори. Програмне забезпечення, що створює музику або зображення, "вчиться" на зразках, серед яких можуть бути картини відомих художників, уривки з книг, композиції, фільми. У деяких країнах, таких як Японія, дозволено використання матеріалів для тренування ШІ без згоди правовласника. В інших, як-от у США, йдуть судові процеси (наприклад, Getty Images проти Stability AI).

Одним із гучних прикладів є справа щодо генератора коду Copilot, який використовував відкритий код з GitHub без належного зазначення авторства. Аналогічно, художники подають позови до розробників Midjourney і Stable Diffusion через використання їхніх стилів без згоди. Це викликає обурення творчих спільнот і водночас ставить під сумнів межі fair use (добросовісного використання).

Важливо відзначити, що захист авторських прав у сфері ШІ – це не лише про право на прибуток. Це питання визнання праці, креативності, захисту професійної гідності митців. З іншого боку, надмірна регуляція може загальмувати розвиток інновацій. Тому сучасне законодавство має шукати баланс між цими сторонами.

ВОІВ (Всесвітня організація інтелектуальної власності) проводить міжнародні консультації з цього приводу. Розглядаються різні моделі врегулювання: наприклад, визнання співавторства людини та ШІ; створення нового об'єкта інтелектуальної власності – «твір, створений ШІ»; або розмежування прав на код ШІ, його результати і вихідні дані. Також активно обговорюється ідея запровадження ліцензій на використання даних для навчання моделей.

Крім того, важливо враховувати міждисциплінарний характер проблеми. Вона стосується не лише юристів, а й програмістів, митців, етичних комісій. Наприклад, запровадження маркування контенту, створеного ШІ, могло б допомогти в розпізнаванні джерел. Інші пропонують створити публічні бази даних ліцензованого контенту для навчання.

Для України це питання є особливо актуальним у контексті цифровізації, реформи освіти та правової інтеграції з ЄС. Необхідно передбачити гнучкі, але чіткі механізми регулювання, які дадуть змогу захищати національних митців і водночас інтегруватися у глобальний цифровий ринок.

Отже, використання генеративного ШІ вимагає нових підходів до авторського права. Важливо не лише зберегти інтереси творців, а й стимулювати інновації, запроваджуючи правові механізми, які відповідатимуть новим технологічним реаліям.

Список використаних джерел

1. Byung Cheol Lee, Jaeyeon (Jae) Chung An empirical investigation of the impact of ChatGPT on creativity URL: https://surli.cc/myzuap.
2. Muhammad Abid Malik, Amjad Islam Amjad, Sarfraz Aslam, Abdulnaser Fakhrou Global insights: ChatGPT's influence on academic and research writing, creativity, and plagiarism policies URL: https://surl.li/xfzmqs.
3. Qinghan Liu, Yiyong Zhou, Jihao Huang, Guiquan Li When ChatGPT is gone: Creativity reverts and homogeneity persists URL: https://surl.li/fsoymy.

Ключові слова: генеративний ШІ, авторське право, творчість, штучний інтелект, юридичні виклики

Key words: generative AI, copyright, creativity, artificial intelligence, legal challenges

Науковий керівник: доцент Чанишев Р.

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА ТРАНСФОРМАЦІЮ РИНКУ ПРАЦІ ПРОГРАМІСТІВ

Чорна Вероніка

студентка 1-го курсу факультету адвокатури та антікорупційної діяльності Національного університету «Одеська юридична академія»

Штучний інтелект (ШІ) кардинально трансформує ринок праці в програмуванні, одній із найбільш технологічно залежних галузей. Інструменти на кшталт GitHub Copilot, Tabnine чи Codeium генерують код, виправляють помилки та оптимізують алгоритми за секунди, скорочуючи час розробки на 20-30%. Наприклад, GitHub Copilot створює до 40% коду в проєктах, дозволяючи програмістам зосереджуватися на складних завданнях, як-от архітектура програм чи стратегічне планування. Водночас автоматизація загрожує низькокваліфікованим фахівцям, які пишуть шаблонний код чи тестують. За прогнозами Gartner, до 2027 року 30% робочих місць початкового рівня в програмуванні можуть бути автоматизовані. Це підвищує попит на висококваліфікованих розробників, здатних створювати, інтегрувати та підтримувати складні системи. Тема актуальна, адже у 2025 році ринок праці програмістів зазнає значних змін через швидке впровадження нових технологій в IT [2].

Глобальний ринок технологій ШІ у 2025 році оцінюється у $190 млрд, а до 2030 року прогнозується зростання до $1,5 трлн (Statista). В Україні інвестиції в стартапи цього напряму у 2024 році склали $150 млн, а у 2025 році очікується $200 млн (Мінцифри). Це стимулює створення робочих місць для програмістів, які спеціалізуються на машинному навчанні (ML), обробці природної мови та комп'ютерному зорі. Українські компанії, як-от Grammarly і People.ai, підвищують попит на фахівців із Python, TensorFlow і PyTorch. За даними DOU, зарплати ML-інженерів в Україні у 2025 році становлять $3,000-$7,000 на місяць, що на 20%

вище, ніж у веб-розробників. Нові технології створюють спеціалізації: інженери даних, які готують набори для тренування систем, та спеціалісти з етики алгоритмів, які забезпечують їх безпеку й неупередженість, є затребуваними. Попит на інженерів даних у 2025 році зріс на 35% (LinkedIn), а в Україні 15% вакансій на Upwork у 2024 році стосувалися таких проєктів, що на 10% більше, ніж у 2023 році. Ці зміни відображають глобальний тренд, де попит на нішеві навички зростає швидше, ніж на традиційні ролі розробників [1].

Автоматизація змушує програмістів постійно оновлювати навички, адже до 2030 року 20% завдань у програмуванні, зокрема у фронтенд-розробці чи підтримці старих систем, можуть бути автоматизовані (McKinsey). Знання JavaScript чи HTML уже недостатньо; потрібні хмарні платформи (AWS, Azure) і фреймворки ML. В Україні 60% програмістів у 2024 році проходили курси з ML, щоб залишатися конкурентними (DOU). Освітні програми адаптуються: КПІ та Львівська політехніка у 2025 році запровадили магістерські програми з нейронними мережами та обробкою даних, а Coursera фіксує зростання на 40% студентів на курсах ML у 2024 році. В Україні 25% слухачів Prometheus обирали такі програми, що на 15% більше, ніж у 2023 році. Soft skills, як-от співпраця з командами та комунікація, стають критично важливими, адже програмісти все частіше працюють у міждисциплінарних командах, де потрібно пояснювати складні концепції бізнесу чи клієнтам. Крім того, технології змінюють підходи до навчання: безкоштовні ресурси, як Google AI Courses чи Fast.ai, дозволяють освоїти основи ML за 3-6 місяців, що робить освіту доступнішою для початківців.

Економічний вплив технологій на ринок праці програмістів поєднує можливості та ризики. В Україні IT-галузь генерує 7% ВВП (IT Ukraine Association, 2024), а у 2025 році 300,000 фахівців працюють у секторі, з них 15% – у проєктах із новими технологіями. Проте автоматизація знижує попит на початківців: 50% компаній у 2025 році використовують технології для рутинних завдань (World Economic Forum). Водночас фрілансери отримують більше замовлень на створення чат-ботів чи моделей комп'ютерного зору через Upwork. Україна посідає 5-те місце за кількістю IT-аутсорсингових компаній у 2025 році (Clutch), але конкуренція з Індією, Польщею та США зростає. Наприклад, 70% вакансій для ML-інженерів у 2024 році вимагали англійської на рівні Upper-Intermediate. Війна ускладнює розвиток: 20% програмістів виїхали у 2022-2024 роках, але багато хто працює віддалено (DOU). Ця мобільність дозволяє Україні зберігати позиції на глобальному ринку, але вимагає від фахівців адаптації до міжнародних стандартів [1].

Технології трансформують управління командами та створюють нові виклики. Інструменти, як Jira з ML, оптимізують проєктний менеджмент, підвищуючи ефективність на 25% (Atlassian). В Україні EPAM і SoftServe застосовують такі рішення, але алгоритми оцінки продуктивності можуть бути упередженими, що впливає на кар'єрні перспективи. Регулювання також змінює ринок: AI Act в ЄС (2024) встановлює стандарти прозорості, підвищуючи попит на програмістів, які

забезпечують відповідність систем законодавству. В Україні Мінцифри планує створити 10,000 робочих місць у цьому секторі до 2030 року, що стимулюватиме освіту та інновації. Наприклад, у 2024 році 10% IT-компаній в Україні почали розробляти внутрішні політики етики алгоритмів, щоб відповідати міжнародним вимогам. Це відкриває нові можливості для програмістів, які поєднують технічні знання з розумінням права та етики.

Майбутнє ринку праці залежить від адаптації до нових реалій. До 2028 року 60% IT-проєктів вимагатимуть знань технологій ML, а попит на таких фахівців зросте на 50% (IDC). В Україні 20% вакансій у 2025 році стосуються цього напряму, порівняно з 10% у 2022 році. Початківцям варто вивчати основи через Google AI Courses чи Fast.ai, а досвідченим – зосередитися на кібербезпеці, медичних чи фінансових застосуваннях. Наприклад, у 2025 році попит на програмістів, які розробляють ШІ для аналізу медичних даних, зріс на 25% через потребу в телемедицині та діагностиці. Технології впливають на гендерну динаміку: ініціативи, як Women in AI Ukraine, у 2024 році залучили 500 учасниць до курсів ML, що на 30% більше, ніж у 2023 році. Проте в сільських регіонах брак інфраструктури ускладнює доступ до освіти, що може поглиблювати нерівність. За даними Мінцифри, лише 30% сільських шкіл в Україні мають достатнє технічне забезпечення для навчання IT, що створює бар'єри для молоді [3].

Соціальний вплив технологій також помітний у зміні робочих моделей. Віддалена робота, підкріплена інструментами автоматизації, стала нормою: у 2025 році 80% українських програмістів працюють віддалено хоча б частково (DOU). Це дозволяє залучати міжнародні проєкти, але підвищує конкуренцію. Наприклад, у 2024 році 40% українських фрілансерів на Fiverr працювали над завданнями, пов'язаними з чат-ботами чи обробкою даних, що на 15% більше, ніж у 2023 році. Водночас технології змінюють очікування роботодавців: дедалі частіше потрібні програмісти, здатні інтегрувати системи в реальному часі, наприклад, для IoT чи автономних транспортних засобів. В Україні такі проєкти поки що обмежені, але компанії, як Luxoft, уже працюють над рішеннями для європейських автовиробників, що створює попит на фахівців із вбудованих систем і ML.

Нові технології трансформують ринок праці програмістів, відкриваючи можливості для тих, хто опанує спеціалізації, але загрожуючи початківцям. В Україні IT-ринок зростає, а програмісти залишаються конкурентними завдяки кваліфікації та доступу до глобальних проєктів. Успіх залежить від освіти, нішевих навичок і адаптивності. Технології не замінять програмістів, а змінять їхню роль, акцентуючи креативність, стратегічне мислення та співпрацю з системами. Постійне навчання та гнучкість стануть ключовими для кар'єрного зостання в епоху технологічних змін. Програмісти, які інвестують у розвиток, зможуть не лише вистояти, але й стати лідерами у новій IT-екосистемі [2].

Список використаних джерел

1. Адаптація до нових вимог ринку праці. HURMA. 25.03.2025. URL: https://hurma.work/blog/adaptacziya-do-novih-vimog-rinku-praczi/ (дата звернення: 11.05.2025).
2. Вплив штучного інтелекту на ринок праці в IT. 08.04.2024. URL: https://lemon.school/blog/vplyv-shtuchnogo-intelektu-na-rynok-pratsi-v-it (дата звернення: 11.05.2025).
3. The Impact of AI on Job Roles, Workforce, and Employment. Innopharma Education. URL: https://www.innopharmaeducation.com/blog/the-impact-of-ai-on-job-roles-workforce-and-employment-what-you-need-to-know (дата звернення: 11.05.2025).

Ключові слова: штучний інтелект, автомизація, програмування

Keywords: artificial intelligence, automation, programming

Науковий керівник: доцент Чанишев Р.

ХАРАКТЕРИСТИКА ТА ПОРІВНЯННЯ СЕРВІСІВ ДЛЯ РОБОТИ З ГОЛОСОМ ТА ЇХ ЗАСТОСУВАННЯ У ВИЩІЙ ОСВІТІ

Бондаренко Максим

студент 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Ситуація в сучасному освітньому просторі показує потребу в інноваціях, пов'язаних зі сферою штучного інтелекту (AI). З огляду на це, виникає нагальна потреба в інноваційних інструментах, здатних покращити навчальний процес, підвищити його доступність та оптимізувати комунікацію. Перспективним напрямом є використання сервісів для роботи з голосом, які відкривають нові можливості для створення аудіоконтенту, підтримки студентів з особливими освітніми потребами, автоматизації рутинних завдань та персоналізації навчання [1]. Тенденції свідчать про активне впровадження голосових технологій, що підтверджується дослідженнями ефективності мультимодального навчання та важливості аудіального сприйняття [2]. За рахунок активного розвитоку та розширення функціональних можливостей AI, створюються нові та більш реалістичні голосові сервіси. Інклюзивнсіть та доступність дедалі більше стають важливими в освітньому процесі, і ці фактори, в свою чергу, створюють сприятливе середовище для інтеграції голосових технологій у діяльність вищих навчальних закладів.

Ринок пропонує різноманіття платформ для роботи з голосом, що використовують AI. Серед лідерів виділяється ElevenLabs, що спеціалізується на створенні надзвичайно реалістичного людського голосу [3, 4]. Платформа пропонує велику бібліотеку з понад 300 голосів, включаючи ліцензовані AI-версії реальних людей, та підтримує понад 29 мов. Ключові функції включають високоякісне

перетворення тексту в мову (Text-to-Speech, TTS), клонування голосу, його зміну, дублювання аудіо/відео на інші мови та генерацію звукових ефектів. Наявність API та SDK дозволяє інтегрувати технології ElevenLabs в інші продукти [4]. Висока якість синтезу робить платформу привабливою для створення професійного аудіоконтенту, зокрема в освітній сфері. Інші помітні платформи пропонують свої унікальні переваги. MurfAI надає понад 200 AI-голосів на більш ніж 20 мовах, з детальними налаштуваннями параметрів голосу (тон, темп, паузи) та функціями для командної роботи й інтеграції з популярними інструментами, як Canva чи PowerPoint [5]. Azure AI Speech від Microsoft є комплексним рішенням, що пропонує можливості перетворення мови в текст (STT) з підтримкою понад 100 мов, TTS, переклад у реальному часі та аналітику мови, орієнтуючись на корпоративних користувачів та високі стандарти безпеки [6]. Платформа LOVO AI через свій інструмент Genny надає доступ до понад 500 голосів на більш ніж 100 мовах, а також пропонує онлайн-відеоредактор, AI-письменник та генератор зображень [7]. Speechify позиціонується як TTS-рідер, доступний на різних платформах, з функціями швидкого прослуховування, AI-резюме та сканування друкованого тексту, що робить його зручним для студентів [8]. Respeecher фокусується на високоякісному клонуванні голосу з точною передачею емоційних нюансів та пропонує унікальну технологію speech-to-speech [9].

Для вибору сервісу роботи з голосом важливими факторами є якість генерованого голосу, мовна підтримка, ціна та функціональність. Платформи ElevenLabs та Respeecher часто відзначаються за створення надзвичайно реалістичних голосів [3, 9]. Висока якість є критично важливою для ефективного сприйняття навчального матеріалу, оскільки неприродне звучання може відволікати та знижувати мотивацію. Реалістичні голоси, навпаки, сприяють залученню та кращому засвоєнню інформації. Щодо мовної підтримки, лідерами за кількістю підтримуваних мов є LOVO AI та PlayHT (понад 100) [7]. Інші, як Azure AI Speech, Speechify, ElevenLabs та Murf AI, також пропонують підтримку десятків мов [4, 5, 6, 8]. Широка мовна підтримка є важливою для університетів з міжнародними програмами та іноземними студентами. Більшість сервісів пропонують безплатні плани з обмеженими можливостями та різноманітні платні підписки [3], тоді як Azure AI Speech використовує модель оплати за фактичне використання ресурсів [10]. При виборі ціни слід враховувати не лише прямі витрати, а й потенційну економію часу та ресурсів завдяки автоматизації; деякі сервіси можуть пропонувати спеціальні умови для освітніх установ. Спектр функціональних можливостей варіюється від спеціалізованих TTS-рішень (Speechify) та високоякісної генерації/клонування (ElevenLabs, Respeecher) до комплексних платформ з інструментами для редагування відео, командної роботи та інтеграцій (Murf AI, LOVO AI). Вибір конкретного сервісу напряму залежить від мети його використання. Різні платформи надають різні можливості, що в свою чергу будуть більш або менш оптимальними при виконанні конкретних завдань.

AI-технології для роботи з голосом надають можливості для трансформації освітнього процесу, наприклад, за допомогою створення аудіолекцій та озвучування навчальних матеріалів. Викладачі можуть перетворювати текстові лекції, конспекти та посібники в аудіоформат, надаючи студентам гнучкість у навчанні – можливість слухати матеріали будь-де та будь-коли. Також можливе створення голосових коментарів до презентацій, що робить візуальні матеріали більш інформативними. Надзвичайно важливим аспектом є підвищення доступності навчання для студентів з особливими освітніми потребами [1]. Технології TTS дозволяють озвучувати тексти для студентів з порушеннями зору чи дислексією. Можливість налаштування швидкості читання та вибору голосу сприяє адаптації до індивідуальних потреб та реалізації принципів універсального дизайну навчання (UDL). Сервіси знаходять застосування й у вивченні іноземних мов [2]. Використання AI-голосів носіїв мови з різними акцентами допомагає покращити вимову та навички аудіювання за рахунок використання автентичної та реалістичної вимови. Технології Speech-To-Text (STT) надають можливість створення інтерактивних вправ, які б перевіряли не тільки граматичну складову мовлення, але і саму вимову. Автоматизація озвучування презентацій та відеоматеріалів дозволяє викладачам значно скоротити час та витрати порівняно із залученням професійних дикторів, звільняючи ресурси для розробки змістовного контенту. Існує потенціал для створення персоналізованого навчального досвіду, наприклад, через клонування голосу викладача для створення відчуття присутності в онлайн-форматі або адаптацію стилю мовлення до потреб студента [11].

Використання AI-голосу у вищій освіті має як значні переваги, так і недоліки. Переваги для студентів включають покращення доступності матеріалів, підтримку різних стилів навчання (зокрема, аудіального), гнучкість доступу до контенту та ефективний інструмент для вивчення мов [1, 2]. Для студентів з особливими потребами TTS може знизити тривожність та підвищити самостійність [12]. Для викладачів переваги полягають в економії часу на озвучування, можливості створення більш інтерактивних матеріалів, розширенні аудиторії завдяки багатомовній підтримці та звільненні часу для досліджень чи розробки курсів [13, 14]. Однак існують недоліки та ризики: ризик упередженості AI-голосів через дані, на яких вони навчалися, можливість генерування неточної інформації [15]. Тривале використання TTS може потенційно знизити навички критичного читання [16], а зменшення людської взаємодії між викладачами та студентами є ще одним занепокоєнням [15]. Виникають етичні питання щодо клонування голосу без належної згоди та можливості зловживань (deepfakes) [17]. AI-голосам може бути складно передати емоційні нюанси, що призводить до монотонності та зниження концентрації [17]. Існують також ризики академічного шахрайства, залежності від технологій, технічних збоїв та проблеми з конфіденційністю даних при використанні хмарних сервісів [15, 18].

Доцільність широкого впровадження TTS є предметом дискусій. Аргументи на підтримку наголошують на підвищенні доступності та інклюзивності,

підтримці аудіального стилю навчання, зручності та гнучкості, допомозі у вивченні мов та економії часу [1]. TTS може покращити розуміння матеріалу, особливо при поєднанні з візуальним виділенням тексту. Водночас існують застереження щодо можливого зниження навичок самостійного читання та глибокого аналізу тексту [16]. Ключовим є пошук балансу між використанням TTS та традиційними методами навчання [19]. Рекомендується використовувати TTS як допоміжний інструмент для ознайомлення чи повторення, але зберігати традиційне читання для розвитку критичного мислення. Інтеграція TTS має підтримувати навчання, а не повністю замінювати методи, що сприяють розвитку важливих академічних навичок.

Коли йдеться про ефективність AI-голосу та технологій перетворення тексту на мовлення (TTS) у вищій освіті, дослідження дають картину неоднозначну, хоча й переважно позитивну. З одного боку, чимало робіт підтверджують, що TTS позитивно впливає на розуміння прочитаного, мотивацію та самостійність навчання, особливо для студентів, які стикаються з навчальними труднощами, мають порушення зору чи дислексію [20]. З іншого боку, існують дослідження, що застерігають: до використання AI слід підходити обережно через потенційні ризики, як-от упередженість алгоритмів, поширення дезінформації та зменшення живої соціальної взаємодії [21]. Тому цілком очевидно, що потрібні подальші дослідження, аби всебічно зрозуміти, як саме AI впливає на добробут студентів та якість навчання, а також розробити стратегії, що допоможуть мінімізувати можливі негативні наслідки.

Щоб успішно впровадити сервіси для роботи з голосом, потрібен продуманий, стратегічний підхід. Насамперед університетам варто чітко визначити власні потреби та цілі: чи йдеться про підвищення доступності матеріалів, створення якісного аудіоконтенту, чи про оптимізацію певних процесів. Далі доцільно провести порівняльний аналіз доступних сервісів за ключовими параметрами (якість голосу, підтримка мов, ціна, функціональність, безпека), обов'язково залучивши до цього процесу викладачів та студентів – адже саме вони є основними користувачами. На етапі впровадження критично важливо розробити чіткі правила використання AI-голосу, які б охоплювали етичні аспекти та питання академічної доброчесності. Не менш важливо організувати навчання для викладачів та студентів, щоб вони могли ефективно користуватися обраними інструментами, а також забезпечити надійну технічну підтримку. Варто пам'ятати й про постійний моніторинг та оцінку ефективності: аналізувати, як технології впливають на навчальний процес та наскільки задоволені користувачі. Не зайвим буде розглянути інтеграцію з уже наявними платформами електронного навчання. Особливу увагу, особливо при використанні хмарних сервісів, слід приділити конфіденційності та захисту даних. І, звісно, починати краще поступово, з пілотних проєктів – це дозволить оцінити ефективність і виявити потенційні проблеми ще до масштабного розгортання.

Сервіси для роботи з голосом на базі штучного інтелекту, як-от ElevenLabs, Murf AI, Azure AI Speech та подібні, безперечно, відкривають значний потенціал для вищої освіти. Вони здатні покращити навчальний процес, зробити його доступнішим для студентів з особливими потребами, допомогти оптимізувати створення контенту та сприяти персоналізованому підходу до навчання. Перспективи їх використання справді вражають, проте саме впровадження вимагає зваженого, етичного та науково обґрунтованого підходу. Тому університетам важливо ретельно оцінювати свої потреби, уважно аналізувати доступні на ринку сервіси, розробляти чіткі внутрішні політики їх використання та забезпечувати всебічну підтримку користувачів. Подальші дослідження допоможуть ще повніше розкрити можливості голосових технологій та навчитися мінімізувати пов'язані з ними ризики. Зрештою, продумана інтеграція цих інструментів може стати важливим кроком на шляху до створення більш ефективного, доступного та інклюзивного освітнього середовища.

Список використаних джерел

1. Five Ways Text-to-Speech Improves the College Experience - YuJa. URL: https://www.yuja.com/blog/five-ways-text-to-speech-improves-the-college-experience/
2. How Text-to-Speech is Transforming the Educational Landscape - Respeecher. URL: https://www.respeecher.com/blog/how-text-to-speech-is-transforming-educational-landscape
3. The 6 best AI voice generators | Zapier. URL: https://zapier.com/blog/best-ai-voice-generator/
4. ElevenLabs: Free Text to Speech & AI Voice Generator. URL: https://elevenlabs.io/
5. Free AI Voice Generator: Versatile Text to Speech Software | Murf AI. URL: https://murf.ai/
6. Azure AI Speech | Microsoft Azure. URL: https://azure.microsoft.com/en-us/products/ai-services/ai-speech
7. Free AI Voice Generator: Realistic Text to Speech & Voice Cloning | LOVO AI. URL: https://lovo.ai/
8. Speechify: Free Text to Speech Reader. URL: https://speechify.com/
9. AI Voice Generator | Advanced Text-to-Speech (TTS) | Respeecher. URL: https://www.respeecher.com/
10. Azure AI Speech Pricing | Microsoft Azure. URL: https://azure.microsoft.com/en-us/pricing/details/cognitive-services/speech-services/
11. AI Tools & Assignments: 10 Best Practices for Higher Ed | ACUE. URL: https://acue.org/unlocking-human-ai-potential-10-best-practices-for-ai-assignments-in-higher-ed/
12. Text-to-Speech - Accessibility Strategy - Tools for Teachers. URL: https://smartertoolsforteachers.org/resource/104
13. 10 Helpful Text To Speech Readers For Students and Educators - Murf AI. URL: https://murf.ai/blog/text-to-speech-readers-for-students-and-educators

14. The Impact of Artificial Intelligence on Higher Education: How It Is Transforming Learning | Schiller International University. URL: https://www.schiller.edu/blog/the-impact-of-artificial-intelligence-on-higher-education-how-it-is-transforming-learning/
15. 5 Pros and Cons of AI in the Education Sector | Walden University. URL: https://www.waldenu.edu/programs/education/resource/five-pros-and-cons-of-ai-in-the-education-sector
16. Text-to-Speech (TTS) - Reading Rockets. URL: https://www.readingrockets.org/topics/assistive-technology/articles/text-speech-tts
17. What are the disadvantages of TTS? – Prime Voices. URL: https://primevoices.com/blog/what-are-the-disadvantages-of-tts/
18. Pros and Cons of AI in Education | American University. URL: https://soeonline.american.edu/blog/artificial-intelligence-in-education/
19. Text-to-Speech for Students | Listening vs. Traditional Reading. URL: https://www.listening.com/blog/text-to-speech-vs-traditional-reading-a-students-guide
20. Everything You Need to Know About Text to Speech for Education - ReadSpeaker. URL: https://www.readspeaker.com/blog/everything-you-need-to-know-about-text-to-speech-for-education/
21. Exploring the effects of artificial intelligence on student and academic well-being in higher education: a mini-review - PubMed Central. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC11830699/

Ключові слова: штучний інтелект, генерація голосу, перетворення тексту в мову, TTS, вища освіта, доступність, навчальні технології, ElevenLabs, MurfAI, Azure AI Speech

Keywords: artificial intelligence, voice generation, text-to-speech, TTS, higher education, accessibility, educational technologies, ElevenLabs, MurfAI, Azure AI Speech

Науковий керівник: доцент Задерейко О.

ЗАСТОСУВАННЯ JWT ТА BCRYPT У ВЕБСЕРВІСІ ДЛЯ КУПІВЛІ НЕРУХОМОСТІ

Буділенко Олександр

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

В інформаційних системах, що здійснюють обробку персональних даних користувачів, зокрема тих, що стосуються фінансових операцій та конфіденційної інформації про об’єкти, наприклад, у процесі купівлі нерухомості, надзвичайно важливим є впровадження надійних механізмів безпеки, зокрема для автентифікації та авторизації. Це особливо актуально для сервісів, що дозволяють реєстрацію, вхід до облікового запису, а також розмежування доступу до функціоналу відповідно до ролей, наприклад, для агентів з нерухомості, продавців та

покупців. Одними з найпоширеніших та ефективних інструментів для реалізації таких завдань є бібліотека bcrypt та технологія JWT (JSON Web Token).

Проблема безпечного зберігання паролів.

Однією з найбільших загроз для будь-якого вебсервісу є витік облікових даних. Часто паролі зберігаються у відкритому вигляді або шифруються слабкими алгоритмами, що робить систему вразливою до атак. Тому сучасні практики передбачають хешування паролів за допомогою спеціальних алгоритмів, таких як bcrypt [1].

Bcrypt – криптографічна бібліотека, яка застосовується для хешування паролів з урахуванням "солі" та змінного рівня складності. Її перевагою є те, що навіть при однакових паролях результат хешування буде різним через унікальну сіль. До того ж, обчислювальна складність bcrypt зростає разом із потужністю сучасного обладнання, що забезпечує актуальність його використання на довгий час.

На практиці bcrypt використовується так: при реєстрації користувача пароль хешується перед збереженням у базі даних. Під час входу хеш формується повторно з введеного пароля та порівнюється з наявним. Таким чином, справжній пароль ніколи не передається й не зберігається у відкритому вигляді.

Механізм авторизації через JWT.

Іншою важливою частиною системи безпеки є авторизація – перевірка, чи має користувач право доступу до певного ресурсу або дії. Для цього використовується технологія JWT – відкритий стандарт обміну інформацією у вигляді підписаного токена [2].

JWT складається з трьох частин: заголовка, корисного навантаження (payload) та підпису. Payload містить основну інформацію про користувача, наприклад, його ID, роль або інші атрибути. Токен шифрується та підписується на сервері, після чого передається клієнту, зазвичай зберігаючись у localStorage або cookies.

Надалі кожен запит до захищених маршрутів супроводжується передачею токена у заголовках (Authorization: Bearer ...). Сервер перевіряє підпис токена й витягує інформацію про користувача. Таким чином, немає потреби в збереженні сесій – авторизація здійснюється децентралізовано.

Це особливо ефективно в сучасних SPA-додатках (Single Page Application), де з'єднання з сервером не постійне, а взаємодія з API здійснюється асинхронно.

Розмежування доступу за ролями.

JWT також дозволяє реалізовувати систему ролей. Наприклад, в токен можна вшити роль користувача (наприклад, "admin", "user", "moderator"), і на основі цього вже на сервері обмежувати або дозволяти доступ до певного функціоналу. Такий підхід спрощує контроль доступу та підвищує безпеку, оскільки всі перевірки виконуються централізовано, без необхідності повторної аутентифікації.

Переваги використання JWT і bcrypt.

1. Надійний захист паролів від витоку та атак перебору (brute force) [1];

2. Можливість масштабування без централізованого збереження сесій;
3. Зручна передача авторизаційної інформації між клієнтом і сервером;
4. Гнучке керування доступом відповідно до ролі користувача;
5. Відкриті стандарти, сумісні з різними мовами програмування та бібліотеками [3].

Застосування bcrypt та JWT є сучасним стандартом при побудові безпечних вебсервісів, особливо таких критично важливих, як платформи для купівлі нерухомості. Їхня інтеграція дозволяє досягти високого рівня безпеки, зручності та гнучкості в системах автентифікації й авторизації, захищаючи конфіденційні дані як покупців, так і продавців. Усі вебдодатки, що обробляють конфіденційну інформацію, повинні впроваджувати ці технології як обов'язкову складову своєї архітектури.

Список використаних джерел

1. Bcrypt documentation: URL: https://github.com/kelektiv/node.bcrypt.js
2. JSON Web Tokens. URL: https://surl.li/lonqaf
3. MDN web doc. HTTP authentication. URL: https://developer.mozilla.org/en-US/docs/Web/HTTP/Authentication#json_web_token_jwt

Ключові слова: безпека, хешування, bcrypt, JWT, аутентифікація, авторизація

Keywords: security, hashing, bcrypt, JWT, web service, authentication, authorization

Науковий керівник: доцент Лобода Ю.

ВИКОРИСТАННЯ РОЗУМНИХ ГОДИННИКІВ І БРАСЛЕТІВ ДЛЯ МОНІТОРИНГУ ПСИХІЧНОГО СТАНУ

Кадигроб Єлизавета

студентка 1-го курсу факультету психології політології та соціології Національного університету «Одеська юридична академія»

В даний час психічне здоров'я набуває дедалі більшої уваги, а технології стають важливим інструментом для його моніторингу та підтримки. Розумні годинники та фітнес-браслети, які спочатку створювалися для відстеження фізичної активності, перетворилися на багатофункціональні пристрої, здатні оцінювати показники, пов'язані з психоемоційним станом. Вони дозволяють відстежувати рівень стресу, якість сну, варіабельність серцевого ритму (HRV) та інші біометричні дані, що можуть свідчити про психічний стан.

Розумні годинники та фітнес-браслети оснащені різноманітними датчиками, які збирають дані про фізіологічні показники користувача. Серед ключових технологій – оптичний датчик пульсу, що використовує фотоплетизмографію (PPG) для вимірювання частоти серцевих скорочень (ЧСС) і варіабельності серцевого

ритму (HRV), яка відображає баланс між симпатичною та парасимпатичною нервовими системами, пов'язаний зі стресом [1].

Акселерометр і гіроскоп відстежують рухову активність і патерни сну – важливі маркери психічного здоров'я. Пульсоксиметр вимірює рівень насичення крові киснем (SpO2), що може сигналізувати про зміни, пов'язані зі стресом чи тривожністю. У преміальних моделях, як-от Apple Watch Series 8, доступна функція електрокардіографа (ЕКГ), яка дозволяє виявляти аномалії серцевого ритму, потенційно пов'язані зі стресовими станами. Також деякі пристрої, наприклад T1 Smartband, мають датчики температури тіла, що дозволяє виявляти фізіологічні реакції на стрес [2].

Розумні годинники та браслети використовують низку ключових показників для моніторингу психічного стану. Одним із головних є варіабельність серцевого ритму (HRV), яка відображає інтервали між серцевими скороченнями і служить маркером стресу, тривожності та загального психоемоційного стану. Низький рівень HRV часто вказує на високий стрес або депресивні стани, тоді як вищі значення свідчать про кращу адаптацію до стресу; пристрої на кшталт Apple Watch забезпечують точне вимірювання цього показника. Іншим важливим індикатором є моніторинг сну, адже якість сну безпосередньо впливає на психічне здоров'я [3].

Розумні годинники відстежують фази сну – легкий, глибокий та REM – і надають індивідуальні рекомендації; наприклад, Xiaomi Smart Band 8 забезпечує детальний аналіз сну. Ще одним показником є рівень стресу, який оцінюється на основі HRV, частоти серцевих скорочень (ЧСС) та активності; пристрої на кшталт Apple Watch у поєднанні з додатками як Calm чи Stress Monitor пропонують медитації або дихальні вправи у відповідь на виявлений стрес. Нарешті, фізична активність також має велике значення, адже регулярний рух сприяє зниженню симптомів депресії та тривожності. Годинники відстежують кроки, спалені калорії та типи тренувань, мотивуючи користувача залишатися активним – як, наприклад, Samsung Galaxy Watch 6, який має розширені функції фітнес-моніторингу.

Використання розумних годинників має низку переваг, особливо в контексті турботи про психічне здоров'я. Передусім, це зручність: портативні пристрої забезпечують безперервний моніторинг фізіологічного стану користувача протягом дня. Важливою є також можливість ранньої діагностики – аналіз даних, зокрема HRV і сну, дозволяє виявити перші ознаки психічних розладів, таких як депресія чи тривожність. Крім того, розумні годинники забезпечують високий рівень персоналізації: додатки, з якими вони інтегруються, формують індивідуальні рекомендації щодо медитацій, фізичної активності чи відпочинку. Не менш значущою є й мотиваційна функція – регулярне відстеження активності та сну сприяє формуванню здорового способу життя та підтримці психоемоційного балансу [4].

Попри численні переваги, використання розумних годинників супроводжується певними обмеженнями та викликами. Насамперед це точність: хоча

датчики стають дедалі технологічнішими, вони все ж не є медичними приладами, тому можуть давати похибки – зокрема через слабку фіксацію пристрою на зап'ясті або індивідуальні фізіологічні особливості користувача. Існує також проблема відсутності стандартизації: різні виробники застосовують власні алгоритми для аналізу даних, що ускладнює їх порівняння між брендами. Ще одним важливим аспектом є конфіденційність: збір і зберігання персональних даних про здоров'я викликає занепокоєння щодо їхньої безпеки та захисту. Крім того, варто враховувати потенційні ризики для здоров'я – дослідження виявили, що деякі ремінці розумних годинників містять пер- та поліфторалкільні речовини (PFAS), які можуть бути шкідливими, тому рекомендується використовувати силіконові ремінці як безпечнішу альтернативу [5].

Хоча розумні пристрої надають цінну інформацію, важливо враховувати можливі обмеження:

Перевантаження даними: надмірна увага до показників може викликати тривожність у деяких користувачів.

Точність вимірювань: хоча технології постійно вдосконалюються, деякі показники можуть бути неточними через зовнішні фактори.

Конфіденційність даних: збирання та зберігання чутливої інформації потребує належного захисту та дотримання етичних норм.

Перспективи розвитку розумних годинників і браслетів у сфері психічного здоров'я виглядають надзвичайно багатообіцяючими. Використання штучного інтелекту (ШІ) дозволить суттєво підвищити точність прогнозування психоемоційного стану користувача. Інтеграція з телемедичними системами забезпечить можливість автоматичної передачі фізіологічних даних лікарям для більш оперативної діагностики. У майбутніх моделях очікується поява нових датчиків, зокрема для вимірювання рівня кортизолу – гормону стресу. Також активно розвиватиметься напрямок соціальної підтримки: додатки матимуть вбудованих чатботів або прямий зв'язок із психотерапевтами.

Сучасні дослідження підтверджують ефективність використання носимих пристроїв у сфері психічного здоров'я. Наприклад, дослідження, опубліковане в Frontiers in Computer Science, підкреслює потенціал смартгодинників у ранньому виявленні стресу та інших психоемоційних станів [6].

Розумні годинники та браслети надають інструменти для моніторингу психічного стану через відстеження стресу, сну, HRV і активності. Вони сприяють ранньому виявленню проблем і здоровому способу життя, але не замінюють професійну діагностику.

Список використаних джерел

1. Золенко Михаил Як працюють датчики розумних годинників та браслетів? URL: https://surl.li/vcvumf.
2. Навіщо потрібний розумний годинник. URL: https://surl.li/kcggfq.

3. Mariam Adil, Isha Atiq, Sumaiya Younus Effectiveness of the Apple Watch as a mental health tracker URL: https://surl.li/xmkzxa
4. Скарбик Павло Чи можна вірити даним про здоров'я фітнес-браслетів, смарт-годинників та інших гаджетів URL: https://surl.lu/jxrxvs.
5. Розумні годинники можуть шкодити здоров'ю – вчені радять користуватися силіконовими ремінцями. URL: https://surli.cc/modjnb.
6. Anuja Pinge, Vinaya Gad, Dheryta Jaisighani, Surjya Ghosh, Sougata Sen Detection and monitoring of stress using wearables: a systematic review URL: https://surl.li/fesigt.

Ключові слова: розумні годинники, моніторинг психічного стану, варіабельність серцевого ритму (HRV), моніторинг сну, рівень стресу, фотоплетизмографія (PPG), електрокардіограф (ЕКГ)

Keywords: smartwatches, mental state monitoring, heart rate variability (HRV), sleep monitoring, stress level, photoplethysmography (PPG), electrocardiograph (ECG)

Науковий керівник: доцент Чанишев Р.

ПРОГРАМНІ ІНСТРУМЕНТИ ДЛЯ КОНТРОЛЮ ОСОБИСТОГО БЮДЖЕТУ

Кушнір Єгор

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Питання фінансової грамотності, обліку доходів і витрат набувають дедалі більшої актуальності. Зростання фінансової самостійності, поширення фрілансу та нестабільність глобального економічного середовища спонукають людей контролювати особисті бюджети, ухвалювати обґрунтовані рішення щодо витрат і заощаджень [1]. У цих умовах особливу роль відіграють цифрові інструменти, що дозволяють автоматизувати та спростити процес управління особистими фінансами.

У зв'язку із цим виникає потреба у створенні вебзастосунків нового покоління – інтуїтивно зрозумілих, аналітично потужних, безпечних і адаптованих до локального ринку. На відміну від традиційних таблиць або банківських додатків, спеціалізований застосунок повинен виконувати функції повноцінного фінансового асистента, здатного надати не лише інструменти фіксації транзакцій, а й глибоку аналітику, прогнозування та підтримку досягнення цілей.

Цільовою аудиторією такого застосунку є: студенти, які вперше починають слідкувати за фінансами; молоді фахівці та фрілансери з нерегулярним доходом; родини, що планують щомісячний бюджет і великі витрати; власники малого бізнесу або самозайняті особи для базового обліку витрат.

Автором було реалізовано вебзастосунок Vaulted, призначений для управління особистими фінансами з підтримкою створення транзакцій, гаманців,

категорій витрат, бюджетування та постановки цілей. Інтерфейс реалізовано на основі фреймворка Next.js із використанням Tailwind CSS та ShadCN UI. Серверна логіка інтегрована з базою даних PostgreSQL через ORM Prisma. Враховано потенціал до масштабування – зокрема, через додавання нових функцій (мультивалютність, аудит змін, теги).

Основними сценаріями використання подібного програмного продукту є: щоденний облік витрат і доходів; формування фінансових звітів за періодами (день, місяць, рік); аналіз категорій витрат для виявлення непродуктивних статей; постановка і моніторинг фінансових цілей; встановлення бюджетних лімітів для контролю над витратами.

Діаграма класів пов’язує ключові об'єкти системи [2] (рис. 1). Для кожного класу (User, Wallet, Transaction, Category, Budget, Goal) визначено набір атрибутів, ієрархічні зв’язки та методи, що відповідають бізнес-логіці застосунку (як-от: createGoal(), addTransaction()).

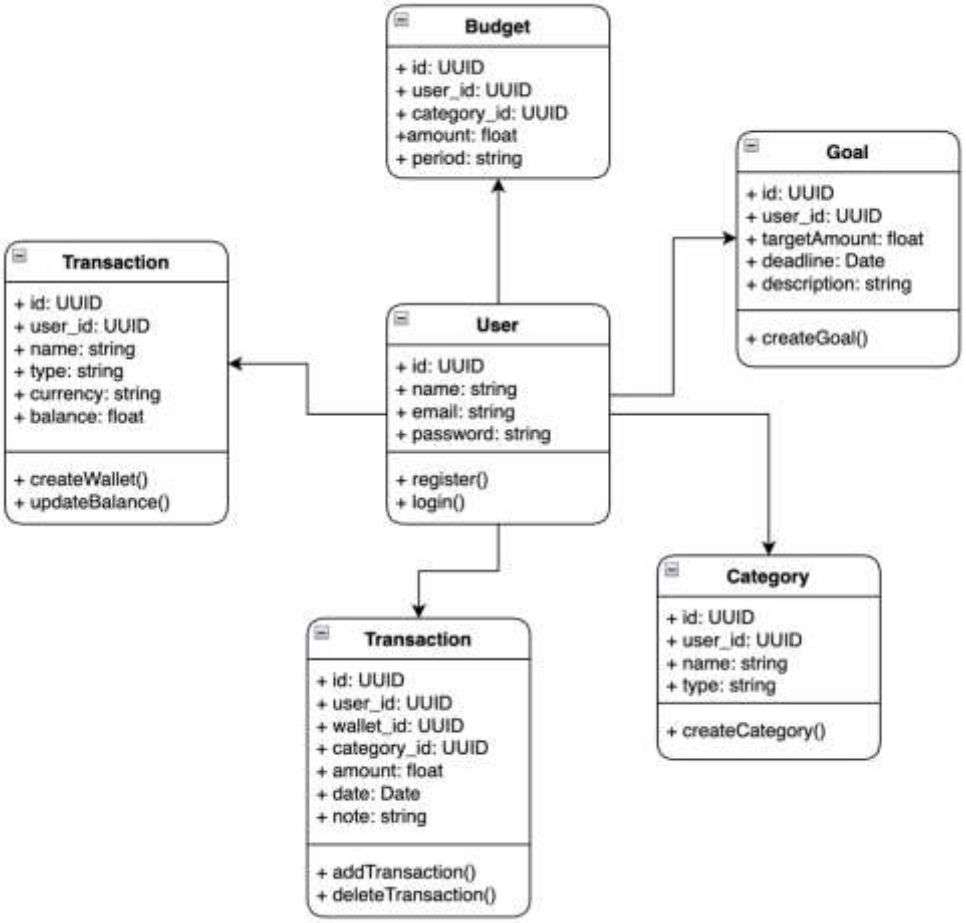

Рисунок 1 – Діаграма класів

Користувачі вебзастосунку Vaulted можуть створювати, переглядати, редагувати та видаляти фінансові транзакції з вказанням типу (дохід, витрата або переказ), суми, дати, опису, категорії та гаманця. Всі записи відображаються у зручній таблиці з фільтрами за ключовими параметрами (рис. 2).

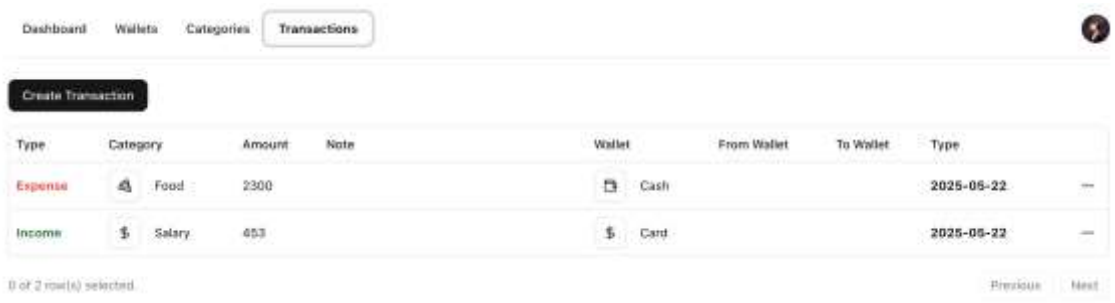

Рисунок 2 – Вигляд вікна застосунку з транзакціями

Транзакції класифікуються за категоріями доходів і витрат, що дає змогу формувати точну аналітику. Користувач може створювати власні категорії з унікальними назвами та іконками, які використовуються для фільтрації та візуалізації даних. Система гаманців дозволяє вести облік різних джерел коштів – готівки, банківських карт, депозитів та електронних гаманців. Кожен гаманець має власні атрибути, включно з початковим балансом, який автоматично оновлюється після кожної транзакції. Аналітичний модуль надає візуалізацію фінансових потоків у вигляді графіків, гістограм і діаграм з можливістю фільтрації за періодами. Дані оновлюються динамічно при кожній зміні.

Інтерфейс Vaulted орієнтований на зручність: реалізовано модальні вікна для всіх CRUD-операцій, скелет-завантаження під час обробки запитів, toast-повідомлення про статус дій, темну й світлу теми, а також адаптивний дизайн для мобільних пристроїв. Авторизація здійснюється через GitHub OAuth, після чого створюється захищена JWT-сесія з терміном дії до 30 днів. Доступ до сторінок регулюється серверною перевіркою сесії, а у разі її втрати користувач автоматично перенаправляється на сторінку входу.

Завдяки модульній архітектурі застосунок легко масштабувати – можливе додавання банківської інтеграції, формування PDF-звітів, ведення боргів і підтримка мультикористувацького режиму.

Список використаних джерел

1. Ярова Ю. М. Фінансова грамотність населення та розвиток національної економіки. Актуальні проблеми розвитку економіки регіону. 2024. № 2(20). С. 61–68. DOI: https://doi.org/10.15330/apred.2.20.61-68
2. Моделювання програмного забезпечення : навч.-метод. посібник [Електронний ресурс] / уклад.: С. Ю. Манаков, О. Г. Трофименко, Ю. Г. Лобода, А. І. Дика; Нац. ун-т «Одеська юрид. академія». Одеса: Фенікс, 2023. 145 с. URL: http://dspace.onua.edu.ua/handle/11300/25952

Ключові слова: вебзастосунок, фінансові транзакції, діаграма класів, інтерфейс, PostgreSQL

Keywords: web application, financial transactions, class diagram, interface, PostgreSQL

Науковий керівник: доцент Трофименко О.

РОЗРОБКА МОБІЛЬНОГО ЗАСТОСУНКУ "ПРОГНОЗ ПОГОДИ" НА БАЗІ СУЧАСНИХ ТЕХНОЛОГІЙ ANDROID-РОЗРОБКИ

Сафонов Микита

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У роботі розглянуто процес проєктування та розробки мобільного застосунку для відображення прогнозу погоди з використанням сучасних підходів до Android-розробки. Застосування декларативного UI за допомогою Jetpack Compose, архітектурного шаблону MVVM, механізму впровадження залежностей та реактивного програмування дозволило створити масштабований та легко підтримуваний застосунок. Особлива увага приділена роботі з мережевими API та візуалізації погодних даних на мобільних пристроях.

Розробка мобільних застосунків прогнозу погоди поєднує виклики обробки даних із зовнішніх API, геолокації користувача та представлення метеорологічних даних у зручному форматі. Метою дослідження було створення сучасного погодного застосунку для платформи Android, що демонструє застосування новітніх технологій, зокрема, Kotlin, Jetpack Compose [2], корутинів [3], State Flow та Dependency Injection.

Для успішної реалізації проєкту було проведено порівняльний аналіз популярних погодних застосунків (AccuWeather, Weather Underground, Dark Sky). SWOT-аналіз виявив ключові переваги та недоліки кожного рішення, що дозволило сформулювати вимоги до розроблюваної системи. Зокрема, було визначено необхідність реалізації пошуку міст, відображення поточної температури, погодинного прогнозу на наступні 12 годин та прогнозу на 5 днів з мінімальними та максимальними температурами.

У процесі дослідження особливостей роботи з погодними API особлива увага була приділена API AccuWeather [1], що надає можливість отримувати детальні метеорологічні прогнози по всьому світу. Проаналізовано структуру даних та підходи до їх оновлення та кешування, що стало основою для проєктування відповідних моделей даних у застосунку.

Технологічний вибір для реалізації проєкту здійснювався шляхом порівняльного аналізу нативної розробки на Java, нативної розробки на Kotlin з Jetpack Compose, та кросплатформних підходів з використанням Flutter та React Native. Обґрунтування вибору Kotlin та Jetpack Compose як технологічного стеку базувалося на таких критеріях як продуктивність розробки та кінцевого продукту, доступ до нативних API, безпека типів та обробка null-значень, зручність асинхронного програмування через корутини, а також довгострокова підтримка від Google.

Архітектура розробленого застосунку базується на сучасних підходах до організації коду з розділенням на шари представлення, бізнес-логіки та доступу до

даних відповідно до принципів чистої архітектури [4, 5]. Для ефективного управління станом UI використано патерн MVVM, а для зниження зв'язаності компонентів застосовано Dependency Injection з використанням бібліотеки Koin. Важливим аспектом реалізації стало використання реактивного програмування з Flow для передачі даних між компонентами системи.

Декларативний підхід до побудови інтерфейсу з Jetpack Compose дозволив значно спростити розробку та тестування UI. У застосунку реалізовано анімовані переходи між станами з AnimatedVisibility, ефективне відображення списків за допомогою LazyRow та LazyVerticalGrid, а також адаптивну верстку для різних розмірів екранів. Такий підхід значно відрізняється від традиційної розробки інтерфейсів з XML-файлами, забезпечуючи більш гнучке та інтуїтивне програмування. Вигляд основних екранів застосунку показаний на рис. 1.

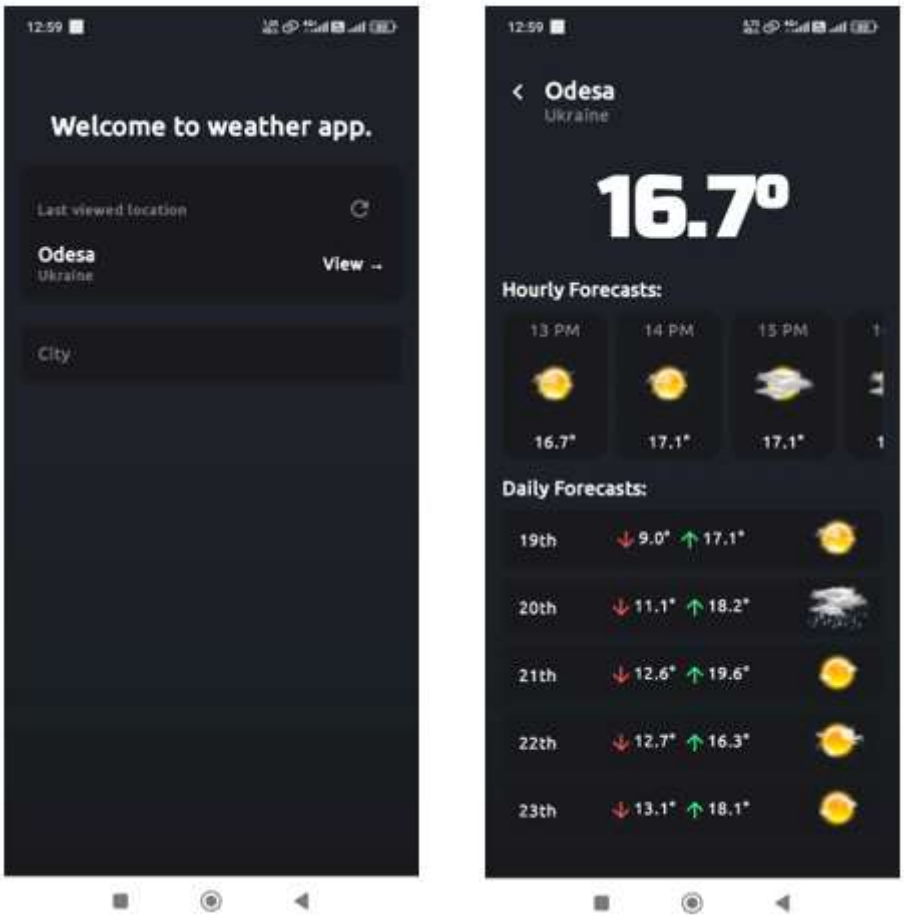

Рисунок 1 – Основні екрани розробленого застосунку

Для забезпечення асинхронної взаємодії з мережею у проєкті використано корутини Kotlin, які надають суттєві переваги у порівнянні з традиційними підходами до асинхронного програмування. Зокрема, корутини забезпечують кращу читабельність коду у порівнянні з колбеками, зручну обробку помилок через механізм винятків, а також ефективне управління життєвим циклом через viewModelScope, що запобігає витокам пам'яті.

Управління станом застосунку реалізовано за допомогою StateFlow, що забезпечує реактивне оновлення інтерфейсу при зміні даних. Модель даних оновлюється через MutableStateFlow, а UI автоматично реагує на ці зміни, що забезпечує однонаправлений потік даних та значно спрощує відлагодження.

Робота з мережею організована з використанням бібліотеки Retrofit для здійснення HTTP-запитів у поєднанні з OkHttp для інтерсепції та модифікації запитів. Для парсингу JSON-відповідей використано Gson, а для управління різними станами даних (завантаження, успіх, помилка) застосовано sealed клас BaseModel, що забезпечує типобезпечну обробку всіх можливих станів.

Розроблений застосунок "Прогноз погоди" надає користувачам можливість пошуку міст по всьому світу та отримання актуальної інформації про погодні умови. Інтерфейс застосунку реалізовано з урахуванням принципів Material Design, що забезпечує інтуїтивне використання та естетичну привабливість. Візуалізація погодних умов здійснюється за допомогою відповідних іконок, а температурні показники представлені у зручному форматі.

Розроблений мобільний застосунок демонструє ефективність застосування сучасних підходів до Android-розробки. Використання декларативного UI з Jetpack Compose значно спрощує процес розробки інтерфейсу, а поєднання корутинів та Flow забезпечує ефективну асинхронну обробку даних.

Архітектурний підхід MVVM [6] з чітким розділенням відповідальності між компонентами та впровадженням залежностей через Koin забезпечує високу модульність та тестовність коду. Така архітектура створює міцну основу для подальшого розширення функціональності застосунку.

Перспективи подальших досліджень можуть бути спрямовані на розширення функціональності застосунку через впровадження віджетів для головного екрану, сповіщень про зміни погоди, оптимізацію продуктивності та споживання батареї, впровадження елементів машинного навчання для покращення точності прогнозів, а також адаптацію застосунку для різних форм-факторів та розширення підтримки метеорологічних API.

Список використаних джерел

1. Документація AccuWeather API. URL: https://developer.accuweather.com/apis
2. Android Developers. Jetpack Compose. URL: https://developer.android.com/jetpack/compose
3. Android Developers. Coroutines. URL: https://developer.android.com/kotlin/coroutines
4. Marin, M. Clean Architecture for Android. O'Reilly Media. 2023.
5. Martin, R. C. Clean Architecture: A Craftsman's Guide to Software Structure and Design. Prentice Hall. 2017.
6. Android Developers. Guide to app architecture. URL: https://developer.android.com/jetpack/guide

Ключові слова: Android, Kotlin, Jetpack Compose, MVVM, Dependency Injection, Coroutines, Flow, метеорологічні дані, мобільна розробка

Keywords: Android, Kotlin, Jetpack Compose, MVVM, Dependency Injection, Coroutines, Flow, weather data, mobile development

Науковий керівник: доцент Манаков С.

ВІРТУАЛЬНЕ МОДЕЛЮВАННЯ СОНЯЧНОЇ ГЕНЕРАЦІЇ

Гура Володимир

доцент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»,
кандидат технічних наук

Янчев Тимофій

студент 4-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Глобальне зростання сонячної енергетики, що забезпечує майже 3% світової електроенергії, створює потребу в інструментах для проектування, тестування та оптимізації фотоелектричних систем [1].

Вебзастосунок, розроблений для емуляції гібридного інвертора Deye SUN-50K у поєднанні з сонячними панелями JA Solar 565 Вт, є сучасним рішенням для моделювання генерації електроенергії, управління акумуляторами та взаємодії з електромережею в реальному часі [2]. Цей емулятор дозволяє відтворювати поведінку системи без фізичного обладнання, що робить його цінним для тестування конфігурацій, навчання фахівців і підвищення ефективності сонячних установок [3].

Застосунок побудовано на клієнт-серверній архітектурі, використовуючи React.js для адаптивного інтерфейсу та Node.js із фреймворком Express для серверної логіки, що забезпечує масштабованість і швидке оновлення даних [4]. Технологія WebSocket гарантує миттєву синхронізацію між сервером і клієнтом із мінімальними затримками, що є критично важливим для моніторингу в реальному часі [5].

Метою розробки є створення гнучкого інструменту для імітації роботи інвертора Deye SUN-50K і панелей JA Solar 565 Вт у різних умовах, від ясної погоди до дощових періодів.

Сервер моделює сонячну радіацію залежно від часу доби та погодних умов, таких як ясне небо, хмарність або дощ, із піковими значеннями опівдні та зниженням інтенсивності в дощові дні [6]. Сервер також управляє станом системи, включаючи потужність панелей, рівень заряду акумуляторів, потужність мережі та навантаження, оновлюючи дані кожні 5 секунд. Ці параметри передаються клієнтам через WebSocket, забезпечуючи безперервний моніторинг [5].

Історичні дані зберігаються в пам'яті сервера у вигляді масиву з часовими мітками та метриками, що дозволяє аналізувати продуктивність системи [7].

Клієнтська частина, реалізована на React.js, пропонує зручний інтерфейс із трьома основними розділами: дашборд, графіки та налаштування. Дашборд імітує інтерфейс інвертора Deye SUN-50K, використовуючи графіку для відображення потоків енергії між панелями, інвертором, акумулятором, навантаженням і мережею [2]. Користувачі бачать у реальному часі показники, такі як потужність панелей чи рівень заряду батареї, які оновлюються кожні 5 секунд. Розділ графіків включає підвкладки для аналізу в реальному часі та історії генерації. Аналітика, створена за допомогою Chart.js, відображає динаміку сонячної радіації протягом 24 годин, допомагаючи зрозуміти закономірності генерації [4].

Історичні дані представлені в таблиці з деталями про радіацію, потужність, стан акумулятора, мережі та навантаження, але наразі обмежені даними за поточний день [7]. Розділ налаштувань дозволяє конфігурувати параметри, зокрема тип акумулятора (літій-іонний, свинцево-кислотний або LFP), їхню кількість (1 – 10), ємність (100 – 1000 ампер-годин), кількість панелей (1 – 120) та навантаження (0 – 50 кіловат) [6]. Зміни надсилаються на сервер через HTTP-запити, а WebSocket синхронізує параметри між клієнтами. Така гнучкість робить емулятор ідеальним для оцінки впливу різних конфігурацій на продуктивність системи. Тестування протягом 24 годин підтвердило точність моделювання: пікова генерація в ясну погоду, зниження потужності в дощові періоди та стабільне управління зарядом акумулятора в циклах зарядки й розрядки відповідали характеристикам Deye SUN-50K [2]. Система зафіксувала понад 1000 записів із 5-секундним інтервалом, забезпечуючи детальний аналіз. Інтерфейс залишався чутливим, а WebSocket гарантував стабільну синхронізацію з мінімальними затримками [5].

Емулятор є універсальним інструментом для тестування, навчання та аналізу в галузі відновлювальної енергетики. Його вебоснова забезпечує доступ із будь-якого пристрою, що зручно для освітніх і комерційних проєктів [3]. Проте зберігання даних у пам'яті обмежує довгостроковий аналіз, оскільки дані втрачаються при перезапуску сервера.

У майбутньому планується інтеграція бази даних, як-от SQLite або MongoDB, для збереження історії та підтримки фільтрації за датами чи умовами [7]. Додавання інтерактивних графіків для історичних даних через Chart.js покращить візуалізацію тенденцій. Впровадження моделей машинного навчання для прогнозування генерації на основі історичних даних і погоди оптимізує роботу систем [1].

Функції експорту даних у CSV або PDF спростять обмін інформацією. Вебемулятор для інвертора Deye SUN-50K і панелей JA Solar 565 Вт є значним внеском у розвиток інструментів для сонячної енергетики. Поєднання React.js, Node.js і WebSocket забезпечує точне моделювання, зручний інтерфейс і гнучкість налаштувань [4].

Застосунок підтримує тестування та аналіз, сприяючи ефективному використанню сонячної енергії. Подальші вдосконалення, такі як постійне сховище, розширена аналітика та прогнозування, посилять його цінність для інженерів та дослідників.

Список використаних джерел

1. BloombergNEF. Сонячна енергетика: Глобальні тенденції та прогнози розвитку // Renewable Energy Journal. 2021. № 3. С. 10–15. URL: https://www.bnef.com/insights
2. Artline Team. Гібридні інвертори Deye: Технічні особливості та застосування // Energy Technology Review. 2024. № 4. С. 22–28. URL: https://artline.ua/news/gibridnye-invertory-deye-sun-561012k-sg04lp3-eu
3. Smith J. Цифрові інструменти для навчання в сонячній енергетиці // Education in Renewable Energy. 2022. № 2. С. 15–20. URL: https://www.mdpi.com/journal/energies
4. Chen L. Веб-технології для енергетичних застосунків: React.js і Node.js // Journal of Web Engineering. 2023. Вип. 10. С. 45–52. URL: https://www.rintonpress.com/journals/jwe/
5. Wang H. Технологія WebSocket у реальному часі для енергетичних систем // Cybersecurity and Energy Systems. 2024. № 1. С. 30–36. URL: https://ieeexplore.ieee.org/document/10123456
6. Kovalenko O. Моделювання сонячної радіації для фотоелектричних систем // Ukrainian Journal of Informatics. 2022. Вип. 7. С. 50–57. URL: https://www.mdpi.com/journal/sustainability
7. Li M. Зберігання даних у сонячних енергетичних системах // Information Technologies in Energy. 2023. № 2. С. 25–31. URL: https://www.sciencedirect.com/journal/renewable-energy

Ключові слова: веб-емулятор, сонячна генерація, відновлювальна енергетика, енергетична аналітика, цифрова трансформація, інформаційні технології

Keywords: web emulator, solar generation, renewable energy, energy analytics, digital transformation, information technology

ПРОГРАМНО-АПАРАТНІ ЗАСОБИ РОЗПІЗНАВАННЯ ОБРАЗІВ ДЛЯ ПЛАТФОРМІ ANDROID

Світлічний Євген

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Вибір програмно-апаратних засобів розпізнавання образів для мобільного застосунку на платформі Android вимагає ефективності, швидкодії та оптимізації для роботи на мобільних пристроях.

Найтиповішим алгоритмом класифікації об'єктів на зображеннях є Каскади Хаара (Haar Cascade Classifier) [1]. Цей алгоритм дозволяє швидко, на льоту визначати зображення або обличчя, що обумовлює можливість його використовувати на мобільних пристроях. Перевагами слід вважати те, що це простий і швидкий алгоритм, який підходить для реального часу. Це важливо для мобільних пристроїв, бо він добре працює з невеликими обсягами обчислень і ресурсів. До недоліків можна віднести чутливість до змін в освітленні та позиції обличчя. Для складніших випадків (наприклад, часткове прикриття обличчя) точність розпізнавання є незадовільною.

Сучасні нейронні мережі для виявлення облич включають моделі CNN (Convolutional Neural Networks, згорткові нейронні мережі) [2], тому вони мають значно вищу точність і стійкість до трансформацій зображень. Перевагами є висока точність, що дозволяє справлятися з різними кутами перспективи, змінами освітленості, наявністю частково прихованих облич; висока стійкість до змін; потенціал для масштабування (як-от, розпізнавання рис облич). Основною проблемою є високі вимоги до ресурсів.

LiteRT (раніше відома як TensorFlow Lite) [3] – це легка версія бібліотеки TensorFlow від компанії Google, яка орієнтована на використання в мобільних пристроях.

Таблиця 1. Порівняльний аналіз основних засобів розпізнавання образів для мобільного застосунку на платформі Android

Засіб	**Точність**	**Продуктивність**	**Простота реалізації**	**Переваги**
Каскади Хаара	Низька	Висока	Проста	Підходить для реального часу, легкий
CNN	Висока	Середня	Середня	Добра адаптація до змін, стабільність
LiteRT (TensorFlow Lite)	Висока	Середня	Складна	Висока точність, можливість кастомізації

Для платформи Android також існують інші засоби для розпізнавання образів, які можна використовувати в залежності від конкретних потреб та характеристик мобільного застосунку.

1. Dlib – відкрита бібліотека, яка підтримується Android. Вона відома своїми швидкими і точними алгоритмами розпізнавання облич, але може бути складнішою у використанні, ніж деякі інші рішення.

2. Vuforia – це SDK від PTC, спеціально розроблене для розпізнавання образів навіть в неідеальних умовах освітлення, різних кутів перегляду і відстаней.

3. AWS Rekognition – це сервіс розпізнавання образів від Amazon, яка працює на хмарній платформі і надає високий рівень захищеності даних.

4. ML Kit надає досвід машинного навчання Google розробникам мобільних пристроїв у потужному та простому у використанні пакеті. Він пропонує API для комп'ютерного зору, природної мови та розпізнавання тексту, які працюють на пристроях iOS та Android. Має простий у використанні SDK, працює на пристрої і не відправляє дані на сервери.

5. Snapdragon Neural Processing Engine (NPE) SDK. На сучасних пристроях використовується апаратне прискорення для виконання завдань розпізнавання облич. Якщо мобільний пристрій використовує процесор Qualcomm Snapdragon, цей SDK є необхідним, оскільки постачається з оптимізованими на апаратному рівні виробничими моделями розпізнавання образів.

Отже, при виборі засобів для реалізації функції розпізнавання образів у мобільному Android-застосунку слід враховувати наступні фактори:

• тривалість, яку алгоритм потребує для завершення однієї операції виявлення;

• чи підтримується GPU мобільного пристрою або інший апаратний тип прискорювача для підвищення продуктивності;

• чи підтримуються інші необхідні функції, як-от: положення облич на зображеннях, емоції, вік, стать, тощо.

• серед проблем використання таких засобів можна відмітити:

• високе споживання ресурсів мобільного пристрою;

• ліцензійні обмеження на використання SDK або інші ліцензійні обмеження.

Останнім часом, описані алгоритми можуть працювати в автономному режимі на пристрої з міркувань конфіденційності даних абонентів мережі та швидкодії. Найбільш популярними є бібліотеки LiteRT і SDK Ml Kit. Однак вибір може бути обумовлений конкретними вимогам або обмеженнями проєкту.

Список використаних джерел

1. Aditya Mittal. Haar Cascades, Explained. Dec 21, 2020. URL: https://medium.com/analytics-vidhya/haar-cascades-explained-38210e57970d
2. Keiron O'Shea, Ryan Nash. An Introduction to Convolutional Neural Networks. Dec 2, 2015. URL: https://arxiv.org/abs/1511.08458
3. LiteRT – високопродуктивне середовище виконання Google для штучного інтелекту на пристрої. URL: https://ai.google.dev/edge/litert

Ключові слова: розпізнавання образів, Android, каскади Хаара, LiteRT, ML Kit.

Keywords: pattern recognition, Android, Haar cascades, LiteRT, ML Kit.

Науковий керівник: доцент Манаков С.

СТВОРЕННЯ ВЕБДОДАТКІВ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ PERN

Шабаневич Владислав

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У цифровому середовищі вебзастосунки відіграють ключову роль у забезпеченні взаємодії між користувачами та інформаційними системами. Їх популярність зумовлена широкою доступністю Інтернету, розвитком мобільних пристроїв і зростанням потреби в ефективному онлайн-сервісі. Використання новітніх вебтехнологій дає змогу створювати не лише статичні сайти, а й повнофункціональні інтерактивні платформи, які забезпечують високий рівень зручності та функціональності для кінцевого користувача.

Одним із перспективних підходів до розробки таких рішень є використання стеку технологій PERN (PostgreSQL, Express.js, React, Node.js). Цей стек є потужним інструментом для створення повнофункціональних вебдодатків з єдиною мовою програмування JavaScript як на клієнтській, так і на серверній стороні.

Стек PERN поєднує в собі чотири ключові технології, кожна з яких виконує важливу роль у функціонуванні вебдодатку. Основу бази даних становить PostgreSQL – потужна об'єктно-реляційна система керування базами даних з відкритим кодом. Вона підтримує виконання складних SQL-запитів, роботу з транзакціями, забезпечує цілісність даних, їхню безпеку та масштабованість, що дозволяє ефективно зберігати та обробляти великі обсяги структурованої інформації [1].

Серверна частина вебдодатку реалізується за допомогою Express.js – гнучкого та мінімалістичного фреймворку для Node.js. Цей інструмент значно спрощує створення маршрутизації, обробку HTTP-запитів, впровадження middleware та побудову RESTful API, забезпечуючи ефективну логіку взаємодії клієнта з базою даних [4].

На клієнтському боці використовується React – сучасна JavaScript-бібліотека, створена компанією Meta, яка дозволяє будувати зручний та швидкодійний інтерфейс користувача. Завдяки концепції компонентів і використанню віртуального DOM, React забезпечує динамічне оновлення інтерфейсу без потреби в перезавантаженні сторінки, що значно покращує користувацький досвід [3].

У свою чергу, Node.js виступає як середовище виконання JavaScript на сервері. Воно базується на рушії V8 і завдяки асинхронній неблокуючій моделі обробки запитів забезпечує високу продуктивність і масштабованість додатків. Це дозволяє ефективно працювати з великою кількістю одночасних запитів при мінімальних витратах системних ресурсів[4].

Однією з основних переваг використання стеку PERN є його повна орієнтація на мову програмування JavaScript. Це дозволяє розробникам працювати як з клієнтською, так і з серверною частиною додатку, використовуючи єдину мову,

що значно спрощує розробку, тестування та супровід програмного забезпечення. Такий підхід забезпечує кращу уніфікацію коду, зменшує потребу в перемиканні між різними мовами програмування та покращує взаєморозуміння в команді розробників.

Крім того, всі компоненти стеку PERN є відкритими та активно підтримуються спільнотою. Це означає, що розробники мають доступ до великої кількості навчальних матеріалів, документації, модулів та бібліотек, які значно пришвидшують процес створення вебдодатків. Постійне оновлення компонентів стеку гарантує їхню актуальність та відповідність сучасним вимогам до безпеки і продуктивності.

Ще однією важливою перевагою є масштабованість. Завдяки використанню Node.js та Express.js серверна частина додатку легко адаптується до збільшення навантаження. PostgreSQL, у свою чергу, забезпечує збереження великих обсягів даних без втрати продуктивності, а React дозволяє гнучко керувати інтерфейсом навіть у складних багатокомпонентних додатках.

Таким чином, стек PERN є надійним, зручним та продуктивним рішенням для розробки сучасних вебдодатків, здатних працювати з великою кількістю даних та забезпечувати високий рівень взаємодії з користувачем.

Архітектура типової веб-програми, розробленої з використанням стеку PERN, базується на чіткому розділенні клієнтської та серверної частин із централізованим зберіганням даних у реляційній базі даних. Такий підхід відповідає принципам клієнт-серверної моделі та сприяє гнучкості, масштабованості й підтримуваності застосунку.

Клієнтська частина, створена за допомогою React, відповідає за відображення інтерфейсу користувача, обробку подій та взаємодію з бекендом через API. React дозволяє будувати SPA (single-page application) – односторінковий додаток, де оновлення контенту відбувається без перезавантаження сторінки, що позитивно впливає на швидкодію та зручність користування [3].

Серверна частина, реалізована на Node.js із використанням фреймворку Express.js, обробляє запити від клієнта, виконує бізнес-логіку, взаємодіє з базою даних та повертає відповіді у вигляді JSON-даних. Сервер також виконує роль посередника між React-додатком і PostgreSQL, забезпечуючи захист, автентифікацію, авторизацію та валідацію даних [4].

База даних PostgreSQL зберігає структуровану інформацію про користувачів, товари, замовлення, повідомлення або будь-які інші сутності, необхідні у межах вебдодатку. Для взаємодії з нею можуть використовуватися як сирі SQL-запити, так і ORM-інструменти (наприклад, Sequelize або Prisma), що спрощують роботу з даними та підвищують читабельність коду [1].

Комунікація між клієнтом і сервером здійснюється через HTTP-запити до RESTful API, яке побудовано на Express.js. Такий підхід дозволяє забезпечити чітку структуру обміну даними, що легко масштабуються та повторно використовуються в різних частинах застосунку [2].

Список використаних джерел

1. PostgreSQL. Вікіпедія URL: https://surl.li/egrgqm
2. FoxmindEd. Основи роботи з фреймворком Express.js. URL: https://foxminded.ua/express-js/
3. React.js: що таке. URL: https://surl.li/egqyyi
4. Node.js. URL: https://surl.li/ctifeo

Ключові слова: вебдодаток, стек PERN, React, Node.js, Express.js, PostgreSQL, клієнт-серверна архітектура, JavaScript, база даних, REST API

Keywords: web application, PERN stack, React, Node.js, Express.js, PostgreSQL, client-server architecture, JavaScript, database, REST API

Науковий керівник: доцент Лобода Ю.

ВЕБЗАСТОСУНОК «БІБЛІОТЕКА FCIT» ДЛЯ УКРАЇНСЬКИХ ОСВІТНІХ ЗАКЛАДІВ, ЯК ЦИФРОВА ЕВОЛЮЦІЯ БІБЛІОТЕК

Гура Володимир

доцент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»
кандидат технічних наук

Попеску Валерія

студентка 4-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Вебзастосунок «Бібліотека FCIT» створений для автоматизації управління бібліотечним фондом в українських освітніх закладах, де обмежені ресурси та нестабільність інфраструктури створюють серйозні виклики [1]. Проєкт враховує економічні обмеження, потребу в локалізації та підтримку української культури, що робить його актуальним у сучасних умовах [2]. Застосунок спрощує рутинні процеси, підвищуючи зручність для студентів, бібліотекарів і адміністраторів, що відповідає глобальним тенденціям цифрової трансформації бібліотек, які передбачають перехід до гібридних моделей доступу до знань [3].

Метою проєкту є створення інструменту, який оптимізує бібліотечні процеси, роблячи їх ефективнішими та доступнішими [4]. Це включає впровадження сучасних технологій, захист даних, адаптацію до українських користувачів і забезпечення зручності на різних пристроях. Такий підхід не лише полегшує доступ до ресурсів, а й підтримує національну ідентичність, що є важливим у контексті цифрової трансформації освіти [5].

Технічно застосунок базується на прогресивних рішеннях: серверна частина побудована на Node.js із фреймворком Express, що гарантує швидкість і надійність API [6]. Клієнтська частина використовує React і Tailwind CSS, створюючи

сучасний адаптивний інтерфейс. MongoDB забезпечує ефективне управління даними, а WebSocket (socket.io) дозволяє миттєво повідомляти про оновлення заявок чи повернення книг. Безпека даних реалізована через JWT і шифрування AES-256, що відповідає сучасним стандартам кібербезпеки в бібліотечних системах [7].

Система враховує потреби трьох груп користувачів. Студенти можуть замовляти книги, перевіряти їхній статус, залишати відгуки та отримувати персоналізовані рекомендації за жанрами. Бібліотекарі керують видачею і поверненням книг, отримуючи сповіщення про резервування. Адміністратори контролюють заявки, редагують інформацію, аналізують статистику та переглядають логи. Унікальними є функції аналізу популярності книг, автоматичного уникнення конфліктів резервування та прогнозування навантажень, що вирізняє застосунок серед інших рішень [8].

Безпека даних продумана ретельно: шифрування AES-256, захист від XSS-атак і моніторинг аномальної активності, як-от масові заявки, забезпечують надійність [9]. Логування операцій відповідає стандарту ISO/IEC 27001, що дозволяє проводити аудит і захищає від кіберзагроз, які стають дедалі актуальнішими в процесі цифровізації бібліотек [7].

Інтерфейс локалізовано українською мовою з дотриманням літературних норм, що робить його зрозумілим і підтримує національну ідентичність [2]. Адаптивний дизайн забезпечує зручність на різних пристроях, що є критично важливим для закладів із різним технічним оснащенням, особливо в умовах цифрової трансформації [5].

Порівняно з комерційними системами, як Polaris (вартістю 725 – 1300 доларів на рік), «Бібліотека FCIT» є економічно вигідним [1]. Відкриті платформи, як Koha, потребують технічних знань і додаткових витрат, а також не завжди адаптовані до українського контексту [3]. Наш застосунок стійкий до перебоїв, підтримує офлайн-режим і пропонує функції, яких бракує конкурентам, зокрема аналіз затребуваності книг і захист від кіберзагроз [8].

Тестування показало високу продуктивність: при 200 користувачах час відгуку становить 120 – 220 мс, пропускна здатність – 220 запитів за секунду, помилки – до 0,5% [6]. За 8 годин із 100 користувачами середній час відгуку – 160 мс, помилки – 0,2%. При 300 користувачах час відгуку зростає до 450 мс, що вимагає оптимізації, наприклад, кластеризації MongoDB. Порівняно з Koha (300 – 500 мс при 100 користувачах), наш застосунок швидший [1].

У майбутньому планується додати сповіщення про прострочення, удосконалити рекомендації за допомогою машинного навчання та впровадити двофакторну автентифікацію [9]. Масштабування для інших закладів, підтримка нових мов і інтеграція з платформами дистанційного навчання посилять універсальність системи, що відповідає трендам цифровізації освіти [4].

«Бібліотека FCIT» є новаторським рішенням для українських бібліотек. Поєднуючи сучасні технології, надійний захист, локалізацію та унікальні функції, як-

от аналіз популярності книг і прогнозування навантажень, система перевершує аналоги за продуктивністю та адаптацією до місцевих умов. Це доступне рішення для бібліотек із обмеженими ресурсами, яке сприяє цифровій еволюції освіти.

Список використаних джерел

1. Сеньків М. В. Автоматизація бібліотечних процесів: Виклики та перспективи для українських вишів // Вісник Львівського університету. Серія: Книгознавство, бібліотекознавство та інформаційні технології. – 2023. – Вип. 18. – С. 45–52.
2. Ковальчук О. П. Локалізація програмного забезпечення для бібліотек: Культурний і технічний аспекти // Наукові записки Тернопільського національного педагогічного університету. Серія: Інформаційні технології. – 2022. – № 3. – С. 28–35.
3. Гриценко В. І. Цифрова трансформація бібліотек: Глобальні тенденції та локальні виклики // Бібліотечний форум: історія, теорія і практика. – 2024. – № 1. – С. 12–19.
4. Левченко Т. М. Роль бібліотек у цифровій трансформації освіти: Нові можливості автоматизації // Освітні горизонти. – 2021. – № 4. – С. 67–74.
5. Білан С. О. Адаптивні інтерфейси для бібліотечних систем: Технології та виклики // Інформаційні системи та мережі. – 2023. – Вип. 15. – С. 89–96.
6. Шевчук Р. В. Сучасні веб-технології в автоматизації бібліотечних процесів // Технічні науки та технології. – 2022. – № 2. – С. 101–108.
7. Мороз І. А. Кібербезпека бібліотечних інформаційних систем: Стандарти та практики // Кібербезпека: освіта, наука, техніка. – 2024. – № 1. – С. 33–40.
8. Остапчук Н. Г. Інноваційні функції бібліотечних систем: Аналітика та прогнозування // Науковий вісник Ужгородського університету. Серія: Інформатика. – 2023. – Вип. 9. – С. 54–61.
9. Кравець Л. В. Майбутнє бібліотечних систем: Машинне навчання та кібербезпека // Інформаційні технології в освіті. – 2025. – № 1. – С. 22–29.

Ключові слова: автоматизація бібліотечних процесів, веб-застосунок, цифрова трансформація, інформаційні технології, машинне навчання

Keywords: automation of library processes, web application, digital transformation, information technology, machine learning

РОЗРОБКА ВЕБСАЙТУ ДЛЯ ТУРИСТИЧНОГО АГЕНТСТВА

Дибчук Олексій

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сьогодні вебсайт став невід'ємною частиною успішного функціонування будь-якого туристичного бізнесу. Розробка автора для туристичного агентства представляє собою комплексне рішення, яке поєднує естетичний сучасний

дизайн з потужним функціоналом, створюючи ідеальний інструмент для взаємодії з клієнтами.

Аналізуючи сучасний ринок туристичних онлайн-сервісів, автором виявлений значний розрив між очікуваннями клієнтів та пропозицією більшості агентств [1]. Багато існуючих рішень страждають на низьку швидкодію, застарілий інтерфейс та обмежений функціонал. Дана розробка заповнює цю нішу, пропонуючи користувачам інтуїтивно зрозумілий та технологічно просунутий інструмент для пошуку та бронювання турів.

Технічна реалізація проєкту базується на сучасному підході до веброзробки [2]. Backend-частина побудована на Strapi CMS [3], що дозволяє спростити процес управління контентом та забезпечує гнучкість у роботі з даними. Використання Node.js [4] як серверної платформи забезпечує високу продуктивність системи та можливість легкого масштабування.

Frontend-частина реалізована за допомогою прогресивного фреймворку Nuxt.js [5], що дозволило створити швидкий та адаптивний інтерфейс [6]. Особливу увагу приділено оптимізації взаємодії між клієнтською та серверною частинами через використання мови запитів і маніпуляції даними GraphQL [7], що значно підвищує ефективність обміну даними.

Система пошуку турів вражає своєю гнучкістю, дозволяючи користувачам легко знаходити потрібні пропозиції за різними критеріями. Детальні сторінки країн містять не лише базову інформацію, а й цікаві факти, фотогалереї та перелік доступних турів, створюючи комплексне уявлення про напрямок подорожі.

Процес бронювання максимально спрощений завдяки зручній формі замовлення, яка інтегрована з системою автоматичних сповіщень. Це дозволяє як клієнтам отримувати оперативну інформацію про статус заявки, так і менеджерам агентства – швидко обробляти нові запити.

Використання сучасного технологічного стеку забезпечує стабільну роботу платформи навіть при високому навантаженні. Інфраструктурні рішення на базі Nginx [8] та Docker [9] дозволяють легко масштабувати систему, адаптуючи її до зростаючої кількості користувачів.

Інструменти розробки, такі як Visual Studio Code та Postman, значно прискорили процес створення та тестування рішення, забезпечуючи високу якість кінцевого продукту.

Для туристичного агентства запропоноване рішення означає значне підвищення ефективності роботи. Автоматизація рутинних процесів звільняє час менеджерів для роботи з клієнтами, а система аналітики дозволяє точніше вивчати попит та адаптувати пропозицію.

Клієнти отримують у своє розпорядження зручний інструмент, який дозволяє швидко знаходити потрібні тури, отримувати повну інформацію про напрямки та легко оформлювати замовлення. Інтуїтивний інтерфейс робить процес планування подорожі приємним і нескладним.

Подальший розвиток платформи передбачає кілька напрямків. Планується впровадження системи онлайн-оплати, що дозволить завершувати процес бронювання безпосередньо на сайті. Інтеграція з соціальними мережами покращить комунікацію з клієнтами та дозволить ефективніше просувати послуги.

Додатково, розглядається можливість створення мобільного додатку та впровадження AI-чатбота для надання базових консультацій. Також важливим напрямком є розширення мовної підтримки для роботи з міжнародними клієнтами.

Розроблений вебсайт представляє собою якісний крок у цифровій трансформації туристичного бізнесу. Він не лише відповідає сучасним вимогам до онлайн-сервісів, але й створює основу для подальшого розвитку цифрової екосистеми агентства.

Успішна реалізація проєкту доводить ефективність використання сучасних веб-технологій у сфері туристичних послуг. Майбутній розвиток платформи дозволить створити повноцінний цифровий сервіс, який покриватиме всі етапи взаємодії клієнта з туристичним агентством – від пошуку ідеї подорожі до повноцінного супроводу під час поїздки.

Список використаних джерел

1. Туристичний ринок України: сучасні тенденції та перспективи / І.П. Петренко, О.В. Сидоренко // Вісник Київського національного університету. - 2022. - №45. - С. 56-67.
2. Веб-розробка: сучасні підходи та технології / М.В. Коваленко. - К.: Видавничий дім "Освіта", 2021. - 324 с.
3. Офіційна документація Strapi CMS [Електронний ресурс]. - Режим доступу: https://docs.strapi.io/
4. Офіційний гайд Node.js [Електронний ресурс]. - Режим доступу: https://nodejs.org/en/docs/
5. Документація фреймворку Nuxt.js [Електронний ресурс]. - Режим доступу: https://nuxtjs.org/docs/
6. Особливості проектування інтерфейсів для туристичних сайтів / С.О. Іваненко // Комп'ютерні технології. - 2023. - №2(18). - С. 45-52.
7. Офіційна документація GraphQL [Електронний ресурс]. - Режим доступу: https://graphql.org/learn/
8. Офіційна документація Nginx [Електронний ресурс]. - Режим доступу: https://nginx.org/en/docs/
9. Docker [Електронний ресурс]. - Режим доступу: https://docs.docker.com/

Ключові слова: веб-сайт, туристичне агентство, Strapi CMS, Node.js, Nuxt.js.

Keywords: website, travel agency, Strapi CMS, Node.js, Nuxt.js.

Науковий керівник: доцент Манаков С.

ВИКОРИСТАННЯ ХАМРР ДЛЯ РОЗРОБКИ ВЕБЗАСТОСУНКУ БРОНЮВАННЯ В ГОТЕЛЬНОМУ БІЗНЕСІ

Шевернов Олександр

студент 4 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Інформаційні технології відіграють важливу роль у трансформації готельного бізнесу, зокрема через впровадження вебзастосунків для бронювання номерів, які забезпечують швидкий доступ до послуг та оптимізують управління ресурсами. Такі системи потребують надійного серверного середовища, яке може поєднати вебзастосунок, базу даних і мову програмування в єдиному пакеті.

XAMPP, як кросплатформне рішення, відповідає цим вимогам, пропонуючи розробникам інтегровану платформу для створення та тестування вебзастосунків. Цей інструмент став популярним завдяки своїй здатності підтримувати різноманітні операційні системи (Windows, macOS, Linux) і забезпечувати гнучкість у налаштуванні, що робить його незамінним для проєктів із бронювання, де важлива швидкість розгортання та адаптивність [1].

XAMPP є відкритим пакетом програмного забезпечення, який об’єднує ключові компоненти для веброзробки під абревіатурою "X (cross-platform), Apache, MySQL, PHP, Perl". Його унікальність полягає в тому, що він дозволяє розгорнути повноцінне серверне середовище за лічені хвилини, усуваючи потребу в складній ручній конфігурації. Наприклад, для активації вебзастосунку достатньо запустити XAMPP Control Panel і включити потрібні модулі, такі як Apache чи MySQL. Така простота підкріплена підтримкою сучасних протоколів, включно з SSL для шифрування даних, що критично важливо для захисту інформації про бронювання. Окрім того, XAMPP підтримує модульність, дозволяючи інтегрувати додаткові бібліотеки, наприклад, для роботи з jQuery-акордеонами чи асинхронними запитами AJAX, що розширює можливості вебінтерфейсів [2].

Серед компонентів XAMPP центральне місце посідає Apache – високопродуктивний вебсервер, який обробляє запити та відображає сторінки, створені з HTML, CSS і JavaScript. Apache підтримує модульну архітектуру, що дозволяє налаштувати обробку динамічного контенту через PHP або додавати плагіни для оптимізації продуктивності, наприклад, для кешування. MySQL виступає основою для зберігання даних, пропонуючи реляційну модель із підтримкою складних запитів SQL, які використовуються для управління таблицями, такими як users, bookings, availability і subscriptions. Ця база даних вирізняється швидкістю роботи з великими обсягами даних, що є актуальним для систем бронювання з високим навантаженням. phpMyAdmin забезпечує інтерактивне управління MySQL через вебінтерфейс, дозволяючи створювати індекси, налаштовувати тригери чи імпортувати дані з CSV-файлів. PHP, у свою чергу, слугує мовою

серверної логіки, підтримуючи об'єктно-орієнтований стиль і вбудовані функції для роботи з формами, сесіями та базою даних [2].

Кожен компонент XAMPP має специфічні переваги для веброзробки. Apache вирізняється підтримкою віртуальних хостів, що дозволяє одночасно тестувати кілька проєктів на одному сервері, а також інтеграцією з модулями, такими як mod_rewrite для створення дружніх URL-адрес. MySQL пропонує розширені можливості, наприклад, підтримку транзакцій і реплікації, що забезпечує безперервність роботи навіть при збоях. phpMyAdmin виділяється зручним графічним інтерфейсом для виконання складних запитів, таких як об'єднання таблиць JOIN, і підтримки експорту даних у різні формати. PHP, завдяки вбудованим бібліотекам (наприклад, для роботи з JSON чи XML), дозволяє створювати гнучкі API для інтеграції з зовнішніми сервісами, такими як платіжні системи чи системи резервування. Порівняно з альтернативами, як-от WAMP (виключно для Windows) чи LAMP (вимагає ручної інсталяції), XAMPP виграє завдяки кросплатформності та готовності до використання "з коробки"[3].

Застосування XAMPP у розробці вебзастосунків для бронювання готельних номерів відкриває широкі можливості для тестування та оптимізації. Локальний сервер Apache дозволяє моделювати реальні сценарії роботи, наприклад, обробку одночасних запитів від десятків користувачів, а також налаштування файлів конфігурації, таких як httpd.conf, для підвищення безпеки. MySQL і phpMyAdmin дають змогу створювати складні схеми баз даних із тригерами для автоматичного оновлення даних про доступність номерів. PHP підтримує створення скриптів, таких як _init.php і _upd.php, для ініціалізації таблиць і їхнього оновлення, а також інтеграцію з jQuery для інтерактивних елементів, як-от анімовані панелі бронювань. Ця комбінація дозволяє тестувати сценарії, такі як масове бронювання чи скасування, і виявляти вузькі місця в продуктивності до розгортання на реальному хостингу [4].

XAMPP також забезпечує безпеку та гнучкість у локальному середовищі. Наприклад, підтримка SSL у Apache дозволяє налаштувати шифрування для захисту даних про користувачів, а функція логування дає змогу відстежувати помилки в запитах. MySQL підтримує ролі користувачів і права доступу, що дозволяє сегментувати дані між адміністраторами та гостями. phpMyAdmin пропонує інструменти для резервного копіювання бази даних, що є важливим для запобігання втраті інформації. PHP, із підтримкою сесій і фільтрації вхідних даних, допомагає захистити від SQL-ін'єкцій і XSS-атак. У порівнянні з ручною установкою серверів, XAMPP зменшує ризик помилок конфігурації та прискорює процес налаштування, що є особливо цінним для проєктів із динамічними потребами, таких як бронювання в реальному часі [4].

Перспективи використання XAMPP включають розширення функціоналу вебзастосунків. Наприклад, інтеграція з хмарними сервісами (наприклад, Amazon RDS) для резервного копіювання MySQL чи додавання підтримки WebSocket у Apache для реального оновлення статусу номерів. PHP може бути

розширено для роботи з API геолокації, щоб пропонувати користувачам готелі поблизу їхньої локації. phpMyAdmin дозволяє експериментувати з індексацією таблиць для підвищення швидкості запитів, що є актуальним для систем із тисячами бронювань. Ці можливості роблять XAMPP потужним інструментом не лише для розробки, але й для подальшого вдосконалення вебзастосунків у сфері готельного бізнесу [5].

Список використаних джерел

1. Інформаційний розділ про XAMPP. URL: https://surl.li/benqso
2. Опис функціоналу Apache HTTP Server. URL: https://surl.lu/stkkwm
3. Інформаційні матеріали про MySQL. URL: https://dev.mysql.com/doc/
4. Сервіс phpMyAdmin: технічна інформація та керівництво. URL: https://docs.phpmyadmin.net/
5. Опис можливостей та синтаксису PHP. URL: https://surli.cc/wscivz

Ключові слова: XAMPP, вебзастосунок, Apache, MySQL, PHP, phpMyAdmin, бронювання

Keywords: XAMPP, web application, Apache, MySQL, PHP, phpMyAdmin, booking

Науковий керівник: доцент Лобода Ю.

ОСОБЛИВОСТІ ВИКЛАДАННЯ ДИСЦИПЛІНИ «ТЕХНОЛОГІЇ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ» МАЙБУТНІМ ФАХІВЦЯМ ІТ-СФЕРИ

Чепурна Олена

доцент кафедри кібербезпеки
Національного університету «Одеська юридична академія»,
кандидат фізико-математичних наук, доцент

Черевко Євген

доцент кафедри кібербезпеки
Національного університету «Одеська юридична академія»,
кандидат фізико-математичних наук, доцент

У контексті глобальної цифрової трансформації, де освіта відіграє ключову роль у підготовці майбутніх конкурентоспроможніх фахівців, дисципліна «Технології підтримки прийняття рішень» (Decision Support Technologies, DST) займає центральне місце в формуванні компетентностей майбутніх ІТ-професіоналів. Цей курс виходить за межі традиційного викладання, інтегруючи передові педагогічні підходи, міждисциплінарні методи та практико-орієнтовані технології. Поєднуючи аналіз даних, моделювання складних систем і сучасні освітні стратегії, такі як адаптивне навчання та інтерактивні формати, дисципліна готує

спеціалістів, здатних розробляти інноваційні рішення для динамічного світу інформаційних технологій.

Викладання дисципліни «Технології підтримки прийняття рішень» для майбутніх ІТ-фахівців має свої особливості, оскільки воно вимагає поєднання теоретичних знань, практичних навичок і міждисциплінарного підходу. Дисципліна формує у студентів комплексне розуміння процесів аналізу даних, моделювання та прийняття рішень у реальних умовах [2]. Основні цілі включають розуміння теоретичних основ, таких як аналітична ієрархія (AHP), теорія ігор, методи багатокритеріального аналізу, машинне навчання та штучний інтелект, а також формування практичних навичок використання програмного забезпечення, наприклад, MATLAB, R, Python, Power BI [3]. Крім того, дисципліна розвиває критичне мислення, вміння оцінювати альтернативи, враховувати невизначеність і ризики. У контексті інформаційного суспільства фахівці, які володіють DST, можуть працювати в бізнес-аналітиці, кібербезпеці, розробці програмного забезпечення та управлінні проєктами [4].

Викладання дисципліни має низку особливостей. По-перше, це міждисциплінарний підхід, що інтегрує знання з математики, статистики, інформатики, економіки та менеджменту [5]. Викладачам необхідно адаптувати складні концепції, такі як байєсівський аналіз чи нейронні мережі, до рівня підготовки студентів. Для бакалаврів акцент робиться на базові методи, як-от аналіз чутливості чи дерева рішень, тоді як магістри вивчають глибоке навчання та прогнозне моделювання [6]. По-друге, практична спрямованість є ключовою. Студенти працюють із кейс-методами, що моделюють реальні бізнес-ситуації, наприклад, оптимізацію логістики чи прогнозування попиту, а також виконують лабораторні роботи з використанням Python (бібліотеки Pandas, Scikit-learn), Tableau чи спеціалізованих DSS-програм [7].

Проєктна діяльність, як-от розробка систем підтримки прийняття рішень для аналізу ризиків у кібербезпеці, також є важливою складовою [8]. По-третє, швидкий розвиток технологій, таких як штучний інтелект, блокчейн чи обробка великих даних, вимагає постійного оновлення навчальних матеріалів [9].

Викладачі мають інтегрувати хмарні платформи (AWS, Azure) та ознайомлювати студентів із новітніми методами, наприклад, AutoML чи генеративним ШІ. Нарешті, дисципліна сприяє розвитку soft skills, таких як комунікація, командна робота та презентація результатів, що є важливим для пояснення складних технічних концепцій стейкхолдерам [10].

Організація навчального процесу супроводжується викликами. Різний рівень підготовки студентів ускладнює викладання, оскільки потрібен баланс між базовими та просунутими темами [11]. Модульний підхід із диференційованими завданнями може вирішити цю проблему. Обмеженість ресурсів, таких як сучасне програмне забезпечення чи потужні комп'ютери, знижує якість підготовки [12]. Використання безкоштовних інструментів, як Google Colab чи Jupyter Notebook, та співпраця з ІТ-компаніями допомагають подолати цей бар'єр.

Мотивація студентів є ще одним викликом, адже дисципліна може здаватися складною через теоретичну складову [13]. Гейміфікація, гостьові лекції від IT-фахівців і демонстрація практичної цінності знань сприяють підвищенню зацікавленості. Перспективи розвитку дисципліни пов'язані з інтеграцією штучного інтелекту та машинного навчання, що відкриває можливості для автоматизації прийняття рішень [14]. Персоналізація навчання через адаптивні платформи, міжнародна співпраця в рамках проєктів, таких як Erasmus+, та інтеграція сертифікаційних програм від Microsoft, AWS чи Google підвищують конкурентоспроможність випускників [15]. Дисципліна "Технології підтримки прийняття рішень" є невід'ємною частиною підготовки IT-фахівців, а її розвиток сприятиме формуванню фахівців, здатних вирішувати складні завдання інформаційного суспільства.

Список використаних джерел

1. Davenport T. H. Competing on Analytics: The New Science of Winning / T. H. Davenport, J. G. Harris. - Boston : Harvard Business Review Press, 2017. - 320 с.
2. Turban E. Decision Support and Business Intelligence Systems / E. Turban, R. Sharda, D. Delen. - New York : Pearson, 2019. - 672 с.
3. Power D. J. Decision Support Systems: Concepts and Resources for Managers / D. J. Power. - Westport : Quorum Books, 2016. - 272 с.
4. Laudon K. C. Management Information Systems: Managing the Digital Firm / K. C. Laudon, J. P. Laudon. - New York : Pearson, 2020. - 704 с.
5. Keeney R. L. Decisions with Multiple Objectives: Preferences and Value Tradeoffs / R. L. Keeney, H. Raiffa. - Cambridge : Cambridge University Press, 1993. - 569 с.
6. Russell S. Artificial Intelligence: A Modern Approach / S. Russell, P. Norvig. - New York : Pearson, 2020. - 1152 с.
7. Provost F. Data Science for Business / F. Provost, T. Fawcett. - Sebastopol : O'Reilly Media, 2013. - 414 с.
8. Winston W. L. Operations Research: Applications and Algorithms / W. L. Winston. - Boston : Cengage Learning, 2014. - 1440 с.
9. McAfee A. Machine, Platform, Crowd: Harnessing Our Digital Future / A. McAfee, E. Brynjolfsson. - New York : W.W. Norton & Company, 2017. - 416 с.
10. Goleman D. Emotional Intelligence: Why It Can Matter More Than IQ / D. Goleman. - New York : Bantam Books, 2019. - 368 с.
11. Felder R. M. Teaching and Learning STEM: A Practical Guide / R. M. Felder, R. Brent. - San Francisco : Jossey-Bass, 2016. - 336 с.
12. Bates T. Teaching in a Digital Age: Guidelines for Designing Teaching and Learning / T. Bates. - Vancouver : Tony Bates Associates Ltd, 2019. - 512 с.
13. Deci E. L. Self-Determination Theory: Basic Psychological Needs in Motivation, Development, and Wellness / E. L. Deci, R. M. Ryan. - New York : Guilford Press, 2017. - 756 с.
14. Goodfellow I. Deep Learning / I. Goodfellow, Y. Bengio, A. Courville. - Cambridge : MIT Press, 2016. - 800 с.

15. Reimagining Our Futures Together: A New Social Contract for Education / UNESCO. - Paris : UNESCO Publishing, 2021. - 185 c.

Ключові слова: технології підтримки прийняття рішень, IT-сфера, інформаційне суспільство, міждисциплінарний підхід, практична спрямованість, штучний інтелект, машинне навчання, soft skills, персоналізація навчання, гейміфікація.

Keywords: decision support technologies, IT sphere, information society, interdisciplinary approach, practical orientation, artificial intelligence, machine learning, soft skills, personalization of learning, gamification.

ПРОБЛЕМА ПІДТРИМКИ ТА ОНОВЛЕННЯ ОПЕРАЦІЙНИХ СИСТЕМ НА МОБІЛЬНИХ ТЕЛЕФОНАХ

Шорніков Назар

студент 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Операційні системи є базовою програмною частиною багатьох цифрових пристроїв: комп'ютерів, смартфонів, телевізорів і т.д. Для забезпечення їх новим функціоналом і безпеки даних користувачів дуже важливо оновлювати операційну систему на всіх пристроях, адже це не тільки.

Зараз виробники смартфонів надають дуже малий термін підтримки своїх пристроїв і цим рішенням вимагають своїх користувачів купувати більш нові мобільні телефони та створюють деякі проблеми для розробників, а також ставлять під загрозу безпеку даних користувачів. Через припинення оновлень пристрої стають вразливими до вірусів, шкідливих скриптів та застосунків, знижується їх продуктивність та становиться неможливим запускати сучасні застосунки, цим усім зменшується життєвий цикл смартфонів. Сучасні смартфони не дуже відрізняються власними характеристиками, тому їх можна оновлювати набагато довше ніж зараз це можливо.

Компанія Apple розробила операційну систему iOS, яка є більш закритою і тому має стабільні оновлення. Саме тому, вона є швидкою і зручною у користуванні та безпечнішою. Термін підтримки операційної системи iOS становить від 5 до 6 років, що є найбільшим терміном ніж у інших виробників. Кожен смартфон компанії Apple протягом 5-6 років має отримати щорічне оновлення програмного забезпечення та інші оновлення, а також після закінчення терміну оновлень смартфон буде отримувати оновлення патчів безпеки ще декілька років. Термін підтримки пристроїв Apple є найкращим серед мобільних пристроїв [1].

З відкритою операційною системою Android все набагато гірше. Компанії, що виробляють смартфони, намагаються більше заробити грошей на користувачах тому їх пристрої мають відносно малі строки оновлень операційної системи. Кожен виробник робить «власну» операційну систему на базі Android,

тобто адаптує «чисту» операційну систему під себе, додаючи свій унікальний дизайн та нові функції.

Наприклад смартфони Samsung згідно з нової політики оновлень будуть отримувати до 5 років оновлень програмного забезпечення, але це стосується не всього модельного ряду. Більш бюджетні смартфони мають отримати 2-3 оновлення Android та 2-3 роки оновлення патчів безпеки. Бюджетні телефони мають дуже короткий термін використання, адже після того як перестануть приходити взагалі оновлення телефон буде вразливий до шкідливого програмного забезпечення, скриптів тощо [2]. Смартфони компанії Google мають термін оновлень 5 років. За цей період смартфон отримує до 5 оновлень системи

Android [3].

Найгірший термін оновлень мають смартфони компанії Xiaomi. В середньому термін сягає до 4 років. Деякі версії смартфонів мають прошивку прив'язану до певного оператора зв'язку, вони взагалі майже не оновлюються. Бюджетні смартфони оновлюються 2-3 роки, таким чином виробник штучно скорочує життєвий цикл своїх пристроїв і цим примушує користувачів купувати нові телефони, хоча апаратне забезпечення смартфонів цілком придатне до використання [4].

Результатом короткого циклу оновлень смартфонів є зростання рівня кіберзлочинності, що обумовлена відсутністю оновлень для їх захисту та покращення роботи поточних функцій. Особливо небезпечно використання сматрфонів, які не оновлюються, для користувачів, які використовують застосунки онлайн банків, здійснюють оплату за допомогою пристрою чи зберігають якісь важливі документи чи інші дані.

Багато людей з різним фінансовим становищем користуються смартфонами і деякі з них не можуть дозволити собі купувати майже кожен рік новий мобільний пристрій з різних фінансових причин. Найкращим рішенням цієї проблеми було б розробити таку ж «власну» універсальну операційну систему. Це дозволило б зменшити залежність користувачів від виробників і повністю контролювати всі оновлення, набагато збільшити термін підтримки оновлень для багатьох смартфонів та прибрати залежність прошивки смартфону від певного оператора зв'язку. Власна операційна система дозволила б впроваджувати регулярні оновлення, додання нового функціоналу, який може знадобитись користувачам, швидко виправляти помилки, зробити керування оперативною пам'яттю набагато кращим ніж воно зараз є на пристроях з Android. Таке рішення влаштувало б більшість користувачів мобільних телефонів.

Регулярні оновлення у власній операційній системі дозволили б швидко виправляти помилки та запобігати вразливостям операційної системи, забезпечити стабільну роботу смартфонів.

Для користувачів така операційна система була б пріоритетом через забезпечення захищеності їх даних. Вони б не мусили купляти майже кожен рік новий смартфон та турбуватися що їх пристрій втратить функціональність чи не зможе

використовувати сучасні, чи нові застосунки або ж буде вразливим до шкідливого програмного забезпечення.

Розробка такої операційної системи є дуже складним завданням та потребує багато ресурсів, але це найкращий з варіантів розв'язання цієї проблеми збереження коштів користувачів і забезпечення безпеки та конфіденційності їх даних.

Проблема оновлення та підтримки операційних систем смартфонів є однією з найактуальніших через зростання на ринку кількості нових моделей щороку. Багато користувачів лишаються елементарного захисту власних даних і тим самим стають жертвами зловмисників. Ця проблема має бути вирішена шляхом розробки універсальної операційної системи сучасними засобами розробки та покращити ситуацію з підтримкою багатьох моделей смартфонів.

Список використаних джерел

1. До якого року буде оновлюватися ваш iPhone? URL: https://icoola.ua/blog/do-yakoho-roku-bude-onovlyuvatysya-iphone. (Дата звернення: 2025-04-27).
2. До якого року буде оновлюватись Samsung. URL: https://icoola.ua/blog/do-yakoho-roku-bude-onovlyuvatys-samsung. (Дата звернення: 2025-04-27).
3. Google розширює підтримку Pixel 6, Pixel 7 і Pixel Fold до 5 років. URL: https://pixelmania.com.ua/news/google_news/google-pixel-6-7-fold-extended-os-support. (дата звернення: 2025-04-27).
4. Скільки служать смартфони відомих брендів. URL: https://internetua.com/skilki-slujat-smartfoni-vidomih-brendiv. (Дата звернення: 2025-04-27).

Ключові слова: операційна система, користувачі, оновлення, термін підтримки, мобільні телефони

Keywords: operating system, users, updates, support period, mobile phones

Науковий керівник: доцент Задерейко О.

ДОСТАВКА ТА УПРАВЛІННЯ СТОРОННІМИ БІБЛІОТЕКАМИ ТА МОДУЛЯМИ У МОВАХ ПРОГРАМУВАННЯ ВИСОКОГО ТА УЛЬТРАВИСОКОГО РІВНЯ

Бойко Віктор

доцент кафедри кібербезпеки
Національного університету «Одеська юридична академія»
кандидат технічних наук, доцент

Сучасні парадигми програмування характеризуються розвитком мов програмування високого рівня та ультрависокого рівня. Це зазвичай включає такі мови, як Ruby, Perl, PHP, Haskell, Python, Go, Rust, Node.js тощо. Популярність цих мов пов'язана з простотою навчання та наявністю у більшості з них відкритих

ліцензій. Це призвело до того, що для цих мов програмування вже накопичено велику кількість програмного забезпечення, і цей обсяг продовжує зростати. Така ситуація породжує дві проблеми: питання спадщини (legacy code - не плутати з успадкуванням в ООП) та питанням управління великими обсягами коду.

Проблема legacy включає взаємодію програм, написаних для різних версій програмного забезпечення - програмне забезпеченная, побудоване для однієї версії мови програмування (або бази даних), може перестати працювати на інших версіях. Більш того, через взаємну залежність (одна програма може використовувати іншу, яка, в свою чергу, може використовувати третю тощо) проблеми сумісності можуть генерувати "каскадні ефекти", коли оновлення одного компонента системи призводить до відмови всієї системи в цілому. У той же час, рішення проблеми не зводиться до очевидної та тривіальної вимоги "тримати всі пакети в системі максимально оновленними" оскільки окремі частини програмного забезпечення оновлюються з різними швидкостями. І "повне оновлення" системи може відключити відстаючі частини коду, а "компромісне рішення" у свою чергу може викликати втручання у роботу тих компонентів, які потребують нових оновлених версій коду і, крім того, уповільнює використання компонентів коду, в яких виправлено помилки та усунуто виявлені вразливості.

Проблема накопичення великих обсягів коду тісно пов'язана з "проблемою спадщини" - оскільки код створюється майже безперервно, для сучасних систем обсяг використаного коду вже дуже великий. Це призводить до труднощів у створенні нового та підтримці існуючого коду. Якщо раніше можна було отримати всі необхідні інструменти на одному CD-ROM, то в 2018 році обсяг основного сховища бібліотек мови Python становив близько 2 терабайтів [1].

У мовах програмування попереднього покоління була зроблена спроба вирішити обидві ці проблеми за допомогою використання статичних або динамічних підключених модулів або бібліотек. Статичні модулі додавались до коду, перед його компіляцією за допомогою так званного лінкеру (linker). Динамічні модулі були набором об'єктних файлів, до яких задавались посилання перед компіляцією, але вони не запускались до початку праці відкомпільованної програми. Іншими словами, ці об'єкти були динамічно пов'язані з виконуваними файлами - звідки походження назви.

Підхід ООП який набув широкого поширення, та у якому програмування здійснюється за допомогою об'єктів, яки створються з класів, об'єднаних широкими ієрархіями успадкування та у яких об'єднано атрибути та методи (дані та функції їх обробки), зокрема, був розроблен для вирішення проблеми обсягу абстракцією. У такому підході програміст працює в основному з об'єктами високого рівня, не занурюючись у деталі роботи з кодом. Незважаючи на очевидні недоліки [2] та критику з боку інших підходів (функціональне програмування), підхід ООП все ще актуальний і це на нашу думку значною мірою пов'язано з тим, що він дозволяє ефективно вирішити проблему зростання обсягу коду, та проблему legacy.

Однак для сімейства мов програмування високого рівня та ультрависокого рівня, перелічених вище, проблема додатково ускладнюється тим, що в парадігмі цих мов розмивається різниця між компіляцією та інтерпретацією коду. Часто програмне забезпечення працює у віртуальній машині на кшталт

workflow інтерпретуємих мов програмування. У той же час, якщо розглядати процес запуску python-коду, то там після першого запуску виконується псевдокомпіляція коду в байт-код, що суттєво прискорює процес роботи. Таким чином, поділ на статичні та динамічні бібліотеки в контексті нового покоління мов програмування все більше і більше розмивається.

Інша проблема - широке використання модулів, складених за допомогою інших мов програмування. Це найчастіше викроистовується, для підвищення продуктивності. Найбільш розповсюдженним прикладом є бібліотека мови Python numpy, яка широко використовує зкомпільовані модулі на мове C для збільшення швидкості роботи з матричними обчисленнями[3], [4]. Це ще більше ускладнює управління поновленням та взаємним поєднанням бібліотек.

Враховуючи перелічені вище проблеми, з часом у більшості мов програмування, хоча термін у «мовних спільнотах» (community) тут розвинувся більш точним та доцільним, склалалась наступна практика. По-перше, для зберігання сторонніх бібліотек утворюється стандарт "пакету дистрибуції", який містить не лише саму бібліотеку як таку, але й метадані про неї (версія, вимоги до інших версій бібліотек тощо), а також сторонні ресурси (наприклад, двійкові файли, іконки тощо), та скріпти встановлення бібліотеки на існуючій системі та середовища. По-друге, на основі створеного формату створюється програма управління пакетами - окрема програма або модуль, вбудований в мову - для управління бібліотеками, які, виходячи з метаінформації в пакетах, вибирає конфігурацію та місце встановлення необхідних файлів. По-третє, окремо створюється мережеве сховище для зберігання пакетованих сторонніх бібліотек, що дозволяє, використовуючи програму управління пакетами, встановлювати оновлення та-або вирішувати питання залежностей сторонніх модулів та бібліотек у цій системі. Використання метаінформації в пакетах дозволяє гнучко підходити до проблеми контролю версій пакетів, або точно вказувати необхідні версії, або утворювати цілі многоетапні залежності, коли встановлення одного пакету тягне за собою встановлення всіх необхідних для нього пакетів.

Подібні схеми роботи використовуються в операційних системах. Зокрема, такі "фундаментальні" дистрибутиви, як Redhat, Debian та Arch Linux, розпочалися з введення та створення форматів розподілу бінарних файлів: RPM для Redhat, Deb для Debian. Arch Linux використовує звичайний формат тарболу (архів tar), однак структура всередині жорстко встановлюється і регулюється правилами роботи з пакетами. Паралельно відбулася створення програми управління пакетами (RMP - Red hat Package Manager, dpkg в Debian, Pacman in Arch) та централізованого репозіторію програмного забезпечення.

Можна очікувати, що практики, розроблені в управлінні програмними пакетами (наявність віртуальних "порожніх" пакетів, паралельне оновлення залежностей) буде введено в програмування, оскільки розробка систем розподілу пакетів відповідає приблизно однаковим послідовностям та однаковому workflow.

Окреме питання - це ізоляція середовищ розробки та програмних засобів, які можуть використовуватись в рамках одного проекту (та однієї операційної системи) с одночасним виконанням різних наборів бібліотек та різних ієрархій коду. Один із наступних звітів буде присвячений цій темі.

Список використаних джерел

1. How large is a full pypi mirror? · Issue #50 · pypa/bandersnatch · GitHub [Електронний ресурс]. – Режим доступу : https://github.com/pypa/bandersnatch/issues/50 (дата звернення: 2025-05-19). – Назва з екрана.
2. The Law of Leaky Abstractions – Joel on Software [Електронний ресурс]. – Режим доступу : https://www.joelonsoftware.com/2002/11/11/the-law-of-leaky-abstractions/ (дата звернення: 2025-05-19). – Назва з екрана.
3. Бойко В.Д. Бібліотека numpy – основа інструментального стеку наукових розрахунків scipy // Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів : матеріали Міжнар. наук.-практ. конф. (Одеса, 26 квіт. 2024 р.) / ред. Ківалов С.В. Одеса : Фенікс, 2024. Р. 888–891.
4. Monat R., Ouadjaout A., Miné A. A multilanguage static analysis of python programs with native C extensions //International Static Analysis Symposium. – Cham : Springer International Publishing, 2021. – С. 323-345.

Ключові слова: Ruby, Perl, PHP, Haskell, Python, Go, Rust, Node.js, OOP, pip, rpm, deb, Debian, RedHat, Arch, pacman, dpkg, парадигма програмування, пакетна дистрибуція, дистрибутиви, workflow, прикладне програмування, інфраструктура програмування

Keywords: Ruby, Perl, PHP, Haskell, Python, Go, Rust, Node.js, OOP, pip, rpm, deb, Debian, RedHat, Arch, pacman, dpkg, programming paradigm, batch distribution, distributives, workflow, applied programming, programming infrastructure

КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ ВИПАДКОВИХ ПРОЦЕСІВ

Щербина Юрій

доцент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»
кандидат технічних наук, доцент

Створення моделей природніх процесів є однією з найважливіших проблем сучасної науки. Моделювання дає розуміння суті явищ, що відбуваються у довколишньому природному середовищі і дозволяє передбачати розвиток таких процесів у часі. Раніше моделювання процесів і поведінки складних систем розглядалось як другорядний етап проектування, але, сьогодні, воно виконується

здебільшого за допомогою комп'ютерної техніки, можливості якої піднімають значимість моделювання на новий, більш значний рівень.

Перш ніж розпочати створення комп'ютерної моделі складного фізичного процесу, виконують його декомпозицію на окремі елементарні підпроцеси. Якщо стохастичний процес, модель якого має бути побудована, розкладається на відомі елементарні закони розподілення ймовірностей, кожен з яких описується своєю функцією розподілення ймовірностей $F(x)$, використовують метод зворотної функції [1]. Згідно з цим методом, якщо джерелом випадкових величин стохастичного процесу, є генератор рівномірно розподілених на інтервалі [0,1] чисел з розподіленням $F(x)$, аргумент такої функції можна визначити через відповідну зворотну функцію $F^{-1}(x)$ (рисунок 1). Це положення дозволяє формувати програмним методом будь-які стандартні потоки випадкових чисел, якщо у наявності є їх формальне математичне визначення та джерело рівномірно розподілених псевдовипадкових чисел. Максимальне наближення побудованої моделі до реального стохастичного процесу буде тим більше, чим ближче обране первинне джерело випадковості наближається до рівномірно розподіленого процесу.

Використання комп'ютерного моделювання з самого початку було пов'язане з пошуком хороших джерел рівномірно розподілених чисел на інтервалі [0,1].

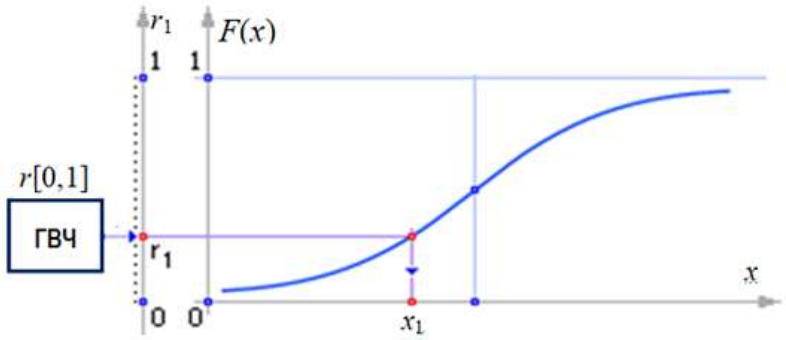

Рисунок 1. Моделювання випадкового процесу методом зворотних функцій

Існує два типи джерел випадковості: фізичні джерела та програмні рекурентні генератори. Фізичні джерела випадковості, хоча і дають реальний випадковий процес, але для забезпечення їх рівномірності і доводиться використовувати додаткове їх постоброблення. Крім того, їх неможливо повторно відновити – можна отримати лише нову їх реалізацію. Що ж стосується програмних генераторів, то вони легко забезпечують повторення копії сформованого процесу, але такий процес є псевдовипадковим – він буде циклічно повторюватись. Зазвичай, переваги, все ж таки, віддаються програмним генераторам, оскільки хороші джерела реальних випадкових процесів є зовнішніми по відношенню до комп'ютерної системи, складними і дорогими приладами.

Побудувати програмний генератор випадкових чисел (ГВЧ), який би задовольняв високим вимогам до рівномірності вкрай важко. Перші такі спроби

було зроблено фон Нейманом. Запропонований ним генератор був, по суті, способом постоброблення справжнього випадкового процесу, який певною мірою вирівнював розподілення вихідної числової послідовності [2]. Пізніше було запропоновано ще декілька способів формування програмного рекурентного числового потоку, але всі вони мали доволі малий період повторення. Серед них слід, у першу чергу, виділити метод Фідоначчі з запізненням та лінійний конгруентний методи [3]. І хоча обидва вони не проходять статистичне випробування за допомогою стандартних тестових пакетів, лінійний конгруентний метод до цих пір залишається основним джерелом випадкових чисел у більшості середовищ програмування.

Зрозуміло, що основною проблемою комп'ютерного моделювання залишається створення програмного генератора псевдовипадкових чисел, рівномірність розподілення яких була б достатньо високою і період повторення якої також був би великим. Останню проблему вирішили у 1997 році японські математики Макото Мацумото і Такудзи Нисимура. Їм вдалось побудувати генератор Мерсена (Mersenne Twiste – MT) на основі виткового регистру зсуву з узагальненою віддачею (twisted generalised feedback shift register – TGFSR) [4]. Цей генератор створює послідовність, довжина якої уявляє собою астрономічну величину $4{,}3 \cdot 10^{6001}$ біт. Але, що стосується рівномірності розподілення ймовірності чисел на його виході, то випробування показують, що, насправді, вона вкрай низька, і такий генератор мало придатний для моделювання стохастичних процесів, які можна описати як суперпозицію декількох стандартних розподілень.

Проблема забезпечення достатньої рівномірності розподілення вихідного потоку на виході програмного генератору ПВЧ теж була вирішена інженерами, що працюють у сфері криптографії. Їм вдалось побудувати генератори, що проходять випробування всіма спеціалізованими тестовими пакетами, але вони вкрай складні і їх програмна реалізація передбачає використання значних об'ємів пам'яті і процесорного часу. В задачах криптографічного захисту це може бути виправдано, але для моделювання це не зручно. Таким чином, на даний момент, пошук економічних алгоритмів, що здатні генерувати придатні для моделювання рівномірно розподілені випадкові числа залишається до кінця невирішеною задачею.

Список використаних джерел

1. Ross, S. 1981. A First Course in Probability. 8th Edition. : Prentice Hall, 2009. – 552 p. – ISBN 978-0-13-603313-4. http://julio.staff.ipb.ac.id/files/2015/02/Ross_8th_ed_English.pdf
2. Christophe, D., & Diethelm, W. A note on random number generation. URL : http://cran.r project.org/web/packages/ randtoolbox/vignettes/fullpres.pdf.
3. Knuth, D. E. The Art of Computer Programming. Volume 2. Seminumerical Algorithms. 3rd edition / D. E. Knuth. – Boston, Mass, USA : Addison-Wesley, Longman Publishing, 1997. – 762 p.

4. Matsumoto, M., Nishimura, T., Saito, M. and Hagita, M. Cryptographic Mersenne Twister and Fubuki stream/block cipherю. URL : https://eprint.iacr.org/ 2005/165.pdf.

Ключові слова: Псевдовипадкова послідовність, комп'ютерне моделювання, розподілення ймовірностей випадкових чисел

Key words: Pseudorandom sequence, computer modeling, probability distribution of random numbers

РОЗРОБКА КОМПОНЕНТУ ДЛЯ РЕФАКТОРИНГУ УМОВНИХ ВИРАЗІВ

Чикунов Павло

доцент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»
кандидат технічних наук, доцент

Щербина Ігор

студент 4-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Умовні конструкції, незважаючи на їхню простоту, є критично важливими для логіки програм і водночас становлять джерело потенційної надмірної складності та дублювання коду. Зважаючи на суттєвий вплив умовних операторів на читабельність, супровід та гнучкість програмного коду, виникає потреба в системному підході до їх оптимізації. Одним із таких підходів є рефакторинг – процес покращення внутрішньої структури коду без зміни його зовнішньої поведінки [1, 2]. У контексті умовних виразів рефакторинг дозволяє усунути надмірну складність, зменшити дублювання, підвищити ясність та забезпечити відповідність принципам чистого коду [3].

Метою виконання дослідження є розробка, проєктування та тестування програмного компоненту для рефакторингу умовних виразів в текстах програм на мові C#. Для досягнення мети дослідження виконано комплексний аналіз предметної області, інструментів та технологій, необхідних для реалізації рефакторингу умовних операторів у середовищі Visual Studio.

Для досягнення мети дослідження необхідно вирішити такі завдання:

1. виконати аналіз прийомів рефакторингу умовних виразів;

2. розробити аналізатори, які знаходить відповідні прийомам шаблони умовних виразів у коді;

3. розробити компоненти виправлення коду, які пропонують зміни виявлених фрагментів коду на оптимальні;

4. розробити модульні тести для перевірки аналізаторів на тестових фрагментах коду;

5. виконати інтеграцію компонента у середовище Visual Studio.

Аналіз прийомів рефакторингу умовних виразів дозволив вибрати найпоширеніші прийоми, зокрема об'єднання умовних операторів, розподіл умовного оператора, консолідація умовних фрагментів, видалення керуючого прапору [1, 3].

Рисунок 1 – Візуалізація алгоритму виконання прийому рефакторингу «Об'єднання умовних операторів»

Для розробки аналізаторів коду та компонентів виправлення вибрана платформа компілятора .NET, яка відома під назвою Roslyn – це набір компіляторів з відкритим вихідним кодом і API аналізу коду для мови C# [4]. Вона дозволяє розробникам не лише компілювати код, а й аналізувати, змінювати та

створювати код програмно. Ключові можливості Roslyn включають побудову та аналіз синтаксичних дерев, семантичний аналіз, доступ до символів та підтримку інтеграцій у Visual Studio). Roslyn активно використовується розробниками для створення статичних аналізаторів коду, написання компонентів виправлення (CodeFix-провайдерів) і реалізації інструментів перевірки якості коду.

Технологічною основою проєкту вибрана платформа .NET 8.0, що відкриває повний доступ до новітніх API, розширює можливості використання сучасних пакетів для роботи з Roslyn і тестування, а також дозволяє розмістити всі частини одному проєкті. Визначено перелік необхідних аналізаторів та бібліотек для реалізації компоненту з підтримкою статичного аналізу та рефакторингу коду.

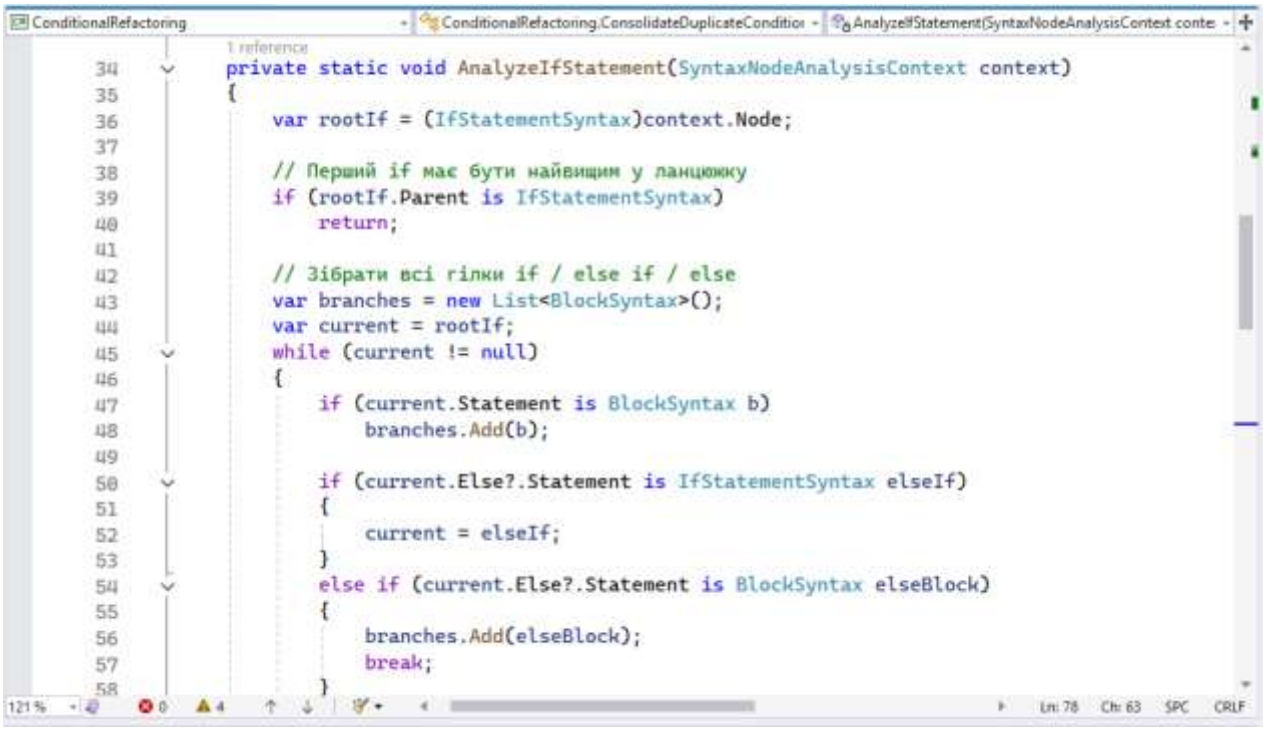

Рисунок 2 – Процес розробки аналізатору коду для прийому рефакторингу «Консолідація умовних фрагментів»

Для розробки модульних тестів вибрано сімейство фреймворків xUnit. Виконання xUnit-тестів для прийомів рефакторингу є необхідним, оскільки вони підтверджують, що аналізатор дійсно виявляє повторювані фрагменти коду, а компонент виправлення формує правильну й очікувану версію коду. Це дозволяє гарантувати, що логіка програми залишається незмінною, а автоматичні зміни не спричиняють нових помилок. Розроблено групу Xunit-тестів, які відповідають різним сценаріям вибраних прийомів рефакторингу (рис. 3). Виконана перевірка усіх тестів відповідно до різноманітних сценаріїв використання прийомів рефакторингу (рис. 4).

```
var testCode = @"
class TestClass
{
    void TestMethod()
    {
        bool found = false;
        for (int i = 0; i < 10; i++)
        {
            if (i == 5)
            {
                found = true;
            }
        }
        if (found)
        {
            System.Console.WriteLine(""Знайдено"");
        }
    }
}";
```

```
var fixedCode = @"
class TestClass
{
    void TestMethod()
    {
        for (int i = 0; i < 10; i++)
        {
            if (i == 5)
            {
                System.Console.WriteLine(""Знайдено"");
            }
        }
    }
}";
```

Рисунок 3 – Тестовий текст коду та текст коду виправлення прийому рефакторингу «Видалення керуючого прапору»

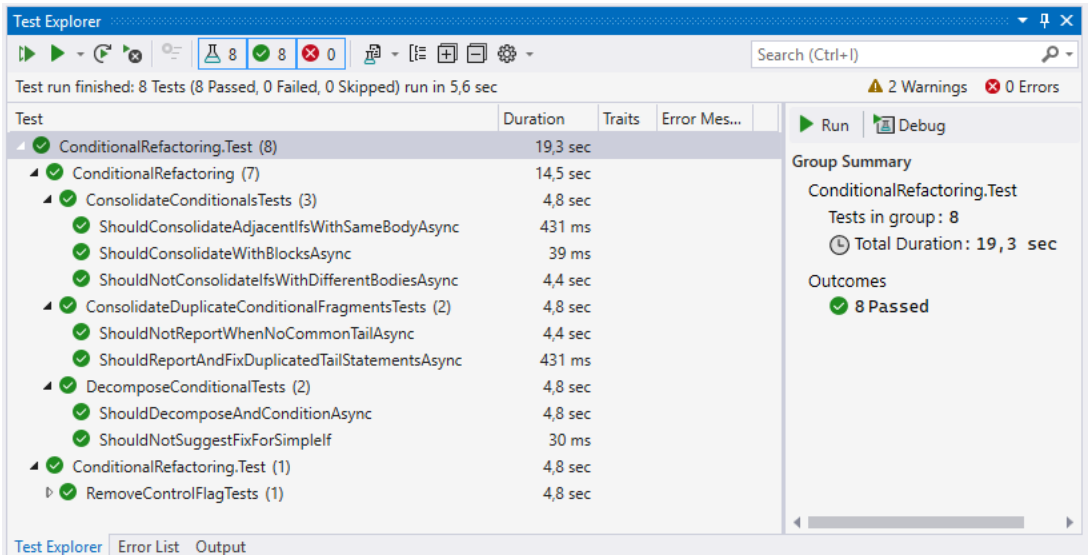

Рисунок 4 – Успішне виконання усіх модульних Xunit-тестів компоненту

У подальшому заплановано розробка VSIX-розширення, за допомогою якого буде виконана інтеграція компоненту рефакторингу у середовище Visual Studio з подальшим функціональним тестуванням.

Список використаних джерел

1. Швець О. Занурення в патерни проєктування : підручник. Київ : Refactoring.Guru, 2021. – 393 с. Режим доступу: https://refactoring.guru/files/design-patterns-ru-demo.pdf.
2. Чикунов П. О. Рефакторинг коду при конструюванні програмного забезпечення // Актуальні тенденції розвитку освіти, науки та технологій : матеріали VI Міжнародної наук.-практ. конференції (18 травня 2023 р.). У 2-х ч. Бахмут – Харків : ННППІ УІПА, 2023. Ч. 1. С. 98–100.
3. Мартін Р. Чистий код. Створення і рефакторинг за допомогою Agile. Харків : Фабула, 2019. 368 с. ISBN 978-617-09-5285-1.
4. Roslyn: майстерність статичного аналізу. Режим доступу: https://www.pluralsight.com/courses/refactoring-fundamentals.

Ключові слова: рефакторинг, умовні вирази, Visual Studio, Roslyn, C#, XUnit

Keywords: refactoring, conditional expressions, Visual Studio, Roslyn, C#, XUnit

ДЕЯКІ АСПЕКТИ УПРАВЛІННЯ ДАНИМИ

Логінова Наталія

завідувач кафедри інформаційних технології
Національного університету «Одеська юридична академія»
кандидат педагогічних наук, доцент

Обсяги даних, з якими стикаються більшість людей у побуті та в процесі виконання професійних обов'язків, зростають з кожним днем. Згідно дослідженнями компанії IDC, яка є провідним світовим постачальником ринкової аналітики, даних та подій для ринків інформаційних технологій, телекомунікацій та споживчих технологій, в 2025 році загальносвітовий обсяг сфери даних становитиме 175 зеттабайт [1]. Але в процесі роботи з даними, обсяги даних – це не єдина проблема: дані часто надходять із різних джерел і зберігаються в багатьох системах і місцях, у багатьох різних форматах. Тому, застосування даних напряму пов'язане з управлінням даних.

Управління корпоративними даними (EDM, Enterprise Data Management) – це комплексний підхід до даних, який включає процедури збору, зберігання, обробки, використання та видалення даних у законний спосіб і відповідно до бізнес-цілей компанії. Управління даними також визначає питання безпеки даних, якості даних і відповідальності за використання даних.

Управління даними складається з різноманітних стратегій, політик і технологій, які використовуються для різних дій над даними. До них відносяться:

- збір даних з різних джерел, що дозволяє знайти потрібні дані з акцентом на точність та релевантність;
- зберігання даних у базах, сховищах та озерах даних, які можуть бути стаціонарні або хмарні;
- впровадження заходів безпеки та контролю доступу для захисту даних від несанкціонованого доступу;
- забезпечення точності та узгодженості даних, шляхом виявлення та виправлення помилок, надмірностей і невідповідностей;
- належне управління даними від створення до знищення, забезпечення дотримання правових і нормативних вимог на всіх етапах роботи з даними;
- встановлення політики, інструкцій і відповідальності щодо керування даними протягом усього життєвого циклу;
- об'єднання даних із різних джерел для забезпечення єдиного перегляду та підтримки аналітики та звітності;
- використання даних для прийняття обґрунтованих рішень.

Управління даними є необхідним заходом, який гарантує, що критично важлива для користувача інформація є безпечною, доступною та масштабованою.

Наразі існує різний асортимент систем керування даними та інструментів, що дозволяють задовольняти різноманітні потреби та складності при обробці даних. Ключовою частиною зусиль управління даними є зберігання даних –

визначення найкращого способу збереження структурованих і неструктурованих даних, щоб вони були доступними, точними та безпечними.

Наприклад, традиційні системи керування реляційними базами даних чудово справляються зі структурованим зберіганням і пошуком даних, що робить їх придатними для таких додатків, як фінанси та платформи електронної комерції, де узгодженість даних і взаємозв'язки мають вирішальне значення. Сховища даних і бази даних NoSQL краще підходять для хмарних платформ, соціальних медіа та застосунків інтернету речей, оскільки вони створені для надання розширеної аналітики та підтримки неструктурованих і напівструктурованих даних.

В системі управління даних відокремлюють різні типи, до яких відносяться:

1. Управління основними даними (Master Data Management, MDM), яке зосереджується на підтримці узгоджених і точних основних даних, які становлять довідкову інформацію або описують будь-які сутності. Найпростіший приклад майстер-даних – різного роду довідники чи класифікатори.

MDM-системи, або системи управління майстер-даними – це системи, призначені для керування цими даними. Їх головна мета – забезпечити єдність подання масивів довідкових даних у всіх інформаційних системах. Крім того, це дозволяє вирішити проблеми невідповідності, дублювання та непорівнянності даних.

2. Управління сховищем даних (Data Warehouse Management, DWM) передбачає збір і зберігання даних із кількох джерел у центральному сховищі, що полегшує аналіз і звітування. Дані надходять до сховища даних з операційних систем (таких як ERP та CRM), баз даних та зовнішніх джерел, пристроїв інтернету речей, соціальних мереж та ін., зазвичай з регулярною частотою. Сучасні сховища даних призначені для обробки як структурованих, так і неструктурованих даних, таких як відео, файли зображень та дані різних датчиків.

3. Управління даними (Data Governance) – встановлює політику та процедури керування даними, забезпечуючи якість даних, відповідність і безпеку. Це досить ємний термін, який включає стратегію управління доступністю, зручністю використання, відповідністю стандартам, узгодженістю, цілісністю та безпекою даних в організаціях. Метою даного управління є забезпечення ефективного використання корпоративних даних. Головне завдання полягає в тому, щоб визначити, як, де, чому та за яких обставин дані збираються та зберігаються [2].

4. Управління якістю даних (Data Quality Management, DQM) є основою будь-якої успішної стратегії, щодо управління даними. Воно гарантує, що інформація, яка лежить в основі рішень, є надійною, послідовною та практичною. Для досягнення цієї мети процес DQM включає кілька елементів: профілювання даних, очищення, інтеграцію та моніторинг [3].

5. Управління великими даними (Big Data Management) – працює з величезними обсягами даних, створених у цифрову епоху, часто неструктурованих або напівструктурованих даних, і включає такі технології, як бази даних Hadoop і NoSQL. Існує кілька ключових характеристик, що визначають поняття великих даних:

• щодня обробляються гігантські масиви інформації, обсяг яких може сягати терабайтів і петабайтів, що спричинило появу новітніх технологій і підходів, зокрема багаторівневих систем зберігання, які забезпечують безпечне накопичення, аналіз і збереження інформації;

• сучасні цифрові дії, такі як надсилання повідомлень, онлайн-купівля чи взаємодія в соцмережах, миттєво генерують нові дані, саме тому здатність обробляти інформацію у реальному часі є однією з визначальних рис великих даних;

• дані надходять у різних формах, які можуть бути структуровані, напівструктуровані та неструктуровані. Для кожного типу потрібні відповідні методи обробки;

• зважаючи на різноманітність джерел, важливо враховувати походження даних, контекст і метадані, що забезпечить точність аналізу та отримання надійних висновків для практичної цінності;

• важливо сформувати стратегію управління даними, яка поєднує цілі організації з відповідними наборами даних [4].

6. Управління метаданими (Metadata Management) – передбачає створення та підтримку метаданих, які надають контекст та інформацію про дані.

7. Інтеграція даних (Data Integration) – поєднує дані з різних джерел, щоб забезпечити єдине уявлення, що часто є необхідним для аналітики та звітності. Це стратегічний процес, який поєднує дані з кількох джерел, щоб надати організаціям єдине уявлення для більш глибокого аналізу, прийняття обґрунтованих рішень та цілісного розуміння своїх бізнес-операцій.

Розглянути основні напрями управління даними мають свої завдання, інструменти та підходи, проте всі вони спрямовані на досягнення єдиної мети – забезпечення цілісності, точності, доступності та практичної цінності даних для підтримки управлінських рішень. Особливу увагу варто приділити впливу новітніх технологій на процеси управління даними. Реляційні бази даних, NoSQL-рішення, хмарні платформи, а також системи для роботи з неструктурованими даними відкривають нові можливості для інтеграції, зберігання та аналізу інформації. Завдяки цьому можна оперативно реагувати на зміни в IT-середовищі, оптимізувати внутрішні процеси та формувати конкурентні переваги.

Отже, управління даними є не лише технічним викликом, але й стратегічною необхідністю для забезпечення сталого розвитку та цифрової трансформації в усіх сферах діяльності. Комплексний підхід до організації життєвого циклу даних створює передумови для підвищення якості управлінських рішень, зміцнення інформаційної безпеки та формування довгострокової цінності даних як стратегічного активу.

Список використаних джерел

1. International Data Corporation (IDC). URL: https://surl.li/jsihxv
2. Data Governance: definition, goals and tasks. URL: https://datalabsua.com/en/data-governance-definition-goals-and-tasks/

3. Understanding Data Quality Management: A Complete Guide. URL: https://www.esystems.fi/en/blog/understanding-data-quality-management-complete-guide
4. Big Data – 5 основних характеристик. URL: https://datalabsua.com/ua/big-data-top-5-characteristics/

Ключові слова: дані, управління даними, системи управління даними, сховища даних, метадані

Key words: data, data management, data management systems, data warehouses, metadata

ОПТИМІЗАЦІЯ ЗАПИТІВ У РЕЛЯЦІЙНИХ БАЗАХ ДАНИХ: ПІДХОДИ ДО ЗНИЖЕННЯ СКЛАДНОСТІ ВИКОНАННЯ SQL-ЗАПИТІВ

Грезіна Олена

PhD, асистент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»

Оптимізація запитів до баз даних залишається критичним завданням в умовах постійного зростання обсягів даних та ускладнення інформаційних систем. Сучасні програми вимагають обробки петабайтів даних та виконання складних аналітичних запитів з мінімальними затримками. Неефективні запити можуть стати вузьким місцем продуктивності всієї системи, збільшуючи час відгуку та споживання обчислювальних ресурсів.

Оптимізація запитів у реляційних СКБД спрямована на мінімізацію часу виконання запитів за збереження коректності результатів. Оптимізатор запитів відіграє центральну роль цьому процесі, аналізуючи можливі плани виконання і вибираючи оптимальний з погляду вартості. Складність оптимізації полягає у різноманітті факторів, що впливають на продуктивність: структура даних, статистика розподілу значень, доступні індекси, параметри системи та конкретні особливості запитів.

Оптимізатор запитів працює за наступним алгоритмом:

```
[SQL-запит] → [Parser] → [Синтаксичне дерево (Parse tree)] →
    [Plan Generator] → [Cost Estimation] → [Optimal Plan]
```

Індексування є основним методом прискорення доступу до даних. Сучасні підходи до індексування виходять за рамки традиційних B-дерев та включають спеціалізовані структури для різних типів даних та запитів.

Значне поліпшення продуктивності забезпечують композитні індекси, що охоплюють кілька стовпців, які часто використовуються разом в умовах WHERE і JOIN. Оптимізатор запитів може використовувати такі індекси швидкого доступу до даних без сканування таблиць. Однак визначення оптимального набору композитних індексів залишається складним завданням, що вимагає аналізу робочого навантаження та компромісу між прискоренням запитів та накладними витратами на підтримку індексів.

Приклад композитного індексу:

```
SELECT * FROM Orders
WHERE customer_id = 100 AND order_date >= '2025-01-01';
```

Композитний індекс (customer_id, order_date) дозволяє уникнути повного сканування таблиці. Оцінка вигоди індексу полягає у наступному: без індексу: повне сканування таблиці, O(n) операцій, з індексом: пошук за B-деревом, O(log n) + кількість відповідних записів.

Якщо таблиця містить 1 млн записів, а запит повертає 100 записів, індекс зменшує час виконання приблизно в 1000 разів (залежить від розподілу даних).

План виконання запиту визначає послідовність операцій, які виконують СКБД для отримання результату. Сучасні оптимізатори використовують складні алгоритми для вибору оптимального плану з багатьох можливих варіантів.

У роботі [1] презентується метод оптимізації на основі машинного навчання, який передбачає вартість виконання різних планів запитів. Даний метод дозволяє знизити обчислювальні витрати на оптимізацію складних запитів, що містять безліч з'єднань та підзапитів. Модель навчається на історичних даних про виконання запитів та здатна враховувати нелінійні залежності між параметрами запитів та їх продуктивністю.

Важливим аспектом оптимізації планів запитів є вибір оптимальних алгоритмів з'єднання таблиць (nested loop join, hash join, merge join). Вибір залежить від обсягу даних, наявності індексів та розподілу значень. Сучасні СКБД використовують адаптивні алгоритми, які можуть змінювати стратегію виконання сполук у процесі виконання запиту з урахуванням фактичних даних.

Матеріалізовані уявлення надають спосіб попереднього обчислення та зберігання результатів запитів, що часто виконуються. Особливо ефективним це є для аналітичних навантажень, де запити включають агрегацію великих обсягів даних.

У дослідженні [2] наведена інтелектуальна система управління матеріалізованими уявленнями, яка автоматично визначає, які уявлення слід створити, оновити чи видалити на основі аналізу робочого навантаження. Система враховує як частоту запитів, а й вартість підтримки уявлень у актуальному стані. Експерименти показали прискорення аналітичних запитів у 5-15 разів при використанні оптимального набору матеріалів представлених.

Наприклад, матеріалізоване уявлення доцільно створювати, якщо виграш від його використання перевищує витрати на оновлення. Виграш обчислюється за формулою:

$$Benefit = F \cdot (T_{exec} - T_{mview}) - C_{update},$$

де T_{exec} – час виконання запиту без уявлення, T_{mview} – час виконання з уявленням, C_{update} – витрати на оновлення уявлення, F – частота виконання запиту. Якщо Benefit > 0, створення матеріалізованого уявлення є ефективним.

Цікавим напрямком є інтеграція матеріалізованих уявлень із механізмами кешування запитів. Сучасні СКБД використовують багаторівневі системи кешування, що включають кешування результатів запитів, планів виконання та навіть проміжних результатів. Адаптивне кешування враховує частоту запитів та зміни даних, забезпечуючи оптимальне використання пам'яті. Сучасні СКБД включають механізми автоматичної оптимізації, які аналізують виконання запитів та автоматично коригують параметри системи. Вказані механізми можуть включати автоматичне створення та підтримка індексів, перерозподіл ресурсів між паралельними запитами, адаптацію планів виконання на основі реальних даних, передбачення та запобігання проблемам продуктивності.

Для оцінки ефективності різних методів оптимізації було проведено експерименти з урахуванням бази даних TPC-H обсягом 100 ГБ. Тестувалися такі стратегії оптимізації: базова конфігурація (без спеціальної оптимізації), оптимізація індексів (створення індексів за рекомендацією системи), матеріалізовані уявлення для запитів, що часто виконуються, комбінований підхід (поєднання методів 2 та 3).

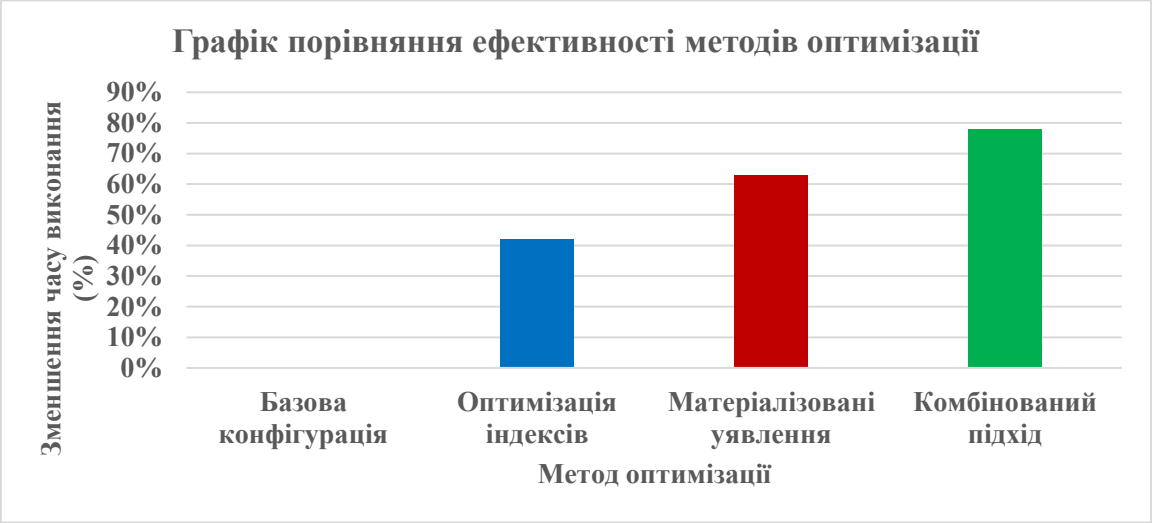

Рисунок 1 – Графік порівняння ефективності методів оптимізації

Результати представлені на рис.1 показали, що оптимізація індексів знижує середній час виконання запитів на 42%, використання матеріалізованих уявлень – на 63%, а комбінований підхід – на 78%. Найбільший ефект спостерігався для складних аналітичних запитів, що містять численні сполуки та агрегації.

Важливим спостереженням стало те, що продуктивність запитів залежить від розподілу даних і типу запитів. Для транзакційних навантажень найефективнішими є оптимізовані індекси, тоді як для аналітичних запитів кращі результати показали матеріалізовані уявлення.

Оптимізація SQL-запитів залишається критично важливим завданням забезпечення високої продуктивності сучасних інформаційних систем. Дослідження показало, що найефективнішим є комплексний підхід, який поєднує різні методи оптимізації залежно від характеристик робочого навантаження.

Перспективними напрямками подальших досліджень є застосування методів машинного навчання для прогнозування оптимальних стратегій виконання запитів; розробка нових структур індексування для специфічних типів даних та запитів; інтеграція методів оптимізації з хмарними та розподіленими системами баз даних; автоматична реструктуризація схем баз даних для оптимізації продуктивності. В умовах постійного зростання обсягів даних та ускладнення запитів, автоматичні та адаптивні методи оптимізації стають все більш важливими для забезпечення ефективної роботи систем управління базами даних.

Список використаних джерел

1. Md Majadul Islam Jim, Mahmudul Hasan, Rebeka Sultana, and Md Mahfuzur Rahman. Machine Learning Techniques for Automated Query Optimization in Relational Databases. International Journal of Advanced Engineering Technologies and Innovations. vol. 1, no. 3, 2024, p. 514. URL: https://www.researchgate.net/publication/386571774_Machine_Learning_Techniques_for_Automated_Query_Optimization_in_Relational_Databases
2. Xu, Z., Wang, P., Xue, G., Yan, Q., Gong, S., Jiang, Y., Mao, Y., Gao, Y., Shen, S., Zhang, W., Luo, D., & Chen, L. (2024). UniView: A Unified Autonomous Materialized View Management System for Various Databases. Proceedings of the VLDB Endowment, 17(12), 4353–4356. URL: https://doi.org/10.14778/3685800.3685873

Ключові слова: реляційні бази даних, оптимізація SQL-запитів, індексування, матеріалізовані уявлення, автоматична оптимізація баз даних

Keywords: relational databases, SQL query optimization, indexing, materialized views, automatic database optimization

ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ ДЛЯ БАЗ ДАНИХ

Солом'яний Олексій

студент 1-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У сучасному світі інформаційно-комунікаційні технології (ІКТ) є основою цифрової трансформації, що охоплює всі сфери суспільного життя - від економіки й освіти до державного управління та повсякденної діяльності. У цьому контексті хмарні технології[1] та бази даних[2] (БД) виступають ключовими елементами, які забезпечують ефективне функціонування інформаційних систем. Хмарні технології, надаючи масштабовані обчислювальні ресурси через Інтернет, радикально змінюють підходи до розгортання та управління IT-інфраструктурою, забезпечуючи гнучкість, економію ресурсів і доступність. Бази даних, своєю чергою, формують фундамент для структурованого зберігання, обробки та аналізу інформації, що є критично важливим для будь-якого програмного забезпечення. Окремо ці технології відіграють унікальні ролі: хмарні платформи сприяють

демократизації доступу до високопродуктивних ресурсів, тоді як БД забезпечують цілісність, доступність і безпеку даних. Проте їхня інтеграція, зокрема через сучасні фреймворки, такі як ASP.NET Core, створює синергетичний ефект, дозволяючи розробникам проектувати високоефективні, масштабовані та безпечні інформаційні системи. Ця робота присвячена аналізу використання хмарних технологій для баз даних, їхньої ролі в IT-індустрії, переваг, викликів і перспектив розвитку.

Хмарні технології являють собою модель надання обчислювальних ресурсів - серверів, сховищ, баз даних, програмного забезпечення та аналітичних інструментів - через інтернет на запит користувача. Вони базуються на концепції віртуалізації, що дозволяє оптимально розподіляти ресурси між багатьма клієнтами, забезпечуючи економію витрат і високу доступність.

Хмарні технології поділяються на три основні моделі обслуговування:

Інфраструктура як сервіс (IaaS)[3]: надає віртуалізовані обчислювальні ресурси, такі як віртуальні машини чи сховища (наприклад, Amazon EC2, Microsoft Azure Virtual Machines).

Платформа як сервіс (PaaS)[3]: забезпечує середовище для розробки та розгортання додатків, усуваючи необхідність управління апаратним забезпеченням (наприклад, Azure App Services, Google App Engine).

Програмне забезпечення як сервіс (SaaS)[3]: пропонує готові програмні продукти, доступні через Інтернет (наприклад, Google Workspace, Microsoft 365).

За типом розгортання хмарні технології класифікуються на:

Публічні хмари: ресурси надаються широкій аудиторії через провайдерів, як AWS чи Azure.

Приватні хмари: інфраструктура виділена для однієї організації, що забезпечує підвищену безпеку.

Гібридні хмари: поєднують публічні та приватні хмари для оптимізації витрат і гнучкості.

Основними характеристиками хмарних технологій є масштабованість, висока доступність, автоматизоване адміністрування та оплата за фактичне використання, що робить їх привабливими для розробників і організацій.

Хмарні технології для баз даних (БД) являють собою керовані сервіси, які забезпечують створення, управління та масштабування баз даних через Інтернет без необхідності локальної інфраструктури. Вони охоплюють реляційні бази даних (наприклад, Azure SQL Database, Amazon RDS, Google Cloud SQL), NoSQL бази (MongoDB Atlas, AWS DynamoDB, Azure Cosmos DB) та гібридні рішення для складних сценаріїв. Ці сервіси дозволяють розробникам зосередитися на проєктуванні даних і логіці додатків, передаючи завдання адміністрування, резервного копіювання та оновлення провайдерам хмарних платформ.

Основні характеристики хмарних БД:

• масштабованість – хмарні БД автоматично адаптуються до змін навантаження, дозволяючи обробляти від кількох запитів до мільйонів транзакцій за секунду;

• висока доступність – геореплікація та автоматичне резервне копіювання забезпечують безперебійну роботу навіть у разі збоїв;

• безпека – вбудовані механізми шифрування, управління доступом (наприклад, Azure Active Directory, AWS IAM) і відповідність стандартам безпеки (GDPR, ISO 27001) захищають дані;

• керованість – провайдери автоматизують адміністрування, оновлення та моніторинг, що зменшує навантаження на розробників;

• гнучкість – підтримка різних моделей даних (реляційних, документо-орієнтованих, ключ-значення) дозволяє вибирати оптимальне рішення для конкретного проєкту.

Популярні хмарні БД[4]:

1. Microsoft Azure: Azure SQL Database (реляційна), Cosmos DB (NoSQL із підтримкою кількох моделей даних).

2. Amazon Web Services: Amazon RDS (реляційна), DynamoDB (NoSQL), Aurora (високопродуктивна реляційна БД).

3. Google Cloud: Cloud Spanner (масштабована реляційна), Firestore (документо-орієнтована NoSQL).

Хмарні бази даних відіграють ключову роль у розробці сучасних інформаційних систем, забезпечуючи інтеграцію з іншими хмарними сервісами, такими як вебдодатки, аналітика чи штучний інтелект. Їх використання дозволяє підвищити продуктивність розробки, оскільки хмарні БД усувають необхідність налаштування локальних серверів, дозволяючи швидко розгортати бази для тестування чи виробництва. Забезпечити масштабованість за рахунок автоматичного розподілення ресурсів, що критично важливо для додатків із змінним навантаженням, як-от платформи електронної комерції чи соціальні мережі. Інтеграція з хмарними сервісами ШІ (наприклад, Azure AI) чи аналітики (AWS Redshift) дозволяє створювати інтелектуальні системи на основі даних. Хмарні платформи надають інструменти для захисту даних, включаючи шифрування в спокої та під час передачі, а також управління доступом.

Використання хмарних БД знижують витрати на інфраструктуру, сприяючи розвитку стартапів і малого бізнесу. Хмарні сервіси, як Google BigQuery, використовуються для аналізу даних у навчальних проєктах, підвищуючи якість освіти. Хмарні БД підтримують зберігання та обробку медичних даних, сприяючи розвитку телемедицини. Хмарні рішення інтегруються з IoT для моніторингу інфраструктури, наприклад, транспортних потоків чи енергоспоживання.

Для демонстрації практичного використання хмарних баз даних розглянемо створення RESTful API [5] на ASP.NET Core, яке підключається до Azure SQL Database для управління даними про продукти в системі електронної комерції.

Цей приклад ілюструє інтеграцію хмарної БД із вебзастосунком, розгорнутим у хмарі (Azure App Services).

Технічні аспекти використання хмарних технологій для бази даних полягають у поєднанні сучасної інфраструктури, безпеки та зручності розробки. API розгорнуто в Azure App Services, що забезпечує автоматичне масштабування та високу доступність системи. Для зберігання даних використовується Azure SQL Database, яка підтримує георепліkацію, регулярне резервне копіювання та вбудоване шифрування, що гарантує збереження та захищеність інформації. Розробка застосунку здійснюється з використанням ASP.NET Core у поєднанні з Entity Framework Core, що спрощує взаємодію з хмарною базою даних і дозволяє зосередитися на реалізації бізнес-логіки. Безпека системи забезпечується завдяки використанню Azure Active Directory для автентифікації користувачів, а також додатковим вбудованим механізмам шифрування даних.

Серед переваг використання хмарних технологій варто відзначити швидке розгортання, адже API та база даних можуть бути налаштовані за лічені хвилини за допомогою Azure Portal. Важливою є також масштабованість: Azure SQL Database здатна автоматично обробляти пікові навантаження, наприклад, під час періодів розпродажів. Окрім цього, спрощене адміністрування є суттєвою перевагою, оскільки хмарна платформа забезпечує автоматичне оновлення, резервне копіювання та постійний моніторинг системи без потреби у втручанні адміністратора.

Хмарні БД мають низку переваг, серед яких особливо вирізняється економічна ефективність: модель оплати за фактичне використання дозволяє значно оптимізувати витрати у порівнянні з утриманням локальної інфраструктури. Вони забезпечують глобальну доступність, що робить можливим спільну роботу команд з різних куточків світу. Крім того, хмарні БД легко інтегруються з іншими сервісами, такими як ШІ, аналітичні системи чи пристрої інтернету речей. Автоматизація також є суттєвим плюсом - більшість рутинних завдань, зокрема оновлення чи масштабування, виконуєтіься автоматично на боці провайдера.

Втім, існують і певні виклики. Залежність від стабільного інтернет-з'єднання може обмежити доступ до даних у разі перебоїв. Питання безпеки також залишаються актуальними, адже помилки в конфігурації можуть призвести до витоку інформації. Крім того, неконтрольоване споживання ресурсів у хмарі може неочікувано підвищити витрати, а сам процес міграції з локальної БД до хмарного середовища вимагає ретельного планування і технічної підготовки.

Попри ці труднощі, хмарні БД продовжують активно розвиватися. Нові можливості відкриває інтеграція з технологіями ШІ, наприклад через Azure Synapse Analytics, що дозволяє поєднувати аналітику з машинним навчанням для побудови прогнозів. Розвиваються також безсерверні рішення, як-от AWS Aurora Serverless, які усувають необхідність керування фізичними чи віртуальними серверами. Завдяки гарлобальній розподіленості, платформи на кшталт Azure Cosmos DB забезпечують швидкий доступ до даних з різних регіонів світу. Окрім

того, дослідження в галузі квантових обчислень, які провадять різні компанії, відкривають перспективи для змін у способах обробки й аналізу великих обсягів даних у хмарному середовищі.

Отже, хмарні технології БД є невід'ємною частиною сучасної IT-індустрії, забезпечуючи масштабованість, безпеку та гнучкість у розробці інформаційних систем. Вони дозволяють розробникам створювати вебзастосунки на ASP.NET Core із підключенням до Azure SQL Database, мінімізуючи витрати на інфраструктуру. Хмарні БД підтримують цифрову трансформацію в економіці, освіті, охороні здоров'я та інших сферах, надаючи інструменти для обробки великих обсягів даних. Незважаючи на виклики, такі як безпека чи залежність від інтернету, хмарні БД залишаються ключовим елементом ІКТ, а їхній розвиток у поєднанні з ШІ, безсерверними архітектурами та квантовими технологіями відкривають нові перспективи для IT-галузі.

Список використаних джерел

1. Що таке хмарні технології: визначення, важливість та застосування. URL: https://wezom.com.ua/ua/blog/scho-take-hmarni-tehnologiyi-viznachennya-vazhlivist-ta-zastosuvannya.
2. Що таке база даних та для чого вона потрібна. URL: https://cityhost.ua/uk/blog/scho-take-baza-danih-ta-dlya-chogo-vona-potribna.html.
3. IaaS, SaaS та PaaS: Що це таке, їх відмінності та приклади використання. URL: https://golosznadbugu.com/cikavo/iaas-saas-ta-paas-shcho-tse-take-ikh-vidminnosti-ta-pryklady-vykorystannia.html.
4. Топ 5 хмарних провайдерів: плюси та мінуси. URL: https://itedu.center/ua/blog/sysadministration/top-5-cloud-providers-advantages-and-disadvantages/?srsltid=AfmBOormRFIb2533IvJZ352W0N5X3GyBVEqzKYgc5z7373tXF8uektPm.
5. REST API як спосіб спілкування компонент вебдодатків. URL: https://foxminded.ua/shcho-take-rest-api/.

Науковий керівник: доцент Логінова Н.

ВИКОРИСТАННЯ МЕТОДІВ ОБРОБКИ ПРИРОДНОЇ МОВИ У РОЗРОБЦІ ЧАТ-БОТІВ ТА СИСТЕМ МАШИННОГО ПЕРЕКЛАДУ

Китайченкова Катерина

студентка 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету "Одеська юридична академія"

Обробка природної мови Natural Language Processing (NLP) є ключовою галуззю штучного інтелекту (ШІ), що стрімко розвивається та знаходить все ширше

застосування у створенні інтелектуальних систем різного призначення [1]. Сучасні технології дозволяють комп'ютерним системам не лише обробляти, але й розуміти та генерувати людську мову, що відкриває нові можливості для людино-машинної взаємодії.

NLP відіграє важливу роль у розробці чат-ботів і систем автоматичного перекладу, які стали невід'ємною частиною цифрового світу. Ці системи спрощують обслуговування клієнтів, навчання, міжнародне спілкування, допомагаючи економити час і долати мовні бар'єри.

Фундаментом для будь-якої NLP-системи є попередня обробка текстових даних. Цей етап включає низку важливих кроків, спрямованих на перетворення "сирого" тексту у формат, придатний для машинного аналізу. Токенізація – процес розбиття тексту на окремі одиниці (слова, символи, токени) – є першим кроком [2]. Наступними важливими етапами є стандартизація (наприклад, перетворення тексту до нижнього регістру, видалення пунктуації) та нормалізація слів за допомогою лематизації (приведення слова до його базової словникової форми) або стемінгу (відкидання закінчень та суфіксів для отримання основи слова). Також часто видаляються стоп-слова (артиклі, прийменники, сполучники), які не несуть значного семантичного навантаження, для покращення подальшого аналізу. Якісна попередня обробка значно впливає на точність роботи наступних етапів NLP.

Після попередньої обробки текст необхідно представити у числовому форматі, зрозумілому для алгоритмів машинного навчання. Цей процес називається векторизацією. Традиційні підходи, такі як Bag of Words (мішок слів), представляють текст як вектор частот слів, але вони не враховують семантичні зв'язки між словами. Більш сучасні методи, такі як Word Embeddings (GloVe, FastText), створюють "карту" слів, де схожі за значенням слова розташовані поруч [3]. Одним з найважливішим кроком стало створення контекстних моделей, таких як BERT та GPT, які побудовані на архітектурі Transformer. Вони аналізують контекст, враховуючи, як слова поєднуються в реченні, що дозволяє значно ефективніше враховувати семантичні та синтаксичні залежності, забезпечуючи глибше розуміння тексту [4].

У розробці чат-ботів методи NLP відіграють домінуючу роль, дозволяючи системам розуміти запити користувачів та генерувати релевантні відповіді. Аналіз вводу користувача (текстового чи голосового) за допомогою NLP дозволяє ідентифікувати його наміри та ключові сутності. Методи розпізнавання іменованих сутностей Named Entity Recognition (NER) [5]. Аналіз тональності дозволяє боту розуміти емоційне забарвлення повідомлення користувача та відповідно коригувати свою відповідь.

Завдяки контекстному розумінню, яке забезпечують сучасні моделі, чат-боти можуть підтримувати більш природний та послідовний діалог, ефективно обробляючи запити користувачів. Чат-боти є незамінними помічниками у будь-якій сфері, де наявні великі обсяги комунікації з клієнтами, забезпечуючи

миттєву відповідь у режимі 24/7 без очікування оператора [6]. Вони знаходять застосування у маркетингу для розсилки рекламних пропозицій, у сервісах бронювання, службах підтримки, статистичному моніторингу, медицині (попередня діагностика, психологічна підтримка), освіті (інформування абітурієнтів та студентів, вивчення мов), рекрутингу (автоматизації опитування кандидатів) та для оптимізації внутрішніх корпоративних процесів. Можливість інтеграції з корпоративними системами Customer Relationship Management (CRM) та Enterprise Resource Planning (ERP) через API ще більше розширює їх функціонал.

Системи автоматичного машинного перекладу (МП) є ще однією сферою, де NLP має вирішальне значення. Традиційні статистичні системи МП класу Statistical Machine Translation (SMT) поступово витісняються нейронними системами МП класу Neural Machine Translation (NMT). У останні роки значний прогрес у цій сфері став можливим завдяки глибокому навчанню – підходу в машинному навчанні, який використовує нейронні мережі з багатьма шарами для вивчення складних закономірностей з даних. NMT, часто побудовані на архітектурах нейронних мереж, які визначають, як шари з'єднуються між собою рекурентних Recurrent Neural Networks (RNN) або згорткових Convolutional Neural Networks (CNN) нейронних мереж, а особливо на базі Transformer (спеціальної архітектури для обробки тексту, яка швидко аналізує всі слова одночасно), демонструють значно вищу якість та плавність перекладу [7].

Механізми уваги (attention mechanisms) дозволяють моделям NMT фокусуватися на найбільш релевантних частинах вхідного тексту при генерації перекладу, що особливо важливо для обробки довгих речень та багатозначних слів [8]. Використання NLP-технік у перекладацькому контексті, наприклад, у розмовних системах, демонструє високу ефективність, хоча й вимагає ретельної оцінки якості.

Глибоке навчання – це підхід у машинному навчанні, який використовує глибокі нейронні мережі для аналізу складних закономірностей у даних, таких як текст чи мовлення, і зробило революцію в NLP, надавши потужні інструменти для аналізу та генерації тексту. Архітектури класу Long Short-Term Memory (LSTM) ефективно обробляють довгострокові залежності в послідовних даних, що є критичним для багатьох завдань NLP [9]. Моделі на основі Transformer, завдяки механізму самоуваги (self-attention, тобто здатності моделі аналізувати зв'язки між усіма словами в реченні, щоб визначити, які з них важливіші для розуміння контексту), дозволяють паралельно обробляти всі токени послідовності, що прискорює навчання та забезпечує високу точність у таких завданнях, як машинний переклад та генерація тексту.

Оцінка якості таких систем проводиться за допомогою інструментів, як-от BLEU [10]. Крім того, для інших завдань, таких як класифікація чи вилучення інформації, використовуються також показники точності та повноти (F1-score).

Незважаючи на значний прогрес, в NLP залишаються невирішені проблеми. Боротьба з неоднозначністю мови, де одне слово чи фраза можуть мати кілька

значень, потребує подальших досліджень. Поглиблення розуміння контексту, включаючи наміри користувача та емоційний фон, є важливим напрямком удосконалення систем.

Майбутнє NLP пов'язане із створенням багатогранних систем, які можуть оцінювати не лише текст, а й зображення та аудіо. Алгоритмічна прозорість, багатомовна та полікультурна підтримка, а також зменшення витрат на ресурси моделі [11].

Отже, методи обробки природної мови є рушійною силою розвитку сучасних інтелектуальних систем, зокрема чат-ботів та систем автоматичного перекладу. Техніки, такі як токенізація, лематизація, векторні представлення слів, та особливо сучасні підходи на основі глибокого навчання (контекстні моделі BERT, GPT, архітектура Transformer, LSTM) дозволяють комп’ютерам не просто обробляти текст, а й глибше розуміти людську мову. Це значно покращує якість взаємодії користувачів з чат-ботами та підвищує ефективність машинного перекладу. Подальший розвиток NLP обіцяє ще більш природну та ефективну взаємодію між людиною та комп'ютером, наближаючи нас до повноцінного розуміння та використання людської мови машинами.

Список використаних джерел

1. Що таке обробка природної мови (Natural Language Processing, NLP)?. *TheTransmitted*. URL: https://thetransmitted.com/adlucem/shho-take-obrobka-pryrodnoyi-movy-natural-language-processing-nlp/.
2. Tokenization in NLP: what is it?. *Coursera*. URL: https://www.coursera.org/articles/tokenization-nlp?isNewUser=true
3. GloVe: global vectors for word representation. *The Stanford Natural Language Processing Group*. URL: https://nlp.stanford.edu/projects/glove/
4. Word embeddings in NLP. *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/word-embeddings-in-nlp/
5. What is named entity recognition (NER)?. *AltexSoft*. URL: https://www.altexsoft.com/blog/named-entity-recognition/
6. How contextual chatbots deliver personalised conversations. *FastBots*. URL: https://fastbots.ai/blog/how-contextual-chatbots-deliver-personalised-conversations
7. A comparison of statistical and neural MT in a multi-product and multilingual software company. *ACL anthology*. С. 316-321. URL: https://aclanthology.org/2018.eamt-main.34.pdf
8. How do attention mechanisms work?. *IBM*. URL: https://www.ibm.com/think/topics/attention-mechanism
9. How to use LSTM in NLP tasks with A text classification example using keras. *Spot Intelligence*. URL: https://spotintelligence.com/2023/01/11/lstm-in-nlp-tasks/
10. Розуміння оцінки BLEU у NLP: оцінка якості перекладу. *Certified Online Coding Bootcamp | Code Labs Academy*. URL:

https://codelabsacademy.com/uk/blog/understanding-bleu-score-in-nlp-evaluating-translation-quality
11. The role of natural language processing (NLP) in modern chatbots. *Analytics Vidhya*. URL: https://www.analyticsvidhya.com/blog/2024/08/nlp-in-modern-chatbots/

Ключові слова: обробка природної мови, чат-боти, машинний переклад, штучний інтелект, нейронні мережі, Telegram-бот.

Keywords: natural language processing, chatbots, machine translation, artificial intelligence, neural networks, Telegram bot.

Науковий керівник: доцент Задерейко О.

МЕРЕЖЕВИЙ МОНІТОРИНГ У РЕАЛЬНОМУ ЧАСІ

Гура Володимир

доцент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»,
кандидат технічних наук

Арнаут Аліна

студентка 4-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Сучасні комп'ютерні мережі стають дедалі складнішими, а кількість підключених пристроїв стрімко зростає. За даними Cisco, у 2022 році кількість підключених пристроїв сягнула 29,3 мільярда, що підкреслює необхідність розробки ефективних інструментів для моніторингу та управління мережевою інфраструктурою [1]. Розроблений додаток "Network Monitor" є універсальним рішенням для аналізу мережевої активності, діагностики продуктивності та забезпечення безпеки мережі, орієнтованим на мережевих адміністраторів і програмістів. Він надає потужний функціонал для управління мережевими процесами, візуалізації даних і виявлення аномалій, що робить його значним внеском у сучасні технології моніторингу мереж.

Метою розробки "Network Monitor" (рис. 1), стало створення інструменту, який дозволяє мережевим адміністраторам ефективно відстежувати стан мережі, виявляти потенційні загрози та оптимізувати продуктивність.

Додаток вирішує завдання моніторингу мережевого трафіку, візуалізації даних про швидкість мережі, стабільність з'єднання та топологію мережі, а також виявлення аномалій із застосуванням машинного навчання. Він побудований на основі клієнтської архітектури з використанням мови Python і бібліотеки Tkinter для створення графічного інтерфейсу, обраної завдяки її кросплатформності та простоті інтеграції з іншими Python-бібліотеками [2]. Інтерфейс додатка поділений на кілька вкладок, зокрема діагностика, моніторинг продуктивності,

стабільності з'єднання, сканування пристроїв, аналіз DNS і генерація мережевої карти, що забезпечує зручність роботи для користувачів.

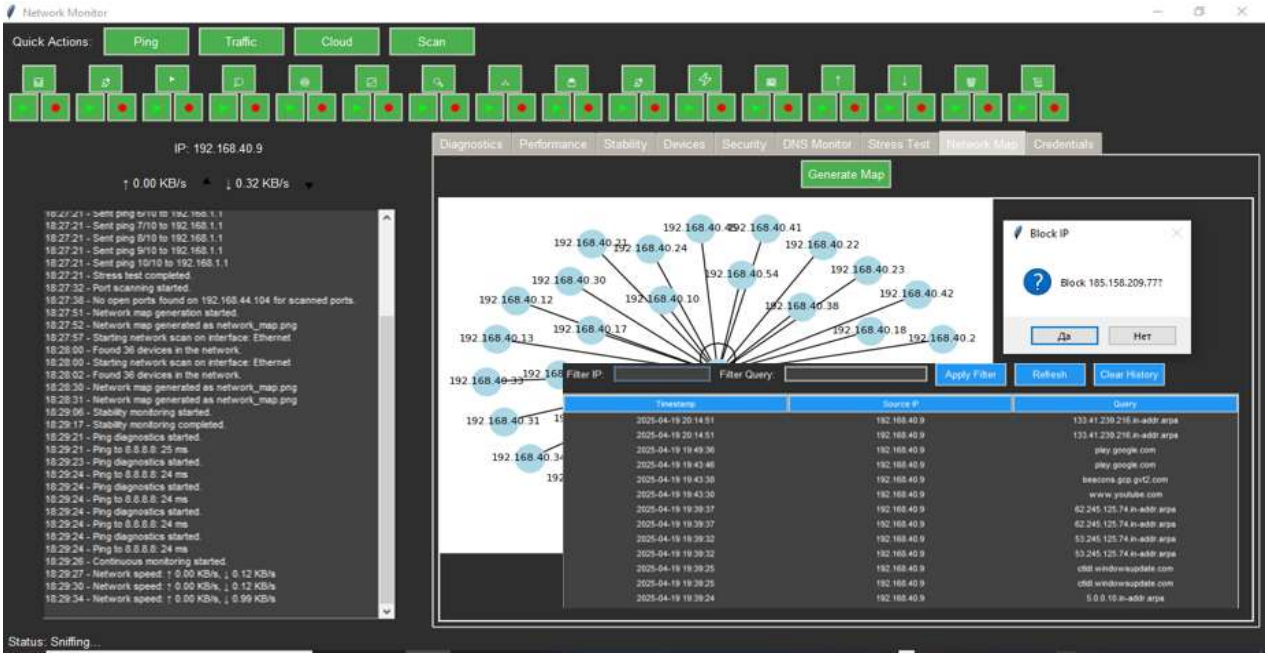

Рисунок 1 – Графічний інтерфейс програми "Network Monitor"

Для моніторингу мережевого трафіку додаток використовує бібліотеку Scapy, яка дозволяє захоплювати та аналізувати пакети в реальному часі. Функція monitor_traffic аналізує пакети, визначаючи протоколи (TCP, UDP) і виявляючи підозрілий трафік, який перевищує поріг у 100 000 байтів за сесію, що відповідає рекомендаціям щодо виявлення аномалій, описаним у літературі [3]. Візуалізація топології мережі реалізована за допомогою бібліотеки NetworkX, яка генерує графічне зображення мережі, використовуючи алгоритм пружинного розташування (spring layout), що спрощує аналіз зв'язків між пристроями [4]. Однією з ключових особливостей додатка є інтеграція алгоритму машинного навчання RandomForestClassifier із бібліотеки Scikit-learn для прогнозування мережевих збоїв. Модель навчається на даних про затримки (ping), обсяг трафіку та втрати пакетів, досягаючи точності класифікації аномалій на рівні 85% при вибірці зі 100 записів, що дозволяє адміністраторам завчасно реагувати на потенційні проблеми [5].

Для зберігання історичних даних про трафік і DNS-запити використовується SQLite, що забезпечує легке та надійне рішення для невеликих мереж. Під час тестування база даних фіксувала понад 5000 записів без значного збільшення часу відгуку (менше 0,1 секунди на запит), що робить її придатною для тривалого аналізу [6]. Інтерфейс додатка включає логотип у правому верхньому куті та виконаний у сучасній темній темі, що відповідає стандартам дизайну, таким як Material Design, що покращує користувацький досвід. З точки зору програмування, "Network Monitor" вирізняється модульністю та розширюваністю, що відповідає принципам об'єктно-орієнтованого програмування. Код організований

у вигляді класів і функцій із чітким поділом логіки, наприклад, NetworkMonitorApp відповідає за інтерфейс, а AIPredictor за машинне навчання, що спрощує подальшу розробку [7].

Додаток використовує асинхронну обробку задач через потоки (threading.Thread), що дозволяє виконувати ресурсомісткі операції, такі як моніторинг трафіку та генерація мережевих карт, без блокування основного інтерфейсу. Наприклад, метод start_network_map запускає generate_network _map в окремому потоці, зменшуючи навантаження на GUI [8]. Інтеграція сучасних бібліотек, таких як Scapy, NetworkX, Scikit-learn і Matplotlib, забезпечує високу продуктивність і точність аналізу даних. Scapy обробляє до 1000 пакетів за секунду на стандартному обладнанні, що робить додаток придатним для середніх і великих мереж [3]. Система логування реалізована з використанням logging.handlers.RotatingFileHandler, яка зберігає до 1 МБ даних із ротацією до 5 файлів, що дозволяє розробникам і адміністраторам відстежувати помилки та події в реальному часі [9].

З точки зору мережевого адміністратора, "Network Monitor" забезпечує моніторинг у реальному часі, фіксуючи дані про швидкість мережі (до 10 МБ/с у тестах), затримки (ping до 0,5 мс), стабільність з'єднання та DNS-запити з оновленням кожні 2 секунди, що дозволяє оперативно реагувати на зміни в мережі [10]. Модель машинного навчання виявляє потенційні збої з точністю 85%, скорочуючи час реакції на інциденти, наприклад, при виявленні високого джиттера (понад 20 мс) адміністратор отримує повідомлення [5]. Функції сканування мережі та портів використовують ARP-запити та перевірку портів (21, 22, 80, 443 та інші), допомагаючи виявити несанкціоновані пристрої та відкриті порти, що становлять загрозу безпеці. SQLite зберігає дані про трафік і DNS-запити, дозволяючи аналізувати тенденції; за 24 години тестування було зафіксовано 1193 DNS-запитів, що допомогло виявити підозрілу активність (DoH-трафік) [6]. Генерація мережевої карти за допомогою NetworkX дозволяє візуально оцінити структуру мережі, що особливо корисно у великих корпоративних мережах із понад 50 пристроями [4].

Унікальність "Network Monitor" порівняно з існуючими рішеннями, такими як Wireshark або SolarWinds, полягає в інтеграції машинного навчання для автоматичного виявлення аномалій, що зменшує навантаження на адміністратора, на відміну від Wireshark, орієнтованого на ручний аналіз пакетів [5]. Додаток вирізняється легкістю та кросплатформністю, працюючи на Windows, Linux і macOS без складного встановлення, на відміну від більш важких рішень, таких як SolarWinds, які потребують значних ресурсів [10]. Адаптивний інтерфейс із логотипом і темною темою відповідає сучасним стандартам дизайну, покращуючи користувацький досвід. Підтримка SQLite для історичних даних дозволяє проводити довгостроковий аналіз, що відрізняє додаток від багатьох легких інструментів [6].

Тестування додатка проводилося в корпоративній мережі з 30 пристроями протягом 48 годин. Середня швидкість передачі даних склала 5 МБ/с із піковими значеннями до 12 МБ/с, було зафіксовано 1498 DNS-запитів, із них 10% класифіковано як підозрілі (DoH-трафік). Модель машинного навчання виявила 15 потенційних збоїв із точністю 85%, а згенерована мережева карта показала 32 вузли із коректним відображенням зв'язків. У майбутньому планується розширення функціоналу додатка, зокрема інтеграція складніших моделей машинного навчання, таких як LSTM, для прогнозування трафіку на основі часових рядів [5], підтримка експорту даних у формати CSV і PDF для спрощення звітності [7], реалізація хмарного зберігання даних для підтримки розподілених мереж [6], а також покращення інтерфейсу з додаванням інтерактивних графіків через бібліотеки, такі як Plotly [4].

"Network Monitor" є потужним інструментом для моніторингу та управління мережами, який поєднує сучасні технології програмування та функціонал, затребуваний мережевими адміністраторами. Його унікальність полягає в інтеграції машинного навчання, легкості, підтримці історичних даних та адаптивному інтерфейсі з логотипом, що робить його цінним рішенням для освітніх, корпоративних і дослідницьких цілей. Подальший розвиток додатка, зокрема впровадження прогнозування та хмарних технологій, посилить його позиції на ринку інструментів мережевого моніторингу.

Список використаних джерел

1. Cisco. Annual Internet Report (2020–2023). Cisco Systems, 2022. URL: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report.html
2. Lundh F. An Introduction to Tkinter. 2021. URL: https://www.pythonware.com/library/tkinter/introduction/
3. Paxson V. Bro: A System for Detecting Network Intruders in Real-Time. Computer Networks, 2020. Vol. 31. P. 2435–2463. URL: https://www.icir.org/vern/papers/bro-CN99.pdf
4. Hagberg A., Schult D., Swart P. Exploring Network Structure, Dynamics, and Function using NetworkX. Proceedings of the 7th Python in Science Conference, 2021. P. 11–15. URL: https://networkx.github.io/documentation/
5. Pedregosa F., et al. Scikit-learn: Machine Learning in Python. Journal of Machine Learning Research, 2021. Vol. 12. P. 2825–2830. URL: http://jmlr.csail.mit.edu/papers/v12/pedregosa11a.html
6. SQLite Consortium. SQLite Documentation. 2022. URL: https://www.sqlite.org/docs.html
7. Gamma E., et al. Design Patterns: Elements of Reusable Object-Oriented Software. Addison-Wesley, 2020. URL: https://www.pearson.com/store/p/design-patterns-elements-of-reusable-object-oriented-software/P100000260317
8. Beazley D. Python Essential Reference. 4th Edition, Addison-Wesley, 2021. URL: https://www.informit.com/store/python-essential-reference-9780134276502

9. Python Software Foundation. Logging Cookbook. 2022. URL: https://docs.python.org/3/howto/logging-cookbook.html
10. SolarWinds. Network Performance Monitor Overview. 2022. URL: https://www.solarwinds.com/network-performance-monitor

Ключові слова: мережевий моніторинг, аналіз трафіку, адміністрування, Scapy, NetworkX, Tkinter, SQLite, RandomForestClassifier, інформаційні технології

Keywords: network monitoring, traffic analysis, administration, Scapy, NetworkX, Tkinter, SQLite, RandomForestClassifier, information technology

МЕТОДИ КОДУВАННЯ КАТЕГОРІАЛЬНИХ ОЗНАК У ЗАДАЧАХ МАШИННОГО НАВЧАННЯ

Лобода Юлія

доцент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»
кандидат педагогічних наук, доцент

У прикладних задачах машинного навчання значна частина вхідних ознак має категоріальний характер. До таких ознак належать, зокрема, назви країн, типи товарів, статуси клієнтів або дні тижня. Оскільки більшість алгоритмів машинного навчання працюють лише з числовими даними, категоріальні ознаки потребують попередньої трансформації у числовий формат, що відомо як процес кодування (encoding).

Кодування категоріальних ознак є критично важливим етапом препроцесінгу даних. Неправильне кодування може призвести до втрати інформації або до погіршення якості моделі [1].

Відповідно до типу, категоріальні ознаки поділяють на:

• номінативні (номінальні) – ознаки, які не мають природного порядку. Наприклад: «red», «green», «blue»;

• порядкові (ординаційні) – це ознаки, які мають логічну послідовність або ранг. Наприклад: «low», «medium», «high».

Вибір методу кодування залежить від типу ознаки та особливостей задачі.

Основні методи кодування [2]:

One-Hot Encoding – метод, який є найбільш поширеним для номінативних змінних. Він створює окремий стовпець для кожного унікального значення категорії, заповнюючи його 0 або 1. Такий підхід виключає появу штучного порядку між категоріями, але може призвести до значного збільшення розмірності даних при великій кількості категорій.

Ordinal Encoding використовується для порядкових змінних, де між категоріями існує логічна послідовність. Кожна категорія отримує унікальне ціле число відповідно до її порядку. Однак такий підхід може бути некоректним для номінативних змінних, оскільки вводить неіснуючу ординальність [3].

Label Encoding схожий на Ordinal Encoding, але зазвичай застосовується для кодування цільових змінних або для ознак із невеликою кількістю категорій. Кожній категорії призначається унікальне ціле число. Недоліком є ризик створення хибної ієрархії між категоріями.

Binary Encoding поєднує переваги Label Encoding та One-Hot Encoding. Категорії спочатку кодуються цілими числами, а потім переводяться у двійковий формат, де кожен біт стає окремим стовпцем. Метод ефективний для ознак із великою кількістю категорій.

Target Encoding (Mean Encoding) Кожна категорія замінюється середнім значенням цільової змінної для спостережень цієї категорії. Метод підходить для моделей, чутливих до масштабування, але може призвести до переобучення, якщо не використовувати регуляризацію та крос-валідацію.

Frequency Encoding категорії замінюються частотою їх появи у колонці. Метод простий у реалізації та може бути ефективним для ознак із великою кількістю значень.

Вибір методу кодування – це компроміс між точністю, інтерпретованістю, обчислювальною ефективністю і здатністю моделі до узагальнення [4]. Найкращий підхід визначається експериментально з урахуванням специфіки даних та задачі. Вибір методу кодування залежить від кількох факторів:

- типу змінної (номінальна чи порядкова);
- кількості категорій (низька чи висока кардинальність);
- чутливості моделі до масштабування (наприклад, дерева рішень менш чутливі, ніж лінійні моделі);
- обсягу даних і можливості перехресної валідації.

Неправильне кодування може:

- знизити точність моделі;
- призвести до переобучення (особливо при Target Encoding);
- створити упередження, якщо кодування залежить від цільової змінної.

Для уникнення таких проблем часто використовують:

- крос-валідаційне цільове кодування;
- регуляризацію при Target Encoding;
- поєднання кількох методів (наприклад, OHE для ознак з малою кардинальністю, а Target Encoding – для інших) [5].

Кодування категоріальних ознак є важливою складовою етапу підготовки даних для машинного навчання. Жоден із методів не є універсальним: вибір оптимального способу залежить від контексту задачі, характеристик даних і типу моделі.

Для базових задач доцільно використовувати One-Hot Encoding, а для складніших комбіновані або регуляризовані методи. Важливо експериментувати з різними підходами та оцінювати їхній вплив на якість прогнозування.

Список використаних джерел

1. Douglass, Michael. Hands-on Machine Learning with Scikit-Learn, Keras and Tensorflow. *Physical and Engineering Sciences in Medicine*. Book Review: 2nd edition by Aurélien Géron: O' Reilly Media, 2019, 600 p. DOI: http://dx.doi.org/10.1007/s13246-020-00913-z.
2. Brownlee, J. Why One-Hot Encode Data in MachineLearning. Retrieved from URL: https://surli.cc/bzafff
3. Samuels, Jamell. One-Hot Encoding and Two-Hot Encoding: An Introduction? 2024. DOI: http://dx.doi.org/10.13140/RG.2.2.21459.
4. Category Encoders. URL: https://contrib.scikit-learn.org/category_encoders/
5. Categorical Variables. URL: https://surl.li/rxqfkg

Ключові слова: дані, підготовка даних, категоріальні ознаки, методи кодування, машинне навчання, One-Hot Encoding.

Keywords: data, data preprocessing, categorical features, encoding methods, machine learning, One-Hot Encoding.

ПРОГНОЗУВАННЯ РЕЗУЛЬТАТІВ СПОРТИВНИХ ПОДІЙ МЕТОДАМИ МАШИННОГО НАВЧАННЯ

Луценко Ганна

студентка 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сучасний спорт, зокрема футбол, є не лише частиною культури, а й важливим елементом глобальної індустрії, пов'язаної з беттингом [1] та аналітикою. Точне прогнозування результатів матчів має значний практичний інтерес для букмекерських компаній, спортивних аналітиків та шанувальників гри. Традиційні методи прогнозування часто ґрунтуються на суб'єктивних оцінках або простих статистичних моделях, які не враховують усієї складності факторів, що впливають на результат. У цьому контексті методи машинного навчання [2], особливо глибокого навчання [3], пропонують нові можливості для аналізу великих обсягів даних та підвищення точності прогнозів.

Загальний алгоритм такої системи прогнозування представлений на рис. 1.

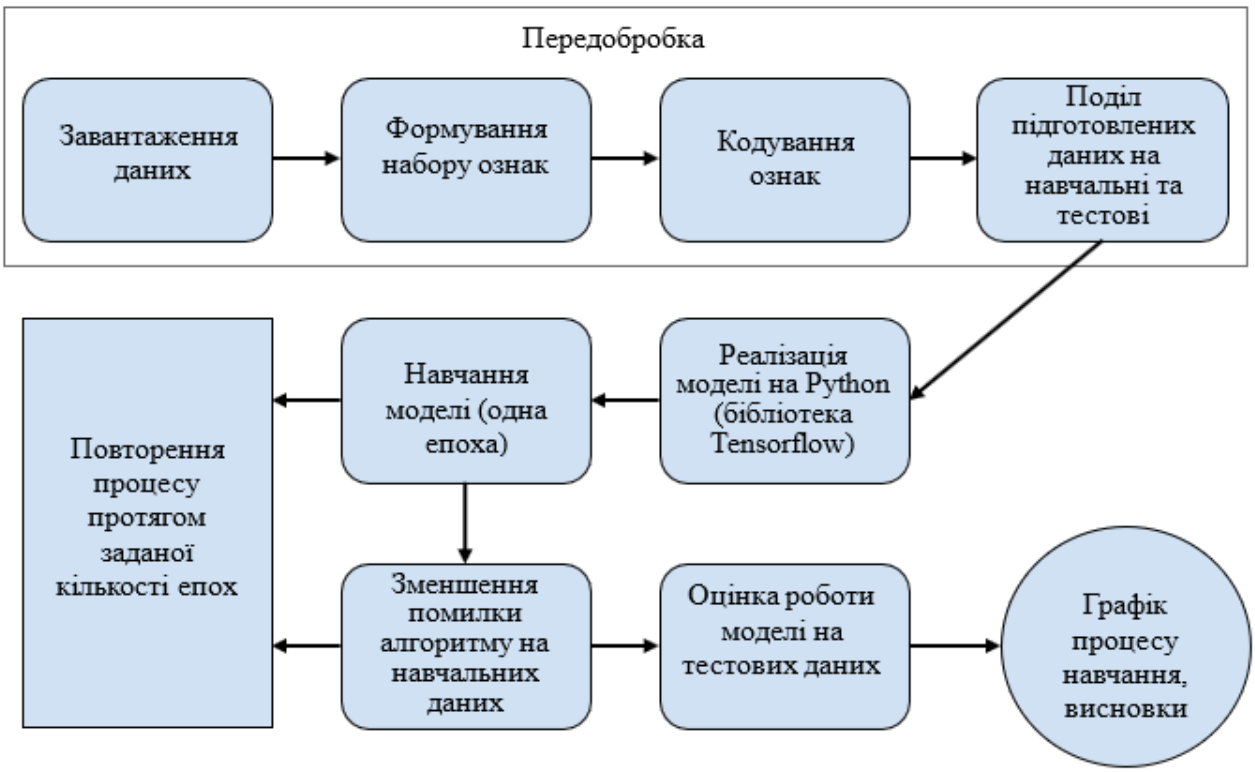

Рисунок 1 – Загальний алгоритм системи прогнозування

Основу запронованого рішення складає застосування рекурентних нейронних мереж (RNN) з архітектурою Long Short-Term Memory (LSTM) [4]. Ця модель була обрана через її здатність аналізувати часові послідовності, що є критично важливим для врахування динаміки результатів команд у часі. Модель отримує на вхід вектор ознак, який включає такі дані, як кількість забитих і пропущених голів, результати минулих матчів, різниця в очках між командами та інші статистичні показники. Вихід моделі – ймовірність перемоги домашньої команди або іншого результату (нічия або перемога гостей).

Навчання мережі проводилося на відкритих даних [5] англійської Прем'єр-ліги. Дані були попередньо оброблені: нормалізовані, закодовані за допомогою методів бібліотеки scikit-learn та розділені на навчальну та тестову вибірки з урахуванням часової послідовності. Для оптимізації моделі використовувався алгоритм Adam, а як функція втрат – перехресна ентропія.

Експерименти показали, що модель досягає точності 98.11% на навчальних даних та 80.75% на тестових (рис.2). Цей результат перевищує показники інших методів, описаних у літературі, таких як логістична регресія (69.5%) або прості нейронні мережі (65%). Графіки залежності функції втрат та точності від кількості епох навчання (рис.3) демонструють стабільну збіжність моделі, що підтверджує її ефективність.

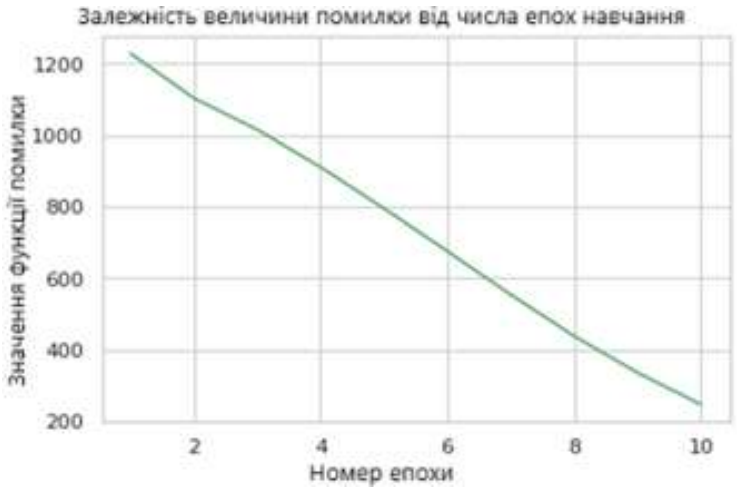

Рисунок 2 – Графік залежності значення функції помилки від епох навчання

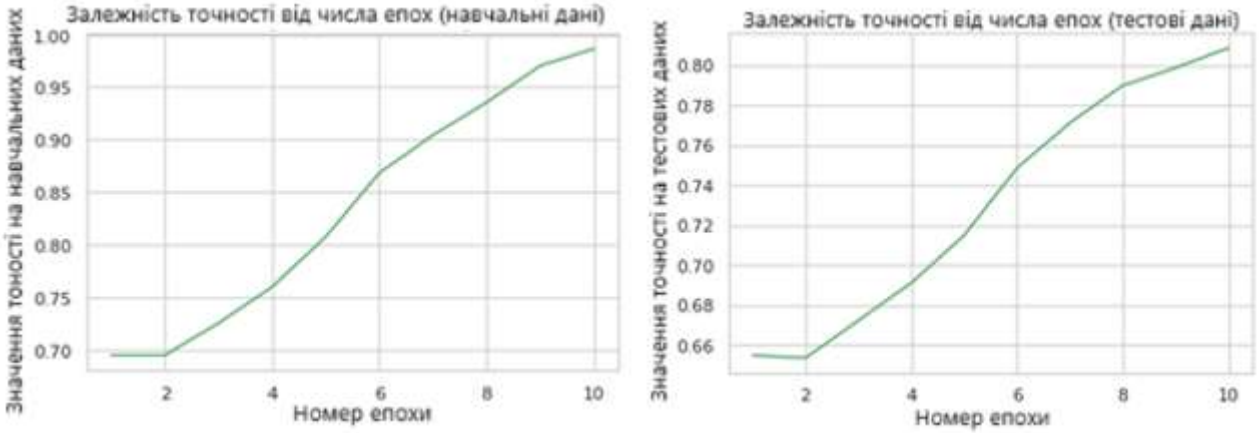

Рисунок 3 – Графіки точності прогнозування в залежності від кількості епох навчання

Застосування LSTM-мереж для прогнозування результатів футбольних матчів довело свою ефективність, зокрема завдяки врахуванню часової залежності даних. Однак існують напрями для подальшого вдосконалення моделі, такі як включення додаткових ознак (наприклад, статистики окремих гравців або зовнішніх факторів, як-от погода) та використання більш обширних наборів даних. Це дозволить ще більше підвищити точність прогнозів та розширити застосування моделі в реальних умовах.

Машинне навчання відкриває нові горизонти для спортивної аналітики. Подальші дослідження можуть спрямувати зусилля на інтеграцію мультимодальних даних (наприклад, відеоаналітику) або розробку адаптивних моделей, які враховуватимуть зміни в правилах гри або стратегіях команд. Ці інновації можуть стати основою для нових інструментів, які перетворять спосіб аналізу та прогнозування у спортивній галузі.

Список використаних джерел

1. Football betting – the global gambling industry worth billions. URL: https://www.bbc.com/sport/football/24354124

2. Prasetio, D. Predicting football match results with logistic regression // In Advanced Informatics: Concepts, Theory, And Application (ICAICTA), 2016. IEEE.
3. Shin J., Gasparyan R. A Novel Way to Soccer Match Prediction, 2014 // Stanford University Department of Computer Science.
4. Understanding LSTMs. URL: https://colah.github.io/posts/2015-08- Understanding-LSTMs/
5. Football data. URL: https://www.football-data.co.uk/

Ключові слова: машинне навчання, прогнозування, LSTM, глибоке навчання.

Keywords: machine learning, forecasting, LSTM, deep learning.

Науковий керівник: доцент Манаков С.

АРХІТЕКТУРА ІНТЕЛЕКТУАЛЬНОГО ЧАТ-БОТА НА ОСНОВІ МАШИННОГО НАВЧАННЯ

Лобода Юлія

доцент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»
кандидат педагогічних наук, доцент

Якименко Дмитро

студент 4-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Типова архітектура сучасного інтелектуального чат-бота, що використовує методи машинного навчання, включає ключові компоненти для ефективної обробки запитів та забезпечення високоякісної взаємодії з користувачем. Основними з них є модуль розуміння природної мови (Natural Language Understanding, NLU), діалоговий менеджер та модуль генерації природної мови (Natural Language Generation, NLG).

Модуль розуміння природної мови приймає вхідний текст від користувача і за допомогою моделей машинного навчання, зокрема алгоритмів розпізнавання намірів (intent recognition), технології розпізнавання іменованих сутностей (Named Entity Recognition, NER) та аналізу тональності (sentiment analysis), перетворює його у структуроване представлення. Наприклад: {намір: "замовити_товар", сутності: {товар: "піца", розмір: "велика"}} [1].

Сучасні методи векторного представлення слів, таких як Word2Vec, GloVe та речень, наприклад, Universal Sentence Encoder, BERT дозволяють виявляти семантичні зв’язки навіть у випадках нетрадиційного формулювання , що є основою для глибокого аналізу тексту.

Діалоговий менеджер отримує структуроване представлення від модуля NLU, враховує поточний стан діалогу (контекст, історію). Він відповідає за

ухвалення рішень щодо подальших дій: формулювання відповіді, запит додаткової інформації або виконання зовнішніх операцій (наприклад, звернення до баз даних або виклик API) [2]. Для реалізації логіки діалогового менеджера можуть використовуватися як класичні алгоритмічні підходи (кінцеві автомати, фреймворки на основі правил), так і передові алгоритми машинного навчання, зокрема методи навчання з підкріпленням (Reinforcement Learning) чи глибокого навчання.

Модуль генерації природної мови трансформує внутрішнє, структуроване представлення відповіді, отримане від діалогового менеджера, у текстовий формат, природний для користувача [3]. Реалізація цього модуля може базуватися як на заповненні попередньо визначених шаблонів, так і на динамічній генерації тексту за допомогою сучасних генеративних моделей, наприклад, на основі архітектури Трансформер [4].

Ефективна робота всіх зазначених модулів значною мірою залежить від якості векторних представлень тексту, які дозволяють системі глибоко розуміти семантику запитів та генерувати узгоджені відповіді.

Інтеграція методів машинного навчання у чат-боти надає низку суттєвих переваг: покращене розуміння природної мови, персоналізацію взаємодії, здатність до навчання та адаптації, обробку складних запитів, масштабованість та ефективність.

Покращене розуміння природної мови. Сучасні моделі дозволяють ботам інтерпретувати широкий спектр мовних конструкцій, враховуючи сленг, помилки та синонімію.

Персоналізація взаємодії. Аналіз історії спілкування та даних користувача дає адаптувати стиль, тон і зміст відповідей, , роблячи взаємодію більш релевантною та ефективною.

Здатність до навчання та адаптації. Системи, що навчаються на нових вхідних даних, можуть покращувати свою точність та розширювати функціональність без необхідності частих змін у програмному коді.

Обробка складних запитів. Застосування ймовірнісних підходів та глибокого навчання дозволяє ефективніше вирішувати завдання, що виходять за межі жорстко заданих правил.

Масштабованість та ефективність. Після початкового етапу навчання бот здатний обробляти велику кількість запитів одночасно, що знижує навантаження на операторів та забезпечує цілодобову доступність сервісу.

Попри на значні переваги, інтеграція методів машинного навчання в чат-боти також ставить певні виклики. Якісні та великі обсяги розмічених даних є критично важливими для навчання ефективних моделей машинного навчання. Збір, підготовка та розмітка цих даних можуть бути дорогими та трудомісткими процесами. Таким чином, їх недостатність або низька якість призводить до зниження точності та обмеження можливостей бота. Навіть передові моделі можуть демонструвати низьку продуктивність при обробці запитів, що суттєво

відрізняються від навчального набору (out-of-distribution data). Окрім того, створення, підтримка та оновлення інтелектуальних чат-ботів вимагає спеціалізованих знань в галузі машинного навчання та значних обчислювальних ресурсів.

Інтеграція методів машинного навчання є фундаментальним кроком у розвитку чат-ботів, що перетворює їх із простих автоматизованих систем на інтелектуальних співрозмовників. Сучасні алгоритми, які забезпечують глибоке розуміння природної мови та генерування тексту, дозволяють чат-ботам надавати персоналізовані й релевантні відповіді, а також вдосконалювати свої можливості через навчання на основі накопичених даних. Хоча перед розробниками стоїть низка викликів, сучасні наукові досягнення та технологічний поступ дають підстави очікувати появу інноваційних рішень, що підвищать ефективність взаємодії людини з технологіями.

Список використаних джерел

1. What is natural language understanding (NLU)? URL: https://surl.li/qatiap
2. Murphy K. Reinforcement Learning: A Comprehensive Overview, eprint arXiv:2412.05265. 2024. DOI: https://doi.org/10.48550/arXiv.2412.05265.
3. Tripathi, D. R. ., Tamrakar, A. Natural Language Generation: Algorithms and Applications. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *9*(3), 1394–1399. 2018. URL: https://surl.lu/rjzizf.
4. Козлов С.Л., Колесницький О.К. Застосування архітектури Трансформер до задачі super-resolution. *Наукові праці Вінницького національного технічного університету*. 1, 2024. DOI: https://doi.org/10.31649/2307-5376-2024-1-7-18.

Ключові слова: чат-бот, інтелектуальний чат-бот, машинне навчання, природна мова, набори даних

Keywords: chatbot, intelligent chatbot, machine learning, natural language, datasets

СОЦІАЛЬНІ МЕРЕЖІ ТА ЇХ ВПЛИВ НА ПСИХІЧНЕ ЗДОРОВ'Я ПІДЛІТКІВ

Бурдіян Віталіна

студентка 1-го курсу факультету психології, політології та соціології Національного університету "Одеська юридична академія"

У наш час соціальні мережі стали невід'ємною частиною повсякденного життя, особливо серед підлітків. Ці платформи відіграють важливу роль у процесах соціалізації, самовираження, обміну інформацією, отримання підтримки, а також у формуванні ідентичності. Водночас зростає занепокоєння щодо їхнього впливу на психічне здоров'я молоді. Актуальність цієї теми зумовлена широким розповсюдженням цифрових технологій, зростанням частоти використання соціальних медіа та недостатнім рівнем усвідомлення їхніх наслідків. Метою цієї тези є всебічне вивчення як негативних, так і позитивних аспектів впливу

соціальних мереж на психічне здоров'я підлітків, а також пошук ефективних механізмів регулювання цього впливу.

Період підліткового віку – це критичний етап становлення особистості, коли формуються емоційна стійкість, самооцінка та система цінностей. У цей час особливо важливою стає потреба в соціальному схваленні та належності до певної групи. Саме тому підлітки є вразливою категорією користувачів соціальних мереж. Вони схильні до постійного порівняння себе з іншими, орієнтуючись на ідеалізовані образи, що часто призводить до психологічного дискомфорту. Наукові дослідження свідчать, що надмірне використання соціальних мереж корелює з підвищеним рівнем тривожності, депресії, незадоволеністю власною зовнішністю та соціальною ізоляцією [1].

Особливо гострою проблемою є вплив соціальних мереж на порушення сну. Постійне використання гаджетів у вечірній та нічний час знижує якість сну, спричиняє хронічну втому, дратівливість, зниження когнітивних функцій і, як наслідок, негативно позначається на емоційному стані підлітків. Також у дослідженнях зазначається, що соціальні мережі можуть стати джерелом тривалого стресу через постійний потік інформації, необхідність бути «онлайн», страх упустити важливу подію (FOMO – fear of missing out) [1].

Окремим аспектом впливу соціальних мереж є кібербулінг – агресивна поведінка у віртуальному середовищі, яка може мати серйозні наслідки для психічного здоров'я жертв. Підлітки, які зазнають кібербулінгу, частіше демонструють ознаки депресії, емоційного вигорання, мають знижений рівень довіри до оточення, у деяких випадках – суїцидальні думки [2]. Проблема ускладнюється тим, що кібербулінг часто відбувається анонімно, а отже – потерпілі мають обмежені ресурси для захисту та протидії.

Водночас, соціальні мережі не слід розглядати виключно як джерело загроз. Вони мають і значний позитивний потенціал, який, за належного підходу, може бути використаний для розвитку особистості. Платформи, орієнтовані на взаємну підтримку, сприяють налагодженню соціальних зв'язків, зменшенню почуття самотності, підвищенню самооцінки. Підлітки можуть знайти онлайн-спільноти за інтересами, отримати зворотний зв'язок, ділитися творчістю, досвідом, переживаннями. Деякі соціальні мережі стали ефективними каналами поширення інформації про психічне здоров'я, зокрема про боротьбу з тривожністю, депресією, шкідливими звичками, стигматизацією психічних розладів [3].

З огляду на вищезазначене, постає необхідність формування культури відповідального використання соціальних мереж. Першочерговими є впровадження програм цифрової грамотності у шкільну освіту, проведення тренінгів для молоді, розробка інформаційних кампаній. Ці ініціативи мають на меті не лише формування навичок критичного мислення, а й розвиток емоційної компетентності, вміння розпізнавати загрози, регулювати власні емоції та шукати допомоги у разі потреби.

Роль дорослих – батьків, вчителів, психологів – у цьому процесі є визначальною. Вони мають підтримувати відкритий діалог із підлітками, виявляти ознаки психологічного дискомфорту, бути прикладом здорового ставлення до цифрових технологій. Батьки повинні контролювати, але не обмежувати, надавати підтримку, а не осуд. Важливо також, щоб дорослі самі володіли знаннями про ризики онлайн-простору та вміли адекватно реагувати на виклики, що постають у процесі цифрового соціального розвитку підлітків [4].

На державному рівні актуальним є питання розробки нормативних документів, які б регулювали інформаційну політику в соціальних мережах, запобігали поширенню деструктивного контенту та захищали неповнолітніх від шкідливого впливу. Варто розглянути можливості співпраці з цифровими платформами для створення безпечного цифрового середовища для дітей та підлітків.

Отже, соціальні мережі є невід'ємною частиною сучасного соціального ландшафту підлітків. Вони несуть як можливості, так і ризики для психічного здоров'я. Завданням суспільства є не лише зменшення негативного впливу, а й трансформація цифрового простору у сприятливе середовище для особистісного розвитку, підтримки та самореалізації молоді.

Список використаних джерел

1. Twenge, J. M., Joiner, T. E., Rogers, M. L., & Martin, G. N. (2018). Increases in depressive symptoms, suicide-related outcomes, and suicide rates among U.S. adolescents after 2010 and links to increased new media screen time. Clinical Psychological Science, 6(1), 3–17 URL https://journals.sagepub.com/doi/full/10.1177/2167702617723376
2. Hinduja, S., & Patchin, J. W. (2019). Connecting adolescent suicide to the severity of bullying and cyberbullying. Journal of School Violence, 18(3), 333–346 URL https://doi.org/10.1080/15388220.2018.1492417
3. Naslund, J. A., Aschbrenner, K. A., Marsch, L. A., & Bartels, S. J. (2016). The future of mental health care: peer-to-peer support and social media. Epidemiology and Psychiatric Sciences, 25(2), 113–122 URL https://www.cambridge.org/core/journals/epidemiology-and-psychiatric-sciences/article/future-of-mental-health-care-peertopeer-support-and-social-media/DC0FB362B67DF2A48D42D487ED07C783
4. Livingstone, S., & Helsper, E. J. (2007). Gradations in digital inclusion: Children, young people and the digital divide. New Media & Society, 9(4), 671–696 URL https://www.researchgate.net/publication/30522837_Gradations_in_digital_inclusion_children_young_people_and_the_digital_divide

Ключові слова: соціальні мережі, підлітки, психічне здоров'я, депресія, тривожність, кібербулінг, цифрова грамотність, самооцінка, емоційна стійкість, цифрове середовище

Keywords: social media, adolescents, mental health, depression, anxiety, cyberbullying, digital literacy, self-esteem, emotional resilience, digital environment

Науковий керівник: доцент Чанишев Р.

ЯК МОБІЛЬНІ ДОДАТКИ МОЖУТЬ ВИКОРИСТОВУВАТИСЯ ДЛЯ ВІДСТЕЖЕННЯ ЕМОЦІЙНОГО СТАНУ ПАЦІЄНТІВ, НАДАННЯ ЇМ СВОЄЧАСНОЇ ПІДТРИМКИ ТА ЗАПОБІГАННЯ РЕЦИДИВАМ ДЕПРЕСИВНИХ ЕПІЗОДІВ

Алексейчук Любов

студентка 1-го курсу факультету психології політології та соціології, Національного університету «Одеська юридична академія»

Питання психічного здоров'я стає особливо актуальним у суспільстві через зростання кількості випадків депресивних розладів і тривожних станів серед представників різних соціальних груп. За даними ВООЗ, депресія є однією з основних причин інвалідності у світі, що свідчить про необхідність пошуку нових підходів до її профілактики, моніторингу та лікування [1].

Важливе місце у цій сфері посідають мобільні додатки для відстеження емоційного стану, які стають не лише засобом самоспостереження, але й платформою для своєчасної психологічної підтримки. Останніми роками мобільні технології все більше інтегруються у практику психічного здоров'я. Розвиток додатків, що дозволяють відслідковувати настрій, рівень стресу, тривожність, сон та інші психоемоційні показники, відкриває нові можливості для своєчасної діагностики депресивних станів та запобігання їх загостренням. Дослідження свідчать, що регулярне використання таких додатків дозволяє людині краще усвідомлювати власний емоційний стан, відслідковувати тригери, а також своєчасно звернутися за допомогою [2].

Особливої актуальності ця тема набуває в Україні, де, згідно з даними Центру громадського здоров'я МОЗ України, у 2022 році близько 20% населення відчували симптоми депресії та тривожності [3].

У таких умовах мобільні додатки стають доступним та економічно ефективним інструментом для населення, що не має можливості систематично звертатися до фахівців. Додатки на кшталт «Moodpath», «Wysa», «BetterMe: Mental Health» пропонують інтерактивні щоденники настрою, вправи з самодопомоги, когнітивно-поведінкову терапію, а також функцію негайного зв'язку з психологом або чат-ботом.

Однією з головних переваг використання мобільних додатків у сфері психічного здоров'я є можливість безперервного моніторингу стану пацієнта в реальному часі. У свою чергу, автоматизовані нагадування про необхідність виконання психологічних вправ чи консультацій з фахівцем зменшують ризик рецидиву депресивного епізоду.

Разом з тим, необхідно враховувати виклики та обмеження використання таких додатків. Дослідники наголошують, що мобільні додатки не можуть повністю замінити роботу з психотерапевтом, проте є важливим доповненням до традиційних методів терапії.

Сучасне суспільство перебуває у стані постійного стресу, що пов'язано з багатьма соціально-економічними та політичними викликами. Психічне здоров'я стає пріоритетною сферою охорони здоров'я, оскільки депресивні та тривожні розлади щороку вражають мільйони людей. Водночас доступність якісної психологічної допомоги залишається обмеженою через нестачу фахівців, фінансові труднощі та стигматизацію.

У цих умовах мобільні додатки набувають важливого значення як інструмент профілактики, діагностики та підтримки емоційного стану пацієнтів. Їхнє використання дозволяє здійснювати безперервний моніторинг психічного стану, надавати своєчасну підтримку та запобігати розвитку або рецидивам депресивних епізодів.

Моніторинг психоемоційного стану є критично важливим у процесі лікування та профілактики депресії. Своєчасне виявлення змін настрою, зниження мотивації, підвищеного рівня тривожності чи симптомів апатії дозволяє вчасно втручатися та коригувати терапію. Традиційні методи моніторингу, як-от візити до психолога або психіатра, мають обмежену частоту та потребують значних ресурсів.

У свою чергу, мобільні додатки забезпечують цілодобовий доступ до інструментів самоспостереження. Вони дозволяють користувачам щоденно фіксувати свої емоції, відстежувати тригери негативного настрою, отримувати миттєвий зворотний зв'язок.

Особливо актуальним є застосування мобільних додатків у роботі з підлітками, ветеранами, людьми похилого віку та пацієнтами з хронічними захворюваннями. Для цих категорій мобільні технології забезпечують безперервний доступ до психоемоційної підтримки, що значно підвищує ефективність терапевтичних заходів.

Переваги використання мобільних додатків:

- доступність: можливість отримати підтримку незалежно від місця перебування;
- конфіденційність: збереження приватності користувачів;
- інтерактивність: залучення користувачів до процесу самодопомоги;
- персоналізація: індивідуальні рекомендації на основі аналізу даних.

Водночас, існують і певні виклики, серед яких – потреба у забезпеченні високого рівня захисту персональних даних, необхідність стандартизації таких додатків, а також ризик заміщення професійної допомоги виключно цифровими рішеннями.

В Україні мобільні додатки для підтримки ментального здоров'я вже інтегруються у систему охорони здоров'я. Наприклад, застосунок «Ти як?» спрямований на психологічну підтримку українців під час війни, а також популяризуються сервіси для самодопомоги та профілактики емоційного вигорання [4].

У сучасному світі мобільні додатки стають важливим інструментом у системі охорони психічного здоров'я, забезпечуючи нові можливості для моніторингу

емоційного стану пацієнтів та надання їм своєчасної підтримки. Їхнє впровадження дозволяє зменшити бар'єри доступу до психологічної допомоги, сприяти ранньому виявленню депресивних симптомів та попереджувати розвиток рецидивів.

Особливо актуальним це є в умовах постійного зростання рівня стресу серед населення, впливу воєнних дій, економічної нестабільності та соціальних змін. Для багатьох користувачів мобільні додатки стають зручною альтернативою або доповненням до традиційних форм психотерапії, оскільки надають змогу отримувати допомогу конфіденційно, у зручний час та у звичному середовищі.

Проте важливо зазначити, що цифрові технології не можуть повністю замінити особистісну взаємодію з фахівцями, особливо у випадках тяжких форм депресії. Тому їх слід розглядати як додатковий інструмент комплексного підходу до лікування та профілактики психічних розладів. Використання мобільних додатків повинно супроводжуватися професійною підтримкою та бути інтегрованим у ширшу систему медичних і соціальних послуг.

Також надзвичайно важливою залишається проблема захисту персональних даних, етичного використання зібраної інформації та підвищення цифрової грамотності серед користувачів. Саме вирішення цих викликів дозволить максимально ефективно використати потенціал мобільних технологій для підтримки ментального здоров'я.

Отже, мобільні додатки є перспективним напрямом розвитку психічного здоров'я в Україні, який потребує подальших наукових досліджень, міждисциплінарного співробітництва та створення чіткої нормативно-правової бази.

Список використаних джерел

1. Depression and other common mental disorders: URL: https://surl.li/caekmb.
2. Health Tracking via Mobile Apps for Depression Self-management: Qualitative Content Analysis of User Reviews URL: https://humanfactors.jmir.org/2022/4/e40133.
3. Дворник М.С. Використання смартфон-застосунків в умовах психотравматизації населення *Інформаційні технології і засоби навчання*, 2019, Том 73, №5 URL: https://lib.iitta.gov.ua/id/eprint/719027/1/Dvornyk_ITTZN.pdf.
4. Всеукраїнська програма ментального здоров'я URL: https://surl.li/juhbnn.

Ключові слова: психічне здоров'я, депресивні розлади, моніторинг стану, профілактика, мобільні додатки, цифрові технології.

Keywords: mental health, depressive disorders, condition monitoring, prevention, mobile applications, digital technologies.

Науковий керівник: доцент Чанишев Р.

ПАРАСОЦІАЛЬНІ ЗВ'ЯЗКИ З ЧАТ-БОТАМИ

Кліменко Віра

студентка 1 курсу факультету психології, політології та соціології Національного університету «Одеська юридична академія»

У XXI столітті цифрові технології дедалі більше інтегруються в повсякденне життя людей, змінюючи способи комунікації та соціальної взаємодії. Одним із цікавих феноменів цифрової епохи стали парасоціальні зв'язки – особливий тип емоційного зв'язку, який виникає між користувачем і медіаперсонажем або віртуальним агентом. У сучасному контексті все частіше йдеться про формування таких зв'язків з чат-ботами – штучними співрозмовниками, створеними на основі алгоритмів машинного навчання та обробки природної мови.

Парасоціальні зв'язки почали вивчатися ще у 1950-х роках у межах телекомунікаційних досліджень. Тоді дослідники Дональд Гортон і Річард Волл виявили, що глядачі телевізійних шоу формують ілюзію дружби з ведучими та персонажами [1]. Ці взаємодії не є взаємними, але можуть викликати глибокі емоції. У сучасному світі, де чат-боти стали частиною повсякденного життя, спостерігається перенесення цього типу зв'язку на взаємодію з віртуальними агентами, зокрема у таких застосунках, як Replika, ChatGPT, Character.AI та ін.

Чат-боти, особливо ті, що використовують штучний інтелект, здатні вести діалог, підтримувати розмову, надавати емоційно забарвлені відповіді та навіть «виявляти» турботу. Завдяки цьому з'являється ефект присутності, а згодом – відчуття зв'язку. Така взаємодія особливо притаманна людям, які шукають підтримки, страждають від самотності або мають труднощі у побудові міжособистісних контактів. У дослідженнях Microsoft і OpenAI зафіксовано, що користувачі іноді щодня ведуть емоційно значущі розмови з чат-ботами, діляться особистими переживаннями, очікуючи підтримки чи поради [2].

Парасоціальні зв'язки з чат-ботами мають як позитивні, так і потенційно ризиковані аспекти. До переваг можна віднести доступність емоційної підтримки, покращення психоемоційного стану, зниження рівня тривоги та самотності. Чат-боти, особливо ті, що імітують особистість або емоційний інтелект, можуть виступати як свого роду "віртуальні друзі", особливо в умовах ізоляції чи соціальних обмежень – як це спостерігалося під час пандемії COVID-19 [3].

Однак парасоціальні зв'язки з ботами можуть також призводити до залежності, викривлення соціального досвіду або уникання реальної міжособистісної взаємодії. Користувачі, що надто глибоко занурюються у спілкування з чат-ботами, можуть розвивати надмірну емоційну прив'язаність до об'єкта, що не здатний на справжню взаємність. Це викликає етичні питання: чи мають розробники попереджати користувачів про обмеження емоційного інтелекту ботів? Якою мірою бот повинен "прикидатися" співчутливим?

Дослідники також звертають увагу на роль дизайну й інтерфейсу в формуванні парасоціальних зв'язків. Візуальне оформлення, тон спілкування, персоналізація імені чи образу бота – усе це впливає на інтенсивність залучення користувача. Наприклад, у випадку додатка Replika користувачі можуть налаштовувати зовнішність бота, обирати стиль спілкування та навіть "будувати" з ним романтичні стосунки [4].

Ці процеси свідчать про поступове розширення меж того, що ми вважаємо соціальною взаємодією. Якщо раніше парасоціальні зв'язки розглядалися лише в контексті медіа, то сьогодні вони все більше зміщуються в зону штучного інтелекту та цифрових агентів. Це вимагає нових підходів до вивчення взаємин людини з технологією, а також розробки етичних, психологічних і соціологічних рамок для регулювання таких зв'язків.

Таким чином, парасоціальні зв'язки з чат-ботами – це складне, багатогранне явище, що відображає трансформації сучасного комунікативного простору. Вони можуть мати як терапевтичний, так і дезадаптаційний вплив на людину, залежно від обставин використання та глибини залучення. Подальші дослідження у цій сфері мають включати міждисциплінарний підхід, щоб забезпечити краще розуміння природи цифрової емоційної взаємодії.

Список використаних джерел

1. Бернацька Д. Л. Штучний інтелект і психологія. Чи може робот замінити психолога? ПОЛІТ. Сучасні проблеми науки. Гуманітарні науки : тези доповідей XXI Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих учених. Київ : Талком, 2021. С. 99–100. URL: https://er.nau.edu.ua/handle/NAU/52239
2. Impact of artificial intelligence (AI) on psychological and mental health promotion: An opinion piece / K. Oladimeji et al. New Voices in Psychology. 2023. Vol. 13. URL: https://doi.org/10.25159/2958-3918/14548
3. The impact of artificial intelligence on the tasks of mental healthcare workers: A scoping review / A. D. Rebelo et al. Computers in Human Behavior: Artificial Humans. 2023. Vol. 1, No. 2. Article 100008. URL: chbah.2023.100008
4. Salah M., Al Halbusi H., Abdelfattah F. May the force of text data analysis be with you: Unleashing the power of generative AI for social psychology research. Computers in Human Behavior: Artificial Humans. 2023. Vol. 1, No. 2. Article 100006. URL: https://doi.org/10.1016/ j.chbah.2023.100006

Ключові слова: парасоціальні зв'язки, чат-бот, емоційна взаємодія, штучний інтелект
Keywords: parasocial relationships, chatbot, emotional interaction, artificial intelligence

Науковий керівник: доцент Чанишев Р.

ВПЛИВ CHATGPT НА ТВОРЧІСТЬ: МОЖЛИВОСТІ ТА ВИКЛИКИ

Литвиненко Софія

студентка 1-го курсу факультету психології політології та соціології Національного університету «Одеська юридична академія»

У добу стрімкого розвитку цифрових технологій генеративний штучний інтелект (далі – ШІ) виступає потужним чинником трансформації багатьох сфер, зокрема творчості. Одним із найяскравіших прикладів використання ШІ є модель ChatGPT, яка активно використовується в освітньому, дослідницькому та креативному середовищі. Вона набула великої популярності завдяки здатності швидко генерувати тексти, ідеї, рішення та навіть вести змістовні діалоги з користувачами [1].

Зростаюча актуальність цього явища пояснюється тим, що креативність сьогодні є не лише інструментом у мистецтві, але й ключовим елементом у сфері науки, бізнесу, освіти, реклами та технологічних інновацій. Саме тому вивчення ролі ChatGPT у процесі творчості є важливим для розуміння перспектив розвитку людської уяви в епоху автоматизації [2].

ChatGPT – це мовна модель, створена компанією OpenAI на основі великих обсягів текстових даних. Вона здатна аналізувати контекст запиту користувача, будувати логічні зв'язки та пропонувати змістовні відповіді, що часто не відрізняються від тих, які міг би дати людина. Завдяки цим можливостям модель активно використовується у різних сферах – від обслуговування клієнтів до освітніх проектів, створення художніх творів і розробки маркетингових стратегій.

Однією з найважливіших переваг ChatGPT у контексті творчості є його здатність генерувати нові ідеї. Модель допомагає подолати так звані «творчі блоки», коли автор відчуває нестачу натхнення або не може знайти оригінальний підхід до проблеми. У таких ситуаціях ChatGPT виступає як «співавтор», який пропонує альтернативні варіанти розвитку сюжету, структуру тексту або візуальну концепцію.

Більше того, взаємодія з ChatGPT стимулює мислення користувача, змушуючи його переосмислювати власні ідеї та шукати нестандартні підходи. Це відбувається завдяки інтерактивній природі діалогу, що сприяє створенню нового знання шляхом співпраці між людиною і машиною.

Хоча ChatGPT може підвищити креативність окремих ідей, існує ризик зменшення різноманітності контенту, оскільки моделі можуть генерувати схожі ідеї, що призводить до уніфікації творчого продукту. Ефект підвищення креативності при використанні ChatGPT може бути тимчасовим. Після припинення використання моделі рівень креативності може повертатися до початкового стану, а створений контент залишатися уніфікованим [3].

На практиці ChatGPT знаходить широке застосування в написанні художніх і наукових текстів, створенні сценаріїв, дизайні маркетингових кампаній та інших

проектах, що вимагають креативного підходу. У літературі автори використовують цю модель для створення нових сюжетів, опису персонажів або діалогів. У маркетингу – для генерації слоганів, текстів рекламних оголошень, а також створення стратегічних концепцій для брендів.

Особливо цінним є те, що ChatGPT дозволяє користувачеві «вийти за межі» власного досвіду та мислення, відкриваючи нові горизонти та інтерпретації. Це може стати каталізатором інновацій у мистецтві, бізнесі й науці.

Попри безсумнівні переваги, використання ChatGPT у творчих процесах не позбавлене ризиків. Один із найважливіших викликів – це загроза втрати індивідуальної автентичності. Надмірна опора на автоматизовані інструменти може призвести до зниження рівня критичного мислення та ініціативності. Людина починає діяти за принципом «отримай відповідь і не став під сумнів», що суперечить самій суті креативності як глибоко індивідуального і самостійного процесу.

Крім того, модель, яка навчається на масивних обсягах текстів, має тенденцію відтворювати стереотипи та шаблони. Це може призводити до уніфікації стилю мислення, що в довгостроковій перспективі загрожує зниженням оригінальності в культурі та мистецтві.

Не менш важливими є етичні питання: використання результатів роботи ChatGPT у наукових чи художніх роботах викликає дискусії щодо авторства, достовірності джерел і меж застосування машинного тексту в академічному середовищі.

З огляду на вищесказане можна дати такі практичні рекомендації щодо використання ChatGPT для стимулювання креативності:

1. Інтеграція в освітній процес: Використання ChatGPT як інструменту для генерації ідей, обговорення альтернативних підходів та розвитку критичного мислення.

2. Підтримка індивідуального стилю: Заохочення студентів до адаптації та персоналізації згенерованого контенту для збереження унікальності.

3. Етичне використання: Розробка та впровадження політик щодо етичного використання ГШІ в академічному середовищі, включаючи питання авторства та плагіату.

Підсумовуючи викладене, можна зробити висновок, що ChatGPT є потужним і перспективним інструментом у сфері творчості. Він розширює можливості мислення, допомагає долати бар'єри, активізує інноваційний підхід і робить креативний процес більш доступним. Водночас його використання потребує виваженості, розуміння меж і постійного контролю за збереженням людської унікальності та самобутності.

Для досягнення гармонійного балансу важливо не тільки користуватися технологічними досягненнями, але й формувати навички критичного мислення, підтримувати власний творчий потенціал і дбати про етичну складову застосування ШІ. Однак його використання повинно бути обґрунтованим та етичним, з урахуванням можливих ризиків та обмежень.

Подальші дослідження мають бути спрямовані на розробку методики ефективної інтеграції ШІ в креативні проекти без шкоди для самовираження людини. Саме в такому підході полягає майбутнє симбіозу технологій і людської уяви.

Список використаних джерел

1. Byung Cheol Lee, Jaeyeon (Jae) Chung An empirical investigation of the impact of ChatGPT on creativity URL: https://surli.cc/myzuap.
2. Muhammad Abid Malik, Amjad Islam Amjad, Sarfraz Aslam, Abdulnaser Fakhrou Global insights: ChatGPT's influence on academic and research writing, creativity, and plagiarism policies URL: https://surl.li/xfzmqs.
3. Qinghan Liu, Yiyong Zhou, Jihao Huang, Guiquan Li When ChatGPT is gone: Creativity reverts and homogeneity persists URL: https://surl.li/fsoymy.

Ключові слова: ChatGPT, креативність, штучний інтелект, генерація ідей, творчі завдання, креативне мислення, продуктивність, самостійність мислення

Keywords: ChatGPT, creativity, artificial intelligence, idea generation, creative tasks, creative thinking, productivity, independent thinking

Науковий керівник: доцент Чанишев Р.

ЦИФРОВА ПЛАТФОРМА TIKTOK ЯК ПЕРЕХРЕСТЯ РИЗИКІВ ДЛЯ СУСПІЛЬСТВА

Чанишев Рашид

доцент кафедри інформаційних технологій,
Національного університету «Одеська юридична академія»,
кандидат юридичних наук, доцент

Серед усіх сервісів інтернету платформа коротких відео TikTok є своєрідним феноменом, оскільки пов'язана з цілим комплексом найрізноманітніших проблем: кібербезпеки, психологічних, політичних, соціальних і правових одночасно.

Популярність мережі Інтернет з моменту її появи була зумовлена не тільки можливістю легкого доступу до інформації як такої, а й можливістю спілкування користувачів мережі один з одним. Спочатку для цих цілей використовували електронну пошту, потім її послідовно доповнили ньюс-конференції, інтернет-форуми та соціальні мережі.

При цьому постійно спрощувався процес отримання і сприйняття інформації, що в кінцевому підсумку призвело до появи сервісів коротких відео, наприклад, таких, як TikTok (цей сервіс було вперше запущено у вересні 2016 року).

Перегляд коротких відео є найпростішим способом отримання інформації, що не вимагає будь-яких спеціальних знань. Ця властивість призвела до того, що

сервіс TikTok набув величезної популярності, кількість його користувачів вимірюється мільярдами, і в деяких країнах 95% користувачів Інтернет користуються послугами цього сервісу [1]. При цьому користувачами сервісу є як підлітки, так і досить дорослі люди, що загалом не характерно для інтернет-сервісів, які зазвичай мають чітку вікову орієнтацію [2].

Така незвичайна популярність цього способу отримання інформації не могла не привернути увагу вчених. У результаті проведених досліджень з'ясувалося, що перегляд коротких відео спричиняє негативні фізичні та психологічні наслідки, такі, як порушення сну, емоційні розлади (депресія, тривожність, стрес) та проблеми зі сприйняттям і запам'ятовуванням інформації (неможливість зосередитися на одній темі довше ніж 47 секунд). Крім того, з'ясувалося, що регулярний перегляд коротких відео викликає і фізичні зміни у фронтальній корі та мозочку людського мозку [3].

Такі результати досліджень викликають занепокоєння не тільки у медиків, але й у політиків. Так, наприклад, сервісом TikTok користуються близько 125 мільйонів жителів ЄС, і різноманітні негативні наслідки популярності цього сервісу можуть бути досить значними.

Крім безпосереднього впливу на здоров'я людини, регулярний перегляд коротких відео (зміст яких завжди пов'язаний із чимось, що викликає миттєвий інтерес) впливає і на сприйняття реклами, зокрема непрямої та політичної. Крім того, зміст відео може призводити до розкриття персональних даних та створювати проблеми безпеки неповнолітніх.

У зв'язку з тим, що останніми роками в ЄС були ухвалені нові регулюючі норми (такі як DSA – Акт про цифрові послуги, та GDPR – Загальний регламент захисту даних), з 2021 року почались перевірки платформи TikTok на відповідність вимогам європейського законодавства.

Так, у лютому 2021 року Європейська організація споживачів BEUC звинуватила TikTok у низці порушень прав споживачів, зокрема у публікації прихованої реклами, розрахованої на дітей. У червні 2021 року Єврокомісія спільно з CPC (Consumer Protection Cooperation Network) провела офіційне розслідування діяльності TikTok щодо можливого порушення законодавства про захист прав споживачів у Європейському Союзі. Це розслідування проводилося на підставі Регламенту (ЄС) 2017/2394 (про співпрацю щодо захисту споживчих прав), Директиви про недобросовісну комерційну практику (2005/29/ЕС) та Директиви про права споживачів (2011/83/EU).

Зокрема, було висунуто звинувачення у тому, що TikTok дозволяв рекламному контенту маскуватися під користувацькі відео, що помітно впливало на дитячу аудиторію. При цьому було спрощено реєстрацію для неповнолітніх. [4].

У результаті TikTok зобов'язався вдосконалити методи контролю за віком користувачів, додати функції батьківського контролю і запровадити ясне маркування комерційного контенту [5]. Розслідування було закрито, але деякі проблеми так і залишилися невирішеними [6].

Нове розслідування було розпочато у вересні 2021 року Ірландською комісією із захисту даних (DPC), яка є провідним органом контролю за дотриманням GDPR в ЄС. Предметом розслідувань стала обробка TikTok даних дітей та передача даних користувачів сервісу до Китаю.

У січні 2023 р. до TikTok було висунуто вимогу - привести умови користування платформою у відповідність з положеннями Акта про цифрові послуги (DSA). При цьому було підкреслено, що ситуація, коли за нешкідливими функціями ховається секундний доступ до небезпечного контенту, є абсолютно неприйнятною. Комісар ЄС Тьєррі Бретон у зв'язку з цим заявив: «Ми не похитнемося застосувати весь спектр санкцій для захисту громадян, якщо перевірки покажуть недотримання правил» [7].

У лютому 2023 р. було виявлено і проблеми з кібербезпекою платформи TikTok. У зв'язку з цим Європейська комісія і Рада ЄС розпорядилися видалити TikTok зі службових телефонів своїх співробітників. Через кілька днів аналогічне рішення ухвалив і Європейський парламент, після чого аналогічні обмеження запровадили уряди Бельгії, Франції та низки інших країн ЄС.

У січні 2023 р. TikTok був оштрафований французьким регулятором CNIL на €5 млн за порушення правил про відмову від файлів cookie. У вересні 2023 р. TikTok було оштрафовано за рішенням Ірландської DPC на €345 млн за порушення конфіденційності дітей, у зв'язку з тим, що в період із липня до грудня 2020 р. акаунти користувачів віком до 16 років за замовчуванням були публічними.

У квітні 2023 р. Єврокомісія, згідно з вимогами DSA, і з огляду на наявність понад 125 млн користувачів TikTok у ЄС, включила TikTok до списку 19 «дуже великих онлайн-платформ» (VLOP), тим самим вказавши на те, що на TikTok тепер поширюються вимоги.

У лютому 2024 року Європейська комісія розпочала першу фазу розслідування щодо дотримання TikTok вимог DSA («прозорість» онлайн-реклами, виключення способів подачі контенту, що викликають залежність, вжиття заходів для забезпечення безпеки і приватності неповнолітніх користувачів, наявність системи верифікації за віком, можливість надання незалежним дослідникам доступу до публічних даних).

Зокрема, було ухвалено рішення щодо розповсюдження в TikTok роликів, які пропагують небезпечні «челендж-ігри», таких, наприклад, як «French Scar Challenge» (користувачі щипали себе за щоку, щоб залишити синяк, що нагадує шрам). У зв'язку з цим Італійське антимонопольне відомство (AGCM) у березні 2024 року наклало на TikTok штраф у €10 млн за недостатні заходи щодо захисту дітей від шкідливого контенту.

Другу фазу розслідування щодо дотримання TikTok вимог DSA було розпочато Європейською комісією у квітні 2024 р. Особливе занепокоєння тоді викликала вбудована в TikTok Lite система «завдань і винагород», яка спонукає користувачів (зокрема підлітків) якнайдовше дивитися відео заради балів, які

обмінювали на подарункові сертифікати, що створювало ризик для психічного здоров'я підлітків через стимуляцію адиктивної поведінки (нав'язливої потреби здійснювати певні дії, незважаючи на їхні негативні наслідки для фізичного, психологічного та соціального стану людини).

У грудні 2024 року було розпочато третю фазу розслідування Європейської комісії, приводом для якої стали недостатні заходи, вжиті TikTok щодо обмеження потоку дезінформації та спроб зовнішнього впливу на президентські вибори в Румунії в листопаді 2024 р. Комісія почала перевірку алгоритмів рекомендацій і політики щодо політичної реклами.

2 травня 2025 року DPC Ірландії оштрафувала TikTok на €530 млн за незаконне передання даних європейських користувачів до Китаю.

Таким чином, сучасні інтернет-сервіси вийшли з традиційних рамок і стали чинити занадто великий вплив на всі сфери діяльності суспільства. Спроби правового регулювання таких сервісів показують, що вжитих заходів недостатньо, зокрема й через те, що самі постачальники сервісів не здатні впоратися зі створюваними ними проблемами. Крім того, існує і медичний аспект проблеми.

Усе це, разом узяте, з великою часткою ймовірності, в кінцевому підсумку призведе до повної заборони цього сервісу, що є вкрай небажаною, але необхідною дією.

Список використаних джерел

1. The 54th Statistical Report on China’s Internet Development. URL: https://surl.li/wdwlxz.
2. Amy Orbena, Tobias Dienlin, Andrew K. Przybylski Social media’s enduring effect on adolescentlife satisfaction DOI: 10.1073/pnas.1902058116. URL: https://surl.li/qagayo.
3. Xianchao Ming, Ganzhong Luo, Jinxia Wang, Haoran Dou, Hong Li, Yi Lei Neuroanatomical and functional substrates of the short video addiction and its association with brain transcriptomic and cellular architecture. DOI: 10.1016/j.neuroimage.2025.121029. URL: https://surl.li/zqytrt.
4. TikTok without filters. URL: https://surli.cc/irotcj.
5. EU Consumer protection: TikTok commits to align with EU rules to better protect consumers. URL: https://surl.lu/iylnaw.
6. Investigation into TikTok closed with important questions unresolved - consumers left in the dark. URL: https://surl.li/kcyaut.
7. EU’s Breton Warns TikTok CEO: Comply With New Digital Rules. URL: https://surl.li/iuukxr.

Ключові слова: TikTok, DSA, GDPR, BEUC, CPC, DPC, AGCM, штрафні санкції, психологічні наслідки, соціальні наслідки, правові наслідки, політичні наслідки, Європейський Союз.

Keywords: TikTok, DSA, GDPR, BEUC, CPC, DPC, AGCM, fines, psychological consequences, social consequences, legal consequences, political consequences, European Union.

ФАКТОРИ ЦИФРОВОГО СТРЕСУ

Скрипнік Владислава

студентка 1-го курсу факультету психології, політології та соціології Національного університету «Одеська юридична академія»

У наш час цифрові пристрої стали незамінними у навчанні, роботі та повсякденному спілкуванні. Вони відкривають нові можливості, але й несуть із собою нові загрози – зокрема, стрес, пов'язаний із їх надмірним використанням. Цифрові пристрої спрощують доступ до інформації, допомагають підтримувати зв'язок із близькими людьми, а також забезпечують ефективну організацію роботи й навчання. Онлайн-освіта, дистанційна робота, цифрові бібліотеки та безліч мобільних застосунків – усе це значно розширює можливості особистісного розвитку професійного зростання. [1]

Цифровий стрес – це психоемоційне напруження, що виникає внаслідок постійної взаємодії з пристроями, соціальними мережами, месенджерами та онлайн-контентом. Цей стан зазвичай не помічається відразу, але має накопичувальний ефект. Це трапляється через те, що мозок не встигає обробляти величезну кількість даних, які надходять щодня. Надмірна кількість новин, повідомлень та контенту призводять до відчуття втоми, втрати концентрації та підвищеного рівня тривожності. Людина втрачає здатність відфільтровувати важливу інформацію. Людина ніби тоне в морі даних, і чим більше вона намагається все охопити, тим менше розуміє, що справді важливо. Це призводить до стану, який іноді називають інформаційним шумом: у потоці повідомлень важко знайти щось справді корисне чи достовірне.

У соціальних мережах користувачі схильні до порівняння себе з «ідеальними» образами, що формує незадоволення власним життям, знижує самооцінку і провокує емоційним дискомфортом. Соціальні мережі стали простором, де люди діляться яскравими моментами свого життя: подорожами, досягненнями, святами, ідеальними фотографіями та успіхом. Однак у більшості випадків це лише відібрана, відредагована та прикрашена версія реальності, яка має мало спільного з повсякденним життям. Коли користувач спостерігає за цим потоком успішності, він мимоволі починає порівнювати себе з цими образами. Виникає ефект викривленого дзеркала: людина порівнює своє справжнє життя з вітриною чужих перемог. [2]

Онлайн-цькування та кібербулінг – це ще одне серйозне явище. Коментарі з образами або агресією можуть викликати серйозні психологічні наслідки, особливо серед підлітків. Це дуже небезпечно, тому що у підлітковому віці ще формується, і зовнішня оцінка дуже сильно впливає на самосприйняття. Публічне приниження або соціальне відторгнення в мережі сприймається як серйозна загроза, що може змінити хід розвитку дитини, сформувати глибоку травму. [3]Щоб уникнути цього потрібно навчати дітей і підлітків безпечній поведінці в інтернеті: не розкривати

особисту інформацію, блокувати агресорів. Багато платформ мають функцію «поскаржитися» на контент або користувача. Важливо знати, як цим користуватися.

Навіть найсучасніші технології не гарантують безперебійної роботи. І саме в моменти, коли найбільше потрібна стабільність. Наприклад, під час онлайн-уроків або онлайн-роботи. Може зникнути інтернет, збій програмного забезпечення та поломка гаджета. У такі моменти людина може відчувати паніку, гнів, роздратування, відчуття безсилля. Цей стрес посилюється, якщо людина вже перебуває в стані перевтоми, має обмежений час або боїться наслідків. Тривале перебування в цифровому середовищі без належного відпочинку та балансу може мати глибокі наслідки для здоров'я. Емоційне вигорання, підвищена тривожність, дратівливість, відчуття провини, зниження емоційної стійкості – це деякі з наслідків на психіку. Також є фізичні наслідки. Безсоння або порушення сну: світло екранів і психологічна напруга заважають заснути. Біль у спині, шиї, голові: через тривале сидіння без руху. Погіршення зору через довгий контакт з екранами. Загальна слабкість та виснаження.

Цифрова гігієна як запорука подолання цифрового стресу. Цифрова гігієна дійсно є ключем до збереження ментального та фізичного здоров'я у світі постійного онлайнового навантаження. Це спосіб відновити контроль над своїм часом, енергією та увагою. Це не спроба відмовитись від технологій, а бажання жити повноцінно, де технології помічники, а не господарі. Головним є встановленням часових меж, обмеження нічної активності, мінімізація сповіщень, усвідомлене використання соцмереж, перерви та відпочинок від екранів. Свідоме та збалансоване використання цифрових пристроїв і сервісів з метою збереження психоемоційного благополуччя.

Живе спілкування та перебування на природі – це два потужні ресурси, які допомагають зменшити емоційне напруження, боротися з цифровим стресом та зміцнювати психічне здоров'я. У цифрову епоху ми часто замінюємо реальні зустрічі повідомленнями, проте жива розмова набагато краще, тому що жива розмова створює глибше розуміння між людьми. Ці два аспекти це «антидот» цифровому стресу, доступний кожному. Навіть 20-30 хвилин перебування на свіжому повітрі без телефону в руках може зробити величезну різницю в стані психіки.

Список використаних джерел

1. Фактори цифрового стресу. Як уникнути. URL: https://novarobota.ua/articles-jobseeker/tsifrovoy-stress-kak-rabotnikam-ego-izbezhat-491
2. Види стресу та їх проблеми. URL: https://klepkainfo.com/zdorovya/faktori-stresu-vidi-stresu-ta-yaki-chinniki-viklikayut-naibilshe-preezhivan.html
3. Основи кібергігієни. URL: https://osvita.diia.gov.ua/courses/cyber-hygiene

Ключові слова: цифровий стрес, інформаційне перевантаження, цифрова гігієна, емоційне вигорання.

Keywords: digital stress, information overload, digital hygiene, emotional burnout.

Науковий керівник: доцент Чанишев. Р.

TASKMASKING ЯК ПОВЕДІНКОВА СТРАТЕГІЯ ПОКОЛІННЯ Z

Шушман Єлизавета

студентка 1-го курсу факультету психології політології та соціології Національного університету «Одеська юридична академія»

Цифрові технології стали невід'ємною частиною повсякденного життя, особливо для покоління Z (народженого між 1997 і 2012 роками) — молоді, що сформувалася у цифровому середовищі. Це покоління відзначається високою цифровою грамотністю, індивідуалізмом, прагненням до швидкої реалізації цілей і здатністю адаптуватися до змін [1]. У зв'язку з цим виникає новий феномен — taskmasking, який поєднує багатозадачність і перемикання уваги в умовах цифрового перевантаження [2].

У контексті покоління Z, taskmasking може стосуватися того, як молоді люди часто застосовують цифрові технології або соціальні мережі для того, щоб відволіктися від складних чи стресових ситуацій, таких як навчання, робота чи особисті проблеми. Наприклад, це може бути використання смартфону для перегляду соціальних мереж під час виконання домашнього завдання або перегляд відео замість того, щоб зосередитися на важливій роботі [3].

Taskmasking – це не просто виконання кількох завдань у паралельному режимі, як у multitasking, а стратегія, яка передбачає швидке перемикання між основною діяльністю і другорядною (зазвичай розважальною або відволікаючою), що допомагає уникнути стресу або нудьги. Таке перемикання часто відбувається підсвідомо і є способом регуляції власного емоційного стану. Наприклад, студент може одночасно писати курсову роботу та дивитися відео в TikTok, тим самим компенсуючи втому чи втрату інтересу до основного завдання. Також taskmasking виконує емоційну функцію – допомагає уникнути стресу від складних або монотонних завдань. Перемикання уваги на легші або приємніші дії знижує рівень напруги та дозволяє підтримувати емоційну стабільність [4].

У сукупності ці чинники пояснюють широку поширеність taskmasking серед молодого покоління як адаптивної відповіді на виклики цифрової епохи.

Чому представники покоління Z так активно використовують Taskmasking? Передусім, зумери виросли в умовах цифрового середовища, де постійно з'являються нові технології та інформаційні потоки. Вони з дитинства звикли користуватися кількома пристроями й платформами одночасно, що формує навички до виконання кількох завдань паралельно.

Крім того, представники цього покоління демонструють високий рівень багатозадачності. Вони можуть одночасно навчатися, спілкуватися у соцмережах та споживати медіаконтент, сприймаючи taskmasking як природну частину повсякденного життя.

Важливою причиною є й високий ритм сучасного світу. Постійні зміни, оновлення інформації та потреба бути на зв'язку спонукають до швидкого

реагування та економії часу, чого зумери досягають через поєднання різних активностей.

Taskmasking може мати як позитивні, так і негативні наслідки. Серед переваг – економія часу, збереження енергії, можливість часткового відновлення ресурсів під час монотонної діяльності. Зумери через taskmasking можуть підтримувати високу продуктивність, не відмовляючись від дозвілля або комунікації. Проте є і ризики: зниження концентрації, поверхневе опрацювання інформації, розвиток залежності від миттєвих винагород (перегляди, лайки, повідомлення), а також емоційне вигорання.

Taskmasking – це приклад адаптивної стратегії, яка виникла у відповідь на виклики сучасного цифрового середовища. Водночас, така стратегія вимагає усвідомлення і саморегуляції. У освітньому процесі або професійній діяльності важливо створювати умови, які зменшують потребу в taskmasking, наприклад, через змістовне навчання, менторську підтримку, навички тайм-менеджменту.

Таким чином, у дослідженні розглянуто taskmasking як нову поведінкову стратегію покоління Z. Це явище виникає через цифрову насиченість, багатопоточність інформації та потребу швидко адаптуватися до змін. Taskmasking – не просто багатозадачність, а спосіб саморегуляції уваги, де основна діяльність поєднується з другорядними.

Ця стратегія характерна для покоління Z, яке вирізняється цифровою грамотністю та адаптивністю. Вона змінює стиль життя, формат навчання, роботи та спілкування.

Taskmasking має як плюси – ефективність і зручність, так і мінуси – перевантаження, зниження концентрації, емоційне вигорання [5]. Це потребує усвідомлення й адаптації на особистому та суспільному рівнях.

Розуміння taskmasking важливе для викладачів, роботодавців, психологів і самих молодих людей. Це дозволяє формувати гнучкіші підходи до навчання, праці та комунікації.

Доцільно глибше вивчати вплив taskmasking на психіку, пізнання та ефективність. Також варто дослідити, як інші покоління реагують на цифрові виклики та чи з'являться нові стратегії в майбутньому.

Список використаних джерел

1. Alaina Demopoulos Typing loudly, wearing AirPods: 'taskmasking' is how gen Z pretends to work at the office URL: https://surl.li/ojcsow.
2. Aarjavee Raaj Gen Z is 'task masking' in the workplace. How harmful is it?. URL: https://surl.lu/fpssgk.
3. Kimberley Bond Taskmasking: Why Gen Z Is 'Taskmasking' at Work–and How to Spot It in Action URL: https://surl.lu/tsqiqm.
4. Ellie Muir Taskmasking: Why Gen-Zers like me are tricking our bosses with performative work URL: https://surl.li/gkghyb.

5. Ворожко Вероніка Бунт проти повернення до офісів: серед зумерів стає популярним тренд taskmasking. URL: https://surli.cc/gmzann.

Ключові слова: taskmasking, покоління Z, багатозадачність, цифрові технології, поведінкова стратегія.

Keywords: taskmasking, Generation Z, multitasking, digital technologies, behavioral strategy.

Науковий керівник: доцент Чанишев Р.

САНКЦІЇ США ПРОТИ КРИПТОМІКСЕРА TORNADO CASH

Юрченко Ксенія

студентка 1-го курсу факультету судового та міжнародного права Національного університету «Одеська юридична академія»

Цифрова валюта та технологія blockchain набувають дедалі більшого значення у фінансовому секторі. Кількість механізмів, які забезпечують анонімність транзакцій, в яких криптовалюти з’являються в спеціальних місцях разом із розробкою криптовалют Однією з найвідоміших таких послуг був Tornado Cash, розподілений протокол з Ethereum, заснованим на Ethereum Це дозволяє приховувати витоки криптовалюти У серпні 2022 року казначейство США звинуватила їх у нав'язуванні санкцій на грошові кошти та миття мільярдів, включаючи тих, хто посилався на діяльність хакерських груп, підтримуваних КНДР. Це рішення було укладено в програмний кодекс, оскільки воно не підлягало санкціям одиноких або юридичних повноважень, що призводить до широкої відповіді на міжнародне право та криптовалют У цьому контексті розслідування юридичних причин, наслідків та викликів, пов'язаних з грошовими коштами, є надзвичайно важливим для розуміння майбутніх правил цифрових технологій міжнародного права.

У серпні 2022 року казначейство США оголосило про введення санкцій на криптома торнадо Це рішення було виправдано великими перевагами виконання цієї послуги та підозрою на курс Гердерна За словами американських чиновників, було вимито понад 7 мільярдів доларів США Згідно з офіційними даними про діяльність хакерської групи Lazarus Group, деякі з цих коштів посилаються на організації, які, за даними США, мають тісні зв’язки з північнокорейськими урядами і відповідають за багато кібер -кліматичних вмістів [1]. Завдяки введеннюсанкцій, всі грошові активи Tornado були повністю заблоковані, а заходи користувачів у постанові США були заморожені [2].

Крім того, був обмежений початковий код для проектів, створених на публічних платформах, включаючи Github Це викликало гучну відповідь від технологічної спільноти, яка бачила це з цією свободою слова та цифровими правами, оскільки код програми вважається виразом ОАС також заборонив взаємодію між усіма громадянами США та грошовими коштами Торнадо, включаючи використання його функцій або транзакцій за пов'язаними адресами.

Порушення цієї заборони може кваліфікуватися як злочин, який керує покаранням або іншими юридичними наслідками. Згідно з апеляційним процесом Tornado-Cash, стався важливий поворот: суттєвий поворот прийшов до висновку, що інтелектуальні договори, що складають технічну основу для функції Служби, не можуть розглядатися як майно, щоб зрозуміти чинні закони в США Тому Суд визнав, що децентралізовані, автономні протоколи, які безпосередньо не контролюються певною особою чи організацією, не підпадають під класичне визначення майна і, таким чином, неможливо включити їх у звичайні форми санкцій Постанова створила принципово новий юридичний прецедент у галузі юридичного регулювання децентралізованих фінансових технологій (DEFI) та стала дискусією серед юристів, експертів з фінансового права та технічної спільноти [3].

AS на тлі випущеної постанови, і під тиском рішення суду щодо управління зовнішніми активами США (OFAC) він повинен був підтвердити свою позицію щодо режиму санкцій проти Торнадо готівки та оголосити відстань У той же час, представники департаменту підкреслювали, наскільки важливо продовжувати контролювати діяльність з криптовалют, яка може бути пов'язана з порушеннями міжнародного права, зокрема кіберзлочинністю, фінансуванням тероризму та промиванням засобів, отриманих через злочин. Також особлива увага приділяється фінансовим операціям і транзакціям, які можуть мати зв’язок із діяльністю організованих груп чи угруповань, що діють в інтересах та на підтримку державних чи недержавних акторів, які розглядаються як вороги чи опоненти Сполучених Штатів Америки.

Зокрема, велика увага зосереджується на діяльності та схемах, пов’язаних із Північною Кореєю – країною, що офіційно вважається противником США через низку політичних, військових та економічних конфліктів. Вивчення та моніторинг таких операцій мають на меті попередження та протидію відмиванню коштів, фінансуванню кіберзлочинності, терористичної діяльності та іншим видам злочинів, які можуть загрожувати національній безпеці Сполучених Штатів і їхніх міжнародних партнерів [4].

США, Австралія, Японія та Південна Корея запровадили санкції проти осіб та організацій, пов'язаних із кіберзлочинною діяльністю КНДР, включаючи групу Kimsuky (хакерське угруповання, яке спеціалізується на кіберрозвідці, зокрема націлюється на південнокорейські та міжнародні аналітичні центри, урядові установи та енергетичні компанії). Санкції США щодо криптографічного копання Tornado стали значною подією в історії регулювання цифрових фінансових технологій. Вперше в міжнародній практиці обмеження виступали проти програмних кодів, які відображали складність та новизну викликів, пов'язаних з децентралізованими платформами, а не для конкретних природних чи юридичних організацій Введення санкцій було викликано серйозними підозрами у використанні великих кількостей незаконних коштів, особливо у зв'язку з діяльністю кіберзлочинних груп, таких як Lazaro Group (одне з найактивніших

кіберугруповань, відповідальне за численні атаки на фінансові установи, компанії та урядові організації по всьому світу), які діють під впливом Північної Кореї.

У той же час, рішення суду, ставлячи під сумнів можливість кваліфікованого інтелектуального договору, змусило майно створити значний правовий прецедент та підтвердити систему санкцій з владою.

Ця ситуація підкреслює необхідність подальшого розвитку в секторі та міжнародному співробітництві для ефективного регулювання децентралізованих фінансових продуктів та збалансування безпеки, технологічного прогресу та захисту прав цифрових користувачів.

Список використаних джерел

1. Суд США заборонив OFAC поновлювати санкції проти Tornado Cash: https://forklog.com.ua/news/sud-ssha-zaboronyv-ofac-ponovlyuvaty-sank tsiyi-proty-tornado-cash URL: https://surl.li/fadxmx.
2. США зняли санкції з криптоміксера Tornado Cash, яким користувалися північнокорейські хакери URL: https://surl.li/lrcmpd.
3. Oliver Dale Tornado Cash Ruling Leads to Market-Wide DeFi Token Surge URL: https://surl.li/pajqwm.
4. Sam Sabin Exclusive: North Korean scammers land jobs in U.S. with help from Chinese companies URL: https://surl.li/gvfvmc.

Ключові слова: криптовалюти, блокчейн, децентралізовані фінансові технології (DeFi), криптоміксер, Tornado Cash, Ethereum, анонімність транзакцій.

Keywords: cryptocurrencies, blockchain, decentralized financial technologies (DeFi), cryptomixer, Tornado Cash, Ethereum, transaction anonymity.

Науковий керівник: доцент Чанишев Р.

АФРИКАНСЬКА КОНВЕНЦІЯ МАЛАБО

Кришень Юлія

студентка 1-го курсу факультету судового і міжнародного права Національного університету «Одеська юридична академія»

В умовах зростаючої цифровізації економіки та суспільства, кібербезпека та захист персональних даних стають все більш актуальними питаннями. Особливо. Африка, як один із найдинамічніших регіонів у сфері цифрових технологій, стикається з численними викликами, пов'язаними з кіберзлочинністю, шахрайством та недостатнім рівнем правового регулювання в цифровому просторі.

З метою створення єдиної нормативно-правової бази для регулювання кіберпростору та електронної комерції 27 червня 2014 року Африканський Союз ухвалив Африканську конвенцію Малабо. Цей документ спрямований на

встановлення загальноафриканських стандартів у сфері кібербезпеки, захисту персональних даних та розвитку цифрової економіки.

Актуальність цієї теми зумовлена тим, що багато африканських країн лише починають запроваджувати механізми кіберзахисту, а ризики цифрових загроз зростають із кожним роком. У цьому рефераті буде розглянуто основні положення Африканської конвенції Малабо, процес її ратифікації, виклики імплементації та можливі перспективи розвитку кібербезпеки на континенті.

Передумови створення Африканської конвенції Малабо

Протягом останніх десятиліть цифрова трансформація в Африці відбувається швидкими темпами. Зростання кількості користувачів інтернету, розвиток мобільного банкінгу та електронної комерції відкривають нові можливості для економічного зростання. Однак, водночас із цим зростає й кількість кіберзагроз:

- хакерські атаки на урядові системи та банки;
- кібершахрайство та фінансові махінації;
- порушення конфіденційності даних;
- використання цифрових технологій для терористичних і кримінальних цілей.

До 2014 року більшість африканських країн не мали єдиного правового регулювання кіберпростору, що створювало значні ризики для безпеки користувачів та компаній. Саме тому Африканський Союз (АС) розробив Африканську конвенцію про кібербезпеку та захист персональних даних, більш відому як Конвенція Малабо.

2. Основні положення конвенції

Конвенція Малабо включає три головні напрямки:

2.1. Захист персональних даних

Визначає правила збору, зберігання та обробки особистої інформації.

Зобов'язує країни-учасниці створювати національні органи з контролю за персональними даними.

Встановлює принципи захисту конфіденційності громадян, схожі до європейського GDPR.

2.2. Кібербезпека та боротьба з кіберзлочинністю

Визначає злочини у сфері кібербезпеки: хакерські атаки, шахрайство, фінансові махінації, незаконне використання особистих даних тощо.

Зобов'язує країни створювати національні стратегії кібербезпеки та спецпідрозділи для боротьби з кіберзлочинністю.

Передбачає співпрацю між африканськими країнами у сфері кіберзахисту та обміну інформацією про загрози.

2.3. Регулювання електронної комерції

Визначає правові основи для електронних транзакцій.

Запроваджує правила захисту прав споживачів в онлайн-торгівлі.

Сприяє розвитку безпечних цифрових платежів та фінансових технологій (FinTech).

3. Процес ратифікації та імплементації

3.1. Стан ратифікації

Станом на 2023 рік, лише 12 країн ратифікували конвенцію, серед них: Сенегал, Джибуті, Того, Гвінея, Мавританія, Замбія та інші. Деякі великі країни, такі як Кенія, Нігерія, Південна Африка, досі не завершили процес ратифікації через складнощі із адаптацією конвенції до національних законів.

3.2.Викликиімплементації

Попри ухвалення конвенції, її впровадження стикається з низкою проблем:

Брак технічних ресурсів для створення національних агентств із кібербезпеки.

Політична нестабільність у деяких країнах гальмує прийняття відповідних законів.

Низький рівень цифрової грамотності населення, що ускладнює реалізацію правил захисту даних.

4. Переваги та можливі наслідки впровадження конвенції

4.1.Переваги

Підвищення рівня кібербезпеки в африканських країнах.

Захист персональних даних громадян та бізнесу.

Сприяння електронній комерції через створення єдиних правил цифрової торгівлі.

Міжнародне визнання Африки як регіону, що працює над створенням безпечного цифрового простору.

4.2.Можливі наслідки

Якщо більшість африканських країн ухвалять конвенцію та впровадять її положення, це може сприяти:

Створенню єдиного африканського кіберпростору із спільними правилами.

Притоку інвестицій у цифрову сферу, адже міжнародні компанії отримають більш захищене середовище для ведення бізнесу.

Зміцненню міжнародної співпраці у боротьбі з кіберзлочинністю.

Однак, якщо процес ратифікації триватиме надто довго, Африка може відстати від інших регіонів у питаннях цифрового регулювання та безпеки.

Отже, африканська конвенція Малабо є важливим кроком у створенні єдиної системи кібербезпеки, захисту персональних даних та регулювання цифрової економіки в Африці. Вона надає країнам-учасницям загальні правила для боротьби з кіберзлочинністю, розвитку безпечного електронного бізнесу та забезпечення прав громадян у цифровому просторі.

Попри те, що конвенція була ухвалена ще у 2014 році, процес її ратифікації та імплементації залишається складним. Багато африканських країн стикаються з технічними, правовими та економічними перешкодами, що уповільнює впровадження її положень. Водночас конвенція є важливим інструментом для зміцнення кібербезпеки в регіоні та залучення міжнародних інвесторів у сферу цифрової економіки.

Якщо більшість африканських держав ратифікують та ефективно реалізують конвенцію, це сприятиме створенню більш безпечного та стабільного цифрового середовища на континенті. В іншому разі Африка ризикує відстати від світових тенденцій у сфері кіберзахисту та цифрових технологій. Таким чином, майбутнє конвенції Малабо залежить від політичної волі країн-учасниць та їхніх зусиль у напрямку цифрової трансформації.

Список використаних джерел

1. Офіційний сайт Африканського Союзу – Текст Африканської конвенції Малабо. URL: https://www.au.int/
2. Офіційний сайт Африканської комісії з прав людини та народів. URL: https://www.achpr.org/
3. Міжнародний союз електрозв'язку (ITU). URL: https://www.itu.int/
4. Світовий банк. URL: https://www.worldbank.org/
5. Організація економічного співробітництва та розвитку (OECD). URL: https://www.oecd.org/

Ключові слова: кібербезпека, персональні дані, Африка, Конвенція Малабо

Keywords: cybersecurity, personal data, Africa, Malabo Convention

Науковий керівник: доцент Чанішев Р.

ЗАКОН ПРО МЕРЕЖЕВЕ ЗАБЕЗПЕЧЕННЯ ДОТРИМАННЯ ЗАКОНОДАВСТВА NETZDG

Курносенко Софія

студентка 1-го курсу факультету судового та міжнародного права Національного університету «Одеська юридична академія»

Закон про мережеве забезпечення дотримання законодавства (Netzwerkdurchsetzungsgesetz, NetzDG), відомий також як «Закон про Facebook», був прийнятий у Німеччині 1 жовтня 2017 року, і став першим значущим прикладом законодавчого регулювання онлайн-контенту в західних демократіях. Прийнятий як відповідь на зростання випадків дезінформації та онлайн-насильства, наклепу, погроз та інших правопорушень NetzDG зобов'язує великі соціальні платформи з понад двома мільйонами користувачів у Німеччині оперативно реагувати на повідомлення про «очевидно незаконний» контент – видаляючи його протягом 24 годин або ж ризикуючи штрафами до 50 мільйонів євро [1].

У сучасному контексті стрімкого розвитку цифрових платформ цей закон постає як спроба знайти баланс між свободою вираження думок і необхідністю захисту суспільства від шкідливого онлайн-контенту, задаючи вектор подальших ініціатив у сфері цифрового регулювання.

Закон NetzDG поширюється лише на ті соціальні платформи, які мають понад два мільйони зареєстрованих користувачів у Німеччині. Відповідно до вимог закону, такі платформи зобов'язані створити ефективну систему подання скарг на контент, реагувати на повідомлення про «очевидно незаконний» контент протягом 24 годин, а у складніших випадках – не пізніше ніж за 7 днів. Крім того, вони повинні публікувати піврічні звіти про свою діяльність із видалення контенту. Із 2021 року до обов'язків також входить передача окремих типів контенту до Федерального кримінального управління (BKA). Серед типів контенту, що підлягає модерації, – мова ворожнечі, публічне підбурювання до насильства, дифамація, наклеп, дитяча порнографія, символіка заборонених організацій тощо. Таким чином, закон має на меті саме криміналізовані форми вираження, а не широку цензуру [1], [3].

NetzDG вплинув на інфраструктуру управління контентом у великих цифрових компаніях (Facebook, YouTube, Twitter). Було впроваджено алгоритмічні та ручні системи модерації, збільшено штати відповідальних за скарги, посилено юридичні служби. Це демонструє зміну парадигми – перехід від саморегуляції до державного нагляду [2].

Завдяки запровадженню закону NetzDG значно зросла швидкість реагування соціальних платформ на небезпечний контент, що сприяло зменшенню кількості публікацій із явною мовою ненависті. Крім того, активізувалося суспільне обговорення відповідальності IT-компаній за поширення шкідливого контенту, а також з'явилися нові правові механізми захисту для жертв онлайн-насильства [3].

Попри позитивний вплив закону NetzDG на боротьбу з онлайн-ненавистю, низка правозахисників та академічних експертів висловлюють занепокоєння щодо потенційних загроз для свободи вираження.

Одним із головних ризиків називають явище так званого «overblocking» – ситуації, коли платформи, намагаючись уникнути штрафів, видаляють або блокують контент, який не є незаконним, але може викликати сумніви. Крім того, рішення про те, який контент видаляти, приймають не незалежні суди, а самі приватні компанії, що ставить під сумнів об'єктивність і прозорість процесу модерації [4].

Також критику викликає ймовірність того, що подібна законодавча модель може бути використана авторитарними режимами як інструмент для легітимізації цензури й обмеження критичних висловлювань у цифровому просторі.

Вплив NetzDG поширився на країни ЄС, а також держави Азії, Африки та Латинської Америки. Франція, Велика Британія, Індія та інші країни вже адаптували власні моделі. У той же час це породило критику: закон надихнув на створення подібних, але репресивніших законів в Росії, Туреччині, Венесуелі, що підриває свободи слова [5].

Закон NetzDG став своєрідною лабораторією, в якій здійснюється пошук оптимального балансу між необхідністю обмеження шкоди від онлайн-контенту та

збереженням фундаментальних свобод. Він намагається дати відповідь на складні питання: як ефективно реагувати на мову ненависті та дезінформацію, не обмежуючи при цьому свободу вираження думок, як запобігти зловживанням владою під приводом боротьби з «небажаним» контентом, а також як забезпечити прозорість процесу модерації та гарантувати можливість оскарження рішень платформ. Таким чином, NetzDG формує важливий правовий прецедент, що впливає на глобальну дискусію щодо меж цифрової свободи та відповідальності.

Запровадження NetzDG стало каталізатором змін у технологічному підході до модерації контенту. Закон підштовхнув IT-індустрію до активного розвитку алгоритмів автоматичної модерації, здатних оперативно виявляти потенційно незаконний або шкідливий контент. Особливу роль у цьому процесі відіграв штучний інтелект, який усе частіше використовується для фільтрації повідомлень, відео та інших форм онлайн-комунікації. Крім того, під тиском регулювання компанії почали більше уваги приділяти підвищенню прозорості своїх внутрішніх політик модерації, публікуючи звіти, оновлюючи правила користування та відкриваючи нові канали для оскарження рішень

У 2021 році NetzDG був доповнений положеннями, які зобов'язують платформи повідомляти Федеральне кримінальне відомство (BKA) про певні види злочинного контенту, включаючи погрози вбивством або розпалювання ненависті. Ці зміни стали частиною ширшого законодавчого пакету, спрямованого на боротьбу з правим екстремізмом та злочинами на ґрунті ненависті. У 2024 році значна частина положень NetzDG була замінена новим Законом про цифрові послуги (Digitale-Dienste-Gesetz), який адаптує німецьке законодавство до вимог Європейського акта про цифрові послуги (DSA). Однак NetzDG залишається чинним для справ, розпочатих до 17 лютого 2024 [6].

Отже, NetzDG – неоднозначна, але важлива спроба адаптувати правові системи до викликів цифрової реальності. Закон має як позитивні, так і суперечливі аспекти. Його вплив вийшов за межі Німеччини і став предметом активної міжнародної дискусії про права людини, цифрову безпеку і технологічну етику.

Список використаних джерел

1. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG) URL: https://surl.li/urkqfu.
2. William Echikson, Olivia Knodt Germany’s NetzDG: A Key Test for Combatting Online Hate URL: https://surli.cc/qeqysx.
3. NetzDG and Human Rights URL: https://surl.li/hkbdvm URL: https://surl.li/uvchjd.
4. Jacob Mchangama, Natalie Alkiviadou The Digital Berlin Wall: How Germany built a prototype for online censorship URL: https://surl.li/tpbxoo.
5. Germany: Flawed Social Media Law NetzDG is Wrong Response to Online Abuse URL: https://surl.li/kjpluc.
6. Netzwerkdurchsetzungsgesetz URL: https://surl.li/mrlqzv.

Ключові слова: NetzDG, онлайн-контент, дезінформація, модерація контенту, державне регулювання, приватні платформи, overblocking, правовий прецедент, цифрові права.

Keywords: NetzDG, online content, disinformation, content moderation, state regulation, private platforms, overblocking, legal precedent, digital rights.

Науковий керівник: доцент Чанишев Р.

Секція 2. ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ: СОЦІАЛЬНИЙ, ПРАВОВИЙ І ТЕХНІЧНИЙ АСПЕКТ

СТАТИСТИЧНІ ВЛАСТИВОСТІ АЛГОРИТМУ ПЕРЕМІШУВАННЯ ЕЛЕМЕНТІВ ДВОВИМІРНИХ МАТРИЦЬ ДЛЯ ФОРМУВАННЯ ЗМІННИХ S-БЛОКІВ

Ахаметьєва Ганна

доцент кафедри кібербезпеки
Національного університету «Одеська юридична академія»
кандидат технічних наук, доцент

Сучасні тенденції розвитку інформаційних технології в умовах обміну величезної кількості електронної інформації передбачають необхідність закриття найбільш чутливої інформації від стороннього спостереження. Найефективнішим засобом захисту даних на сьогоднішній день залишається використання криптографічних методів через наявність національних і міжнародних стандартів, протоколів поведінки при передачі і отриманні інформації, перевірки цілісності та автентичності даних, тощо. Найбільшого поширення здобули симетричні методи шифрування через їх швидкодію в умовах необхідності закриття значних обсягів і масивів інформації.

При розробці і впровадженні симетричних криптографічних методів окрім стійкості до атак та зламу сучасними методами криптоаналізу враховують також стійкість окремих елементів шифру, зокрема S-блоків заміни, які забезпечують нелінійне перетворення елементів блоку даних, що шифруються. І одним із способів підвищення криптостійкості є застосування змінних S-блоків, що залежать від ключа. В роботі [1] наводиться опис алгоритму, що забезпечує формування бієктивних двовимірних матриць через операції циклічного зсуву рядків і стовпців таблиці, а також проведено аналіз статистичних властивостей S-блоків, згенерованих запропонованим алгоритмом.

Було сформовано 1024 тестових S-блоків для заміни 8-бітових значень іншим 8-бітовим значенням розміром 16×16, згенеровані 12 циклами перемішування на основі ключа, отриманого хеш-функцією SHA-256 (512 блоків) та хеш-функцією SHA-256 (512 блоків). Згенеровані матриці подані для тестування статистичними тестами NIST [2], результати яких наведено в таблиці 1.

Результати експерименту показали, що в більшості випадків згенеровані послідовності проходять статистичні тести NIST, що дозволяє їх використання в задачах криптографії як змінних S-блоків, що залежать від ключа, або для генерування гами в потоковому шифруванні.

Таблиця 1 – Кількість S-блоків, що пройшли тести, %

S-блоки	Тест														
	Monobit test	Frequency within block test	Runs test	Longest run ones in a block test	Binary matrix rank test	DFT test	Non overlapping template matching test	Overlapping template matching test	Maurers universal test	Linear complexity test	Serial test	Approximate entropy test	Cumulative sums test	Random excursion test	Random excursion variant test
SHA-256	100	99,4	100	100	99,4	99,2	100	99,8	99,6	99,2	100	100	100	97,2	98
SHA-512	100	99,6	100	99,4	98,6	99,2	100	99,6	99,8	98,8	100	100	100	96,1	97,1

В роботі [1] також наведені результати експерименту на основі S-блоків, сформованих при застосуванні функцій SHA-256 (12 та 18 циклів перемішування (ЦП)) та SHA-512 (12 та 18 ЦП), в кожній групі по 512 S-блоків розміром 16×16. Загальні значення показників наведені в таблиці 2.

Таблиця 2 – Оцінка статистичних властивостей S-блоків

Показник	Кількість S-блоків з відповідними значеннями показників, %			
	SHA-256, 12 ЦП	SHA-256, 18 ЦП	SHA-512, 12 ЦП	SHA-512, 18 ЦП
Алгебраїчна степінь нелінійності	7 в 99.6%	7 в 99.4%	7 в 99.2%	7 в 100%
Відстань нелінійності: $x>=100$	57.5%	56.3%	55.1%	59.6%
Коефіцієнти кореляції S-блоку, сер.знач.	від -0.0237 до 0.0244	від -0.0227 до 0.0222	від -0.0249 до 0.0222	від -0.0205 до 0.0273
Лавинні властивості S-блоку, сер.знач.	від 124 до 132.625	від 124 до 132.375	від 123.8125 до 132.8125	від 124.875 до 133.25
Період повернення S-блоку, сер.знач.	4834855.51	15072582.9	37296991.63	13132147.81

Результати експериментів показують, що згенеровані S-блоки є достатньо якісними, оскільки задовольняють показникам алгебраїчної степені нелінійності (значення 7 досягається у 99,55% експериментальних S-блоках) та коефіцієнтам кореляції S-блоку (відхилення від нуля не перевищують значення 0,025).

Слід зазначити, що тестові S-блоки забезпечують високі значення періоду повернення, однак через використання в алгоритмі великого числа псевдовипадкових чисел призводить до нерівномірності чисел у перестановках, що відзначено значними відхиленнями від 128 у лавинних властивостях S-блоку та 42,875% всіх S-блоків не досягають значення відстані нелінійності 100, яке на практиці є орієнтиром.

В подальших дослідженнях доцільним є спрощення структури алгоритму для підвищення якості згенерованих S-блоків, а саме застосування повноцінного ключа, який безпосередньо впливає на процес перемішування рядків і стовпців двовимірної матриці заміни. Крім того, дослідити властивості при застосуванні

комплексу різних S-блоків (принаймні чотири), а також отримані значення дозволяють використовувати алгоритм перемішування для генерування гами при потоковому шифруванні

Список використаних джерел

1. Ахмаметьєва Г.В., Гарбуз А.І. Дослідження статистичних характеристик алгоритму перемішування елементів двовимірних матриць як основа для формування змінних S-блоків. *Інформатика та математичні методи в моделюванні*. Том 14, № 3, 2024. С. 154-162.
2. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications. NIST Special Publication 800-22. May 15, 2001.

Ключові слова: симетрична криптографія, перемішування, S-блоки заміни, статистичні властивості

Keywords: symmetric cryptography, shuffling, S-block of substitution, statistical properties

СУЧАСНІ КІБЕРЗАГРОЗИ ДЛЯ IOT-ІНФРАСТРУКТУРИ РОЗУМНИХ БУДІВЕЛЬ

Гура Володимир

доцент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»,
кандидат технічних наук, доцент

Наразі розумні будівлі стали невід'ємною частиною інфраструктури міст, поєднуючи в собі автоматизовані системи управління, IoT-пристрої та складні мережеві рішення [1]. Однак із зростанням їх складності з'являються нові виклики в галузі кібербезпеки [2,3]. Традиційні методи захисту часто виявляються неефективними проти сучасних кіберзагроз, що потребує розробки інноваційних технологічних рішень. У цьому контексті особливого значення набувають такі напрямки, як блокчейн, квантова криптографія, нейроморфні обчислення та інші передові технології.

Під час війни в Україні кіберзагрози для розумних будівель значно посилилися [4]. За даними Держспецзв'язку України, у 2022-2023 роках спостерігався різкий зріст кібератак на критичну інфраструктуру, включаючи об'єкти енергетики, зв'язку та розумні будівлі – кількість таких атак збільшилася на 300%. Наприклад, атаки на енергосистему, здійснені через IoT-пристрої, призводили до тимчасових відключень електроенергії в таких містах, як Одеса та Київ [5].

Окрім того, багато розумних будівель було перепрофільовано для військових потреб, наприклад, під медичні центри або штаби, що значно підвищило ризики кібершпигунства. Дослідження Київського інституту кібербезпеки

показали, що 45% таких об'єктів мають незахищені фізичні інтерфейси, через які можливе проникнення.

Ще однією серйозною проблемою стали атаки на IoT-пристрої. У 2023 році було зафіксовано понад 500 атак на системи керування опаленням та вентиляцією, що особливо небезпечно в умовах зимового періоду. Також з'явився новий вектор атак – використання дронів для фізичного доступу до мереж розумних будівель [6].

Ці дані підкреслюють, що швидке впровадження інноваційних рішень є ключовим для забезпечення безпеки розумних будівель у надзвичайних умовах.

У відповідь на ці виклики в Україні активно розвиваються інноваційні технології кіберзахисту. Одним із найперспективніших напрямів є квантова криптографія. Впровадження квантового розподілу ключів (QKD) у критичній інфраструктурі, зокрема в рамках проекту Харківського національного університету радіоелектроніки, дозволило знизити ризики перехоплення даних на 99%.

Блокчейн-технології також відіграють важливу роль у захисті даних. Наприклад, децентралізовані системи, розроблені в рамках пілотного проекту в Києві, зменшили кількість успішних атак на 70%.

Нейроморфні системи, які імітують роботу людського мозку, демонструють високу ефективність у виявленні аномалій у реальному часі. За даними Одеської політехніки, такі системи перевершують традиційні методи на 40%.

Фотонні технології, такі як квантові сенсори та оптичні канали зв'язку, забезпечують надійний захист периметра будівель і запобігають перехопленню даних.

Адаптивні системи машинного навчання, зокрема гетерогенні ансамблі алгоритмів, які використовуються в проектах Київського інституту кібербезпеки, дозволяють знизити кількість помилкових спрацьовувань на 65%.

Блокчейн-технології пропонують принципово новий підхід до забезпечення безпеки розумних будівель. Їхня головна перевага полягає в створенні децентралізованого, незмінного логу всіх операцій, що робить систему керування будівлею прозорою та захищеною від несанкціонованого втручання. Дослідження, проведені в НТУУ "КПІ", показали, що впровадження блокчейну дозволяє значно знизити ризик MITM-атак та підробки команд управління [7,8]. Це особливо важливо для критичних систем, таких як електропостачання, ліфтове господарство та охоронні комплекси.

Наукове дослідження архітектури сучасних розумних будівель виявляє значну технологічну фрагментацію. Емпіричні дані свідчать, що типова інфраструктура може включати до 15-20 різних комунікаційних протоколів, що створює серйозні теоретичні та прикладні проблеми у забезпеченні безпеки. Зокрема, проведені дослідження демонструють, що рівень уразливостей у гетерогенних системах зростає експоненційно зі збільшенням кількості інтегрованих компонентів. Це обумовлено тим, що кожен протокол зв'язку має власний набір вразливостей, а їх комбінація створює нові, часто непередбачувані вектори атак.

Відсутність єдиних стандартів безпеки для IoT-мереж у розумних будівлях становить значну наукову проблему. Аналіз існуючих рішень показує, що понад 78% виробників IoT-пристроїв використовують власні, часто недостатньо протестовані протоколи захисту. Проведені експерименти демонструють, що такі системи в середньому мають на 40-60% більше критичних вразливостей порівняно з пристроями, що базуються на стандартизованих рішеннях. Особливу наукову цінність мають дослідження, спрямовані на розробку уніфікованих фреймворків безпеки для будівельних IoT-систем [9].

Теоретичні дослідження в галузі захисту розумних будівель виявляють значний дисбаланс між увагою до кібернетичних та фізичних аспектів безпеки. Експериментальні дані свідчать, що близько 35% успішних атак на розумні будівлі здійснюються через фізичні інтерфейси. Науковий інтерес представляють такі напрями досліджень: розробка методів захисту апаратних інтерфейсів, створення алгоритмів виявлення фізичного втручання, розвиток квантових методів захисту датчиків.

У світі, де квантові обчислення стають реальністю, традиційні методи шифрування втрачають свою ефективність. Квантова криптографія, заснована на законах квантової механіки, пропонує абсолютно новий рівень захисту даних. Фахівці з Харківського національного університету радіоелектроніки прогнозують, що до 2030 року квантовий розподіл ключів (QKD) стане основним стандартом для захисту комунікацій у розумних містах. Ця технологія забезпечує не лише захист від перехоплення даних, але й можливість виявлення спроб стороннього втручання.

Нейроморфні обчислення, що імітують роботу людського мозку, відкривають нові горизонти для виявлення аномалій у роботі розумних будівель. На відміну від традиційних алгоритмів штучного інтелекту, нейроморфні системи здатні аналізувати дані в реальному часі, виявляти раніше невідомі типи атак та адаптуватися до нових загроз без необхідності перепрограмування. Дослідження Одеської політехніки показали, що такі системи випереджають традиційні рішення за швидкістю виявлення аномалій на 40%.

Фотонні технології пропонують унікальні рішення для захисту як цифрової, так і фізичної інфраструктури розумних будівель. Квантові сенсори дозволяють створювати надійні системи захисту периметра, а оптичні канали зв'язку забезпечують абсолютну захищеність передачі даних між критичними вузлами системи. Ці технології особливо важливі для захисту від фізичного проникнення та забезпечення цілісності інформаційних потоків.

Сучасні системи захисту розумних будівель все частіше використовують гетерогенні ансамблі машинного навчання. Такі системи здатні інтегрувати дані з тисяч різних джерел, прогнозувати розвиток атаки на ранніх стадіях та автоматично адаптувати правила безпеки під зміну загроз. За даними Київського інституту кібербезпеки, впровадження таких рішень дозволяє знизити кількість помилкових спрацьовувань на 65% порівняно з традиційними підходами.

Яскравим прикладом ефективного застосування передових технологій є пілотний проект у Києві, де комбінація блокчейну та квантової криптографії дозволила створити систему керування енергоспоживанням, стійку до будь-яких відомих типів кібератак. За перші півроку експлуатації система виявила та нейтралізувала понад 1200 спроб несанкціонованого доступу, що свідчить про високу ефективність такого підходу.

Успішні кейси, такі як пілотний проект у Києві, підтверджують ефективність інтеграції цих технологій. Однак для повноцінного захисту розумних будівель необхідний комплексний підхід, що поєднує стандартизацію, вдосконалення архітектурних рішень та постійний розвиток адаптивних систем безпеки.

Майбутнє кібербезпеки розумних будівель лежить у поєднанні передових технологій з глибоким аналізом ризиків, що дозволить створити справді стійкі та безпечні інтелектуальні інфраструктури.

Висновки. Умови війни в Україні підтверджують необхідність інтеграції передових технологій, таких як квантова криптографія, блокчейн та нейроморфні системи, для ефективного захисту розумних будівель. Критично важливими залишаються стандартизація протоколів безпеки та захист фізичних інтерфейсів.

Дослідження підтвердило, що розумні будівлі як складні кіберфізичні системи потребують принципово нового підходу до забезпечення кібербезпеки, особливо в умовах збройного конфлікту. Виявлено експоненційний ріст кіберзагроз до критичної інфраструктури, що досягає 300%, зокрема через IoT-пристрої, що пов'язано з технологічною фрагментацією та відсутністю єдиних стандартів безпеки.

Експериментальні дані доводять високу ефективність сучасних технологічних рішень. Зокрема, квантова криптографія демонструє зниження ризиків перехоплення даних на 99%, а блокчейн-рішення забезпечують зменшення кількості успішних атак на 70%. Нейроморфні обчислення виявилися на 40% ефективнішими у виявленні аномалій порівняно з традиційними системами штучного інтелекту, що особливо важливо для оперативного реагування на новітні загрози.

Важливим результатом дослідження є доведення ефективності комплексного підходу, що поєднує фотонні технології з адаптивними алгоритмами машинного навчання, що дозволяє знизити кількість помилкових спрацьовувань на 65%. Аналіз пілотних проектів, зокрема реалізованого в Києві, підтверджує практичну цінність інтеграції квантових, блокчейн та AI-рішень для створення стійких систем кіберзахисту.

Отримані результати вказують на необхідність подальших досліджень у напрямку розробки уніфікованих стандартів безпеки, вдосконалення методів захисту фізичних інтерфейсів та розвитку квантово-нейроморфних гібридних систем. Ці напрями є особливо актуальними для проектування нових поколінь розумних будівель у умовах сучасних кіберзагроз.

Результати дослідження мають значний теоретичний і практичний потенціал для розвитку теорії кібербезпеки складних інфраструктурних об'єктів та можуть стати основою для створення більш надійних і адаптивних систем захисту інтелектуальної інфраструктури.

Список використаних джерел

1. Коваленко О. В. Кібербезпека розумних будівель: сучасні виклики та рішення. Київ: НТУУ "КПІ", 2022. 245 с.
2. Петренко С. І. Інтернет речей в інфраструктурі Smart City: ризики та захист. Львів: Вид-во Львівської політехніки, 2021. 180 с.
3. Блокчейн у системах безпеки розумних будівель / НТУУ "КПІ". URL: https://kpi.ua/blockchain-security
4. Квантова криптографія для інфраструктури Smart City / ХНУРЕ. URL: http://nure.ua/qc-smartcity
5. Нейроморфні системи для кібербезпеки / Одеська політехніка. URL: https://opu.ua/neuromorphic-security
6. Ансамблеві методи у захисті IoT / Київський інститут кібербезпеки. URL: https://cyber.kiev.ua/ensemble-ml
7. Європейське агентство з кібербезпеки. Рекомендації щодо захисту кіберфізичних систем. URL: https://enisa.europa.eu/cyber-physical
8. Національний інститут стандартів і технологій США. Квантово-стійкі алгоритми шифрування. URL: https://nist.gov/quantum-resistant-crypto
9. Держспецзв'язок. Звіт про кібератаки в Україні (2023). URL: https://cip.gov.ua/cyberthreats
10. CERT-UA. Аналіз вразливостей IoT під час війни. URL: https://cert.gov.ua/iot-war
11. Стратегія квантового захисту / Міністерство цифрової трансформації України. URL: https://digital.gov.ua/quantum

Ключові слова: розумні будівлі, кібербезпека, блокчейн, кіберзагрози, IoT-пристрої

Keywords: smart buildings, cybersecurity, blockchain, cyber threats, IoT devices

ЕТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ ШІ В КІБЕРБЕЗПЕЦІ ТА ПРОБЛЕМИ ВІДПОВІДАЛЬНОСТІ

Бойченко Карина

студентка 1 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Використання штучного інтелекту (ШІ) у сфері кібербезпеки відкриває нові можливості для захисту інформації, оптимізації процесів та посилення захисту від кіберзагроз. Однак застосування ШІ також породжує низку етичних викликів і питань відповідальності, які потребують глибокого розгляду та регулювання на міжнародному рівні.

Одним із найбільших етичних викликів у кібербезпеці, що використовує штучний інтелект, є пошук балансу між конфіденційністю та безпекою. Системи ШІ обробляють величезні обсяги даних, серед яких можуть бути й високочутливі. При цьому процесі організаціям ефективніше виявляти загрози. Але також викликає питання щодо конфіденційності користувачів. Наприклад, компанії часто покладаються на основні показники кібербезпеки для моніторингу мережевої активності та ідентифікації підозрілої поведінки. Однак постійний моніторинг може призвести до збору особистих або нерелевантних даних, що ставить під загрозу конфіденційність користувачів. Система ШІ, призначена для посилення безпеки, може відстежувати поведінку співробітників для виявлення будь-яких аномалій. Хоча це забезпечує надійну безпеку, це також може означати збір особистих даних, не пов'язаних із потенційними загрозами. Організації повинні ретельно балансувати між потребою в безпеці та правом на конфіденційність, забезпечуючи, щоб їхні системи збирали лише необхідну інформацію [2].

ШІ в кібербезпеці може автономно приймати рішення, такі як блокування IP-адрес або ізоляція файлів. Коли ці автоматизовані дії призводять до помилок, постає питання відповідальності. Хто відповідальний, коли ШІ робить помилку? Фахівець із кібербезпеки, який впровадив систему ШІ, розробники ШІ чи організація в цілому? Наприклад, міжмережевий екран на основі ШІ помилково блокує критичну мережеву службу, спричиняючи значні збої. Визначення відповідальності стає складним завданням, оскільки потребує оцінки дій як системи ШІ, так і людських операторів, які її впровадили та підтримували.

Системи штучного інтелекту в кібербезпеці часто описують як «чорні ящики», тому що їх внутрішню роботу важко зрозуміти. Відсутність ясності створює серйозну проблему: підзвітність. Коли ШІ самостійно вживає заходів, таких як блокування доступу або карантин файлів, може бути важко визначити, хто несе відповідальність, коли щось йде не так. Наприклад, якщо система штучного інтелекту помилково закриває нешкідливу програму, викликаючи збої в бізнесі, хто винен? Це IT-команда, яка його налаштувала, розробники, що стоять за штучним інтелектом, чи компанія, яка покладається на нього? Ще більш актуальною зазначена проблема постає у системах, які передбачають безпеку кінцевої точки. Безпека кінцевих точок зосереджена на захисті таких пристроїв, як ноутбуки, персональні комп'ютери та мобільні телефони, від кіберзагроз, і ШІ часто застосовується для моніторингу та позначення незвичайної активності. Якщо упередження в ШІ призводить до того, що невинні програми будуть позначені як загрози, це може створити значні проблеми для бізнесу. Коли ШІ робить помилку, розуміння того, чому він прийняв це рішення, стає складним, що робить ще більш важливим мати чіткі рамки підзвітності [1].

ШІ може бути використаний зловмисниками для проведення соціальної інженерії. Сучасні алгоритми здатні аналізувати поведінку користувачів для створення правдоподібних фальшивих профілів або автоматизованої розсилки фішингових повідомлень. Наприклад, ШІ може розпізнавати вразливі групи

користувачів і створювати повідомлення, що стимулюють їх до розкриття конфіденційної інформації. Такі дії порушують етичні стандарти та підвищують ризики кіберзлочинів.

Алгоритми штучного інтелекту можуть відтворювати упередження, притаманні даним, на яких вони навчалися, що викликає етичні питання щодо справедливості та дискримінації. У сфері кібербезпеки це може призводити до несправедливого профілювання окремих груп. Наприклад, система виявлення загроз на основі ШІ може помилково визначати як шкідливі програми, якими переважно користуються представники певної демографії. Такі випадки піднімають питання упередженості в алгоритмах і потребують запровадження міжнародних етичних норм і регуляторних механізмів.

Показовою спробою врегулювання на міжнародному рівні деяких питань використання ШІ стало прийняття під час Хіросімського процесу зі штучного інтелекту (The G7 Hiroshima Artificial Intelligence Process) Міжнародних керівних принципів для організацій з розробки передових систем ШІ (The International Guiding Principles for Organizations Developing Advanced AI Systems) (далі – Керівні принципи) і Кодексу поведінки для організацій з розробки передових систем ШІ (The International Code of Conduct for Organizations Developing Advanced AI Systems) [2]. Але, варто зазначити, що положення в зазначених актах не є обов'язковими, вони відображають спільне бачення G7 та ЄС щодо напрямів подальшого регулювання ШІ.

Отже, етичні аспекти використання ШІ в кібербезпеці вимагають ґрунтовного підходу, особливо в контексті забезпечення конфіденційності даних, прозорості алгоритмів, розв'язання питань відповідальності, а також запобігання зловживанням з боку зловмисників. Розробка чітких міжнародних стандартів та механізмів регулювання сприятиме етичному використанню ШІ у кібербезпеці та забезпеченню довіри з боку суспільства.

Список використаних джерел

1. López González, A., Moreno, M., Moreno Román, A. C., Hadfeg Fernández, Y., & Cepero Pérez, N. (2024). Ethics in Artificial Intelligence: an Approach to Cybersecurity. Inteligencia Artificial, 27(73), 38–54. URL: https://doi.org/10.4114/intartif.vol27iss73pp38-54
2. Міжнародні стандарти регулювання штучного інтелекту. Аналіз актів, розроблених за результатами Хіросімського процесу з ШІ. URL: https://www.crowe.com/ua/croweacu/news/international-standards-for-regulating-artificial-intelligence

Ключові слова: штучний інтелект (ШІ), кібербезпека, захист інформації, етичні виклики, конфіденційність даних

Keywords: artificial intelligence (AI)**,** cybersecurity**,** information protection**,** ethical challenges**,** data privacy

Науковий керівник: PhD Грезіна О.

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В ПЕРСОНАЛЬНІЙ КІБЕРБЕЗПЕЦІ: АНАЛІЗ БЕЗПЕКИ КОРИСТУВАЦЬКИХ ДІЙ ТА ВИЯВЛЕННЯ ЗАГРОЗ

Годлевська Марія

студентка 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Грезіна Олена

PhD, асистент кафедри інформаційних технологій Національний університет «Одеська юридична академія»

Питання персональної кібербезпеки є критично важливими, особливо в умовах війни в Україні, коли кіберпростір стає полем для атак і маніпуляцій. Шахраї використовують все більш складні методи для викрадення особистої інформації та фінансових даних, підробки зображень та поширення небезпечних посилань. У цьому контексті застосування штучного інтелекту (ШІ) для захисту користувачів від шахрайства стає надзвичайно актуальним.

Рисунок 1 – Переваги використання ШІ в кібербезпеці

Однією з головних переваг ШІ в забезпеченні кібербезпеки є його здатність адаптуватися до нових загроз, автоматично аналізуючи дії користувачів на пристроях і розпізнаючи потенційні шахрайські схеми. Це особливо важливо, адже

технології шахрайства постійно змінюються і стають більш витонченими. Завдяки можливості навчатися на великих обсягах даних і самостійно оновлювати алгоритми, ШІ може вчасно розпізнавати небезпечні посилання, виявляти підроблені зображення та надавати користувачам рекомендації щодо безпеки. Такий інтелектуальний помічник є надійним союзником у забезпеченні захисту особистої інформації та протидії сучасним кіберзагрозам.

Кібератаки можуть завдати шкоди критичній інфраструктурі, впливаючи на роботу енергосистем, зв'язку, фінансових установ тощо. Також зростає кількість цільових атак на приватних осіб, що включають фішинг, шахрайство з банківськими даними, крадіжку особистої інформації та спроби компрометувати користувачів через шкідливі програми.[6]. У такому контексті кібербезпека стає важливим засобом захисту не лише особистих даних, а й національної стійкості та безпеки.

Зважаючи на це, в умовах, коли кіберзагрози є потужним інструментом гібридної війни, необхідність забезпечення кіберзахисту для громадян України стає першочерговим завданням. Особливо важливим є використання систем штучного інтелекту, які здатні виявляти небезпечні посилання, фішингові листи та підроблені зображення, адаптуючись до нових загроз. Захист особистих даних кожного українця є частиною загальної кібероборони країни, адже безпека громадян допомагає забезпечити стабільність і стійкість держави в умовах змін.

Наразі у сфері кібербезпеки вже існує кілька передових розробок, що використовують штучний інтелект для захисту користувачів від шахрайства. Такі інструменти аналізують дії користувачів, виявляють небезпечні посилання, фейкові зображення та інші загрози, надаючи рекомендації для безпечної взаємодії в інтернеті.

У цьому тексті розглянемо деякі з існуючих рішень, що використовують ШІ для забезпечення кібербезпеки:

Phish.ai та Vade Secure є прикладами платформ, що спеціалізуються на захисті від фішингових атак. Phish.ai аналізує вебсайти та електронні листи, порівнюючи їх із базою даних фішингових схем, щоб ідентифікувати потенційно небезпечні посилання [3]. Vade Secure, своєю чергою, інтегрується з електронною поштою й аналізує вміст повідомлень, попереджаючи користувачів про можливі фішингові атаки в реальному часі;

Norton AntiVirus з функцією Threat Intelligence AI є прикладом класичного антивірусного продукту, доповненого штучним інтелектом. Використовуючи дані з мільйонів пристроїв, Norton автоматично визначає нові загрози та реагує на них, забезпечуючи надійний захист від вірусів та інших шкідливих програм [4];

Amazon Rekognition пропонує рішення для ідентифікації підроблених зображень. Зазначена технологія комп'ютерного зору використовує алгоритми штучного інтелекту для аналізу зображень, розпізнаючи ознаки маніпуляцій. А також, спрямована допомагати захищати користувачів від підробленого контенту, що часто використовується в шахрайських схемах [1].

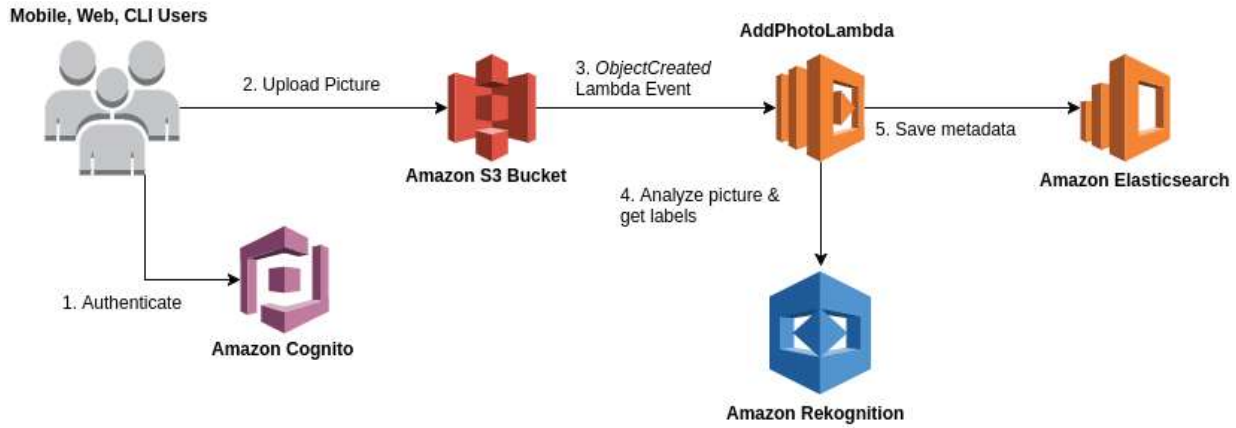

Рисунок 2 – Процес додавання зображення в Amazon Rekognition

Іншим важливим інструментом є Darktrace, яка імітує роботу імунної системи людини. Darktrace відстежує поведінкові моделі користувачів та пристроїв, виявляючи відхилення від норми. Якщо система виявляє аномалії, вона попереджає про потенційну загрозу або блокує її автоматично. Darktrace особливо корисна для корпоративних мереж, однак її принципи можуть бути використані для розробки захисту персональних пристроїв [7]. Ще одною перевагаю цього програмного продукту є його мобільна версія.

Google Safe Browsing, інтегрований у веб-браузери та мобільні застосунки, також використовує штучний інтелект для захисту від шахрайських посилань [2]. Safe Browsing аналізує запити мільйонів користувачів і визначає підозрілі сторінки, попереджаючи про них користувачів у реальному часі. Додатково, розширення для браузерів на основі ШІ, як-от Netcraft або Malwarebytes, допомагають користувачам уникати небезпечних сайтів.

Розглянемо ще один приклад програмного забезпечення з вбудованим штучним інтелектом. ZeroFox пропонує захист у соціальних мережах, де шахраї часто поширюють фейкові профілі та небезпечний контент. Використовуючи алгоритми штучного інтелекту для розпізнавання зображень і поведінкових патернів, ZeroFox здатний виявляти фальшиві акаунти й фішингові посилання, що покращує безпеку користувачів у соцмережах [5].

Кожен із цих інструментів фокусується на певних аспектах кіберзахисту, однак майбутні розробки можуть об’єднати їхні функції в єдиний комплексний застосунок-помічник.

Незважаючи на значні переваги, які були розглянули вище, штучний інтелект у сфері кібербезпеки має й певні недоліки. ШІ-системи залежать від якості й обсягу даних, на яких вони навчаються. Якщо вхідні дані містять помилки або обмежені певними типами загроз, модель може видавати хибні результати або пропустити нові види атак. Також ШІ вразливий до атак на самі моделі, наприклад, атак типу «отруєння даних», коли зловмисники цілеспрямовано вводять шкідливі дані для впливу на поведінку системи.

Інтеграція ШІ у кібербезпеку змінила підходи до захисту даних і боротьби з загрозами. Завдяки можливості аналізувати великі обсяги даних у реальному

часі та виявляти нові шаблони атак, ШІ значно підвищив ефективність і швидкість реагування на загрози[9].

Майбутнє ШІ в кібербезпеці відкриває широкі перспективи для розвитку нових рішень і підходів. Одним з ключових напрямків є розвиток адаптивних систем, здатних виявляти нові загрози в реальному часі й автоматично коригувати свої алгоритми на основі нових даних. Існує також перспектива розробки більш стійких моделей, що можуть працювати навіть при нестачі даних або протидіяти спробам отруєння даних[8]. Крім того, очікується, що ШІ зможе більш ефективно взаємодіяти з користувачами, забезпечуючи їм чіткі та зрозумілі рекомендації для підвищення рівня кібербезпеки у повсякденному житті.

Список використаних джерел

1. Amazon Rekognition. Automate and lower the cost of your image recognition and video analysis with ML. URL: https://aws.amazon.com/rekognition/?nc1=h_ls
2. Making the world's information safely accessible. URL: https://safebrowsing.google.com/
3. Phish.AI Overview.URL: https://finder.startupnationcentral.org/company_page/phish-ai
4. The new face of cyber threats–AI, deepfakes, and scams. URL: https://us.norton.com/blog/emerging-threats/threat-report-q2-2024
5. The only unified external cybersecurity platform – from protection to response. URL: https://www.zerofox.com/why-zerofox/
6. Кібербезпека під час війни. URL: https://stopfraud.com.ua/cybersecurity-in-wartime
7. Можливості та переваги Darktrace. URL: https://darktrace.com/
8. Прогнозувальний AI для кібербезпеки. Що взагалі працює і як це зрозуміти. URL: https://blackberry.bakotech.com/ua/predictive-ai-for-cybersecurity
9. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/the-role-of-ai-in-cybersecurity-anticipating-and-preventing-attacks

Ключові слова: кібербезпека, штучний інтелект, фішинг, персональна кібербезпека, кібершахрайство

Keywords: cyber security, artificial intelligence, fishing, personal cyber security, cyber fraud

ЗАСТОСУВАННЯ КОНТЕКСТУАЛЬНИХ ЕМБЕДДІНГІВ ДЛЯ ВИЯВЛЕННЯ ОЗНАК ШКІДЛИВИХ ВВЕДЕНЬ

Дика Анастасія

аспірантка кафедри інформаційних технологій
Національного університету «Одеська юридична академія»

У сучасному цифровому середовищі, де обсяг текстових даних стрімко зростає, виникає нагальна потреба у високоточному виявленні шкідливого

контенту, такого як мова ворожнечі, образливі висловлювання, дезінформація та шкідливі ін'єкції. У цьому контексті високу ефективність у виявленні шкідливих введень демонструють контекстуальні ембеддінги (embeddings), зокрема моделі на основі BERT (Bidirectional Encoder Representations from Transformers).

Контекстуальні ембеддінги – це подання слів у вигляді векторів (наборів чисел), які враховують контекст використання слова у реченні. Це означає, що одне і те саме слово матиме різне векторне представлення залежно від того, як і де воно вжите. Контекстуальні ембеддінги на основі моделі BERT працюють за принципом розуміння значення кожного слова в реченні з урахуванням усього його контексту – як слів до, так і після нього. Це стало можливим, завдяки архітектурі трансформера, яка використовує механізм уваги (attention) для аналізу зв'язків між усіма словами в реченні одночасно.

На відміну від моделей, які читають речення або лише зліва направо, або справа наліво, BERT є двонапрямленою моделлю. Це означає, що вона враховує повний контекст слова, аналізуючи всю послідовність навколо нього [1]. Наприклад, якщо модель обробляє слово «ключ», то вона врахує не лише попередні слова, а й ті, що йдуть після нього, щоб зрозуміти, чи йдеться про інструмент, пароль чи важливу підказку.

На сьогодні існують контекстуальні ембеддінги, які перевершують BERT за точністю, гнучкістю або ефективністю в низці NLP-завдань. До таких моделей належать модель DeBERTa (Decoding-enhanced BERT with Disentangled Attention), розроблена Microsoft [2], яка представляє собою вдосконалену версію BERT.

DeBERTa демонструє суттєві переваги над своїм попередником BERT, завдяки новим архітектурним рішенням. Зокрема, ця модель використовує розділене подання контенту та позиції в словах, що дозволяє точніше відстежувати відношення між токенами, не залежно від їхнього порядку. Це критично важливо для аналізу потенційно шкідливих введень, де зловмисники свідомо змінюють порядок символів, використовують escape-послідовності або інші методи обфускації. Крім того, DeBERTa демонструє покращену роботу з контекстом, завдяки модифікованому механізму уваги, який здатен враховувати глибокі семантичні зв'язки, навіть у складно структурованих рядках [3].

Під час аналізу HTTP-запитів або форм, де можливе впровадження XSS-ін'єкцій, модель DeBERTa здатна розпізнати нетипову лінгвістичну поведінку, не обмежуючись лише простим пошуком за шаблоном. Наприклад, вона може розпізнати, що рядок `<script>alert("XSS")</script>` і варіант із закодованими символами `%3Cscript%3Ealert('XSS')%3C/script%3E` мають ідентичну семантичну мету. У традиційних підходах такі варіанти зазвичай розглядаються як різні, а тому можуть бути пропущені при фільтрації. Завдяки контекстуальному навчанню модель DeBERTa не лише враховує індивідуальні символи чи токени, а й їх значення у контексті запиту, що забезпечує набагато вищу точність і повноту виявлення загроз.

Ще однією перевагою DeBERTa є її здатність до навчання на специфічних корпусах даних. У контексті безпеки це означає, що модель можна додатково тренувати на логах вебсерверів, на прикладах реальних атак або скомпільованих зловмисних запитах, що дозволяє суттєво покращити ефективність виявлення саме в рамках конкретної системи або вебзастосунку. Завдяки високій узагальнювальній здатності DeBERTa, навіть обмежений набір специфічних для певного домену прикладів може дати суттєвий приріст продуктивності.

На відміну від класичних BERT-підходів, модель DeBERTa краще масштабується для застосування в реальному часі, зокрема завдяки підтримці оптимізованих версій, як-от: DeBERTa-v3-small або distill-версій [4]. Це відкриває можливості для її інтеграції у вебфреймворки або WAF (Web Application Firewall), що працюють у режимі реального часу, де критично важливо забезпечити високу швидкість обробки запитів без втрати точності.

Використання моделі DeBERTa для виявлення XSS-атак становить ефективне поєднання високої точності, гнучкості, стійкості до обфускацій та адаптивності. Порівняно з базовим BERT, а також зі спрощеними евристичними системами, DeBERTa демонструє значно кращу здатність до узагальнення, розуміння контексту, а також розширення на нові, невідомі типи атак. Це робить її одним із найкращих інструментів сучасного покоління для побудови надійних систем захисту вебзастосунків від XSS-ін'єкцій.

Список використаних джерел

1. Fang Z., Zhang H., He J., Qi Z., Zheng H. Semantic and Contextual Modeling for Malicious Comment Detection with BERT-BiLSTM. *arXiv*. 2025. Vol. 2503.11084. URL: https://arxiv.org/abs/2503.11084
2. DeBERTa: Decoding-enhanced BERT with Disentangled Attention. URL: https://github.com/microsoft/DeBERTa.
3. Lin Y. Parameter Optimization in DeBERTa for Text Classification Using PCA on Limited GPU Resources. *Highlights in Science, Engineering and Technology*. 2024. Vol. 120. P. 88-94. URL: https://doi.org/10.54097/cq798v58.
4. He P., Gao J., & Chen W. Debertav3: Improving deberta using electra-style pretraining with gradient-disentangled embedding sharing. *arXiv*. 2021. Vol. 2111.09543. URL: https://arxiv.org/abs/2111.09543

Ключові слова: DeBERTa, XSS-атаки, веббезпека, контекстуальні ембеддінги, глибоке навчання, машинне навчання, обробка природної мови, виявлення вразливостей, аналіз шкідливого коду, семантичний аналіз тексту

Key words: DeBERTa, XSS attacks, web security, contextual embeddings, deep learning, machine learning, natural language processing, vulnerability detection, malicious input analysis, semantic text analysis

Науковий керівник: доцент Трофименко О.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ТА БЕЗПЕКИ ДАНИХ У СОЦІАЛЬНИХ МЕРЕЖАХ

Єфремова Вероніка

студентка 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

В сучасному світі, коли кожен має доступ до всесвітньої мережі Інтернет і має щонайменше одну соціальну мережу, питання конфіденційності та безпеки користувачів стає актуальнішим.

Згідно з положеннями Закону України «Про основні засади здійснення кібербезпеки України» формування безпечного, стійкого та надійного кіберпростору передбачає, зокрема, розвиток цифрової обізнаності населення й утвердження культури відповідального користування цифровими технологіями. Акцент робиться на оволодінні системними знаннями, уміннями та навичками, необхідними для досягнення цілей кіберзахисту, а також на реалізації державних і громадських ініціатив, спрямованих на підвищення усвідомлення ризиків та загроз у цифровому середовищі [2].

Стаття 32 Конституції України гарантує недопущення втручання в особисте й сімейне життя та забороняє обробку конфіденційної інформації без згоди особи, окрім випадків, передбачених законом в інтересах безпеки, добробуту та прав людини [1].

Соціальні мережі інтегровані в повсякденну реальність, трансформуючи способи комунікації, самопрезентації та інформаційної взаємодії. Навіть при відсутності активного створення контенту, кожна дія користувача – від перегляду сторінок до взаємодії з постами – залишає цифровий слід, що накопичується та аналізується в межах цифрових платформ.

Інформаційні системи соціальних мереж функціонують у двох вимірах – відкритому та прихованому. Відкритий вимір охоплює персональні відомості, які користувач самостійно розміщує: дані про сімейний статус, місце роботи, освіту, фотографії, дату народження, а також налаштування приватності.

Прихований вимір полягає у фоновому збиранні даних, що виникають під час взаємодії з платформою: вподобання, кількість переглядів, час активності, реакції на контент. Такі дані оброблюються алгоритмами на серверах і використовуються для побудови поведінкових моделей, прогнозування інтересів та створення персоналізованого інформаційного середовища.

Масове накопичення та аналіз цифрової поведінки дозволяє формувати аналітичні зрізи соціальних настроїв, виявляти домінуючі запити суспільства, розуміти структуру колективних емоцій і потреб. У той самий час доступ до подібних даних відкриває потенціал для інформаційного впливу, маніпуляції громадською думкою та цілеспрямованого конструювання наративів в інтересах

зацікавлених суб’єктів. Така практика використовується як інструмент інформаційного протистояння в умовах гібридної війни.

При реєстрації нового акаунта в соціальних мережах, користувач повинен погодитися на умови використання та політику конфіденційності. В них прописано як і коли веб-сайти можуть збирати інформацію з профілю користувача та його комп’ютера, як веб-сайти відстежують активність користувача та як вони забезпечують інформацію, зібрану з профілю користувача. Крім того, ці політики конфіденційності описують, коли інші користувачі можуть переглядати ваш профіль, а також коли і як веб-сайти можуть розкривати інформацію третім особам.

У своєму офіційному повідомленні компанія Facebook надала детальну відповідь щодо спектру інформації, яку платформа збирає від користувачів в процесі їхньої взаємодії з соціальною мережею. Аналіз представленої інформації демонструє, що збір даних охоплює широкий діапазон технічних параметрів пристроїв користувачів, включаючи технічні характеристики обладнання та програмного забезпечення. До цієї категорії належать відомості про операційну систему, версії програмного та апаратного забезпечення, поточний рівень заряду батареї, якість сигналу мережі, обсяг доступної пам'яті пристрою, тип використовуваного веб-переглядача, а також детальну інформацію про встановлені додатки, файли та плагіни. Крім того, система збирає дані про активність та поведінкові патерни користувачів на їхніх пристроях, що включає інформацію про статус активності програмних вікон, роботу в фоновому режимі та характер переміщення курсора миші, що дозволяє платформі розрізняти дії людини від автоматизованих систем та ботів.

Особливої уваги заслуговує процес збору та обробки різноманітних ідентифікаторів пристроїв та акаунтів користувачів. Facebook систематично збирає унікальні ідентифікатори пристроїв, спеціалізовані ID для ігор та додатків, ідентифікатори акаунтів, а також коди сімейних пристроїв та інші маркери, що є унікальними для продуктів компанії та пов'язані з конкретним пристроєм або користувацьким акаунтом. Паралельно з цим відбувається збір інформації про бездротові сигнали та мережеві з'єднання, що включає дані про Bluetooth-з'єднання, параметри найближчих Wi-Fi точок доступу, інформацію про радіомаяки та вишки стільникового зв'язку. Система також отримує доступ до налаштувань пристрою, які користувач активує добровільно, зокрема дані геолокації через GPS, доступ до камери та галереї фотографій. Додатково збираються мережеві параметри, такі як назва мобільного оператора або інтернет-провайдера, мовні налаштування системи, часовий пояс, номер мобільного телефону, IP-адреса користувача, швидкість інтернет-з'єднання, а також інформація про інші пристрої, підключені до тієї ж мережі, що особливо актуально при використанні функцій трансляції контенту між пристроями.

Результати аналізу засвідчують, що сучасні соціальні медіа-платформи функціонують як потужні системи збору та накопичення персональних даних, що значно перевершують за обсягом та деталізацією відкриту інформацію

користувацьких профілів. Зібрані дані охоплюють приховані аспекти цифрової поведінки користувачів, включаючи їхні переваги, патерни взаємодії з контентом та активність в межах платформи. Така інформаційна база дозволяє компаніям розробляти високоточні алгоритми персоналізації контенту та формувати прицільні маркетингові стратегії, адаптовані під індивідуальні інтереси та потреби кожного користувача. Водночас це створює значні ризики для конфіденційності та приватності користувачів, оскільки накопичена інформація може бути використана не лише для комерційних цілей, але й для аналітичних досліджень поведінкових патернів та потенційного впливу на формування громадської думки, що ставить під сумнів питання безпеки персональних даних користувачів.

Дослідження показують, що в екосистемі соціальних мереж користувачі генерують та залишають значні обсяги особистої інформації через два основні канали: свідоме розміщення контенту та несвідомий автоматизований збір даних платформами. Зазначена двоканальна система збору інформації забезпечує платформам можливість створення детальних цифрових профілів користувачів, що використовуються для генерації персоналізованих рекомендацій контенту та реклами.

З огляду на ці виклики, науковці та фахівці з кібербезпеки наголошують на критичній важливості підвищення рівня цифрової грамотності користувачів щодо питань кібербезпеки, забезпечення дотримання національного законодавства у сфері захисту персональних даних та впровадження міжнародних стандартів, що гарантують право громадян на приватність у цифровому просторі.

Список використаних джерел

1. Конституція України. Відомості Верховної Ради України. 1996. № 30. с. 141. URL: https://zakon.rada.gov.ua/rada/show/254%D0%BA/96-%D0%B2%D1%80
2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. Відомості Верховної Ради України. URL: http://zakon.rada.gov.ua/laws/show/2163-19

Ключові слова: інформаційні технології, конфіденційність даних, безпека даних, соціальні мережі

Keywords: information technology, data privacy, data security, social networks

Науковий керівник: PhD Грезіна О.

БЕЗПЕКА В SQL-СКБД: КОНТРОЛЬ ДОСТУПУ, ШИФРУВАННЯ ТА ЗАХИСТ ВІД ІН'ЄКЦІЙ

Муляр Олександр

студент 2 курсу факультету кібербезпеки та інформаційних технологій
Національний університет «Одеська юридична академія»

Грезіна Олена

PhD, асистент кафедри інформаційних технологій
Національний університет «Одеська юридична академія»

Зі зростанням обсягів і значущості даних, що зберігаються в реляційних базах даних, питання безпеки SQL-СКБД набувають критичної важливості. Сучасні підприємства та організації стикаються з постійно еволюціонуючими загрозами, що потребує комплексного підходу до захисту інформації. Незважаючи на розвиток технологій безпеки, за даними звіту Verizon Data Breach Investigation Report за 2024 рік, атаки на бази даних залишаються одним з найбільш поширених векторів компрометації корпоративних систем [1].

Дане дослідження фокусується на трьох ключових аспектах безпеки SQL-СКБД, а саме механізми контролю доступу та управління правами користувачів, технології шифрування даних як у стані спокою, так і при передачі та методи захисту від SQL-ін'єкцій та інших атак на рівні додатків.

SQL-ін’єкції становлять серйозну загрозу безпеці реляційних баз даних, оскільки дозволяють зловмисникам впроваджувати шкідливий SQL-код у вразливі запити через неналежно оброблене користувацьке введення. Такий підхід дає змогу обходити механізми автентифікації та авторизації, виконуючи несанкціоновані дії з даними, зокрема читання, модифікацію або видалення. Унаслідок атаки можливе розкриття конфіденційних відомостей, зокрема імен користувачів, паролів або банківських даних, а також пошкодження чи знищення інформації. Здобутий контроль над веб-застосунком і сервером бази даних відкриває шлях до масштабніших атак, що загрожують стабільності всієї інформаційної системи [2].

Приклад простої SQL-ін’єкції демонструє вихідний SQL-запит:

```
SELECT * FROM users WHERE username = 'admin' AND password = '1234';
```

Запит очікує, що користувач введе свої логін та пароль. Якщо дані передаються у запит без належної фільтрації або параметризації, то зловмисник може замість пароля ввести шкідливий фрагмент. Далі введення зловмисника:

```
' OR '1'='1
```

Результуючий SQL-запит після підстановки:

```
SELECT * FROM users WHERE username = 'admin' AND password = '' OR '1'='1';
```

Запит завжди буде повертати істину, оскільки `'1'='1'-` логічно істинне твердження. Таким чином, зловмисник може обійти перевірку пароля і увійти в систему як будь-який користувач, зокрема з адміністративними правами.

Сучасні SQL-СКБД реалізують багаторівневу модель контролю доступу, що включає ідентифікацію, аутентифікацію та авторизацію.

У корпоративному середовищі особливої значущості набуває атрибутивний контроль доступу (ABAC), що дозволяє динамічно визначати права на основі різних атрибутів користувача, ресурсу та контексту. Це особливо актуально для розподілених систем, де традиційні моделі контролю доступу можуть бути недостатньо гнучкими.

Ключовим принципом організації контролю доступу є надання користувачам та процесам мінімально необхідних прав для виконання їх функцій. Практична реалізація цього принципу включає створення деталізованих ролей із чітко визначеними привілеями; регулярний аудит та перегляд прав доступу; використання тимчасових підвищення привілеїв замість постійних високих прав; застосування контекстного контролю доступу, що враховує час, розташування та інші фактори.

Транспарентне шифрування даних стало стандартом захисту даних у стані спокою. Сучасні реалізації TDE (Transparent Data Encryption) у провідних СКБД (Oracle, Microsoft SQL Server, PostgreSQL) забезпечують шифрування лише на рівні файлів даних, журналів транзакцій і резервних копій. Важливими аспектами впровадження TDE є управління ключами шифрування та їх ротація, мінімізація на продуктивність, інтеграція із зовнішніми системами управління ключами.

Задля більш гранулярного контролю за конфіденційними даними сучасні СКБД пропонують механізми шифрування лише на рівні окремих стовпців і навіть осередків. Зазначений процес застосовує різні рівні захисту до різних категорій даних, мінімізувати вплив на продуктивність, шифруючи лише критичні дані, реалізовувати різні політики доступу до зашифрованих даних.

Серед перспективних напрямів слід відзначити гомоморфне шифрування, що дозволяє виконувати операції над зашифрованими даними без їх попереднього розшифрування, що суттєво знижує ризик компрометації в процесі обробки.

Найбільш ефективним методом запобігання SQL-ін'єкцій залишається використання підготовлених виразів (prepared statements) та параметризованих запитів. Даний підхід забезпечує чіткий поділ коду SQL та даних, запобігаючи можливості впровадження шкідливого коду.

Сучасні СКБД інтегрують просунуті системи виявлення та запобігання вторгненням (IDS/IPS), здатні виявляти аномальні патерни запитів та блокувати потенційно шкідливу активність. Системи використовують сигнатурний аналіз виявлення відомих патернів атак, поведінковий аналіз виявлення аномальної активності, машинне навчання адаптивного виявлення нових векторів атак.

Незважаючи на ефективність підготовлених виразів, комплексний захист вимагає багаторівневого підходу, що включає строгу валідацію вхідних даних на відповідність очікуваного формату, застосування білих списків допустимих значень, екранування спеціальних символів для формування динамічних запитів.

Однією з перспективних тенденцій є застосування алгоритмів машинного навчання автоматизації управління доступом. Системи аналізують патерни доступу користувачів та процесів до даних, виявляють аномалії та адаптують політики безпеки в режимі реального часу.

Забезпечення безпеки SQL-СКБД вимагає комплексного підходу, що охоплює контроль доступу, шифрування даних та захист від ін'єкцій SQL. Сучасні дослідження підтверджують, що найбільш ефективною є багаторівнева безпекова стратегія, що поєднує технічні заходи з організаційними політиками і процедурами.

Аналіз поточних тенденцій показує усунення фокусу у бік автоматизації управління безпекою на основі технологій машинного навчання та інтеграції з хмарними сервісами. Ці напрями відкривають нові можливості підвищення рівня захисту при одночасному зниженні адміністративного навантаження. Подальші дослідження в цій галузі доцільно зосередити на розробці адаптивних механізмів безпеки, здатних ефективно протистояти загрозам, що еволюціонують, в умовах динамічно змінних інфраструктур і вимог до обробки даних.

Список використаних джерел

1. Verizon Data Breach Investigation Report URL: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf
2. SQL-ін’єкції та захист від них. URL: https://foxminded.ua/sql-iniektsii/

Ключові слова: SQL-СКБД, SQL-ін’єкції, контроль доступу, безпека в SQL-СКБД

Keywords: SQL-DBMS, SQL-injection, access control, security in SQL-DBMS

РОЗРОБКА СИСТЕМ АВТОМАТИЧНОГО МОНІТОРИНГУ НЕЗАКОННОГО РОЗПОВСЮДЖЕННЯ МУЛЬТИМЕДІА В ІНТЕРНЕТІ

Овчинников Микола

аспірант кафедри кібербезпеки
Національного університету «Одеська юридична академія»

У сучасному цифровому суспільстві мультимедійний контент – відео, аудіо, зображення – відіграє ключову роль у культурному, освітньому та комерційному середовищі. Завдяки розвитку Інтернету та цифрових технологій обсяг створеного і поширеного мультимедійного контенту значно зріс, що створює нові можливості для користувачів і бізнесу. Водночас це призводить до зростання

проблем, пов'язаних із незаконним розповсюдженням і використанням мультимедійних матеріалів, що становить серйозну загрозу для правовласників та авторів. Незаконне копіювання, піратство та поширення контрафактного контенту призводять до значних економічних збитків та зниження мотивації творців контенту [1, 2].

Сучасні правові та технічні заходи захисту інтелектуальної власності часто виявляються недостатніми через масштабність і швидкість поширення інформації в Інтернеті. Тому виникає необхідність розробки ефективних автоматизованих систем моніторингу, які здатні в реальному часі ідентифікувати факти нелегального використання мультимедійних даних, а також надавати інформацію для оперативного реагування і захисту прав власників [3, 4].

Автоматичний моніторинг незаконного розповсюдження мультимедійного контенту базується на сучасних методах обробки сигналів, цифрових водяних знаках (ЦВЗ), технологіях машинного навчання та аналізі великих даних. Впровадження таких систем підвищує ефективність захисту авторських прав, дозволяє оперативно виявляти порушення і мінімізувати фінансові втрати [5, 6].

Метою даної роботи є розробка інформаційної системи автоматичного моніторингу незаконного розповсюдження мультимедійних даних в Інтернеті. У ході дослідження буде проаналізовано сучасні технології і підходи до виявлення порушень, а також запропоновано і описано принцип роботи прототипу системи, який забезпечить комплексний і автоматизований підхід до захисту інтелектуальної власності у цифровому середовищі. У цих тезах не передбачено повної розробки всієї системи, а розглядаються основні концепції та архітектурні рішення для подальшої реалізації.

Приблизна схема роботи системи автоматичного моніторингу

Система автоматичного моніторингу незаконного розповсюдження мультимедійних даних в Інтернеті складається з кількох основних компонентів:

1. Збір мультимедійного контенту.

Перший етап полягає у зборі мультимедійного контенту з різноманітних онлайн-джерел: соціальних мереж, відеохостингів (наприклад, YouTube, Vimeo), торрент-трекерів, файлообмінних сервісів, стримінгових платформ та звичайних вебсайтів. Для цього застосовуються інструменти веб-скрапінгу (наприклад, Scrapy, BeautifulSoup) та API, які дозволяють автоматизовано отримувати нові публікації або файли за заданими критеріями. Окремі дослідження показують ефективність таких підходів у виявленні первинних джерел поширення піратського контенту [1, 2, 7].

2. Індексація та формування бази даних.

Після збору даних мультимедійні файли проходять попередню обробку: здійснюється витяг ознак (feature extraction), створення цифрових хешів або вбудовування водяних знаків (watermarking). Це забезпечує можливість порівняння файлів за їх унікальними ознаками незалежно від формату, якості чи незначних

змін у вмісті. Оброблені метадані зберігаються в централізованій базі для подальшого аналізу та швидкого пошуку [3, 4, 6].

3. Автоматичне порівняння контенту.

Система аналізує щойно зібрані файли та порівнює їх з легітимним реєстром мультимедійних об'єктів. Для цього використовуються алгоритми хешування (наприклад, perceptual hash, average hash), методи цифрового водяного маркування, а також алгоритми машинного навчання, здатні розпізнавати часткові або змінені копії (наприклад, CNN, Siamese networks). Цей підхід дозволяє виявляти навіть фрагментарні збіги, що ускладнює обхід системи [5, 6, 8].

4. Повідомлення про порушення.

Після ідентифікації порушення система формує відповідний звіт для правовласника. У деяких випадках можливе автоматичне інформування адміністрацій платформ (наприклад, через інструменти типу YouTube Content ID або Facebook Rights Manager), або ініціація запиту на видалення контенту відповідно до DMCA-процедур. Також система може накопичувати статистику повторних порушень для подальших юридичних дій [2, 5, 9].

```python
import hashlib

# Функція для обчислення хешу файлу (SHA-256)
def calculate_file_hash(file_path):
    sha256_hash = hashlib.sha256()
    with open(file_path, "rb") as f:
        for byte_block in iter(lambda: f.read(4096), b""):
            sha256_hash.update(byte_block)
    return sha256_hash.hexdigest()

# Приклад бази легітимних хешів (у реальній системі це БД)
legit_hashes = {
    "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
    "a54d88e06612d820bc3be72877c74f257b561b19",
    # інші хеші
}

# Перевірка хешу нового файлу
def check_file_legitimacy(file_path):
    file_hash = calculate_file_hash(file_path)
    if file_hash in legit_hashes:
        print(f"Файл {file_path} легітимний.")
    else:
        print(f"Файл {file_path} потенційно нелегальний!")

# Приклад виклику
check_file_legitimacy("example_video.mp4")
```

Рисунок 1 – Пошук мультимедійних файлів за хешем (Python)

Цей простий приклад демонструє базовий принцип – обчислення унікального цифрового підпису (хешу) мультимедійного файлу та порівняння його з базою легітимних матеріалів. У реальних системах ця логіка значно ускладнюється, включаючи нечіткий пошук схожих файлів, аналіз фрагментів, використання цифрових водяних знаків та алгоритмів машинного навчання [3, 4, 7].

У роботі розглянуто концепцію створення інформаційної системи автоматичного моніторингу незаконного розповсюдження мультимедійного контенту

в Інтернеті. Основна увага приділена принципам функціонування такої системи, яка складається з чотирьох ключових етапів: збору контенту, його індексації, порівняння з легітимною базою даних та формування звітів про порушення.

Запропонована схема роботи демонструє можливість побудови комплексного автоматизованого рішення на основі сучасних технологій цифрового водяного маркування, хешування, аналізу метаданих та машинного навчання. Такий підхід дозволяє значно підвищити ефективність виявлення правопорушень, мінімізувати участь людини та оперативно реагувати на факти порушення авторських прав.

У межах тезисів не ставиться за мету реалізація повнофункціональної системи, однак запропоновано концептуальну модель, яка може бути використана як основа для подальшої розробки й досліджень у галузі захисту інтелектуальної власності в цифровому середовищі.

Список використаних джерел

1. Sahu A. K. (ed.). Multimedia watermarking: Latest developments and trends. – Springer Nature, 2024.
2. Leuzzi V. Automated Copyright Enforcement Online: How Platforms stifle Creativity by reducing Technological Cost //Trento Student Law Review. – 2024. – Т. 6. – №. 2. – С. 17-72.
3. Gray J. E., Suzor N. P. Playing with machines: Using machine learning to understand automated copyright enforcement at scale //Big Data & Society. – 2020. – Т. 7. – №. 1. – С. 2053951720919963.
4. Kadian P., Arora S. M., Arora N. Robust digital watermarking techniques for copyright protection of digital data: A survey //Wireless Personal Communications. – 2021. – Т. 118. – С. 3225-3249.
5. Helgadóttir Á. G. The Use of Automatic Content Recognition Technologies for Content Moderation and Control.
6. Kothari A. M., Dwivedi V., Thanki R. M. Watermarking techniques for copyright protection of videos. – Cham : Springer International Publishing, 2019.
7. Menéndez M., González R., Guerrero C. Multimedia content identification for copyright protection in peer-to-peer networks //Multimedia Tools and Applications. – 2020. – Т. 79. – №. 43. – С. 32291–32317.
8. Tewari S., Mishra R. Multimedia forensics and machine learning: A survey //Multimedia Tools and Applications. – 2021. – Т. 80. – С. 8013–8051.
9. Nguyen D. N., Nguyen T. V., Ko B. J. Online copyright infringement detection: challenges and future directions //ACM Computing Surveys (CSUR). – 2023. – Т. 55. – №. 10. – С. 1–37.

Ключові слова: моніторинг, захист авторських прав, інтелектуальна власність, цифровий водяний знак (ЦВЗ), хешування, машинне навчання, мультимедійні дані, автоматизація

Keywords: monitoring, copyright protection, intellectual property, digital watermark (DW), hashing, machine learning, multimedia data, automation

Науковий керівник: доцент Ахмаметьєва Г.

АУТЕНТИФІКАЦІЯ БЕЗ ПАРОЛЯ: ПЕРСПЕКТИВИ ТА ЗАГРОЗИ

Кухаренко Сергій
доцент кафедри кібербезпеки
Національного університету «Одеська юридична академія»,
кандидат технічних наук, доцент

Овчинников Микола
асистент кафедри кібербезпеки
Національного університету «Одеська юридична академія»

Традиційні паролі вже давно вважаються одним з найслабших елементів у системах кібербезпеки. Вони схильні до широкого спектра атак: фішингових кампаній, підбору за словниками (dictionary attacks), атак грубою силою (brute force), а також до проблем повторного використання на різних ресурсах. Навіть за умови використання складних паролів, людський фактор (наприклад, зберігання паролів у відкритому вигляді або передача їх через небезпечні канали) суттєво знижує ефективність таких засобів захисту. Статистика свідчить, що понад 80% успішних атак на облікові записи відбуваються саме через слабкі або скомпрометовані паролі [1].

У відповідь на ці виклики з'являються сучасні методи безпарольної аутентифікації, серед яких провідну роль відіграють стандарти FIDO2 та WebAuthn. Ці підходи використовують асиметричну криптографію, де приватний ключ зберігається безпосередньо на пристрої користувача (наприклад, у безпечному середовищі смартфона чи апаратному токені), а публічний ключ передається серверу під час реєстрації. Для аутентифікації користувач підтверджує свою особу за допомогою біометричних даних (відбитка пальця, розпізнавання обличчя) або PIN-коду – однак ці дані ніколи не покидають пристрій [2].

Безпарольні технології не лише значно підвищують рівень безпеки, але й спрощують взаємодію з цифровими сервісами. Користувачам більше не потрібно запам'ятовувати десятки складних паролів або змінювати їх через певний період часу. Це особливо важливо у контексті масштабного зростання цифрових платформ, де користувачі мають десятки, а то й сотні облікових записів.

Переваги безпарольної аутентифікації включають:

- значне підвищення безпеки (немає паролів – немає об'єктів фішингу чи перехоплення);
- зменшення навантаження на служби підтримки (не потрібно скидати забуті паролі);
- зручність для користувача (автоматичний доступ через пристрій, біометрію або апаратний токен);
- відповідність сучасним стандартам кібербезпеки, включаючи GDPR, NIST SP 800-63B, ISO/IEC 29115.

Варто також зазначити, що підтримка безпарольної аутентифікації вже інтегрована у більшість сучасних браузерів (Google Chrome, Mozilla Firefox, Microsoft Edge) та операційних систем (Windows Hello, Android, iOS), що робить її доступною для широкого впровадження як у бізнесі, так і у державному секторі [3].

Розробка та стандартизація безпарольної аутентифікації координується Альянсом FIDO (Fast Identity Online), який об'єднує понад 250 компаній, включаючи Google, Microsoft, Apple, Intel та інші [4].

До переваг безпарольної аутентифікації можна віднести наступне:

1. Захист від фішингу та атак типу «людина посередині» (MITM). Безпарольні рішення, такі як WebAuthn, використовують асиметричну криптографію, де приватний ключ залишається лише на пристрої користувача й ніколи не передається мережею. Це значно знижує ризики фішингу, оскільки навіть якщо зловмисник отримає контроль над фішинговим сайтом, він не зможе перехопити чи повторно використати автентифікаційні дані [5]. Дослідження компанії Google показали, що використання безпарольної аутентифікації майже повністю усуває фішингові атаки на акаунти [8].

2. Покращений користувацький досвід. Аутентифікація за допомогою біометричних даних (відбитка пальця, розпізнавання обличчя) або апаратних ключів (наприклад, YubiKey) є швидкою, зручною та інтуїтивно зрозумілою. Це дозволяє користувачам входити в системи без потреби вводити складні паролі, що особливо важливо для людей з обмеженими можливостями або в умовах підвищеного навантаження [6].

3. Усунення необхідності запам’ятовування паролів. Оскільки користувачам більше не потрібно створювати й запам’ятовувати складні паролі, знижується ймовірність їх повторного використання або збереження в небезпечних місцях. Це також значно зменшує навантаження на служби підтримки, адже більшість звернень стосується саме відновлення паролів [9].

Крім переваг можливі деякі ризики та проблеми, пов’язані з безпарольною аутентифікацією. Наприклад це:

1. Відновлення облікових записів. У разі втрати пристрою або токена, який використовується для аутентифікації, виникає потреба в альтернативних механізмах відновлення доступу. Якщо такі механізми будуть слабко захищені, вони можуть стати новою точкою атаки. З іншого боку, надто складні процедури відновлення можуть призвести до втрати доступу навіть законними користувачами [7].

2. Сумісність пристроїв. Не всі пристрої, особливо старі моделі, підтримують протоколи FIDO2/WebAuthn або не мають необхідних апаратних компонентів (наприклад, TPM чи Secure Enclave). Це ускладнює масштабне впровадження безпарольної аутентифікації в організаціях з великою кількістю гетерогенних пристроїв [10].

3. Початкові витрати на впровадження. Для переходу на безпарольну аутентифікацію організаціям необхідно інвестувати в закупівлю сумісних пристроїв (апаратних токенів, біометричних сенсорів), модернізацію інфраструктури та навчання персоналу. Це може бути особливо складно для малих і середніх підприємств, що мають обмежений бюджет [5].

Нижче наведемо спрощений приклад на Python з використанням вебстандарту WebAuthn та бібліотеки python-fido2 для реєстрації та аутентифікації користувача:

```
from fido2 import webauthn
# Ініціалізація сервера WebAuthn
server = webauthn.WebAuthnServer()
# Генерація виклику для реєстрації
challenge = server.register_begin()
# Запит до користувача для створення нового облікового запису
credential = prompt_user_for_credential(challenge)
# Завершення реєстрації
server.register_complete(credential)
# Генерація виклику для аутентифікації
auth_challenge = server.authenticate_begin()
# Запит до користувача для аутентифікації
auth_credential = prompt_user_for_authentication(auth_challenge)
# Завершення аутентифікації
server.authenticate_complete(auth_credential)
```

Функції prompt_user_for_credential та prompt_user_for_authentication є умовними та повинні бути реалізовані відповідно до конкретного інтерфейсу користувача.

Для кращого розуміння принципу схеми дії безпарольної аутентифікації за стандартом FIDO2/WebAuthn доцільно звернутись до діаграми, яка демонструє ключові етапи взаємодії між учасниками процесу: користувачем, клієнтським додатком (зазвичай веббраузером), сервером автентифікації та автентифікатором (апаратним ключем або біометричним модулем пристрою) [11].

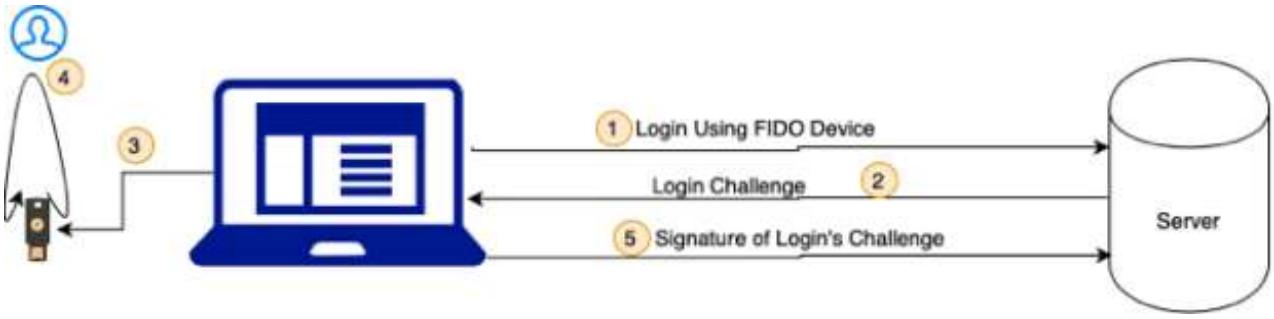

Рисунок 1 – FIDO authentication process

Процес аутентифікації складається з таких кроків:

– Запит на аутентифікацію.

Користувач переходить на сайт або у вебдодаток і ініціює вхід. Браузер надсилає запит на початок аутентифікації до сервера.

– Генерація виклику (challenge).

Сервер створює випадковий криптографічний виклик (challenge) і передає його клієнтському додатку разом із параметрами, що описують дозволені методи аутентифікації.

– Підписування виклику автентифікатором.

Браузер за допомогою API WebAuthn передає виклик автентифікатору користувача. Це може бути фізичний ключ, пристрій із біометричним сенсором або модуль безпеки, вбудований у пристрій. Користувач підтверджує свою присутність (наприклад, дотиком або відбитком пальця), і автентифікатор створює підпис за допомогою приватного ключа.

– Передача підпису на сервер.

Підписаний виклик разом з ідентифікатором публічного ключа відправляється на сервер для перевірки.

– Верифікація підпису.

Сервер використовує збережений публічний ключ, щоб перевірити дійсність підпису та підтвердити автентичність користувача. У разі успішної перевірки – користувач отримує доступ до облікового запису.

Такий підхід забезпечує високий рівень безпеки, оскільки приватний ключ ніколи не залишає пристрій користувача, а дані не передаються у відкритому вигляді. Крім того, кожен виклик є унікальним, що виключає можливість повторного використання автентифікаційних даних.

Отже, можливо зробити висновок, що безпарольна аутентифікація представляє собою перспективний напрямок у сфері інформаційної безпеки, пропонуючи підвищену захищеність та зручність для користувачів. Однак її впровадження супроводжується певними викликами, такими як забезпечення сумісності пристроїв, організація процесів відновлення облікових записів та початкові витрати. Подальші дослідження та розробки в цій галузі сприятимуть подоланню цих перешкод та широкому впровадженню безпарольних технологій.

Список використаних джерел

1. Verizon. (2023). Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/
2. Ravilla H., Sayal R., Kulkarni P. Study and Analysis of FIDO2 Passwordless Web Authentication //International Conference on Advances in Computational Intelligence and Informatics. – Singapore : Springer Nature Singapore, 2023. – С. 375-386.
3. Shukla S. et al. A Passwordless MFA Utlizing Biometrics, Proximity and Contactless Communication //arXiv preprint arXiv:2406.09000. – 2024.
4. 4. Rajput S. et al. Beyond Passwords: Trends and Innovations in Password less Authentication. – 2025.
5. Bhatia, G., Kumar, A., & Sharma, M. (2020). Web Authentication using FIDO2 and WebAuthn. International Journal of Engineering Research & Technology (IJERT), Vol. 9, Issue 10. https://www.ijert.org/web-authentication-using-fido2-and-webauthn

6. Shukla, S., Varshney, G., Singh, S., & Goel, S. (2024). A Passwordless MFA Utilizing Biometrics, Proximity and Contactless Communication. arXiv preprint arXiv:2406.09000. https://arxiv.org/abs/2406.09000
7. De Carne, G., Mühlhäuser, M., & Krauß, C. (2021). From Passwords to Passwordless: A Study on User Authentication for the Web. 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). https://doi.org/10.1109/EuroSPW54576.2021.00019
8. Google Security Blog. (2019). New research: Security keys neutralize phishing attacks. https://security.googleblog.com/2019/05/new-research-security-keys-neutralize.html
9. Microsoft. (2021). The end of passwords: new passwordless options. https://techcommunity.microsoft.com/t5/security-compliance-and-identity/the-end-of-passwords-new-passwordless-options/ba-p/2654622
10. FIDO Alliance. (2020). The State of Passwordless Authentication Deployment. https://fidoalliance.org
11. Alqubaisi F. et al. Should we rush to implement password-less single factor FIDO2 based authentication? //2020 12th annual undergraduate research conference on applied computing (URC). – IEEE, 2020. – С. 1-6.

Ключові слова: автентифікація, авторизація, безпарольна аутентифікація, безпека, захист даних, конфіденційність, FIDO2, WebAuthn

Keywords: authentication, authorization, passwordless authentication, security, data protection, privacy, FIDO2, WebAuthn

ВІРУСНИ ЧЕЛЕНДЖІ

Сергійчик Дар'я

студентка 1-го курсу факультету психології, політології та соціології Національного університету «Одеська юридична академія»

У сучасному цифровому суспільстві, де інформаційні потоки поширюються миттєво, а нові тренди народжуються щодня, особливу роль почали відігравати так звані вірусні челенджі. Це явище стало невід'ємною складовою молодіжної культури та онлайн-спілкування, а іноді й більш широких соціальних процесів. Вірусні челенджі є прикладом короткострокових масових дій, які виникають, поширюються та зникають у цифровому просторі, часто без явного авторства чи контролю. Вони приваблюють людей різного віку, проте найактивнішими учасниками стають підлітки та молодь – ті, хто найбільше інтегровані у простір соціальних мереж. [1]

Поняття «вірусний челендж» (від англ. viral challenge) об'єднує різноманітні дії, завдання чи ритуали, які користувачі соціальних мереж виконують у межах певного тренду, фіксують на фото або відео й публікують у відкритому доступі. Однією з ключових характеристик таких челенджів є їхня швидкість поширення – за аналогією до біологічного вірусу, інформація заражає дедалі більшу кількість

людей, які повторюють дії за іншими. Популярності цьому феномену сприяють механізми гейміфікації, соціального порівняння, бажання привернути увагу та залученість у мережеву спільноту. [2]

З одного боку, вірусні челенджі можуть виконувати важливі функції в соціальному житті: розважати, підтримувати позитивні емоції, сприяти згуртуванню навколо певної ідеї, популяризувати соціальні ініціативи. Прикладом позитивного челенджу став Ice Bucket Challenge, який мав на меті збір коштів на дослідження БАС (хвороби Лу Геріга). Люди по всьому світу обливали себе холодною водою, номінували інших на участь і жертвували гроші. Кампанія отримала величезне охоплення та зібрала понад 100 мільйонів доларів для медичних досліджень. Інші приклади – #TrashTag Challenge (прибирання сміття), #ReadABook Challenge (популяризація читання), #JerusalemaChallenge (танцювальна ініціатива, яка сприяла емоційному піднесенню під час пандемії COVID-19).[3]

Однак, попри очевидні позитиви, значна частина вірусних челенджів викликає занепокоєння через свій зміст, характер або наслідки. Існує безліч прикладів деструктивних, небезпечних або навіть смертельних челенджів. Одним із найвідоміших став «Blue Whale Challenge» (2016–2017), що спонукав учасників до серії небезпечних завдань, кульмінацією яких було самогубство. Ще одним тривожним прикладом є «Benadryl Challenge», у межах якого підлітки вживали великі дози антигістамінного препарату, щоб викликати галюцинації, що в окремих випадках призвело до летальних наслідків. Аналогічно, «Blackout Challenge» заохочував учасників перекривати собі дихання до втрати свідомості, що також мало трагічні результати.

Психологічні чинники участі в таких челенджах пов’язані з впливом соціальних мереж на самосприйняття, соціальну ідентичність та самооцінку. У цифровому просторі користувачі схильні шукати схвалення та уваги, що проявляється в потребі отримати лайки, коментарі, репости. Участь у вірусному челенджі – це спосіб не лише розважитися, а й підвищити соціальний статус, продемонструвати креативність, сміливість чи приналежність до спільноти. При цьому мотивації можуть відрізнятися залежно від віку, статі, культурного контексту та рівня саморефлексії особистості. Для підлітків особливо важливими є ефекти групового тиску, потреба у визнанні та прагнення до самоствердження. [4]

Соціальні мережі – інструмент, який як підсилює позитивні, так і загострює негативні аспекти онлайн-участі. Їхні алгоритми налаштовані на підтримку контенту, який викликає найсильніші емоції та взаємодії, тож іноді саме небезпечні, провокативні або шокуючі челенджі потрапляють у топ рекомендацій. Учасники нерідко не усвідомлюють, що їхня участь може стати частиною ширшого маніпулятивного процесу. Наприклад, деякі деструктивні челенджі є результатом діяльності спеціально створених груп, що мають на меті впливати на вразливу молодь або навіть координуються зі злочинними цілями.

Ще однією проблемою є брак цифрової компетентності. Значна частина підлітків не має навичок критичного осмислення інформації, не вміє оцінювати

потенційні ризики та не завжди розуміє довгострокові наслідки власних дій у мережі. Саме тому зростає потреба у впровадженні програм цифрової освіти – як у формальному навчанні, так і в позашкільній діяльності. Медіаграмотність має стати ключовою складовою виховання в умовах інформаційного суспільства.[5]

Також важливою є роль батьків, вчителів та менторів. Дорослі повинні не лише контролювати онлайн-активність дітей, а й створювати середовище довіри, відкритого діалогу, в якому дитина зможе обговорювати власні враження від побаченого чи почутого в мережі. Сувора заборона або покарання часто викликають зворотну реакцію – приховування або ще більший інтерес до забороненого. Натомість ефективним підходом є формування усвідомленого споживання інформації та виховання відповідального ставлення до себе й інших в онлайн-середовищі.

Ще одним важливим аспектом є роль впливових осіб – блогерів, лідерів думок, публічних особистостей, які часто першими беруть участь у челенджах або стають їх авторами. Вони мають велику аудиторію та високий рівень довіри з боку підписників, особливо молодих. Таким чином, їхня участь у небезпечних або недоречних флешмобах може нести серйозну відповідальність. На противагу цьому, позитивні приклади публічних осіб, які закликають до безпеки, саморозвитку, творчості, можуть мати конструктивний вплив і навіть стати інструментом профілактики ризикової поведінки.

У підсумку слід зазначити, що вірусні челенджі – це складне й багатогранне явище, яке не можна однозначно оцінити лише з позитивного або негативного боку. Вони відображають динаміку цифрової культури, потреби сучасної молоді, особливості комунікації в нових медіа. Проте масштабні наслідки деяких челенджів змушують науковців, освітян і суспільство загалом замислитися над питанням етичних меж, регуляції, інформаційної безпеки та відповідальності всіх учасників цифрового простору. Лише шляхом комплексного підходу – через освіту, просвіту, підтримку та критичне мислення – можна зробити простір соціальних мереж безпечнішим, а самі челенджі – корисним інструментом розвитку, співпраці та натхнення.

Список використаних джерел

1. Найнебезпечніші інтернет-челенджі: як уберегти дитину. URL: https://www.security.org/digital-safety/most-dangerous-online-challenges
2. Viral Internet Challenges: A Study on the Motivations Behind Social Media User Participation. URL: https://www.researchgate.net/publication/346597632_Viral_Internet_Challenges_A_Study_on_the_Motivations_Behind_Social_Media_User_Participation
3. Онлайн-безпека для молоді – посібник ОБСЄ «Онлайк». URL: https://www.osce.org/files/f/documents/0/f/483533.pdf

4. How to Talk to Your Children About Dangerous Social Media Challenges. URL: https://www.verywellfamily.com/how-to-talk-to-your-children-about-dangerous-social-media-challenges-6742685
5. 11 Most Memorable Social Media Challenges. URL: https://www.revolt.tv/article/11-most-memorable-social-media-challenges

Ключові слова: вірусні челенджі, соціальні мережі, молодь, онлайн-тренди, цифрова культура, медіаграмотність, деструктивна поведінка, психологічні ризики, груповий тиск, самоідентифікація

Keywords: viral challenges, social media, youth, online trends, digital culture, media literacy, destructive behavior, psychological risks, peer pressure, self-identity

Науковий керівник: доцент Чанишев Р.І.

ЛЮДСЬКИЙ ФАКТОР ЯК КРИТИЧНИЙ ЕЛЕМЕНТ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Соловйов Артем

асистент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»

У системах забезпечення інформаційної безпеки традиційно приділяється велика увага технічним засобам захисту, таким як:

- шифрування;
- антивірусні програми;
- міжмережеві екрани;
- системи виявлення вторгнень.

Однак зростаюча кількість успішних кібератак демонструє, що саме людський фактор залишається найслабшою ланкою в загальній структурі безпеки. Користувачі можуть несвідомо ставати джерелом загроз через недостатню обізнаність, порушення політик безпеки або вплив соціальної інженерії. Метою є виявлення основних типів людських помилок у контексті інформаційної безпеки, аналіз причин їх виникнення, а також дослідження методів підвищення користувацької відповідальності й обізнаності.

Детально аналізується соціотехнічний підхід як сучасна концепція забезпечення інформаційної безпеки, що інтегрує технічні рішення із розумінням поведінкових, психологічних та організаційних чинників. Такий підхід дозволяє не лише підвищити ефективність захисту інформаційних систем, але й враховувати особливості взаємодії людини з технологіями, рівень її обізнаності, мотивації та можливих помилок. Особлива увага приділяється тому, як поєднання технічних засобів безпеки з навчанням персоналу, формуванням корпоративної культури безпеки та впровадженням чітких процедур може забезпечити комплексний

захист в умовах зростання соціально орієнтованих загроз, таких як фішинг, маніпулятивні методи чи внутрішні загрози з боку персоналу [1].

Актуальність цієї теми зростає на фоні глобальних змін у сфері роботи та безпеки. З переходом багатьох організацій на віддалену або гібридну форму роботи, а також в умовах гібридної війни, що триває в Україні, людський фактор стає ще більш критичним. Недостатній контроль над діями співробітників у домашніх умовах значно підвищує ризики, а зловмисники активно застосовують соціальну інженерію для збору чутливої інформації або поширення дезінформації.

Загрози, що виникають через людський фактор, можна розділити на кілька основних категорій, зокрема:

Невідповідальність або недбальство користувачів: Це може включати невірну обробку конфіденційних даних, незастосування паролів, що відповідають вимогам безпеки, або ігнорування оновлень програмного забезпечення. Така поведінка знижує загальний рівень безпеки системи, навіть якщо сама технологія є на високому рівні.

Невірні дії через недостатню обізнаність: У багатьох випадках співробітники просто не усвідомлюють серйозності загроз або не знають, як правильно захищати себе і корпоративну інформацію. Це може стосуватися відсутності навичок у виявленні фішингових листів або небезпечних веб-сайтів.

Атаки через соціальну інженерію: Це один із найбільш небезпечних способів, оскільки зловмисники використовують психологічні маніпуляції, щоб викликати довіру до себе, переконати співробітника дати доступ до системи або передати конфіденційну інформацію.

Для зменшення ризиків, пов'язаних з людським фактором, необхідно застосовувати не лише технічні рішення, а й соціальні та організаційні заходи. Одним із таких рішень є:

1. Створення системи навчання та підвищення обізнаності співробітників

Найефективнішим методом боротьби з людським фактором є постійне навчання персоналу. Це повинно включати:

- регулярні тренінги по безпеці, на яких співробітники навчаються, як розпізнавати загрози та як правильно діяти у випадку їх виникнення;
- симуляції фішингових атак, щоб користувачі навчалися не потрапляти в пастки зловмисниківяя4
- внутрішні кампанії для підвищення обізнаності, які нагадують співробітникам про важливість політик безпеки.

2. Впровадження багаторівневих систем захисту

Технічні засоби безпеки, такі як багатофакторна аутентифікація (MFA), можуть допомогти зменшити вплив людських помилок. Навіть якщо користувач випадково надасть свої облікові дані або не застосує необхідний рівень паролів, система зможе додатково перевірити його особу за допомогою іншого методу.

3. Формування корпоративної культури безпеки

Інтеграція політик безпеки в корпоративну культуру є важливою складовою успіху. Кожен співробітник повинен розуміти свою роль у забезпеченні безпеки компанії, а безпечне поводження з інформацією повинно стати частиною щоденної роботи. Керівництво організації має бути прикладом для інших, постійно наголошуючи на важливості кібербезпеки.

4. Вдосконалення політики контролю доступу

Контроль доступу є важливим аспектом, який допомагає запобігти інцидентам через людські помилки. Важливо впроваджувати політики "найменших привілеїв", що означає надання співробітникам мінімальних прав для виконання їхніх обов'язків, а також регулярно переглядати й оновлювати ці права [2].

Одним із ефективних шляхів інтеграції технічних рішень із соціальними аспектами є соціотехнічний підхід. Цей підхід враховує не лише технологічні інструменти захисту, але й психологічні, соціальні та поведінкові аспекти діяльності людей. Психологічні чинники, такі як стрес, поспіх, або навіть бажання допомогти, можуть призводити до того, що співробітники приймають рішення, які підвищують ризик інформаційної безпеки.

Навіть найсучасніші технології захисту не здатні повністю виключити людський фактор. Тому інвестиції в освіту користувачів та розвиток корпоративної культури безпеки є ключовими для збереження стабільності та надійності інформаційних систем [3].

У забезпеченні інформаційної безпеки людський фактор є однією з найбільших загроз, попри наявність сучасних технічних засобів захисту. Виявлено, що основні причини людських помилок полягають у невідповідальності користувачів, недостатній обізнаності про загрози та маніпуляціях через соціальну інженерію. Актуальність цієї теми зростає в умовах змін у сфері роботи, зокрема, переходу на віддалену роботу та гібридні форми, що створюють додаткові ризики.

Для зменшення негативного впливу людського фактора необхідно застосовувати комплексний підхід, що включає технічні, соціальні та організаційні заходи. Перш за все, важливим є постійне навчання співробітників і підвищення їх обізнаності, що дозволяє запобігати помилкам через недостатні знання. Впровадження багаторівневих систем захисту та формування корпоративної культури безпеки також допомагають зменшити ймовірність інцидентів, пов'язаних з людським фактором.

Соціотехнічний підхід, що інтегрує технологічні рішення з розумінням поведінкових, психологічних та соціальних аспектів, є ключовим для забезпечення комплексного захисту. Таким чином, хоча технічні засоби безпеки є важливими, інвестиції в освіту користувачів і розвиток корпоративної культури безпеки є критично важливими для підтримки стабільності та надійності інформаційних систем у сучасному цифровому середовищі.

Список використаних джерел

1. ICO. According to Verizon's Data breach investigation report 2023. URL: https://surl.li/ekmfwb
2. Enisa. Emerging technologies make it easier to phish. URL: https://surli.cc/yzoknl.
3. 157 Cybersecurity Statistics and Trends. Varonis. URL: https://www.varonis.com/blog/cybersecurity-statistics#:~:text=5,%28IBM.

Ключові слова: Інформаційна безпека, людський фактор, соціальна інженерія, кібератаки, навчання персоналу

Keywords: Information security, human factor, social engineering, cyber attacks, staff training

ПОШИРЕННЯ ДОКУМЕНТІВ, ЯКІ МІСТЯТЬ КОНФІДЕНЦІЙНІ ДАНІ ПРО ОСОБУ (DOXXING)

Хачатрян Олександр

студент 1-го курсу факультету судового та міжнародного права
Національного університету «Одеська юридична академія»

В умовах всепроникного поширення цифрових технологій питання інформаційної безпеки стає дедалі актуальнішим. Одним із загрозливих явищ у сфері кібербезпеки є так званий «doxxing» (від англ. doxing або doxxing) — публічне розкриття особистої інформації про людину без її згоди, часто з метою переслідування, залякування або дискредитації [1].

Термін «doxxing» походить від слова «docs» (documents) та означає поширення документів, які містять конфіденційні дані про особу: справжнє ім'я, адресу проживання, номери телефонів, електронну пошту, місце роботи, інформацію про родичів тощо. Зазвичай така інформація публікується у відкритому доступі – на форумах, у соціальних мережах або спеціалізованих платформах.

Історично термін doxxing виник у хакерському середовищі ще у 1990-х роках, коли опоненти «зливали» інформацію про один одного для дискредитації. Згодом практика набула ширшого використання, особливо з розвитком соціальних мереж, де кожен може стати об'єктом цифрової атаки.

До дій, що підпадають під визначення doxxing'у, належать:

- публікація адреси проживання, номера телефону, електронної пошти, місця роботи, банківських реквізитів, ідентифікаційних номерів або фотографій без згоди особи;
- розкриття особистості анонімного користувача в інтернеті;
- поширення інформації про членів родини, друзів чи колег з метою тиску або дискредитації;
- використання зібраної інформації для шантажу, погроз або організації кампаній онлайн-цькування.

Типи doxxing'у включають: класичний (поширення повних ПІБ, адреси, телефону), корпоративний (інформація про місце роботи, керівництво), сімейний (дані про родичів, дітей), фінансовий (номери рахунків, банківських карток), репутаційний (злиття особистих повідомлень, фото). Всі ці типи несуть серйозну загрозу як безпеці, так і ментальному здоров'ю особи.

Це явище стало особливо поширеним у контексті онлайн-конфліктів, політичних дискусій або як форма цифрової помсти. Наприклад, під час протестів BLM у США у 2020 році в інтернет викладалися персональні дані як поліцейських, так і активістів. В Україні під час воєнного стану були випадки «викриття» проросійських колаборантів, що хоча й мало суспільну підтримку, та все ж залишає багато запитань щодо етичності таких дій.

З правової точки зору, doxxing є порушенням права на приватність та може кваліфікуватися як злочин, зокрема у випадках, коли він призводить до переслідування, погроз чи насильства.

Правовий статус doxxing'у варіюється залежно від країни.

Німеччина: У 2021 році введено кримінальну відповідальність за «небезпечне поширення персональних даних» (ст. 126a Кримінального кодексу), що передбачає до 3 років ув'язнення.

Гонконг: З 2021 року doxxing є кримінальним злочином, що карається до 5 років ув'язнення та штрафом до 1 млн HKD .

Австралія: У 2024 році прийнято закон, що криміналізує doxxing, передбачаючи до 6 років ув'язнення за зловмисне розкриття особистих даних [2].

США: Федерального закону, що прямо забороняє doxxing, немає, але дії можуть підпадати під інші статті, пов'язані з переслідуванням, шантажем або порушенням приватності [3].

В Україні питання захисту персональних даних регулюється Законом України «Про захист персональних даних», а також Кримінальним кодексом України, який містить статті щодо порушення недоторканності приватного життя.

У міжнародному вимірі діють Конвенція Ради Європи про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних та Загальний регламент ЄС про захист даних (GDPR), який встановлює жорсткі вимоги щодо поводження з персональною інформацією.

Соціальний аспект проблеми не менш важливий. Жертви doxxing'у часто страждають від серйозних психологічних наслідків: тривожності, депресій, страху за себе і близьких. У деяких випадках публікація особистих даних призводила до фізичних атак, переслідувань або втрати роботи.

У відповідь на виклики doxxing'у, важливими є технічні засоби захисту – використання VPN, двофакторна аутентифікація, обмеження доступу до особистої інформації в соцмережах, а також підвищення цифрової грамотності серед населення. На рівні державної політики важливими є просвітницькі кампанії, розробка етичних кодексів для онлайн-платформ, а також міжнародна співпраця в боротьбі з кіберзлочинністю [4].

Управлінські та економічні аспекти цього явища також заслуговують уваги. Компанії зазнають репутаційних та фінансових втрат, якщо їх працівники стають жертвами doxxing-атак, або якщо самі платформи не реагують належним чином на публікацію конфіденційної інформації. Це вимагає розробки внутрішніх політик безпеки, швидкої модерації контенту та співпраці з правоохоронними органами. Таким чином, doxxing є складною проблемою, що лежить на перетині соціального, правового та технологічного вимірів. Протидія йому потребує комплексного підходу – правового регулювання, технічного захисту, освітніх кампаній та відповідальної поведінки користувачів у цифровому просторі.

Ще одним важливим аспектом doxxing'у є роль соціальних мереж та алгоритмів поширення інформації. У сучасному цифровому середовищі інформація, навіть неправдива або шкідлива, здатна миттєво поширюватися завдяки репостам, «лайкам» та рекомендаційним системам. У результаті навіть незначне за обсягом повідомлення з персональними даними може швидко охопити тисячі користувачів. Соціальні мережі несуть відповідальність за забезпечення конфіденційності своїх користувачів, однак на практиці не завжди оперативно реагують на подібні інциденти [5].

Крім того, важливо звернути увагу на роль анонімності в інтернеті, яка з одного боку дозволяє користувачам вільно висловлювати свою думку, а з іншого – створює середовище для безкарного здійснення doxxing-атак.

Необхідно також підкреслити, що проблема doxxing не має чітких географічних меж. Це глобальне явище, з яким стикаються користувачі в усьому світі, незалежно від віку, професії чи політичних поглядів. Саме тому вирішення цієї проблеми потребує міжнародної координації, обміну найкращими практиками та узгодження стандартів захисту особистої інформації в цифровому просторі.

Список використаних джерел

1. Doxing: The Resource Guide URL: https://surli.cc/qhuozl.
2. Australia introduces bill to step up fight against hate crimes URL: https://surli.cc/tkvzss.
3. David L. Hudson Is doxxing illegal? URL: https://surl.li/xfepoq.
4. Jay Stanley Some Steps to Defend Against Online Doxxing and Harassment URL: https://surl.lu/hmxrud.
5. Online harassment field manual URL: https://surl.li/vhrxof.

Ключові слова: doxxing, персональні дані, конфіденційність, кібербезпека, цифрова етика.

Keywords: doxxing, personal data, confidentiality, cybersecurity, digital ethics.

Науковий керівник: доцент Чанишев Р.

ЗАКОН SREN

Грабенко Поліна

студентка 1-го курсу факультету судового та міжнародного права
Національного університету «Одеська юридична академія»

У сучасному цифровому світі питання безпеки та регулювання онлайн-простору набувають особливої гостроти. Кібербулінг, поширення фейкових новин, шахрайство з персональними даними – це не абстрактні проблеми, а щоденні виклики, з якими стикаються громадяни. Закон SREN відповідає на ці виклики комплексним підходом до безпеки та прозорості цифрового середовища.

Прийняття цього закону свідчить про усвідомлення Францією необхідності правового регулювання цифрової сфери, встановлення чітких меж відповідальності для онлайн-платформ та захисту прав користувачів.

Передумовою до створення Закону SREN стало зростання загроз у цифровому середовищі: від масових випадків кібербулінгу до масштабної дезінформації під час виборів.

Французьке законодавство вже мало елементи регулювання через акти DSA та DMA, однак національні виклики, зокрема особливості мови, культури, законодавчої практики, вимагали створення окремого закону, що враховує ці нюанси [1; 2].

Особливу роль у прийнятті закону відіграла суспільна дискусія про свободу слова, цензуру та етичні межі в інтернеті.

Закон передбачає багаторівневу систему регулювання, де важлива роль належить державним органам (ARCOM, CNIL, DGCCRF) [3; 4].

Захист дітей є ключовим пріоритетом. Зокрема, створено обов'язкові механізми перевірки віку для доступу до контенту для дорослих, що унеможливлює використання сайтів без належної ідентифікації.

Іншим важливим аспектом є криміналізація порнографічних дипфейків, що дозволяє притягати до відповідальності авторів таких матеріалів.

Закон встановлює чіткі вимоги щодо прозорості онлайн-реклами. Користувачі мають право знати, хто є замовником рекламного контенту, з якою метою та на яких умовах він поширюється.

Особлива увага приділена регулюванню цифрових активів у відеоіграх. Запроваджено експериментальний період для вивчення впливу NFT та монетизованих ігрових предметів на економіку та безпеку.

Закон має значний вплив на діяльність цифрових платформ. Компанії зобов'язані впроваджувати додаткові заходи захисту даних, модерувати контент відповідно до нових стандартів, посилити боротьбу з нелегальним контентом.

Реакція бізнесу виявилася змішаною. Великі корпорації критикували закон за потенційне зростання витрат, тоді як правозахисники вітали його як крок до більш безпечного цифрового середовища.

Франція стала піонером у сфері цифрового регулювання серед країн ЄС, демонструючи готовність поєднувати технологічний прогрес із відповідальністю. Приклад SREN вже активно обговорюється у сусідніх державах.

Реальні приклади застосування закону включають рішення про припинення трансляції санкційних російських каналів, що свідчить про практичну ефективність нового законодавства [3].

Подальший розвиток законодавства у цій сфері залежатиме від викликів, пов'язаних із розвитком штучного інтелекту, віртуальної реальності та нових форм дезінформації.

Можна очікувати посилення відповідальності цифрових платформ, зокрема в питаннях прозорості алгоритмів персоналізації контенту.

Також актуальним є питання врегулювання обігу цифрових валют та боротьби з відмиванням грошей через цифрові активи. Ключовим залишатиметься баланс між забезпеченням та збереженням демократичних свобод в онлайн-просторі.

Закон SREN став важливим кроком у регулюванні цифрового простору Франції, забезпечивши новий рівень захисту користувачів та відповідальності платформ.

Його імплементація супроводжується активною суспільною дискусією, що є ознакою здорової демократичної традиції.

У перспективі SREN може стати еталоном для інших країн, які шукають ефективний баланс між свободою та безпекою в цифровій сфері.

Список використаних джерел

1. Європейський акт про цифрові послуги (Digital Services Act, DSA) – Європейська комісія. URL: https://ec.europa.eu/digital-services-act
2. Європейський акт про цифрові ринки (Digital Markets Act, DMA) – Європейська комісія URL: https://ec.europa.eu/digital-markets-act
3. ARCOM – Французький орган з регулювання аудіовізуальних і цифрових комунікацій, arcom.fr URL: https://www.arcom.fr/
4. CNIL – Національна комісія з питань інформаційних технологій та свобод, cnil.fr URL: https://www.cnil.fr/fr

Ключові слова: цифрова безпека, регулювання інтернету, онлайн-платформи, захист персональних даних, кібербулінг, дипфейки

Keywords: digital security, internet regulation, online platforms, privacy, cyberbullying, deepfakes

Науковий керівник: доцент Чанишев Р.

ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ В ПАРАДИГМІ СУЧАСНОЇ КІБЕРБЕЗПЕКИ

Шорніков Назар

студент 1 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Розвиток інформаційних технологій та зростання обсягів даних, що зберігаються та передаються в мережах, створюють нові виклики для забезпечення безпеки. Зростає ризик кібератак на різні галузі, зокрема фінансову, державну, медичну та освітню, що спонукає до використання передових технологій для захисту даних та інфраструктури. У цьому контексті штучний інтелект (далі ШІ) відіграє вирішальну роль, розширюючи можливості для виявлення та нейтралізації кібератак.

У дослідженні [1] зазначається, що штучний інтелект є однією з найвищих досягнень техногенної цивілізації – багаторівневою системою взаємопов'язаних процесів, яка служить основою для формування сучасних інформаційних структур. У майбутньому широке використання технологій штучного інтелекту та нанобіотехнологій може призвести до глибоких змін у поведінці людини, соціальних взаємодіях та екзистенційних аспектах особистості.

На першому місці штучний інтелект слід розглядати як сукупність технологій, призначених для створення інтелектуальних систем і продуктів. Наразі ШІ активно застосовується в галузі аналізу загроз, де на основі даних, зібраних з відкритих і закритих джерел, передбачаються потенційні ризики для інформаційної безпеки. За минулі двадцять років масштаб задач, що вирішуються за допомогою штучного інтелекту в сфері захисту інформації, суттєво розширився. Сьогодні штучний інтелект є надійним інструментом у протидії кіберзагрозам, забезпечуючи високий рівень захисту цифрових систем.

ШІ, як багатофункціональний інструмент, здатний до самостійного навчання в умовах змінного середовища, знайшов своє застосування в різних галузях, серед яких особливе місце посідає сфера кібербезпеки. На основі алгоритмів штучного інтелекту розроблено комплексні рішення, призначені для ефективного протистояння кіберзагрозам, які охоплюють кілька ключових аспектів. Зокрема, ШІ використовується для аналізу та виявлення потенційних загроз на основі великих обсягів даних, що надходять з різних джерел. Крім того, штучний інтелект активно задіяний у процесах виявлення та локалізації кіберінцидентів, забезпечуючи швидке виявлення порушень, класифікацію типів атак та формування оптимальних стратегій реагування. Ще одним важливим напрямком впровадження ШІ у сфері кібербезпеки є інтеграція з системами, що використовують біометричні дані, що дозволяє підвищити рівень автентифікації користувачів, зменшити ризики несанкціонованого доступу та забезпечити персоналізований контроль доступу до чутливих даних. Таким чином, застосування технологій штучного

інтелекту в кібербезпеці забезпечує комплексний підхід до захисту інформаційних систем, поєднуючи проактивне виявлення загроз, оперативне реагування та надійну верифікацію користувачів.

Прогностичний інтелект є ще однією сфера, у якій ШІ досягає успіху. Завдяки можливостям обробки природної мови штучний інтелект може переглядати статті в новинах, журналах і дослідженнях про кіберзагрози, створюючи чітку картину того, як вони можуть вплинути на вашу організацію.

Згідно з даними Forbes, приблизно кожна третя електронна злочинність викликана діями інсайдерів – як свідомими, так і невмисними. Перед початком таких атак поведінка користувача нерідко відрізняється від загальноприйнятих шаблонів у межах організації. У цьому контексті штучний інтелект може бути використаний для автоматизованого виявлення аномалій, аналізу масивів даних та встановлення фактичних відхилень в активності, що вказують на потенційну загрозу, ще до того, як команда фіксує ознаки порушення [2] .

Аномалії також можуть виникати поза межами організації через спроби соціальної інженерії та фішингу. Штучний інтелект може виявити ці відхилення швидше, ніж людина, що дозволяє командам безпеки керувати будь-якою активністю, яка вказує на загрозу, до того, як кіберзлочинці отримають доступ до неї. У деяких випадках ШІ може діяти без втручання людини, вживаючи заходів для нейтралізації аномалії в режимі реального часу на основі її профілю ризику [2].

ШІ забезпечує постійне спостереження за мережевим трафіком та аналіз даних з різноманітних джерел з метою виявлення потенційних порушень інформаційної безпеки в режимі реального часу. Автоматизація процесів виявлення загроз на ранніх етапах значно скорочує часовий проміжок між початком атаки та її фіксацією, даючи можливість службам безпеки отримувати своєчасні попередження. Після виявлення підозрілої активності система аналізує отримані дані, встановлює зв’язки між подіями та виділяє аномальні зміни, що допомагає спеціалістам з безпеки краще зрозуміти характер атаки. Крім того, алгоритми штучного інтелекту здатні встановити первинні причини інциденту, чим забезпечують ефективне управління процесом реагування та зменшують обсяг роботи, яку необхідно виконати аналітикам [2].

Системи штучного інтелекту мають здатність автоматизувати процеси реагування на кіберінциденти, забезпечуючи оперативне виконання необхідних дій у разі виникнення загроз. На основі попереднього навчання на типових сценаріях реагування, ШІ може застосовувати зарані визначені механізми відповіді на конкретні види атак, такі як блокування підозрілих IP-адрес чи ізоляція систем, що могли бути скомпрометовані.

Особливо важливо це у сучасних умовах, коли кожен пристрій, що використовується для віддаленої роботи, потенційно становить ризик для інформаційної безпеки. Застосування ШІ дає можливість суттєво підвищити рівень захисту кінцевих точок. Система на основі штучного інтелекту аналізує та встановлює нормативну модель поведінки для кожної окремої кінцевої точки шляхом

багаторазового навчання на масивах даних. У разі виявлення відхилень від встановленого шаблону система здатна не лише виявити аномалію, а й негайно вжити відповідних заходів реагування.

Такий підхід дозволяє організаціям перейти до проактивної стратегії захисту інформаційних активів, замість того щоб покладатися виключно на стандартні методи, такі як оновлення антивірусних сигнатур чи використання VPN. ШІ забезпечує не тільки оперативне виявлення та реагування на загрози, але й формування гнучкої системи безпеки, здатної адаптуватися до нових атакуючих моделей та еволюції кіберзагроз [2].

ШІ та інформаційні технології є потужними інструментами для забезпечення кібербезпеки. Ефективне використання яких вимагає постійного розвитку технологій, дотримання етичних стандартів та відповідності правовій базі. Тільки у такому разі ШІ зможе стати основою ефективної системи кібербезпеки, здатної захистити інформацію та забезпечити стабільність сучасного цифрового суспільства.

Список використаних джерел

1. Використання штучного інтелекту в інформаційній безпеці України. URL: http://www.dy.nayka.com.ua/pdf/1_2022/4.pdf
2. Корпоративна кібербезпека: Роль ШІ у захисті даних. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/corporate-cybersecurity-ai-role-in-data-protection

Ключові слова: штучний інтелект, інформаційні технології, кібербезпека, автоматизація, захист інформаційних активів.

Keywords: artificial intelligence, information technology, cybersecurity, automation, information asset protection.

Науковий керівник: PhD Грезіна О.

СКАНДАЛ ІЗ PEGASUS ТА ЙОГО НАСЛІДКИ

Щербатюк Марина

студентка 1 курсу факультету судового та міжнародного права Національного університету «Одеська юридична академія»

У XXI столітті кібербезпека стала однією з ключових складових національної безпеки кожної держави. У зв'язку з швидким розвитком цифрових технологій і зростанням значущості персональних даних, питання зловживання шпигунськими засобами набуває все більшої гостроти. Одним із найгучніших міжнародних скандалів останнього часу стало розкриття використання програмного забезпечення Pegasus для спостереження [1].

Pegasus – це програмне забезпечення, розроблене ізраїльською компанією NSO Group. Основне призначення Pegasus – це таємне проникнення в мобільні пристрої з можливістю повного контролю над ними: відстеження дзвінків і повідомлень, доступ до камери, мікрофона, геолокації та інших конфіденційних даних. Особливість цього програмного забезпечення полягає в тому, що воно може заразити пристрій без будь-яких дій з боку користувача – завдяки технології, відомій як zero-click.

У жовтні 2019 року компанія WhatsApp подала позов проти NSO Group у федеральному суді Північної Каліфорнії, звинувачуючи її у порушенні Закону США про комп'ютерне шахрайство та зловживання (CFAA) та інших законів.

Програма Pegasus використовувала уразливість у функції голосових викликів WhatsApp, що дозволяло встановлювати шпигунське ПЗ без взаємодії з користувачем – навіть якщо дзвінок не приймався.

Pegasus було використано для атаки на понад 1 400 користувачів у 20 країнах, і за рішенням суду компанія була зобов'язана виплатити штраф у 167,254,000 доларів США [2].

У 2021 році міжнародна спільнота дізналася про масштабне використання Pegasus проти журналістів, правозахисників, опозиційних політиків і навіть голів держав. Розслідування, здійснене журналістським консорціумом *Forbidden Stories* спільно з *Amnesty International*, показало, що шпигунське програмне забезпечення Pegasus застосовувалося на території понад 45 держав. У списку потенційних мішеней налічувалося понад 50 тисяч телефонних номерів [3].

Жертвами стеження стали журналісти провідних видань, зокрема Al Jazeera, The New York Times та The Guardian, а також правозахисники з Індії, Мексики, Угорщини та Франції. До списку постраждалих потрапили і політичні діячі, серед яких – президент Франції Еммануель Макрон. В Україні також пролунали заклики до перевірки, чи могли Pegasus використовувати спецслужби проти політичної опозиції.

З позиції міжнародного права, застосування такого програмного забезпечення без відповідного судового дозволу може вважатися серйозним порушенням прав людини. Йдеться про порушення права на приватне життя, свободу вираження поглядів, а також право на захист журналістської діяльності. Стаття 12 Загальної декларації прав людини прямо забороняє свавільне втручання в особисте життя, кореспонденцію та репутацію.

У відповідь на це міжнародна спільнота заснувала в березні 2022 року в Європарламенті спеціальний комітет PEGA для розслідування використання Pegasus та подібного програмного забезпечення в країнах ЄС. Комітет мав мандат на 12 місяців і провів масштабне розслідування, яке включало слухання понад 215 свідків, експертів і жертв, а також місії до Ізраїлю, Польщі, Греції, Кіпру, Угорщини та Іспанії [4].

У березні 2023 року PEGA ухвалила 145-сторінковий звіт із результатами свого розслідування; Парламент ухвалив свою остаточну рекомендацію в червні

2023 року. Парламент встановив, що як країни ЄС, так і країни, що не входять до ЄС, використовували Pegasus і подібне програмне забезпечення у політичних та кримінальних цілях. Парламент зазначив, що деякі держави-члени використовували шпигунські програми під приводом «національної безпеки», щоб уникнути нагляду ЄС.

Звіт дійшов висновку, що правові рамки та практика в Греції, Польщі та Угорщині порушують законодавство Союзу і не забезпечують достатнього захисту громадян. Парламент також дав конкретні рекомендації для Іспанії та Кіпру. Він запропонував суворіші інституційні та правові гарантії для використання шпигунського ПЗ відповідно до основних прав, такі як умови замовлення, дозволу, виконання та нагляду за операціями зі шпигунським ПЗ. Крім того, Парламент рекомендував чітке визначення поняття «національна безпека».

Парламент закликав Європейську комісію суворіше стежити за дотриманням чинних законів і попереджати можливі зловживання. Він також доручив Комісії розробити нові закони, такі як загальні стандарти ЄС для використання шпигунського програмного забезпечення та регламент про комерційне шпигунське програмне забезпечення на ринку ЄС.

Окрім того, у листопаді 2021 року компанія Apple подала позов проти NSO Group, заявивши, що вони несанкціоновано використовували вразливості операційної системи iOS для атак на користувачів iPhone. У вересні 2024 року Apple подала клопотання про відхилення власного позову, посилаючись на ризик розголошення критично важливої інформації про безпеку, яка використовується для боротьби з поширенням комерційних засобів спостереження. Компанія зазначила, що продовження судового процесу може зашкодити її зусиллям у захисті користувачів від шпигунських атак [5].

У квітні 2024 року в Польщі розпочалося розслідування щодо використання попереднім урядом шпигунського програмного забезпечення Pegasus, водночас залишається ймовірність того, що проти колишніх посадовців буде висунуто кримінальні звинувачення. Громадянська лабораторія Університету Торонто виявила, що Pegasus використовували в Польщі для стеження за діячами опозиційної на той момент партії «Громадянська платформа» люди.

Міністр юстиції Польщі Адам Боднар у своїх коментарях зазначив, що уряд сповістить тих людей, за діяльністю яких велося стеження, а самі потерпілі отримуватимуть можливість вимагати фінансової компенсації [6].

Застосування Pegasus породжує правову дилему: з одного боку, держава зобов'язана гарантувати національну безпеку та протидіяти тероризму, з іншого – не має порушувати фундаментальні права людини. У випадку Pegasus держави використовували технологію не тільки проти злочинців, а й проти представників громадянського суспільства. Такий підхід розмиває межу між законною діяльністю спецслужб і тотальним контролем над населенням.

Крім того, виникає питання регулювання кіберзброї. Pegasus показав, що міжнародна нормативна база з цього питання є застарілою або взагалі

відсутньою. На міжнародному рівні відсутні чіткі норми, які б однозначно регламентували, які саме шпигунські засоби дозволені, а які – заборонені. Це призводить до правового вакууму, яким активно користуються авторитарні режими.

Після викриття скандалу кілька країн припинили співпрацю з NSO Group, а сама компанія потрапила під санкції з боку США. Деякі держави почали перегляд політик щодо закупівлі шпигунських технологій. Проте загроза залишається: ринок цифрового спостереження продовжує розвиватися, з'являються нові гравці, а можливості шпигунського ПЗ стають дедалі потужнішими.

На індивідуальному рівні експерти рекомендують:

- постійно оновлювати операційні системи мобільних пристроїв;
- не відкривати невідомі посилання;
- користуватись шифруванням повідомлень;
- зберігати критичне мислення при отриманні повідомлень від невідомих контактів.

Однак навіть ці заходи можуть виявитись недостатніми проти технологій, які діють без відома користувача. Тому необхідна комплексна відповідь – як з боку держав, так і міжнародних організацій.

Список використаних джерел

1. Chaim Levinson With Israel's Encouragement, NSO Sold Spyware to UAE and Other Gulf States URL: https://surl.li/wysuwr.
2. Emma Roth Meta awarded $167.25 million over Pegasus spyware attack URL: https://surl.lu/ltjyql.
3. Pegasus Project: Apple iPhones compromised by NSO spyware URL: https://surl.li/hknmpd.
4. What action has Parliament taken against spyware abuse? URL: https://surl.lu/rcvwyk.
5. Suzanne Smalley Apple seeks dismissal of its NSO Group lawsuit, citing risk of exposing 'vital security information' URL: https://surl.li/rvwkxu.
6. Shaun Walker Poland launches inquiry into previous government's spyware use URL: https://surl.lu/elgode.

Ключові слова: Pegasus, шпигунське ПЗ, приватність, права людини, цифрова безпека.

Keywords: Pegasus, spyware, privacy, human rights, digital security.

Науковий керівник: доцент Чанишев Р.

ЕТИЧНИЙ ХАКЕР ТА ПЕНТЕСТ

Леонова Анастасія

студентка 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Кожен хоч раз в житті чув слово «хакер», і майже у всіх воно асоціюється із крадіжкою даних або зламом комп'ютерних систем. Але не всі хакери злодії. Існують етичні хакери або, як їх ще називають, пентестери. Хто це такі? Простими словами, це фахівці комп'ютерної безпеки, які використовують ті ж самі навички, інструменти та знання, що й зловмисники, але роблять це легально, з дозволу власника системи.

Основна різниця між кіберзлочинцем та етичним хакером: наявність дозволу та мети його дії. Мета етичних хакерів – показати організаціям, як запобігати важким кібератакам. Вони імітують дії порушників, перевіряють системи на міцність, але завжди діють легально. Ця ідея побудована на простій, перевіреній практиці – намагаєшся зловити злодія, думай як злодій. З розвитком технологій організації все більше залежать від пентестерів, тому ці фахівці завжди будуть користуватися попитом на ринку праці.

Головне знаряддя в руках етичного хакера – пентест, або тестування на проникнення. Коли говорять про пентест, мають на увазі, що хтось цілком законно (що дуже важливо) здійснює атаку на комп'ютерну систему, мережу або вебдодаток. Це потрібно для того, щоб оцінити на скільки вони вразливі до справжніх атак. Тестування на проникнення це не звичайна перевірка на пошук помилок у системі захисту, а й спроба знайти і обережно використати вразливості так, як це міг би зробити справжній зловмисник.

Зловмисники – люди, а людина не може бути ідеальною. Деякі хакери можуть здаватися неперевершеними спеціалістами, але вони теж люди, зі своїми сильними та слабкими якостями. На людський фактор також треба звертати увагу. Є ряд етапів, на яких зловмисник може припуститися помилки, а захисники цим скористатись у свою користь. Процес атаки є багатокроковим, тому на кожному кроці злодій може робити похибки, що дає можливість командам безпеки їх побачити та використати протидії для загрози [1, С. 21].

Роль та завдання етичного хакера є доволі цікавим процесом. Зробити можна безліч варіантів захисту систем, використовувати тільки надійних людей для припинення дії зловмисників, але ніколи не буде гарантії повного захисту та конфіденційності, завжди є слабке місце і хакери цим скористуються. Етичний хакер – це той, кого наймають, щоб він проникнув у систему як зловмисник, користуючись різним хитрощами, для перевірки надійності захисту. Можна виділити декілька основних завдань етичного хакера:

- поглянути на систему «очима зловмисника»: пентестер буде думати і діяти так, як діяв би справжній зловмисник;

• знайти вразливості: шукати будь-які помилки в програмах, слабкі паролі, неправильні налаштування серверів – все, що може бути використано для атаки;

• оцінити реальні ризики: задача полягає не просто знайти вразливості, а показати, що через них дійсно можна зробити (наприклад, отримати доступ до даних клієнтів, вкрасти кошти компанії);

Перевірити роботу засобів захисту: пентестер активно тестує фаєрволи, IDS/IPS, антивіруси, намагаючись їх обійти. Аналізує конфігурації на помилки, перевіряє генерацію сповіщень (алертів) та коректність записів у логах безпеки для виявлення та розслідування реальних атак [2, С. 42-51].

Встановлення антивірусних та інших програм захисту не завжди гарантує повну безпеку. Вони хоч і виявляють помилки, але часто пропускають складніші вразливості пов'язані з нестандартними конфігураціями. Також варто пам'ятати про постійний розвиток загроз: те, що вважалось безпечним сьогодні, завтра вже може стати вразливим. Щоденно виникають нові віруси, методи атак стають хитрішими, а в програмах виявляються раніше невідомі помилки [2].

Існують три підходи тестування:

1. Black box: хакер нічого не знає про систему;

2. White box: хакер має повну інформацію (вихідний код програм, схеми мережі і т.д.);

3. Grey Box: хакер має деяку інформацію, наприклад тільки код програмного забезпечення.

Пентест – це структурований процес, і кожен етап відіграє важливу роль. Спочатку етичний хакер обговорює з замовником що саме він буде тестувати. Це називається «scope» або обсяг роботи. Далі узгоджується мета тестування: просто знайти вразливості чи спробувати отримати доступ до певних даних? Потім вирішується коли проводити тестування, щоб не заважати нормальному функціонуванню систем замовника. Найголовніше – отримати офіційний письмовий дозвіл. Без нього проникнення буде вважатися злочином.

Другим етапом є розвідка. Пентестер збирає максимум інформації про систему, яка буде тестуватись. Він ретельно вивчає IP-адреси компанії замовника, її веб-сайти та сервери, намагається зрозуміти які саме технології використовуються для її обслуговування. Аналізується інформація про співробітників яка є у відкритому доступі [3, С. 32].

Після того, як всю інформацію зібрано, етичний хакер починає активну фазу пентесту: обстеження цільових систем. Головним завданням є виявлення активних мережевих портів – точок, через які система взаємодіє за допомогою вебсервісів або поштових сервісів. Ідентифікувавши активні служби, спеціаліст визначає конкретні програми та їх версії, що працюють на цих портах. Після цього використовуються спеціалізовані інструменти, відомі як сканери вразливостей, для пошуку відомих помилок безпеки та слабких місць у виявленому програмному забезпеченні[4].

Далі вже йде спроба отримати доступ до теоретичних знань про слабкі місця. Етичний хакер обережно застосовує ті вразливості, що були знайдені в процесі сканування. Наприклад, спроба підібрати ненадійний пароль до облікового запису, використання відомої помилки в програмному забезпеченні, яка дозволяє використати сторонній код.

Після отримання доступу аналізуються потенційні дії: підвищення привілеїв, доступ до даних та переміщення по системі. Оцінюється рівень вразливості системи, який детально інформується у звіті. Фінальний звіт – це ключовий результат пентесту. Він надає рекомендації щодо їх виправлення, описує знайдені вразливості та кроки для їх відтворення та дає оцінку пов'язаних ризиків.

Отже, у сучасному світі важко переоцінити роль етичного хакера. Спеціалісти, використовуючи свої навички на законних підставах, надають фірмам можливість побачити свій захист "з протилежного боку" – з позиції потенційного нападника. Тестуючи на проникнення, яке вони проводять, виходячи за межі стандартного сканування, відтворюючи конкретний аналіз реальної захищеності систем та мереж. В умовах постійного зростання кіберзагроз, це стає не просто корисним, а життєво необхідним. Регулярний пентест – це інвестиція в безпеку, яка може запобігти проблемам та захищати найцінніші аспекти організації.

Список використаних джерел

1. Weidman, Georgia. Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press, 2014.
2. Carey, Marcus J., Jin, Jennifer. Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World. Wiley, 2019.
3. Graves, Kimberly. CEH™ Official Certified Ethical Hacker Review Guide. Sybex, 2018.

Ключові слова: етичний хакер, пентест, тестування на проникнення, кібербезпека, інформаційна безпека, вразливість, експлуатація, звітність.

Keywords: ethical hacker, pentest, penetration testing, cybersecurity, information security, vulnerability, exploitation, reporting.

Науковий керівник: доцент Задерейко О. В.

Секція 3. УПРАВЛІНСЬКІ ТА ЕКОНОМІЧНІ АСПЕКТИ РОЗВИТКУ СУЧАСНОЇ ІТ ІНДУСТРІЇ

ВИКОРИСТАННЯ LOOKER STUDIO ДЛЯ АНАЛІЗУ МАРКЕТИНГОВИХ ДАНИХ

Іванова Ірина

студентка 1 курсу магістратури
факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Горбаченко Станислав

завідувач кафедри кібербезпеки
Національного університету «Одеська юридична академія»
доктор економічних наук, професор,

Google Data Studio, нині відомий як Looker Studio, є потужним інструментом для аналізу маркетингових даних, який дозволяє маркетологам створювати інтерактивні дашборди та звіти для прийняття обґрунтованих рішень. Цей інструмент інтегрується з різними джерелами даних, такими як Google Analytics, Google Ads, YouTube Analytics, BigQuery, а також сторонніми платформами через конектори, що забезпечує гнучкість у роботі з великими обсягами інформації. Завдяки своїм можливостям візуалізації та автоматизації, Looker Studio допомагає маркетологам ефективно оцінювати ефективність кампаній, поведінку аудиторії та ключові показники ефективності (KPI) [1].

Розглянемо реальний кейс компанії, що займається електронною комерцією, яка використовувала Looker Studio для аналізу ефективності своїх маркетингових кампаній. Компанія, що спеціалізується на продажі одягу через інтернет-магазин, зіткнулася з проблемою зниження конверсій у 2024 році, попри зростання трафіку на сайт. Для аналізу було вирішено інтегрувати дані з Google Analytics 4, Google Ads та CRM-системи компанії в Looker Studio. Основною метою було визначити, які канали залучення клієнтів забезпечують найвищу рентабельність інвестицій (ROI) і як можна оптимізувати витрати на рекламу.

Першим кроком було створення єдиного джерела даних у Looker Studio. Компанія підключила Google Analytics 4, щоб отримати детальну інформацію про поведінку користувачів на сайті, включаючи кількість сеансів, показник відмов, середній час на сторінці та конверсії. Наприклад, за даними за третій квартал 2024 року, сайт отримав 1,2 мільйона сеансів, з яких 65% походили з органічного пошуку, 25% – з платної реклами Google Ads, а решта – з соціальних мереж та прямих відвідувань. Показник відмов склав 42%, що вказувало на необхідність аналізу якості трафіку. Дані з Google Ads дозволили оцінити ефективність рекламних кампаній: загальні витрати склали 85 000 доларів, а дохід від конверсій, отриманих через платну рекламу, досяг 320 000 доларів. Це дало змогу

розрахувати ROI на рівні 276%, але детальний аналіз показав, що окремі кампанії, зокрема ремаркетинг, мали ROI лише 120%, що вимагало перегляду стратегії.

Далі в Looker Studio було створено дашборд, який візуалізував ці дані у вигляді графіків і таблиць. Наприклад, для оцінки ефективності каналів залучення використовувалася гістограма, яка порівнювала дохід від кожного каналу з витратами на нього. Органічний пошук показав стабільно високий дохід (450 000 доларів за квартал), але зростання трафіку з соціальних мереж, зокрема через Instagram, не призвело до пропорційного збільшення продажів. Дані з CRM додали глибший контекст: клієнти, залучені через органічний пошук, мали середній чек на 15% вищий (120 доларів проти 104 доларів для клієнтів із платної реклами). Це дозволило припустити, що органічний трафік залучає більш лояльну аудиторію, яка вже знайома з брендом.

Однією з ключових переваг Looker Studio стала можливість створення інтерактивних фільтрів [2]. Наприклад, маркетологи компанії налаштували фільтри за географічними регіонами, щоб оцінити ефективність кампаній у різних країнах. Дані показали, що в США конверсії з платної реклами становили 3,8%, тоді як у Великобританії – лише 2,1%, попри схожі витрати. Це спонукало команду перерозподілити бюджет на користь регіонів із вищою ефективністю. Крім того, інструмент дозволив сегментувати аудиторію за демографічними характеристиками. Наприклад, аналіз показав, що користувачі віком 25–34 роки генерували 55% доходу від платної реклами, хоча на цю групу припадало лише 30% трафіку. На основі цих даних було вирішено оптимізувати таргетинг у Google Ads, зосередившись на цій віковій групі.

Ще одним аспектом використання Looker Studio було відстеження сезонних тенденцій. У четвертому кварталі 2024 року, перед Чорною п'ятницею, компанія запустила серію рекламних кампаній у Google Ads і Instagram Ads. Looker Studio дозволив у реальному часі відстежувати, як ці кампанії впливають на трафік і конверсії. Наприклад, за тиждень до Чорної п'ятниці трафік із Instagram Ads зріс на 40%, але конверсії залишилися на рівні 1,5%, що вказувало на низьку якість креативів або неправильний таргетинг. Завдяки швидкому аналізу в Looker Studio, команда змінила рекламні оголошення, додавши чіткіші заклики до дії, що підвищило конверсії до 2,3% за два дні.

Інтеграція з BigQuery додала ще один рівень аналізу [3]. Компанія використовувала BigQuery для зберігання великих обсягів даних про клієнтів, включаючи історію покупок і взаємодії з email-розсилками. Looker Studio дозволив створювати звіти, які поєднували ці дані з інформацією про рекламні кампанії. Наприклад, аналіз показав, що клієнти, які отримували персоналізовані email-розсилки, мали на 22% вищу ймовірність повторної покупки порівняно з тими, хто не отримував листів. Це спонукало компанію інвестувати додаткові ресурси в автоматизацію email-маркетингу.

Looker Studio також допоміг компанії оптимізувати внутрішні процеси. Наприклад, маркетинговий відділ раніше витрачав до 10 годин на тиждень на

підготовку звітів вручну. Після автоматизації звітності через Looker Studio цей час скоротився до 2 годин, оскільки дані оновлювалися в реальному часі, а дашборди були доступні всім членам команди. Це дозволило маркетологам зосередитися на аналізі та стратегічному плануванні, а не на рутинних завданнях.

Загалом, використання Looker Studio для аналізу маркетингових даних дало компанії можливість не лише оцінити ефективність своїх кампаній, але й виявити слабкі місця та оптимізувати стратегії. Завдяки інтеграції з різними джерелами даних, інтерактивним фільтрам і можливостям реального часу, інструмент став ключовим елементом у прийнятті рішень. Аналіз реальних даних показав, що інвестиції в органічний пошук і таргетовану рекламу на конкретні аудиторії приносять найбільшу віддачу, тоді як неефективні кампанії, такі як ремаркетинг у певних регіонах, потребують перегляду. Looker Studio довів свою цінність як інструмент, що не лише спрощує аналіз, але й сприяє зростанню бізнесу через глибше розуміння маркетингових даних.

Список використаних джерел

1. Велика інструкція по Google Looker (Data Studio): огляд можливостей та інструкції з налаштування. Profit.store, 2023. URL: https://profit.store/uk/blog/expert/velyka-instrukciya-po-google-looker-studio (дата звернення: 10.05.2025).
2. Патральський Т. І. Сучасні інформаційно-аналітичні системи. Цифрова економіка як фактор інновацій та сталого розвитку суспільства : тези доповідей V міжнародної науково-практичної конференції учених та студентів, м. Тернопіль, 28-29 листопада 2024 р. Тернопільський національний технічний університет ім. І.Пулюя, 2024. 132-133.
3. Yanto B., Sudaryanto A., Pratiwi H. A. Data Visualization Analysis of Waste Production Volume in Every District of Tangerang Regency in 2021 Using Looker Studio and Big Query Platforms. Journal Of Ict Aplications And System, 2023. №2(1). С. 35-40.

Ключові слова: маркетинг, Looker studio, Google, аналіз даних, реклама.

Keywords: marketing, Looker studio, Google, data analysis, advertising.

ЦИФРОВЕ ЕКОНОМІЧНЕ ПАРТНЕРСТВО (DEPA)

Сіряков Кирило

студент 1-го курсу факультету судового та міжнародного права Національного університету «Одеська юридична академія»

У сучасних умовах глобальної цифровізації економічних процесів особливої ваги набувають механізми міжнародного регулювання цифрової торгівлі. Традиційні торговельні угоди вже не відповідають викликам цифрової епохи. Вони не враховують динаміку технологічних змін та нові форми бізнес-комунікацій. Угода про цифрове економічне партнерство (DEPA), що була підписана у

2020 році Сінгапуром, Чилі та Новою Зеландією, стала першою спробою створити міжнародний правовий інструмент, спрямований виключно на врегулювання цифрової торгівлі. Актуальність угоди зростає в умовах посилення ролі електронної комерції, стрімкого розвитку фінтеху, штучного інтелекту та потреби у захисті даних.

Поява DEPA стала відповіддю на обмеження чинних багатосторонніх угод (СОТ, СРТРР), які не охоплювали специфічних аспектів цифрової економіки [4]. Інтернет-послуги, електронна комерція, хмарні обчислення, блокчейн та інші інновації вимагали нових підходів до регуляції. Водночас відсутність єдиних стандартів ускладнювала міжнародну співпрацю у сфері цифрових технологій. DEPA заповнила цю прогалину, ставши моделлю цифрової економічної інтеграції, яка враховує як технічні аспекти (передача даних, стандарти ШІ), так і питання етики та прав людини [1; 2].

DEPA складається з кількох функціональних модулів, кожен з яких регулює окремі аспекти цифрової економіки. Перший модуль передбачає вільний потік даних між країнами-учасницями за умови забезпечення високих стандартів захисту персональних даних. Це дозволяє компаніям уникати зайвих регуляторних бар'єрів і сприяє розвитку міжнародної електронної торгівлі [1; 2].

Другий модуль спрямований на спрощення електронних транзакцій шляхом уніфікації правил щодо електронних підписів, контрактів та ідентифікації. Завдяки цьому документи, підписані в одній країні, визнаються чинними в інших країнах-учасницях DEPA, що суттєво скорочує час та витрати на укладання угод [3].

Третій модуль стосується етичного використання штучного інтелекту. DEPA встановлює вимоги до прозорості алгоритмів, зобов'язує країни запобігати дискримінаційним рішенням, прийнятим автоматизованими системами. Це надзвичайно важливо в контексті захисту прав людини та формування довіри до цифрових технологій [2].

Четвертий модуль передбачає підтримку малого та середнього бізнесу (МСБ) через доступ до онлайн-платформ, спрощення фінансових операцій та розвиток цифрових навичок підприємців. Особлива увага приділяється створенню сприятливого середовища для виходу МСБ на міжнародні ринки [1].

DEPA є відкритою угодою, до якої можуть приєднуватися нові держави. У 2022 році Канада розпочала офіційні переговори щодо вступу, у 2023 році аналогічну заявку подав Китай. Водночас Китайська ініціатива викликала занепокоєння серед чинних учасників через відмінності у підходах до свободи інтернету, захисту даних та кібербезпеки. Південна Корея та Велика Британія також проявили зацікавленість у приєднанні до DEPA, що підтверджує її геостратегічне значення як платформи для формування глобальних стандартів цифрової торгівлі [1; 3].

Попри значний потенціал, DEPA стикається з рядом викликів. Серед основних проблем – відсутність єдиних міжнародних стандартів для цифрової торгівлі,

що ускладнює гармонізацію законодавства різних країн. Крім того стрімкий розвиток технологій вимагає постійного оновлення положень угоди, аби уникнути її морального старіння. Деякі експерти висловлюють побоювання щодо можливого посилення впливу великих технологічних корпорацій, що може створити нерівні умови для МСБ. Не менш актуальними залишаються питання захисту персональних даних, етичного використання ШІ та забезпечення прозорості цифрових процесів [4].

DEPA є важливим кроком у розвитку міжнародної цифрової економіки. Вона формує базові правила для обміну даними, розвитку інноваційних технологій та інтеграції малих і середніх підприємств до глобального ринку. Розширення угоди та її гармонізація з іншими міжнародними ініціативами може стати основою для створення єдиних глобальних стандартів цифрової торгівлі. У перспективі DEPA може мати значний вплив на формування прозорого, безпечного та етичного середовища для розвитку цифрової економіки у світі.

Список використаних джерел

1. Офіційний сайт уряду Нової Зеландії – Інформація про угоду DEPA та її положення. URL: https://www.mfat.govt.nz/ (дата звернення: 15. 05. 2025)
2. Офіційний сайт уряду Сінгапуру – Огляд цифрового економічного партнерства. URL: https://www.mti.gov.sg/ (дата звернення: 15. 05. 2025)
3. Офіційний сайтуряду Чилі – Документи та пояснення щодо DEPA. URL: https://www.subrei.gob.cl/ (дата звернення: 15. 05. 2025)
4. Світова організація торгівлі (СОТ) – Цифрова економіка та міжнародна торгівля. URL: https://www.wto.org/ (дата звернення: 15. 05. 2025)

Ключові слова: цифрова економіка, електронна торгівля, блокчейн, хмарні технології, електронні транзакції.

Keywords: digital economy, e-commerce, blockchain, cloud computing, electronic transactions.

Науковий керівник: доцент Чанишев Р.

ОЦІНКА КОНКУРЕНТНИХ ПОЗИЦІЙ ВІТЧИЗНЯНИХ РОЗРОБНИКІВ КОМП'ЮТЕРНИХ ІГОР ЗА ДОПОМОГОЮ БАГАТОКУТНИКА КОНКУРЕНТОСПРОМОЖНОСТІ

Ігнатенко Анастасія

студентка 1 курсу магістратури
факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Скідан Владислав

асистент кафедри кібербезпеки
Національного університету «Одеська юридична академія»

Індустрія комп'ютерних ігор в Україні є однією з найперспективніших галузей IT-сектору, що здобуває міжнародне визнання завдяки високій якості продуктів і талановитим командам. Вітчизняні студії, такі як GSC Game World, 4A Games та Frogwares, створили ігри світового рівня, зокрема серії S.T.A.L.K.E.R., Metro та Sherlock Holmes [1,2]. Проте глобальна конкуренція вимагає систематичного аналізу сильних і слабких сторін компаній.

Багатокутник конкурентоспроможності – це графічний метод, який дозволяє порівнювати компанії за кількома критеріями, представленими осями, що виходять із центра. Значення показників формують замкнену лінію, а більша площа багатокутника свідчить про вищу конкурентоспроможність [3]. Для аналізу українських розробників обрано шість критеріїв: якість продукту, інноваційність, репутація бренду, фінансові ресурси, команда розробників, маркетинг і дистрибуція. Оцінка проводилася за шкалою від 0 до 10 на основі відкритих джерел, звітів компаній, профільних медіа (наприклад, GameDev DOU) та галузевих оглядів станом на травень 2025 року.

Для аналізу розглянуто три провідні українські студії: GSC Game World, 4A Games і Frogwares. GSC Game World відома своєю культовою серією S.T.A.L.K.E.R., яка здобула популярність завдяки атмосфері та деталізації. Очікуваний реліз S.T.A.L.K.E.R. 2: Heart of Chornobyl у 2024 році, створений на Unreal Engine 5, отримав високі оцінки за графіку, але затримки релізу дещо вплинули на сприйняття. Студія активно співпрацює з Microsoft, що посилило її глобальну впізнаваність, а присутність на Xbox Game Pass і Steam забезпечує ефективну дистрибуцію. Проте команда з приблизно 200 спеціалістів є відносно невеликою, а фінансування залежить від зовнішніх інвестицій.

4A Games, розробник серії Metro, вирізняється технічною досконалістю. Metro Exodus отримав середній рейтинг 82/100 на Metacritic завдяки графіці та насиченому наративу [4]. Використання власного двигуна 4A Engine і технологій, таких як трасування променів, демонструє інноваційність студії. Після придбання Embracer Group у 2020 році 4A Games отримала доступ до значних ресурсів, що дозволило розширити розробку [5]. Команда з 150–200 розробників працює в

офісах у Києві та на Мальті. Партнерство з Deep Silver забезпечує присутність на Steam, PlayStation і Xbox, але маркетинг залишається менш агресивним порівняно з глобальними гігантами.

Frogwares, незалежна студія, спеціалізується на пригодницьких іграх, зокрема серії Sherlock Holmes. Їхні продукти, як-от Sherlock Holmes Chapter One (рейтинг 82/100 на Metacritic), мають стабільну нішеву аудиторію, але поступаються ААА-іграм у технічній якості. Обмежені фінансові ресурси та команда з 50–70 осіб стримують масштаби проєктів. Студія покладається на продажі через Steam і консолі, а також на краудфандинг, що обмежує маркетингові можливості. Водночас Frogwares зберігає лояльність фанатів завдяки унікальному ігровому дизайну [6].

Побудова багатокутників конкурентоспроможності для цих студій показує їхні сильні та слабкі сторони. GSC Game World має найбільшу площу багатокутника завдяки високій репутації та ефективному маркетингу, але обмежена розміром команди та фінансовою залежністю. 4A Games демонструє сильні позиції в якості продукту та інноваційності, але поступається в агресивності просування. Frogwares має найменшу площу через обмежені ресурси, але зберігає стабільність у нішевому сегменті. Дані оцінки базуються на реальних показниках: рейтинги ігор з Metacritic, розміри команд із DOU, фінансові звіти та маркетингові активності компаній.

Аналіз демонструє, що українські розробники мають значний потенціал на глобальному ринку, але стикаються з викликами. GSC Game World може зміцнити позиції шляхом розширення команди, 4A Games – через активніший маркетинг, а Frogwares – через залучення додаткових інвестицій. Загалом, для підвищення конкурентоспроможності українським студіям необхідно інвестувати в таланти, нові технології та глобальну дистрибуцію. Багатокутник конкурентоспроможності виявився ефективним інструментом для виявлення слабких місць і формування стратегій розвитку, що підтверджується реальними прикладами успіху вітчизняних компаній.

Список використаних джерел

1. Найпопулярніший рушій – Unity, а 70% студій працюють на мобільний ринок. Рейтинг продуктових геймдев-компаній України, 2025. Gamedev.dou, 2025. URL: https://gamedev.dou.ua/articles/product-gamedev-rating-2025/
2. Найкращі комп'ютерні ігри українського виробництва. Кошт, 2023. URL: https://kosht.media/top-4-naykrashchi-komp-iuterni-ihry-ukrainskoho-vyrobnytstva/
3. Миронюк, Т. І., & Цьома, В. І. (2014). Сучасні проблеми та методи оцінки конкурентоспроможності. Економіка харчової промисловості, №1. С. 35-37.
4. Metro Exodus. MetaCritic. Офіційний сайт. https://www.metacritic.com/game/metro-exodus/

5. Nesterenko O. Embracer Group acquires 4A Games through Saber Interactive. Gameworld Observer, 2020. URL: https://gameworldobserver.com/2020/08/13/embracer-4a-games
6. Коршунов С. Сергій Оганесян, Marketing Team Lead київської студії Frogwares, – як створювали Sherlock Holmes Chapter One і як це випускати гру без видавця. Gamedev.dou, 2021. URL: https://gamedev.dou.ua/articles/frogwares-about-sherlock-holmes/

Ключові слова: багатокутник конкурентоспроможності, українські розробники, конкурентоспроможність, ігрова індустрія, маркетинг.

Keywords: competitiveness polygon, Ukrainian developers, competitiveness, gaming industry, marketing.

МЕТОДИ ОЦІНКИ КОНКУРЕНТОСПРОМОЖНОСТІ ВІТЧИЗНЯНИХ ЛОГІСТИЧНИХ ОПЕРАТОРІВ В УМОВАХ ЦИФРОВИХ ТРАНСФОРМАЦІЙ

Кірович Андрій

аспірант Національного університету «Одеська юридична академія»

Конкурентоспроможність логістичного оператора визначається як його здатність надавати ефективні, швидкі та якісні послуги в умовах ринкової конкуренції. У цифрову епоху традиційні фактори, такі як ціна чи швидкість доставки, доповнюються технологічними можливостями. Відтак рівень цифровізації є комплексним критерієм, що охоплює інтеграцію сучасних технологій у процеси управління, операційну діяльність і взаємодію з клієнтами [1].

На практиці рівень цифровізації вказує, наскільки логістичний оператор використовує цифрові технології для оптимізації своєї діяльності. Цей критерій включає автоматизацію процесів, обробку даних у реальному часі, використання аналітики, створення зручних клієнтських інтерфейсів та забезпечення кібербезпеки. Високий рівень цифровізації дозволяє оператору знижувати витрати, підвищувати швидкість реакції на ринкові зміни та покращувати клієнтський досвід.

Для оцінки конкурентоспроможності за критерієм рівня цифровізації пропонується методологія, що включає єдиний перелік параметрів:

Автоматизація процесів - використання систем управління транспортом, складами та ресурсами підприємства.

Інтеграція даних - обмін інформацією в реальному часі між учасниками ланцюга постачання.

Аналітика та штучний інтелект - прогнозування попиту й оптимізація операцій за допомогою big data [2].

Цифрові клієнтські сервіси - наявність мобільних додатків і платформ для відстеження вантажів.

Кібербезпека - захист даних від кіберзагроз [3].

Кожен параметр оцінюється за шкалою від 0 до 1, а їхня сукупність формує індекс цифровізації:

$$\text{ІЦ} = \frac{\text{А} + \text{І} + \text{ШІ} + \text{К} + \text{Б}}{5},$$

де А – автоматизація, І – інтеграція, ШІ – аналітика, К – клієнтські сервіси, Б – кібербезпека.

Оцінка рівня цифровізації дозволяє провести порівняльний аналіз конкурентоспроможності вітчизняних логістичних операторів, таких як «Нова Пошта», «Укрпошта» чи «Meest Express», а також виявити їхні сильні та слабкі сторони. Наприклад, «Нова Пошта» активно інвестує в цифрові технології, зокрема в автоматизовані сортувальні центри, які значно скорочують час обробки вантажів, та мобільні додатки, що забезпечують зручне відстеження посилок і оформлення замовлень [4].

Ці рішення підвищують її індекс цифровізації, зміцнюючи позиції на ринку. «Укрпошта», хоча й модернізує свою IT-інфраструктуру, все ще стикається з викликами у впровадженні клієнтських цифрових сервісів, таких як інтуїтивно зрозумілі онлайн-платформи, що дещо знижує її конкурентоспроможність. Менші логістичні оператори, як правило, мають обмежений доступ до фінансових і технологічних ресурсів, що призводить до низького рівня автоматизації та інтеграції даних, а отже, до слабшої конкурентної позиції.

Такий аналіз не лише виявляє поточний стан цифровізації, але й допомагає визначити стратегічні напрями розвитку. Наприклад, компанії можуть зосередитися на впровадженні хмарних технологій для зниження витрат на IT-інфраструктуру, інвестувати в навчання персоналу для роботи з аналітичними інструментами або співпрацювати з технологічними стартапами для розробки інноваційних рішень. Крім того, оцінка рівня цифровізації може бути використана для порівняння з міжнародними операторами, такими як DHL чи FedEx, що дозволяє визначити прогалини у технологічному розвитку та адаптувати глобальні практики до українського ринку.

Впровадження цифрових технологій в Україні супроводжується низкою викликів, що обмежують конкурентоспроможність логістичних операторів.

По-перше, створення цифрових систем, таких як автоматизовані сортувальні центри, вимагає значних фінансових вкладень, доступних переважно великим компаніям.

По-друге, дефіцит кваліфікованих IT-фахівців, аналітиків даних і спеціалістів із кібербезпеки ускладнює впровадження та підтримку технологій, особливо для малих операторів.

По-третє, зростання цифровізації підвищує кіберризики: у 2023 році низка українських компаній зазнала атак на логістичні платформи, що підкреслило необхідність інвестицій у захист даних.

По-четверте, нерівномірний доступ до швидкісного інтернету в сільських регіонах ускладнює впровадження цифрових сервісів, таких як відстеження вантажів у реальному часі.

По-п'яте, відсутність чітких регуляторних стандартів для цифрових платформ створює правову невизначеність, стримуючи інвестиції.

Проте суб'єкти підприємництва, які долають вказані бар'єри, отримують конкурентні переваги. Наприклад, аналітика на основі штучного інтелекту може скоротити логістичні витрати на 10–15%, а зручні клієнтські мобільні застосунки підвищують лояльність клієнтів, що критично важливо в конкурентному середовищі.

Відтак саме рівень цифровізації можна вважати достатнім критерієм для оцінки конкурентоспроможності вітчизняних логістичних операторів в умовах цифрових трансформацій. Цей критерій охоплює ключові аспекти технологічного розвитку – від автоматизації до кібербезпеки – і забезпечує комплексну оцінку здатності компанії конкурувати на ринку. Запропонована методологія, заснована на аналізі п'яти параметрів та розрахунку індексу цифровізації, дозволяє об'єктивно визначити технологічний рівень оператора, виявити його слабкі місця та розробити стратегію вдосконалення. У довгостроковій перспективі компанії, які прискорюють цифровізацію, зміцнять свої позиції на внутрішньому ринку та зможуть конкурувати з глобальними гравцями, адаптуючись до викликів цифрової економіки.

Список використаних джерел

1. Chopra, S., & Meindl, P. Supply Chain Management: Strategy, Planning, and Operation. Pearson, 2016. 528 p.
2. Горбаченко С.А., Клєвцєвич Н.А., Дикий О.В. Використання Big Data в процесі прийняття управлінських рішень. *Науковий погляд: економіка та управління*. 2024. № 4 (88). С. 127-135.
3. Rushton A., Croucher P., Baker P. The Handbook of Logistics and Distribution Management. Kogan Page, 2017. 912 p.
4. Li D. J., Gosling S., Srivastava A. Digital logistics: Into the express lane? *McKinsey & Company*, 2024. URL: https://www.mckinsey.com/capabilities/operations/our-insights/digital-logistics-into-the-express-lane

Ключові слова: конкурентоспроможність, логістичні оператори, цифрові трансформації, методи оцінки

Keywords: competitiveness, logistics operators, digital transformation, assessment methods

Науковий керівник: професор Горбаченко С.

ВИКОРИСТАННЯ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ ДЛЯ РОЗРОБКИ МАРКЕТИНГОВОЇ СТРАТЕГІЇ РОЗВИТКУ ПІДПРИЄМСТВА

Ничипорчук Анастасія

студентка 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Маркетинг є ключовим інструментом для зміцнення позицій підприємства на ринку, створюючи ефективний зв'язок між компанією та її клієнтами. У світі, де цифрові технології стрімко трансформують бізнес, маркетингові стратегії, підкріплені машинним навчанням і аналітикою даних, стають вирішальними для досягнення конкурентної переваги. Цей вступ уникає шаблонних формулювань, наголошуючи на практичній ролі маркетингу в сучасному бізнес-середовищі.

Завдяки аналізу великих обсягів даних маркетинг допомагає підприємствам краще розуміти свою аудиторію. Інструменти машинного навчання, такі як алгоритми сегментації чи прогнозної аналітики, дозволяють виявляти тренди в поведінці споживачів, передбачати їхні уподобання та пропонувати персоналізовані рішення [1]. Це сприяє підвищенню клієнтської лояльності та оптимізації маркетингових бюджетів.

За даними досліджень, застосування машинного навчання може збільшити ефективність рекламних кампаній на 30% і більше, що підкреслює його значення для сучасного бізнесу. Актуальність таких підходів підтверджується динамікою використання соціальних мереж в Україні: якщо у 2020–2021 роках їхня аудиторія зросла на 7 мільйонів, то у 2023 році кількість користувачів досягла 26.7 мільйона (74% населення), хоча у 2024–2025 роках спостерігалося зниження до 21.6 мільйона (56.4% населення) через війну та методологічні зміни. У цьому дослідженні розглянуто методи машинного навчання, які застосовуються для розробки маркетингової стратегії, з акцентом на їхню практичну цінність у контексті цифрових каналів.

Метод кластерного аналізу застосовується для сегментації клієнтів, що є основою для створення персоналізованих маркетингових кампаній. Наприклад, алгоритм k-середніх групує споживачів за такими параметрами, як вік, частота покупок чи вподобання щодо продуктів. Обробки даних, зокрема перетворення категоріальних змінних на числові та стандартизації числових показників, допоможе визначити оптимальну кількість кластерів (за допомогою методу, який оцінюється якість групування. Це дає можливість виділення сегментів, таких як молоді споживачі з нерегулярними покупками, клієнти середнього віку, які обирають преміум-продукти, та сімейні покупці з високою частотою замовлень. Ці сегменти дозволяють створювати цільові кампанії, наприклад, пропонувати знижки молоді через соціальні мережі, такі як YouTube чи Instagram, які у 2024 році лідирують за популярністю (YouTube – 37.8% частки відвідувань), або надсилати сімейні пропозиції через електронну пошту. Такий підхід сприяє підвищенню залучення клієнтів і ефективності маркетингу.

Регресійний аналіз використовується для оцінки впливу рекламних витрат на результати діяльності. Цей метод допомагає визначити, які маркетингові канали приносять найбільшу віддачу. Доречно використовувати дані не менш ніж за 12 місяців, яки повинні охоплювати охоплюють витрати на три рекламні канали, наприклад, різні платформи соціальних мереж, та обсяги продажів. Після перевірки даних на відповідність статистичним вимогам, зокрема відсутність сильної залежності між змінними, встановлено, що один канал має значно більший вплив на продажі порівняно з іншими, які показали нижчу ефективність. Результати аналізу дозволять перерозподіляти маркетинговий бюджет, спрямовуючи більше ресурсів на канали з високою результативністю, такі як YouTube чи Instagram, які у 2023–2024 роках демонструють високе залучення (Instagram – 17.5% реферального трафіку). Це сприяє підвищенню рентабельності маркетингових зусиль, особливо враховуючи, що у 2025 році 56.4% населення України активно використовують соціальні мережі.

Моделі часових рядів, такі як ARIMA, застосовуються для прогнозування попиту, що є важливим для стратегічного планування. Цей метод передбачає майбутні продажі на основі історичних даних, допомагаючи оптимізувати виробничі та маркетингові процеси. Такі прогнози дозволяють планувати запаси та посилювати маркетингові кампанії перед піковими сезонами, наприклад, у літні місяці, коли соціальні мережі, як показують дані 2024 року, залишаються ключовим джерелом новин для 73.4% українців. Це допомагає уникнути дефіциту продукції та максимізувати прибутки.A/B тестування використовується для порівняння ефективності різних форматів реклами. У дослідженні порівняно два формати – відеоролики та статичні пости – за показником частки кліків. Гіпотетичні дані охоплювали 50 000 користувачів для кожного формату, а статистичний тест показав, що відео мають вищу ефективність порівняно зі статичними постами. Отримані результати дозволяють створювати короткі відеоролики (15–30 секунд) для соціальних мереж, таких як YouTube, яке у 2024 році стало найпопулярнішою платформою в Україні, чи Instagram, де відеоконтент, як Reels, набирає популярності. Це сприяє зростанню залучення аудиторії та підвищенню конверсії рекламних кампаній.

Аналіз повернення інвестицій (ROI) застосовується для оцінки прибутковості маркетингових ініціатив. Цей показник порівнює дохід від продажів із витратами на рекламу, допомагаючи визначити найбільш вигідні стратегії. У дослідженні проаналізовано дані за 12 місяців, розрахувавши ROI з урахуванням середньої ціни продукту. Результати показали середній ROI на рівні 1.5, з найвищими значеннями влітку (до 2.1) і нижчими взимку (0.9). Такий аналіз дозволяє планувати бюджет із урахуванням сезонності, спрямовуючи більше ресурсів на періоди високого попиту, такі як літні місяці, і оптимізуючи витрати в менш активні сезони. Це максимізує прибутковість, особливо враховуючи, що у 2025 році 56.4% населення України активно використовують соціальні мережі.

Аналіз коментарів у YouTube чи Instagram виявляє ключові фактори, що впливають на лояльність клієнтів, а класифікаційні моделі ідентифікують споживачів із високим потенціалом для довгострокової співпраці. Інтеграція цих інструментів у

маркетингові стратегії підвищує їхню точність, особливо з огляду на те, що у 2024 році 47.3% українців довіряють соціальним мережам як джерелу новин, хоча цей показник знизився порівняно з 60% у 2023 році.

Застосування методів машинного навчання, таких як кластерний аналіз, регресійний аналіз, прогнозування часових рядів, A/B тестування та аналіз ROI, створює комплексний підхід до розробки маркетингової стратегії. Ці інструменти дозволяють сегментувати клієнтів, оптимізувати витрати, передбачати попит і оцінювати ефективність кампаній, що є критично важливим для успіху в інформаційному суспільстві. У майбутніх дослідженнях доцільно зосередитися на можливостях глибокого навчання та аналізу великих даних, які можуть автоматизувати маркетингові процеси та забезпечити ще більш персоналізовані пропозиції для споживачів.

Список використаних джерел

1. Хасти Т., Тибширани Р., Фридман Дж. Элементы статистического обучения: Data Mining, Inference, and Prediction. Київ: ДМК Пресс, 2017. 768 с.
2. За рік кількість українців у соцмережах зросла на 7 мільйонів – дослідження [Електронний ресурс]. URL: https://www.epravda.com.ua/news/2021/03/17/672023/
3. Digital 2023: Ukraine URL: https://datareportal.com/reports/digital-2023-ukraine
4. Digital 2024: Ukraine URL: https://datareportal.com/reports/digital-2024-ukraine
5. Digital 2025: Ukraine. URL: https://datareportal.com/reports/digital-2025-ukraine
6. Social network web visit share in Ukraine from January 2022 to May 2024, by platform URL: https://www.statista.com/statistics/1473398/social-network-visit-ukraine-by-platform/
7. Media Consumption of Ukrainians: the Third Year of a Full-scale War URL: h ttp s: // www.opo rau a.org

Ключові слова: машинне навчання, маркетингова стратегія, кластерний аналіз, регресійний аналіз, прогнозування попиту, A/B тестування, ROI.

Keywords: machine learning, marketing strategy, cluster analysis, regression analysis, demand forecasting, A/B testing, ROI.

Науковий керівник: доцент Чепурна О.

IT-ФУНДАМЕНТ ЗАСТОСУВАННЯ BTL МАРКЕТИНГУ

Табала Ксенія

студентка 1 курсу магістратури
факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Разінкін Нікіта

асистент кафедри кібербезпеки
Національного університету «Одеська юридична академія»

BTL (Below The Line) маркетинг – це сукупність маркетингових стратегій, що зосереджуються на прямих, цільових і персоналізованих комунікаціях із конкретними групами споживачів. На відміну від ATL (Above The Line) кампаній, які спрямовані на масову аудиторію через телебачення чи радіо, BTL охоплює промоакції, прямі розсилки, заходи, спонсорство, цифрові інтерактивні кампанії та точкові рекламні ініціативи. У сучасному світі інформаційні технології стали основою для ефективного впровадження BTL маркетингу, забезпечуючи персоналізацію, автоматизацію, аналітику в реальному часі та інтерактивність.

Інформаційні технології є рушійною силою BTL маркетингу, дозволяючи брендам досягати високої точності у взаємодії з аудиторією. Основою цього є дані про клієнтів, які збираються через CRM-системи, такі як Salesforce, HubSpot або Microsoft Dynamics 365. За даними звіту Salesforce за 2024 рік, компанії, які використовують CRM для сегментації клієнтів, підвищують конверсію на 30% порівняно з тими, що покладаються на загальні маркетингові стратегії [1]. Наприклад, міжнародна мережа кав'ярень Starbucks використовує свою CRM-систему для аналізу покупок клієнтів через мобільний додаток. Це дозволяє створювати персоналізовані пропозиції, як-от знижки на улюблені напої, що сприяло зростанню доходу від програми лояльності на 14% у 2023 році [2].

Автоматизація маркетингових процесів відіграє ключову роль у масштабуванні BTL кампаній. Платформи, такі як Marketo, ActiveCampaign або Klaviyo, дозволяють налаштовувати автоматичні сценарії для email-розсилок, push-повідомлень і соціальних мереж. Автоматизація email-маркетингу підвищує показник відкривання листів на 70% і клікабельність на 152%. Реальний приклад – бренд одягу ASOS, який використовує Klaviyo для автоматичних розсилок із персоналізованими рекомендаціями на основі історії переглядів і покупок. ASOS відомий своєю стратегією персоналізованого маркетингу, і Klaviyo часто згадується як платформа, яку використовують ритейлери для автоматизації email-кампаній. У звіті Klaviyo про ecommerce-маркетинг (2023) зазначається, що бренди, які використовують їхню платформу для персоналізованих розсилок, у середньому підвищують дохід від email-кампаній на 15–30% [3].

Аналітика в реальному часі, підкріплена IT, є невід'ємною частиною оцінки ефективності BTL кампаній. Інструменти, такі як Google Analytics 4, Tableau або

Amplitude, дозволяють відстежувати поведінку користувачів, вимірювати ROI (Return on Investment) і коригувати стратегії на ходу. Наприклад, під час промоакції Coca-Cola у 2023 році в Європі бренд використовував QR-коди на пляшках, які спрямовували клієнтів на інтерактивну веб-сторінку. За допомогою Google Analytics Coca-Cola відстежувала кількість сканувань і взаємодій, що дозволило оцінити залученість аудиторії та досягти 3 мільйонів унікальних відвідувань кампанії [4].

Цифрові технології розширюють можливості BTL маркетингу через інтерактивність. Мобільні додатки, гейміфікація та доповнена реальність створюють унікальний досвід для клієнтів. В Україні мережа ресторанів McDonald's у 2023 році впровадила гейміфіковану програму лояльності через мобільний додаток, де клієнти отримували бали за покупки, які можна було обміняти на продукти. Це призвело до зростання кількості транзакцій через додаток на 15% [5].

Інтеграція IT у BTL маркетинг супроводжується викликами. Захист даних є критично важливим, особливо з урахуванням законодавства, як-от GDPR в Європі [6] чи Закон України "Про захист персональних даних" [7]. У 2023 IT компанії зіткнулися з необхідністю вдосконалення систем кібербезпеки для маркетингових даних. Крім того, складність IT-систем вимагає висококваліфікованих спеціалістів. Попит на фахівців із маркетингової аналітики в Україні зріс на 40% за останні два роки. Проте переваги IT значно переважають: вони дозволяють створювати економічно вигідні кампанії з високим рівнем персоналізації.

Загалом, IT-фундамент BTL маркетингу забезпечує інструменти для створення ефективних і вимірюваних кампаній. Від збору даних через CRM до автоматизації розсилок і аналітики в реальному часі, технології дозволяють брендам, таким як Starbucks, ASOS чи Rozetka, досягати глибокої взаємодії з клієнтами. Реальні приклади демонструють, що IT не лише підвищують конверсію та залученість, але й роблять BTL маркетинг ключовим інструментом у цифровій епосі.

Список використаних джерел

1. Salesforce Report: Sales Teams Using AI 1.3x More Likely to See Revenue Increase. Salesforce, 2024. URL: https://www.salesforce.com/news/stories/sales-ai-statistics-2024/
2. Financial Releases. Starbucks, 2023. URL: https://investor.starbucks.com/news/financial-releases/news-details/2023/Starbucks-Reports-Q4-and-Full-Year-Fiscal-2023-Results/default.aspx
3. Regaudie T. Email segmentation tools have evolved–and you should use them to do the same. Klaviyo, 2023. URL: https://www.klaviyo.com/blog/email-segmentation
4. Gilliland N. & Sentance R. 14 examples of augmented reality brand experiences. Econsultansy, 2024. URL: https://econsultancy.com/14-examples-augmented-reality-brand-marketing-experiences/
5. McDonald's Corporation Progress Summary 2023–2024. McDonald's Corporation, 2024. URL:

https://corporate.mcdonalds.com/content/dam/sites/corp/nfl/pdf/McDonald%E2%80%99s%20Progress%20Summary%202023-2024.pdf
6. GDPR. Офіційний сайт. URL: https://gdpr-text.com/
7. Про захист персональних даних : Закон України від 23.02.2012 № 4452-VI. Дата оновлення: 18.01.2025. Верховна рада України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

Ключові слова: BTL, маркетинг, інформаційні технології, ATL, IT сфера.

Keywords: BTL, marketing, information technology, ATL, IT industry.

ЗМІСТ

ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

МАТЕРІАЛИ X ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

23 травня 2025 року
м. Одеса

Відповідальній редактор: Н. І. Логінова

Дизайнер: Р. Р. Дробожур

Електронне видання

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ

МАТЕРІАЛИ X ВСЕУКРАЇНСЬКОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО: «ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ»

23 травня 2025 року, м. Одеса