СИНЕРГІЯ ІНТЕРНЕТ-ТЕХНОЛОГІЙ

Матеріали

І ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

(26 березня 2026 року)

м. Івано-Франківськ
2026 рік

Міністерство освіти і науки України
Заклад вищої освіти
«Університет Короля Данила»
Факультет суспільних і прикладних наук
Кафедра інформаційних технологій

СИНЕРГІЯ ІНТЕРНЕТ-ТЕХНОЛОГІЙ

Матеріали І Всеукраїнської науково-практичної конференції

(м. Івано-Франківськ, 26 березня 2026 року)

Івано-Франківськ

2026

DOI 10.33098/2026.1.26.03

УДК 004.774(0.064)

С 38

Рекомендовано до розміщення в електронних сервісах
ЗВО «Університет Короля Данила»
(протокол № 8 від 26 березня 2026 р.)

С 38 **Синергія інтернет-технологій**: матеріали І Всеукраїнської науково-практичної конференції (м. Івано-Франківськ, 26 березн. 2026 року). Івано-Франківськ: ЗВО «Університет Короля Данила», 2026. 156 с.

ISBN 978-617-8850-10-4

Видання вміщує тези доповідей учасників І Всеукраїнської науково-практичної конференції «Синергія інтернет-технологій», яка відбулася 26 березня 2026 року у закладі вищої освіти «Університет Короля Данила». Розраховане на наукових та науково-педагогічних працівників закладів вищої освіти і наукових установ, здобувачів вищої освіти, а також на широкий читацький загал.

Організаційний комітет не завжди поділяє думку учасників конференції. Відповідальність за достовірність фактів, статистичних даних, точність викладеного матеріалу покладається на авторів.

УДК 004.774(0.064)

Зміст

УДК 004.8:794

Андрейко Анастасія,
студентка І курсу спеціальності
121 Інженерія програмного забезпечення,
ЗВО «Університет Короля Данила»
Науковий керівник:
Іванов Олександр,
завідувач кафедри інформаційних технологій,
доктор філософії,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0003-4678-795

ВИКОРИСТАННЯ ШІ В РОЗРОБЦІ ІГОР

Кожного разу, коли виходить нова велика гра, ми чекаємо від неї чогось неймовірного: крутої графіки, цікавого сюжету та живого світу. Але розробляти такі проєкти стає все складніше і дорожче [1]. Саме через це зараз так багато говорять про ШІ. Нещодавно Сергій Григорович (колишній власник фірми, яка розробила S.T.A.L.K.E.R. і S.T.A.L.K.E.R. 2) сказав, що в нових іграх ШІ буде дуже багато [2]. Він має допомагати створювати текстури, 3D-моделі та музику. Виникає багато питань, одне з них – чи не перетворяться ігри в майбутньому на однотипні проєкти без душі?

З однієї сторони, ШІ – це класний помічник. Якщо раніше розробникам доводилося витрачати місяці, щоб розставити дерева в лісі чи намалювати цеглу в кожному будинку, то зараз нейромережі роблять це за секунди. Це економить дуже велику кількість часу і дозволяє авторам не вигоріти під час розробки. Завдяки ШІ ігри можуть стати дешевшими, тому маленькі студії зможуть випускати проєкти, які будуть конкурувати з гігантами індустрії.

Хоча є ще й мінуси. Як мінімум, це втрата унікальності. ШІ не вміє бути креативним у людському розумінні, просто комбінує те, на чому його навчили. Якщо всі почнуть використовувати одні й ті самі алгоритми, ігри можуть стати дуже схожими між собою. Ще один з мінусів – це коли очікуєш на один результат, а отримуєш зовсім інший, виправляти такі речі буває дуже важко.

Штучний інтелект у геймдеві також використовується для автоматизованого тестування (AI-агенти можуть проходити рівні та виявляти баги значно швидше, ніж люди); розширення поведінки NPC (створення адаптивних персонажів, які реагують на дії гравця); адаптивного сюжету

та квестів (AI генерує варіативні події та діалоги, підлаштовуючись під стиль гри); оптимізації ігрового балансу (аналіз даних гравців і пропозиції змін у механіках для кращого досвіду). Дані наведено в таблиці 1.

Таблиця 1

Приклади застосування ШІ в різних аспектах розробки

Аспект розробки	Приклад використання AI	Пояснення
Генерація графіки	Текстури, 3D-моделі, анімації	Швидке створення великого обсягу контенту
Звуковий супровід	AI-композитор для саундтреку	Музика підлаштовується під дії гравця
NPC та сюжет	Адаптивна поведінка персонажів	NPC реагує на дії гравця та змінює сюжет
Тестування	AI-боти для проходження рівнів	Виявлення багів і недоліків до релізу
Баланс гри	Аналіз даних гравців	Пропозиції щодо покращення ігрового досвіду

Сьогодні в ігровій індустрії реально ведеться багато суперечок щодо того, наскільки глибоко ШІ має проникати в розробку. Хтось бачить у цьому порятунок від перепрацювань, а хтось – загрозу для професії художників. Як уже згадувалося, Сергій Григорович акцентує увагу на тому, що великі проєкти сьогодні забирають занадто багато часу і грошей, тому технології є необхідністю для виживання великих студій [2].

З іншого боку, багато художників і геймдизайнерів переживають, що якщо всюди використовувати нейромережі, то зникне оця людська творчість, яка робить гру особливою. Кажуть, що згенерований контент часто виглядає якимось пустим, без унікального стилю і глибини. Тому зараз активно обговорюють, де застосування ШІ є доречним, а де його використання може реально зіпсувати якість фінального продукту.

На мою думку, ШІ найбільше виправданий саме в технічних процесах, які не вимагають польоту фантазії. Це, наприклад, те ж саме автоматичне тестування, написання технічних скриптів, аналіз статистики гравців або генерація процедурних ландшафтів. У цих випадках нейромережі реально допомагають програмістам і дизайнерам швидше виконувати рутинну роботу, не відволікаючись на дрібниці [3].

А от у творчих питаннях, як-от створення унікальних характерів персонажів чи складних сюжетних ліній, повна автоматизація може просто знизити індивідуальність проєкту. Більшість спеціалістів радять сприймати ШІ лише як ще один інструмент у руках майстра, а не як його заміну.

Для маленьких інді-студій ШІ – це взагалі шанс вижити і показати себе, бо з обмеженим бюджетом вони тепер можуть створювати масштабні світи. Великим же компаніям, де працюють сотні крутих профі, мабуть, не варто занадто сильно покладатися на алгоритми у всьому.

Навіть такі відомі розробники, як Даніель Вавра, дивляться на це з надією. Він сподівається, що штучний інтелект допоможе прискорити процес створення ігор без втрати тієї самої якості, за яку ми їх любимо. Це дозволило б командам реалізовувати набагато більше сміливих ідей, на які раніше просто не вистачало рук чи часу [4].

Підсумовуючи, можна сказати, що штучний інтелект зараз реально стає важливою штукою для розробників. Він дуже допомагає з технічними завданнями, економить купу часу та ресурсів, і це дає шанс навіть невеликим командам робити круті ігри. Але все одно, якщо повністю замінити людину нейромережами, ігри можуть вийти якимись однотипними та нецікавими. Тому найкраще використовувати ШІ як помічника для тестування чи аналізу даних, а от саму творчість і сюжет все-таки залишати людям.

Список використаних джерел:

1. Левицька К. Development of GTA 6 cost «to $2 billion», but the game will pay off in the first year with $3.2 billion in revenue, – Financial Times. *ITC.ua*. 2025. URL: https://itc.ua/en/news/development-of-gta-6-cost-to-2-billion-but-the-game-will-pay-off-in-the-first-year-with-3-2-billion-in-revenue-financial-times/ (дата звернення: 11.03.2026).

2. Кузьменко О. Сергій Григорович працює над новою постапокаліптичною грою S.T.R.A.N.G.E.R.: технології, яких індустрія ще не бачила, зокрема ШІ. *dev.ua*. 2026. URL: https://dev.ua/news/dyvna-hra-hryhorovycha-1772197329 (дата звернення: 11.03.2026).

3. Степанов Л. Створення штучного інтелекту ворогів у іграх. Поради Senior Gameplay Designer компанії Remedy. *DOU.ua*. 2024. URL: https://gamedev.dou.ua/blogs/enemy-ai-in-games/ (дата звернення: 11.03.2026).

4. O'Dwyer M. Kingdom Come: Deliverance 2 director on AI's future role in game development. *Game Rant*. 2025. URL: https://gamerant.com/kingdom-come-deliverance-2-ai-use-in-future-games-comment (дата звернення: 12.03.2026).

УДК 004.75:004.056

Бабак Юрій,
студент І курсу магістратури, МІПЗ-25-1,
факультет суспільних і прикладних наук,
ЗВО «Університет Короля Данила»
Науковий керівник:
Іванов Олександр,
доцент кафедри інформаційних технологій,
доктор філософії,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0003-4678-7956

ЕКОНОМІЧНІ СТИМУЛИ Й ТЕХНІЧНІ ЗАПОБІЖНИКИ У ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ ЗБЕРІГАННЯ ДАНИХ

Актуальність дослідження

У децентралізованих мережах, які надають користувачам такі сервіси, як блоги, форуми, хостинг, місце для бекапа, є потреба у збереженні великих об’ємів даних “off-chain”, тобто за межами бази ключових даних (яка зазвичай зберігається за технологією blockchain). Це зумовлено тим, що збереження будь-яких даних у самому блокчейні є дуже дорогою і повільною операцією. Більше того, записані у блокчейні дані неможливо видалити з часом, що унеможливлює використання цього сховища для деяких сценаріїв [1].

З іншого боку, використання централізованих хмарних сховищ створює ризики цензури та наявності єдиних точок відмови. Яскравим прикладом є кейс, коли один з найбільших провайдерів хмарного сховища Amazon S3 відмовив у хостингу даних соціальній мережі Parler з політичних причин [2]. Також відомі випадки, коли корпорація Google раптово блокувала акаунти, через що бізнеси раптово втрачали доступ до усіх своїх файлів, що зберігалися на цій хмарній платформі [3].

Децентралізовані мережі зберігання даних (Decentralized Storage Networks, DSN), такі як IPFS, Filecoin, Sia, Arweave, Storj, Swarm, MaidSafe, пропонують альтернативу, базуючись на принципах однорангової взаємодії та смартконтрактів [4; 5]. Проте існуючі рішення часто мають або сумнівну надійність (IPFS), або високий поріг входу (Filecoin), або обмежену швидкість доступу до «гарячих» даних, що робить пошук оптимального набору стимулів і запобіжників актуальним завданням.

Предмет дослідження

Практична життєздатність децентралізованих систем сильно залежить від правильної комбінації економічних стимулів і технічних запобіжників, які мають забезпечити довготривале зберігання і захист від шахрайства. Це дослідження спрямоване на формування мінімально необхідного набору таких механізмів, щоб забезпечити економічну обґрунтованість і технічну надійність розподіленого сховища при мінімальних витратах.

Предметом дослідження є набір механізмів двох типів:

– Економічні стимули. Побудова стійкої системи неможлива без теорії ігор. Моделі оплати, ринкові механізми, застави, винагороди, штрафи, мікроплатежі – це все інструменти, які можуть бути використані для досягнення поставленої мети.

– Технічні запобіжники. Для гарантування збереження та цілісності даних у середовищі з нульовою довірою використовуються криптографічні докази зберігання: Proof of Replication (PoRep) та Proof of Space-Time (PoSt). Також можуть бути використані: періодичний аудит, мережеві політики (репутація) тощо.

Дослідження враховує протидію типовим векторам атак [6, с. 9-10]:

– Атаки Сибілли (Sybil Attacks): зловмисники можуть імітувати зберігання (та отримувати за це винагороду) більшої кількості копій даних, ніж зберігається насправді, шляхом створення кількох фіктивних ідентичностей («вузлів»), хоча фактично дані зберігаються лише в одному екземплярі.

– Атаки аутсорсингу (Outsourcing Attacks): зловмисники можуть брати на себе зобов'язання щодо зберігання більшого обсягу даних, ніж вони спроможні вмістити фізично, покладаючись на можливість швидкого завантаження цих даних від інших постачальників за потреби.

– Атаки генерації або підробка (Generation Attacks / Forgery): зловмисники можуть стверджувати, що зберігають значний обсяг даних, коли насправді вони генерують їх «на вимогу» (on-demand) динамічно, замість того, щоб реально тримати їх на диску.

Користь та очікувані результати

Наукова новизна роботи полягає у визначенні «мінімально необхідного» набору параметрів, що дозволить створити систему, доступнішу за існуючі аналоги, зберігаючи високий рівень надійності та захищеності.

Використання вільних ресурсів. Дослідження шукає можливість залучення надлишкових потужностей персональних комп'ютерів та мобільних пристроїв. Оскільки вартість зберігання постійно знижується за законом Крайдера, залучення «idle resources» (вільного місця на дисках)

приватних користувачів теоретично може зробити децентралізоване сховище дешевшим за традиційні хмарні сервіси.

Демократизація інфраструктури. Створення низького порогу входу (наприклад, через легковагові вузли для мобільних платформ) дозволить перетворити DSN на глобальний маркетплейс пам'яті, де кожен користувач може бути і споживачем, і провайдером послуг.

Список використаних джерел:

1. Benet J. IPFS – Content Addressed, Versioned, P2P File System. *arXiv preprint*. 2014. URL: https://arxiv.org/abs/1407.3561 (дата звернення: 30.01.2025).

2. Amazon Is Suspending Parler From AWS. *BuzzFeed News*. URL: https://www.buzzfeednews.com/article/johnpaczkowski/amazon-parler-aws (дата звернення: 30.01.2025).

3. Google Business Profile Suspended, Tried Everything. Desperate for Help. *Reddit*. URL: https://www.reddit.com/r/GoogleMyBusiness/comments/1mdhn24/google_business_profile_suspended_tried/ (дата звернення: 30.01.2025).

4. Khalid M. I. та ін. A Comprehensive Survey on Blockchain-Based Decentralized Storage Networks. *IEEE Access*. 2023. Vol. 11. URL: https://doi.org/10.1109/ACCESS.2023.3240237 (дата звернення: 30.01.2025).

5. E. D., F. T. IPFS and Friends: A Qualitative Comparison of Next Generation Peer-to-Peer Data Networks. *arXiv preprint*. 2021. URL: https://arxiv.org/abs/2102.12737 (дата звернення: 30.01.2025).

6. Pawn, Rookie, Zhuan Cheng. Zero-Knowledge Proof in NuLink. *arXiv.org e-Print archive*. 2024. URL: https://arxiv.org/pdf/2401.03118 (дата звернення: 30.01.2025).

УДК 004.415.2 + 519.8

Бабчук Едуард,
студент ІІІ курсу спеціальності
«Інженерія програмного забезпечення»,
ЗВО «Університет Короля Данила»
ORCID: https://orcid.org/0009-0004-1385-845X
Науковий керівник:
Іванов Олександр,
завідувач кафедри інформаційних технологій,
доктор філософії,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0003-4678-7956

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ У ХМАРНИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМАХ

У сучасних інформаційних системах значна частина обчислювальних процесів виконується у хмарних середовищах. Хмарні обчислювальні

платформи обробляють значні потоки запитів користувачів, що можуть досягати тисяч і навіть мільйонів операцій за секунду. За таких умов ключовим фактором забезпечення стабільної та ефективної роботи системи є оптимальний розподіл навантаження між обчислювальними ресурсами.

Балансування навантаження у хмарних системах полягає у розподілі потоку запитів між кількома серверами з метою запобігання перевантаженню окремих вузлів та зменшення часу обробки запитів. На практиці застосовуються різні алгоритми балансування, серед яких найбільш поширеними є **Round-Robin**, **Least Connections** та **Weighted Load Balancing**. Проте ефективність використання цих алгоритмів значною мірою залежить від характеристик потоку запитів та обчислювальних можливостей серверів.

Для дослідження ефективності балансування навантаження доцільно застосовувати методи математичного моделювання. Одним із найпоширеніших підходів є використання апарату теорії масового обслуговування, що дозволяє описувати поведінку систем обробки запитів у вигляді стохастичних моделей.

Потік запитів до системи характеризується інтенсивністю λ, що визначає середню кількість запитів, які надходять за одиницю часу. Швидкість обслуговування сервером описується параметром μ, який характеризує середню кількість запитів, що можуть бути оброблені сервером за той самий проміжок часу.

У найпростішому випадку систему можна представити у вигляді моделі **M/M/1**, для якої середній час очікування запиту в черзі визначається формулою:

$$W_q = \frac{\lambda}{\mu(\mu - \lambda)}, \quad \lambda < \mu$$

З цієї залежності видно, що зі зростанням інтенсивності потоку запитів λ та наближенням її до швидкості обслуговування μ середній час очікування у черзі різко збільшується. Це свідчить про необхідність використання кількох серверів та ефективного балансування навантаження.

Для систем із кількома обчислювальними вузлами застосовується модель типу M/M/c, де c – кількість серверів. У цьому випадку важливим параметром є коефіцієнт завантаження системи:

$$\rho = \frac{\lambda}{c\mu}$$

який характеризує відношення інтенсивності потоку запитів до сумарної продуктивності системи. Для стабільної роботи системи необхідно виконання умови:

$$\rho < 1$$

Якщо значення ρ наближається до одиниці, система переходить у перевантажений режим, що призводить до різкого зростання часу очікування запитів у черзі. Це підкреслює важливість ефективного розподілу навантаження між серверами.

Для більш точного визначення середнього часу очікування в системах типу M/M/c у теорії масового обслуговування використовується формула Ерланга C (Erlang C). Проте для аналітичного оцінювання рівня завантаження системи та якісного аналізу її поведінки часто достатньо використовувати коефіцієнт завантаження ρ, що дозволяє спростити математичну модель.

Нехай система складається з n серверів, а x_i – кількість запитів, що направляються до сервера i. Тоді задачу оптимального розподілу навантаження можна сформулювати у вигляді задачі мінімізації сумарного часу очікування:

$$min \sum_{i=1}^{n} W_i(x_i)$$

за умов:

$$\sum_{i=1}^{n} x_i = R$$

де $W_i(x_i)$ – середній час очікування запитів на сервері i, а R – загальна кількість запитів у системі.

У рамках **теорії масового обслуговування** середній час очікування для сервера i може бути оцінений за допомогою моделі **M/M/1**. У такому випадку:

$$W_i = \frac{\lambda_i}{\mu_i(\mu_i - \lambda_i)}$$

де λ_i – інтенсивність потоку запитів, що спрямовується до сервера i, а μ_i – швидкість обслуговування відповідного сервера. Якщо x_i – кількість запитів, що надходять до сервера протягом інтервалу часу T, то інтенсивність потоку може бути оцінена як:

$$\lambda_i = \frac{x_i}{T}$$

Така залежність дозволяє пов’язати задачу оптимального розподілу запитів **з параметрами продуктивності серверів**.

Таким чином, задачу балансування навантаження можна представити як задачу оптимального розподілу потоку запитів між обчислювальними вузлами з метою мінімізації сумарного часу очікування та обробки.

У практичних системах балансування навантаження часто використовується оцінка поточного стану серверів. Одним із показників є відносне навантаження сервера, яке можна визначити як:

$$L_i = \frac{C_i}{K_i}$$

де C_i – кількість активних з'єднань на сервері, а K_i – максимальна пропускна здатність відповідного вузла.

Проте для підвищення ефективності балансування доцільно враховувати не лише кількість активних з'єднань, а й прогнозований час обробки запитів. У такому випадку вибір сервера може здійснюватися за критерієм мінімізації очікуваного часу обробки:

$$i^* = \underset{i}{argmin}\left(W_i + \frac{1}{\mu_i}\right)$$

де W_i – поточний час очікування у черзі сервера i, а μ_i – швидкість обслуговування відповідного сервера.

Узагальнюючи наведений підхід, доцільно ввести інтегральну функцію оцінювання навантаження сервера, яка враховує як поточний стан черги, так і продуктивність обчислювального вузла. Таку функцію можна записати у вигляді:

$$F_i = \alpha W_i + \beta \frac{1}{\mu_i}$$

де α та β – вагові коефіцієнти, що визначають відносну важливість часу очікування у черзі та швидкості обслуговування сервера. Їх значення можуть задаватися емпірично залежно від вимог до системи. Наприклад, у системах із високими вимогами до мінімізації затримок більша вага може надаватися параметру W_i, тоді як у системах із неоднорідними обчислювальними ресурсами більшу роль може відігравати швидкість обслуговування μ_i.

Оскільки параметри W_i та 1/μ_i можуть мати різні масштаби значень, доцільно застосувати їх нормалізацію відносно максимальних значень у системі. У такому випадку інтегральну функцію оцінювання можна подати у вигляді:

$$F_i = \alpha \frac{W_i}{max_j W_j} + \beta \frac{\frac{1}{\mu_i}}{max_j \frac{1}{\mu_j}}$$

Така нормалізація дозволяє уникнути домінування одного параметра над іншим та забезпечує коректне використання вагових коефіцієнтів при оцінюванні навантаження серверів.

Тоді вибір обчислювального вузла може здійснюватися за правилом:

$$i^* = \underset{i}{argmin} F_i$$

що дозволяє адаптивно враховувати як завантаженість системи, так і обчислювальні характеристики окремих серверів.

У роботі запропоновано підхід до вибору обчислювального вузла на основі мінімізації очікуваного сумарного часу очікування та обробки запиту, що враховує поточний стан черги та швидкість обслуговування серверів. Такий підхід дозволяє спрямовувати запити до вузла, який забезпечує найменший сумарний час очікування та обробки.

Додатково доцільно ввести узагальнений показник ефективності балансування навантаження, який характеризує середній час перебування запиту в системі. Такий показник можна визначити як

$$T_{avg} = \frac{1}{R}\sum_{i=1}^{n} \quad x_i\left(W_i + \frac{1}{\mu_i}\right)$$

де x_i – кількість запитів, що спрямовуються до сервера i, W_i – середній час очікування у черзі, а $\frac{1}{\mu_i}$ – середній час обробки запиту відповідним сервером. Мінімізація цього показника дозволяє оцінювати ефективність алгоритмів балансування навантаження з точки зору загального часу обробки запитів у системі.

Таким чином, запропонована модель дозволяє формалізувати процес балансування навантаження та оцінювати ефективність різних алгоритмів розподілу запитів у хмарних системах. Використання оптимізаційних критеріїв та оцінки параметрів обслуговування створює можливість зменшення середнього часу обробки запитів і підвищення загальної продуктивності системи.

Подальші дослідження у цьому напрямку можуть бути спрямовані на розробку адаптивних алгоритмів балансування, що використовують методи машинного навчання для прогнозування навантаження та динамічного керування ресурсами хмарної інфраструктури.

Список використаних джерел:

1. IBM Cloud Docs. URL: https://www.ibm.com/topics (дата звернення: 10.03.2026).

2. Microsoft Azure Documentation. URL: https://learn.microsoft.com/en-us/azure/-load-balancer/load-balancer-overview (дата звернення: 10.03.2026).

3. AWS Elastic Load Balancing. URL: https://aws.amazon.com/elasticloadbalancing/ (дата звернення: 10.03.2026).

4. Queueing Theory Overview. *Wikipedia*. URL: https://en.wikipedia.org/wiki/Queueing_theory (дата звернення: 10.03.2026).

УДК 004.89

Бейсюк Ангеліна,
студентка І курсу спеціальності
«Інженерія програмного забезпечення»,
ЗВО «Університет Короля Данила»
Науковий керівник:
Іванов Олександр,
завідувач кафедри інформаційних технологій,
доктор філософії,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0003-4678-7956

АЛГОРИТМИ РЕКОМЕНДАЦІЙ У СОЦІАЛЬНИХ МЕРЕЖАХ

Сучасні соціальні мережі щодня обробляють величезні обсяги інформації, що надходить від мільйонів користувачів у вигляді постів, фотографій, відео та коментарів. У цьому інформаційному потоці важливим завданням стає не лише збереження даних, а й їх ефективний відбір та структуризація. Користувачі очікують отримувати контент, який буде максимально релевантним їхнім інтересам, тому ключовою функцією соціальних платформ є формування персоналізованої стрічки новин. Для цього застосовуються алгоритми рекомендацій – спеціальні програмні методи, що аналізують поведінку користувачів, їхні уподобання та взаємодії з контентом. На основі отриманих даних система формує індивідуальні пропозиції, які підвищують залученість та задоволеність користувачів [1].

Алгоритми рекомендацій працюють на основі багатофакторного аналізу різних типів взаємодії користувачів із платформою. До таких показників належать перегляди, лайки, коментарі, підписки, поширення матеріалів та навіть час, витрачений на перегляд конкретного контенту. Усі ці дані дозволяють системі створити багатовимірний профіль користувача, що відображає його інтереси та поведінкові особливості. На основі цього профілю алгоритм визначає найбільш ймовірні теми чи матеріали, які можуть зацікавити людину, і формує стрічку новин або рекомендації, що відповідають її індивідуальним уподобанням [2].

Найпоширенішими підходами до створення рекомендаційних систем є контентно-орієнтована фільтрація, колаборативна фільтрація та гібридні методи. Контентно-орієнтована фільтрація базується на аналізі характеристик самого контенту, який переглядає користувач, наприклад,

тематики, ключових слів чи жанру. Колаборативна фільтрація, навпаки, враховує поведінку інших користувачів із подібними інтересами, створюючи ефект «колективного досвіду». Гібридні системи поєднують кілька методів одночасно, що дозволяє підвищити точність та адаптивність рекомендацій. У сучасних соціальних мережах дедалі частіше застосовуються саме гібридні моделі, оскільки вони здатні враховувати широкий спектр факторів і забезпечувати більш гнучкі результати [3].

Отже, алгоритми рекомендацій є не просто технічним інструментом, а важливою складовою сучасних інформаційних систем. Вони відіграють ключову роль у функціонуванні соціальних мереж, визначаючи, який контент користувач побачить у своїй стрічці, і тим самим впливаючи на його інформаційне середовище, соціальні зв'язки та навіть світогляд. Ефективність таких алгоритмів безпосередньо впливає на рівень активності користувачів, розвиток бізнес-моделей платформ та формування цифрової культури загалом [4].

Список використаних джерел:

1. Ricci F., Rokach L., Shapira B. Recommender Systems Handbook. New York : Springer, 2015.

2. Aggarwal C. C. Recommender Systems : The Textbook. Cham : Springer, 2016.

3. Jannach D., Zanker M., Felfernig A., Friedrich G. Recommender Systems: An Introduction. Cambridge : Cambridge University Press, 2011.

4. Konstan J., Riedl J. Recommender Systems: From Algorithms to User Experience. *User Modeling and User-Adapted Interaction*. 2012.

УДК 378.147:004.8:355.23

Бужикова Тетяна,
викладач кафедри іноземних мов,
Військовий інститут телекомунікацій
та інформатизації імені Героїв Крут,
м. Київ, Україна
ORCID: https://orcid.org/0000-0002-8117-965X

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В ІНШОМОВНІЙ ПІДГОТОВЦІ ВІЙСЬКОВОСЛУЖБОВЦІВ: МОЖЛИВОСТІ ТА РИЗИКИ

Іншомовна підготовка військовослужбовців є стратегічно важливим компонентом обороноздатності держави, особливо в умовах міжнародної військової співпраці, участі у спільних навчаннях і миротворчих

операціях. Інтенсивний розвиток технологій штучного інтелекту зумовлює трансформацію освітнього процесу, зокрема впровадження інтелектуальних систем підтримки навчання, автоматизованого оцінювання та генеративних мовних моделей. Водночас використання ШІ в освітньому середовищі військових закладів потребує критичного осмислення з огляду на ризики безпеки, правового регулювання та етичних обмежень.

Проблематика впливу генеративного ШІ на процес вивчення іноземної мови висвітлена у праці Р. Чепишка, М. Прохорова, О. Іфтоди, які наголошують на потенціалі адаптивного контенту, автоматизованого зворотного зв'язку та персоналізації навчання [5]. Роль інтерактивних технологій ситуативного моделювання у формуванні комунікативних умінь досліджено К. Мізіним і М. Шемудою, які підкреслюють значення імітаційних моделей для розвитку дискусійних навичок [2]. Проблеми загроз і ризиків застосування ШІ, зокрема в аспекті кібербезпеки, систематизовано у дослідженні О. Скіцька, П. Складанного, Р. Ширшова, М. Гуменюка, де окреслено технічні, інформаційні та соціальні ризики [3]. Правові аспекти функціонування ШІ розкрито у працях С. Р. Корнєєвої та Є. А. Тимошенка, які аналізують проблеми визначення правового статусу ШІ та відповідальності за результати його діяльності [1; 4]. Попри наявність окремих досліджень, питання комплексного аналізу використання ШІ саме в іншомовній підготовці військовослужбовців потребує подальшого наукового осмислення.

Метою статті є визначення дидактичних можливостей і потенційних ризиків використання технологій штучного інтелекту в іншомовній підготовці військовослужбовців.

Технології ШІ відкривають нові перспективи персоналізації навчального процесу. Генеративні мовні моделі забезпечують адаптацію навчального контенту відповідно до рівня володіння мовою, професійної спеціалізації та оперативних потреб військовослужбовця. Як зазначають Р. Чепишко, М. Прохоров, О. Іфтода, ШІ дозволяє формувати індивідуальні траєкторії навчання, що підвищує ефективність засвоєння матеріалу [5]. Це особливо важливо в умовах обмеженого часу на підготовку та необхідності швидкого досягнення функціональної мовної готовності.

Інтелектуальні системи також здатні відтворювати комунікативні ситуації, максимально наближені до реальних військових умов, зокрема переговори з іноземними партнерами, проведення брифінгів, аналіз оперативної інформації. Такий підхід корелює з методикою інтерактивного ситуативного моделювання, описаною К. Мізіним і М. Шемудою [2], однак суттєво розширюється завдяки можливостям автоматичної генерації сценаріїв і варіативності мовленнєвих стратегій.

Важливим аспектом є автоматизований контроль та надання зворотного зв'язку. Системи ШІ можуть здійснювати миттєвий аналіз усного й письмового мовлення, виявляти лексичні, граматичні та прагматичні помилки, пропонувати рекомендації щодо їх усунення. Окрім цього, автоматизовані перекладацькі системи сприяють формуванню навичок роботи з військово-технічною документацією, хоча результати їхньої роботи потребують обов'язкової критичної перевірки фахівцем.

Поряд із дидактичними перевагами існують суттєві ризики використання ШІ у військовій іншомовній підготовці. О. Скіцько, П. Складанний, Р. Ширшов, М. Гуменюк виокремлюють ризики витоку даних, маніпуляції інформацією та використання вразливостей алгоритмів [3]. У військовому середовищі такі загрози можуть призвести до компрометації службової інформації та становити небезпеку для національної безпеки.

Правова невизначеність також залишається актуальною проблемою. С. Р. Корнєєва та Є. А. Тимошенко звертають увагу на складність визначення правового статусу ШІ та розподілу відповідальності за помилки, допущені автоматизованими системами [1; 4]. У випадку використання ШІ для перекладу або аналітичної обробки військової інформації такі помилки можуть мати критичні наслідки.

Не менш значущими є педагогічні та етичні виклики. Надмірна автоматизація навчального процесу може знижувати рівень автономності мислення, критичного аналізу та мовної рефлексії військовослужбовців. Крім того, питання академічної доброчесності, конфіденційності персональних даних і прозорості алгоритмів потребують належного нормативного врегулювання та впровадження чітких інституційних політик.

Ефективне використання технологій ШІ в іншомовній підготовці військовослужбовців можливе за умови створення захищених національних платформ із локалізованими моделями, нормативного врегулювання їх застосування в освітньому процесі, поєднання традиційних методик з інтелектуальними системами та належної підготовки викладачів до роботи з такими технологіями.

Отже, технології штучного інтелекту відкривають значні можливості для підвищення ефективності іншомовної підготовки військовослужбовців завдяки персоналізації навчання, ситуативному моделюванню та автоматизованому оцінюванню. Водночас їх застосування супроводжується кібербезпековими, правовими й педагогічними ризиками. Комплексний підхід до інтеграції ШІ в систему військової освіти має базуватися на принципах безпеки, правової визначеності та педагогічної доцільності.

Список використаних джерел:

1. Корнєєва С. Р. Теоретичні підходи до визначення поняття та правового регулювання штучного інтелекту. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2021. Т. 66. С. 50–55.

2. Мізін К., Шемуда М. Інтерактивні технології ситуативного моделювання та опрацювання дискусійних питань у процесі вивчення іноземної мови. *Науковий вісник Чернівецького національного університету імені Юрія Федьковича. Серія: Германська філологія.* 2023. № 843.

3. Скіцько О., Складанний П., Ширшов Р., Гуменюк М. Загрози та ризики використання штучного інтелекту. *Кібербезпека: освіта, наука, техніка.* 2022. № 2 (22). С. 6–18.

4. Тимошенко Є. А. Правова природа штучного інтелекту: перспективи і проблеми. *Юридичний науковий електронний журнал*. 2023. № 4. С. 424–425.

5. Чепишко Р., Прохоров М., Іфтода О. Вплив генеративного ШІ на вивчення іноземної мови. *Науковий вісник Чернівецького національного університету імені Юрія Федьковича*. *Серія: Германська філологія*. 2025. № 852.

УДК 004.056

Ванджуляк Андрій,
студент ІІІ курсу спеціальності
«Інженерія програмного забезпечення»,
ЗВО «Університет Короля Данила»
Науковий керівник:
Василенко Владислав,
викладач кафедри інформаційних технологій,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна

АНАЛІЗ АНОМАЛІЙ МЕРЕЖЕВОГО ТРАФІКУ В РЕАЛЬНОМУ ЧАСІ ЗА ДОПОМОГОЮ НЕЙРОННИХ МЕРЕЖ

Вступ та актуальність. Сучасні кіберзагрози стають дедалі складнішими, а традиційні системи виявлення вторгнень (IDS), що базуються на сигнатурах, часто не здатні розпізнати атаки «нульового дня» (Zero-day). Використання нейронних мереж дозволяє вийти за межі статичних правил і перейти до динамічного аналізу поведінки мережі. Це критично важливо для захисту інфраструктури в умовах 2026 року, коли швидкість реакції на інцидент визначає рівень потенційних збитків.

Мета дослідження полягає у вивченні методів застосування глибокого навчання для автоматичного виявлення нетипової мережевої активності та розробці підходів до мінімізації помилкових спрацювань у системах безпеки.

Цільова аудиторія: фахівці з кібербезпеки, системні адміністратори, розробники інтелектуальних систем моніторингу.

Ключові аспекти актуальності теми:

– Проактивний захист: виявлення загроз на етапі розвідки або проникнення, а не після нанесення шкоди.

– Автоматизація моніторингу: зменшення навантаження на аналітиків SOC за рахунок інтелектуальної фільтрації трафіку.

– Адаптивність: самонавчання моделі на основі нових патернів трафіку без ручного оновлення баз [1].

Технологічні рішення для аналізу трафіку:

– Рекурентні нейронні мережі (RNN/LSTM): найкраще підходять для аналізу послідовностей пакетів та виявлення часових аномалій.

– Автокодувальники (Autoencoders): використовуються для навчання на «нормальному» трафіку; будь-яке значне відхилення від норми маркується як потенційна атака [2].

– Графові нейронні мережі (GNN): новий підхід, що дозволяє моделювати складні взаємозв'язки між вузлами мережі як топологічні структури.

Таблиця 1

Порівняльний аналіз підходів до детекції

Метод аналізу	Переваги	Недоліки
Сигнатурний аналіз	Висока точність для відомих вірусів.	Безпорадність проти нових атак.
Нейронні мережі	Виявляють невідомі раніше загрози.	Високі вимоги до обчислень.
Гібридні системи	Баланс між точністю та швидкістю.	Складність у налаштуванні.

Отже, впровадження нейронних мереж у процеси аналізу мережевого трафіку є стратегічним пріоритетом для сучасних IT-систем. Використання таких моделей, як автокодувальники та LSTM, дозволяє створювати адаптивні системи захисту, здатні в реальному часі виявляти аномалії, що значно підвищує рівень кіберстійкості організацій у 2026 році.

Список використаних джерел:

1. Kosari A. Real-Time Network Traffic Anomaly Detection Using Spiking Neural Networks (SNNs) with Adaptive Learning. *Contributions of Science and Technology for Engineering*. 2025. Vol. 2 (2). URL: https://cste.journals.umz.ac.ir/article_5536.html (дата звернення: 23.02.2026).

2. Efficient Real-Time Anomaly Detection in IoT Networks Using One-Class Autoencoder and Deep Neural Network / A. Smith et al. *MDPI Electronics*. 2024. Vol. 14 (1). URL: https://www.mdpi.com/2079-9292/14/1/104 (дата звернення: 23.02.2026).

3. AI-Powered Cybersecurity: Neural Networks for Threat Detection and Prevention. *IEEE Xplore: 2025 World Skills Conference on Universal Data Analytics and Sciences*. 2025. URL: https://ieeexplore.ieee.org/document/11199107/ (дата звернення: 24.02.2026).

4. ReGAIN: Retrieval-Grounded AI Framework for Network Traffic Analysis. *arXiv:25-12.22223*. 2026. URL: https://arxiv.org/abs/2512.22223 (дата звернення: 24.02.2026).

УДК 004.89

Василенко Владислав,
студент ІІІ курсу спеціальності
«Інженерія програмного забезпечення»,
ЗВО «Університет Короля Данила»
Науковий керівник:
Гаврилко Сергій,
викладач кафедри інформаційних технологій,
Delivery Director SoftServe,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна

ВПРОВАДЖЕННЯ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ ДЛЯ СТВОРЕННЯ АДАПТИВНИХ АГЕНТІВ У ВИСОКОРЕАЛІСТИЧНИХ СИМУЛЯТОРАХ

На сьогодні сильно зріс попит на інноваційні та унікальні ігри, особливо в жанрі високореалістичних симуляторів, де гравці очікують максимального занурення та адекватної, фізично достовірної реакції середовища. Ігрова індустрія постійно розвивається, створюючи нові виклики для розробників. Класичні неігрові персонажі (NPC) часто діють за заздалегідь написаними скриптами, що руйнує ефект реалізму у складних симуляціях [2].

Впровадження алгоритмів штучного інтелекту (ШІ), зокрема глибокого навчання з підкріпленням (Deep Reinforcement Learning, DRL), у процес створення ігор може значно розширити можливості геймдеву, створюючи агентів, здатних до самостійного прийняття рішень на основі фізики рушія [1].

Метою є виявлення переваг використання інноваційних технологій, зокрема нейронних мереж, для автоматизації процесу створення поведінкових моделей віртуальних агентів, оптимізації їх роботи з телеметрією та покращення взаємодії гравців з віртуальним середовищем.

Методи дослідження включають аналіз наукової літератури, експериментальні дослідження поведінки агентів у фізичних рушіях (наприклад, симуляторі Assetto Corsa) та застосування алгоритмів глибокого навчання з підкріпленням [3].

Цільова аудиторія включає геймерів-ентузіастів (сімрейсерів, фанатів космосимів), кіберспортсменів, геймдизайнерів та розробників ігрових фізичних рушіїв. Також ця система може бути корисною для інженерів-дослідників, що розробляють алгоритми автономного керування для реальних систем, використовуючи ігрові рушії як полігон для тестувань [4].

Аспекти, які підкреслять актуальність цієї теми: створення конкурентоздатних супротивників з людським стилем поведінки, оптимізація тестування фізики об'єктів розробниками, економія обчислювальних ресурсів за рахунок оптимізації нейромереж, а також вдосконалення ігрової інтеракції через роботу з комплексними даними (знос деталей, телеметрія) [3].

В основі покращення геймплею:

– системи штучного інтелекту здатні генерувати унікальних опонентів, які не просто рухаються за лінійною траєкторією, а виконують складні тактичні маневри (наприклад, обгін чи блокування), працюючи на межі зчеплення віртуальних шин з поверхнею [1];

– AI може адаптувати поведінку під конкретного гравця, зчитуючи дані з його пристроїв керування (наприклад, керма з прямим приводом чи HOTAS), щоб створювати динамічний та індивідуалізований рівень складності [2].

Ефективна робота розробників передбачає:

– автоматизацію тестування локацій та фізичних моделей. Віртуальні агенти можуть безперервно знаходитися в симуляції, виявляючи баги та дисбаланс у фізиці рушія [4];

– розподіл логіки: використання високорівневих мов (Python) для тренування моделей DRL на серверах та їх подальшу інтеграцію у гру (наприклад, через C# або C++) для забезпечення максимальної продуктивності в реальному часі.

Вдосконалення ігрової інтеракції: ШІ-агенти можуть приймати багатоцільові рішення. Сучасні дослідження показують, що NPC у симуляторах здатні навчитися не лише їхати чи летіти максимально швидко, а й балансувати швидкість із витратами ресурсів (збереження палива, запобігання перегріву двигуна), самостійно імітуючи реальні професійні стратегії [3].

На даний момент існує та активно досліджується низка інструментів та фреймворків для створення таких систем:

1. Gran Turismo Sophy – інноваційний ШІ-агент, створений за допомогою безмодельного алгоритму DRL [1]. У ході досліджень було доведено, що такий агент здатен перемагати найкращих у світі кіберспортсменів, комбінуючи виняткову швидкість із дотриманням неписаних правил спортивної етики [1].

2. Assetto Corsa RL Environments – використання платформи популярного симулятора для розробки багатоцільових стратегій (наприклад, через алгоритм Soft-Actor-Critic), де агент вчиться керувати технікою в умовах тривалих заїздів на витривалість [3].

3. DRL Control Frameworks – алгоритми глибокого навчання, що дозволяють агенту напряму працювати зі станами об'єкта (швидкість, кут рискання) та самостійно керувати розподілом потужності, оминаючи стандартні скриптові обмеження рушія [4].

На основі аналізу існуючих технологій розробки ігор можна вивести переваги та недоліки, що можуть виникнути під час впровадження системи штучного інтелекту в індустрію симуляторів.

Ключовими елементами системи є:

1. Використання глибокого навчання з підкріпленням для фізики.

– *Переваги:* здатність агента знаходити неочевидні, але високоефективні стратегії керування; створення реалістичних супротивників, що кардинально покращує ігровий досвід [1].

– *Недоліки:* величезні витрати обчислювальних потужностей на симуляцію (самостійна гра агента в уявному середовищі) для досягнення результату; надзвичайна складність налаштування функції винагороди (reward function), щоб дії агента були адекватними [1].

2. Аналіз телеметрії та адаптація середовища.

– *Переваги:* ШІ «відчуває» втрату зчеплення, пошкодження чи зміну погодних умов і моментально змінює тактику, роблячи NPC живими учасниками процесу [2; 3].

– *Недоліки:* висока чутливість до змін: найменше оновлення фізичного рушія гри вимагає повного перенавчання нейронної мережі; складність перенесення навичок агента з однієї віртуальної локації на іншу.

Створення таких просунутих ШІ-систем не лише зробить симулятори більш захоплюючими, а й змінить підхід до створення віртуальних світів, перетворивши їх на живі екосистеми, що розумно реагують на дії гравця [2].

Отже, використання інноваційних алгоритмів машинного навчання дозволяє вивести якість ігрового штучного інтелекту на принципово новий рівень. З урахуванням попиту на хардкорні симулятори та розвиток високоточної периферії, інтеграція адаптивних ШІ-агентів стає необхідністю.

Технології AI відкривають безліч можливостей для творчості розробників та створення небачених раніше стандартів віртуального реалізму.

Список використаних джерел:

1. Wurman P. R., Barrett S., Kawamoto K. та ін. Outracing champion Gran Turismo drivers with deep reinforcement learning. *Nature*. 2022. Vol. 602, No. 7896. P. 223–228. URL: https://pubmed.ncbi.nlm.nih.gov/35140384/ (дата звернення: 12.03.2026).
2. AI NPCs in Gaming: Bringing Characters to Life. *Mimic Minds*. 2025. URL: https://www.mimicminds.com/post/ai-npcs-in-gaming (дата звернення: 12.03.2026).
3. Rusk N. Driving For Endurance: Fuel and Tire Efficient Autonomous Racing in Assetto Corsa Using Reinforcement Learning. *UT Student Theses*. 2025. URL: https://essay.utwente.nl/ (дата звернення: 12.03.2026).
4. Self driving algorithm for an active four wheel drive racecar. *arXiv preprint*. 2025. URL: https://arxiv.org/html/2506.06077v1 (дата звернення: 12.03.2026).

УДК 004.89

Василенко Владислав,
студент ІІІ курсу спеціальності
«Інженерія програмного забезпечення»,
ЗВО «Університет Короля Данила»
Науковий керівник:
Стисло Оксана,
старша викладачка кафедри інформаційних технологій,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна

ВПРОВАДЖЕННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ ТА ПРОТИДІЇ ЧІТИНГУ В КІБЕРСПОРТИВНИХ ДИСЦИПЛІНАХ

На сьогодні індустрія багатокористувацьких онлайн-ігор та кіберспорту стикається з критичною проблемою кібербезпеки – масовим використанням несанкціонованого програмного забезпечення (чітів), що руйнує змагальний баланс [1]. Традиційні системи захисту, які базуються на сигнатурному аналізі пам'яті клієнта (rule-based detection), часто виявляються неефективними проти нових, адаптивних загроз, оскільки розробники шкідливого ПЗ постійно вдосконалюють методи обходу [4].

Впровадження алгоритмів штучного інтелекту (ШІ) та глибокого машинного навчання (Deep Learning) в системи безпеки може значно роз-

ширити можливості виявлення шахраїв шляхом аналізу поведінкових патернів та мережевих аномалій, не порушуючи при цьому конфіденційність користувачів [1; 5].

Метою є виявлення переваг використання інноваційних технологій, зокрема глибоких нейронних мереж (DNN) та архітектури Transformer, для автоматизації процесу виявлення аномальної поведінки користувачів, оптимізації серверного захисту та забезпечення справедливого змагального середовища.

Методи дослідження включають аналіз наукової літератури, роботу з датасетами телеметрії, застосування алгоритмів класифікації часових рядів та методів машинного навчання (зокрема Support Vector Machines та згорткових нейронних мереж) [3; 5].

Цільова аудиторія включає фахівців з кібербезпеки, серверних інженерів, розробників змагальних ігор (зокрема тактичних шутерів від першої особи), кіберспортивні організації та платформотримачів, що зацікавлені у збереженні лояльності аудиторії.

Аспекти, які підкреслять актуальність цієї теми: захист економіки віртуальних предметів (де ціна ігрових активів може сягати десятків тисяч доларів), підтримка конкурентної цілісності турнірів, зниження навантаження на ручний арбітраж та перехід від інвазивного сканування системних файлів до серверного аналізу даних [1; 5].

В основі покращення систем кібербезпеки:

– системи штучного інтелекту здатні аналізувати складні взаємодії людини з комп'ютером (HCI) у вигляді багатовимірних часових рядів, розпізнаючи неприродні мікрорухи, характерні для програм-аімботів (Aimbot) або тригерботів (Triggerbot) [3];

– використання глибокого навчання дозволяє виявляти гравців, які використовують апаратні маніпулятори або змінені драйвери, що працюють на рівні ядра ОС і залишаються невидимими для класичних античітів [4].

Ефективна робота фахівців з безпеки передбачає:

– автоматизацію обробки масивів телеметрії (Big Data) на серверному боці, що зменшує вплив на продуктивність клієнтського ПК користувача [5];

– використання сучасних високорівневих фреймворків (наприклад, мови Python у поєднанні з TensorFlow) для зручного тренування моделей на розмічених базах даних [2].

На даний момент існує і активно досліджується низка інструментів штучного інтелекту для протидії шахрайству:

1. Аналіз на основі архітектури Transformer (наприклад, AntiCheatPT) – модель машинного навчання, спеціально розроблена для виявлення підозрілої поведінки в тактичних шутерах (зокрема Counter-Strike 2) за допомогою ігрових даних. Навчаючись на великих вибірках «контекстних вікон» (секундних зрізів гри), такі моделі здатні досягати точності понад 89 % [2].

2. Системи поведінкового аналізу (VACnet тощо) – серверні інфраструктури, що використовують глибокі нейронні мережі (DNN) для обробки колосальних обсягів історичних даних та виявлення відхилень від очікуваної людської поведінки, що дозволяє превентивно блокувати порушників [1; 5].

3. Згорткові нейронні мережі (CNN) для часових рядів – алгоритми, які класифікують багатоваріантні часові ряди рухів миші гравця, досягаючи вражаючої точності (до 99,2 % для виявлення певних видів втручань) без необхідності прямого сканування файлів системи [3].

На основі аналізу існуючих технологій безпеки можна вивести переваги та недоліки впровадження ML-систем в архітектуру клієнт-серверних додатків.

Ключовими елементами системи є:

1. Евристичний та поведінковий серверний аналіз.

– *Переваги:* неможливість обійти захист шляхом простого приховування коду на комп'ютері клієнта; збереження конфіденційності користувачів, оскільки система не сканує особисті файли на жорсткому диску [1; 5].

– *Недоліки:* потреба у величезних серверних потужностях для обробки даних у реальному часі (частота оновлення ігрового світу може складати 64 і більше разів на секунду) [2; 5].

2. Використання машинного навчання для виявлення аномалій введення.

– *Переваги:* висока точність виявлення (методи Support Vector Machines та Naive Bayes можуть показувати точність до 97,4 % у тестових середовищах); адаптивність до нових, ще невідомих типів шахрайського ПЗ (Zero-day exploits) [4].

– *Недоліки:* ризик хибних спрацьовувань (False Positives) на професійних гравців, чиї рефлекси можуть нагадувати безпомилкову роботу алгоритму; необхідність постійного перенавчання моделей при зміні програмних механік [2].

Створення такої ешелонованої системи безпеки не лише захистить комерційні інтереси розробників, а й забезпечить чесний та прозорий змагальний процес [1; 5].

Отже, використання методів машинного навчання у сфері кібербезпеки відеоігор є критично необхідним етапом еволюції систем захисту. З урахуванням того, що індустрія розробки нелегального ПЗ стає все більш прибутковою та технологічною, класичні методи захисту поступово втрачають свою актуальність. Технології ШІ відкривають надійний шлях до створення стійкого та безпечного віртуального простору.

Список використаних джерел:

1. Dunham H. Cheat Detection using Machine Learning within Counter-Strike: Global Offensive. *Senior Independent Study Theses*. Paper 8948. 2020. URL: https://openworks.wooster.edu/independentstudy/8948/ (дата звернення: 07.03.2026).
2. Loo M. M. Z., Lužkov G., Burelli P. AntiCheatPT: A Transformer-Based Approach to Cheat Detection in Competitive Computer Games. *arXiv preprint.* 2025. URL: https://arxiv.org/html/2508.06348v1 (дата звернення: 07.03.2026).
3. Deep Learning and Multivariate Time Series for Cheat Detection in Video Games. *IEEE Xplore*. 2021. URL: https://ieeexplore.ieee.org/abstract/document/9564219 (дата звернення: 07.03.2026).
4. The Utilization of Machine Learning for Cheating Detection in FPS Games. *ResearchGate*. 2026. URL: https://www.researchgate.net/publication/398846814_The_Utilization_of_Machine_Learning_for_Cheating_Detection_in_FPS_Games (дата звернення: 07.03.2026).
5. Behavioral-based cheating detection in online first person shooters using machine learning techniques. *Academia*. 2025. URL: https://www.academia.edu/91290136/Behavioral_based_cheating_detection_in_online_first_person_shooters_using_machine_learning_techniques (дата звернення: 07.03.2026).

УДК 336.221:330.131.7:519.2

Волошинюк Софія,
студентка І курсу спеціальності
071 «Облік і оподаткування»,
ЗВО «Івано-Франківський національний
технічний університет нафти і газу»
***Науковий керівник*:**
Витвицька Оксана,
доцент кафедри фізико-математичних наук,
кандидат економічних наук, доцент,
ЗВО «Івано-Франківський національний
технічний університет нафти і газу»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0002-8722-5450

ЗАСТОСУВАННЯ ТЕОРІЇ ЙМОВІРНОСТЕЙ ДО ОЦІНКИ ПОДАТКОВИХ РИЗИКІВ

У сучасних економічних умовах, зокрема в умовах війни в Україні, дослідження податкових ризиків набуває особливої ваги через зростання складності податкових систем, часті зміни законодавства та посилення глобалізаційних процесів. Підприємства функціонують у середовищі високої невизначеності, що додатково посилюється воєнними викликами, порушенням логістичних ланцюгів, змінами у фіскальній політиці та нестабільністю економічного середовища, де ризики можуть виникати як через помилки у податковому обліку, так і через неоднозначність трактування норм права. Це може призводити до фінансових втрат, штрафних санкцій і репутаційних ризиків. Водночас для держави податкові ризики пов'язані з недоотриманням бюджетних надходжень, що впливає на фінансову стабільність та ефективність реалізації соціально-економічної політики. Тому ідентифікація, оцінка та мінімізація податкових ризиків є важливою складовою як корпоративного управління, так і державного регулювання.

Застосування методів математичної статистики, економетрики, теорії ймовірностей і оптимізації дозволяє здійснювати кількісну оцінку податкових ризиків, виявляти закономірності ухилення від оподаткування та формувати ризик-орієнтовані підходи до відбору платників для перевірок. Зокрема, теорія ймовірностей виступає фундаментальним інструментом кількісної оцінки податкових ризиків, оскільки дозволяє працювати з невизначеністю, моделювати випадкові події та визначати ймовірність їх настання.

Податковий ризик – це ймовірність виникнення фінансових, правових або репутаційних втрат у платника податків чи держави внаслідок невизначеності, помилок або свідомих порушень у сфері оподаткування [1, с. 15]. Для підприємства податковий ризик проявляється у можливості донарахування податків, штрафів і пені через неправильне тлумачення законодавства, помилки в обліку або зміну позиції контролюючих органів. Для держави податковий ризик означає недоотримання доходів бюджету через ухилення від сплати податків, тіньову економіку або недосконалість механізмів адміністрування. У широкому розумінні податковий ризик можна розглядати як економічну категорію, що характеризує ступінь невизначеності результатів податкових відносин і можливість відхилення фактичних показників від запланованих. Він має ймовірнісний характер і піддається кількісній оцінці за допомогою математичних методів, що дозволяє використовувати його як інструмент аналізу, прогнозування та прийняття управлінських рішень у системі податкового контролю.

Нижче розглянемо деякі моделі оцінки податкового ризику.

1. Для кількісної оцінки ризику застосовується *модель очікуваної втрати,* яка дозволяє порівнювати сценарії та визначати зони підвищеної уваги [2, с. 33]:

$$E(L) = pC,$$

де p – ймовірність настання ризикової події, C – величина можливих фінансових втрат.

2. *Модель умовної ймовірності податкового порушення* дає можливість уточнювати оцінку податкових ризиків з урахуванням нових даних [3, с. 127]. При оновленні інформації про поведінку платника або зміни у податковому середовищі ймовірність ризикової події коригується.

$$P(A/B) = \frac{P(B/A)P(A)}{P(B)},$$

де A – податкове порушення, B – наявність індикатора ризику (наприклад, різке падіння прибутку).

3. *Модель податкового ризику на основі логістичної регресії* застосовується для прогнозування ймовірності податкової перевірки залежно від ризикових індикаторів діяльності:

$$p = \frac{1}{1 + e^{-(\beta_0 + \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_k x_k}},$$

де $x_1, x_2, \ldots$ – фінансові показники, β_i – вагові коефіцієнти, p – прогноз ймовірності перевірки.

4. *Модель частоти податкових порушень (розподіл Пуассона)* застосовується, коли кількість порушень за певний період – випадкова величина [4]:

$$P(X = k) = \frac{\lambda^k e^{-\lambda}}{k!},$$

де X – кількість податкових порушень у звітному періоді, λ – середня кількість порушень.

Слід зазначити, що перелічені моделі мають обмеження, основними з яких є неповнота або викривлення даних, зміни законодавства та вплив людського фактора. Тому ймовірнісні підходи повинні поєднуватися з експертним аналізом.

Теорія ймовірностей є ефективним інструментом для оцінки податкових ризиків. Її застосування дозволяє підприємствам підвищувати прозорість, передбачуваність та обґрунтованість управлінських рішень у сфері оподаткування.

Список використаних джерел:

1. Світовий О., Подзігун С. Податковий ризик у системі управлінських рішень. *Економічні горизонти*. 2025. № 4 (33). С. 15–22. DOI: https://doi.org/10.31499/2616-52-36.4(33).2025.341143

2. Кучеренко С. М. Проблематика оцінки податкових ризиків суб'єктів господарювання. *Український економічний часопис*. 2024. № 6. С. 31–38. DOI: https://doi.org/10.32782/2786-8273/2024-6-5

3. Таращенко В. А. Теоретико-методичні підходи до сутності податкових ризиків та їх класифікації. *Український економічний часопис*. 2024. № 5. С. 125–128. DOI: https://doi.org/10.32782/2786-8273/2024-5-22

4. Грищук Г. В., Пономаренко А. В., Почкай К. М. Ризик-орієнтована модель податкового контролю як інструмент забезпечення бюджетних надходжень. *Економіка та суспільство*. 2025. № 82. DOI: https://doi.org/10.32782/2524-0072/2025-82-9

УДК 159.91:159.93:794.8

Гойсан Юлія,
студентка І курсу спеціальності
«Інженерія програмного забезпечення»,
ЗВО «Університет Короля Данила»
Науковий керівник:
Іванов Олександр,
завідувач кафедри інформаційних технологій,
доктор філософії,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0003-4678-7956

АНАЛІЗ ПСИХОЕМОЦІЙНОГО СТАНУ ТА КОГНІТИВНОЇ ПРОДУКТИВНОСТІ ПІД ЧАС 24-ГОДИННОЇ ІГРОВОЇ СЕСІЇ (НА ПРИКЛАДІ ДИСЦИПЛІНИ VALORANT)

Дослідження динаміки психофізіологічних показників, когнітивної стійкості та сенсомоторної координації в умовах повної 24-годинної депривації сну на прикладі ігрової дисципліни Valorant дозволяє простежити критичні зміни в роботі людського організму під екстремальним ментальним навантаженням. Експеримент розпочався о 10:00 першої доби в умовах ідеального функціонального гомеостазу. На початковому етапі суб'єктивні показники енергії та внутрішнього спокою фіксувалися на рівні 10/10 та 9/10 відповідно, що свідчить про наявність повного нейромедіаторного ресурсу. У цей період когнітивні функції, зокрема вибіркова увага та швидкість обробки візуальної інформації, функціонували на піку можливостей. Стан «радості», зафіксований на старті, вказує на високу дофамінову активність, яка сприяє швидкому засвоєнню ігрових патернів та ефективній комунікації. Сенсомоторна система в перші години демонструвала зразкову стабільність: швидкість нейронного відгуку на появу візуального подразника (реакція) та точність мікромоторних рухів (аїм) перебували в стані повної синергії, що дозволяло демонструвати результативність, яка перевищує середні показники гравця.

Протягом наступних десяти годин безперервної ігрової діяльності (до 19:10–20:00) спостерігався поступовий перехід від стадії компенсації до стадії субкомпенсації. Хоча суб'єктивна оцінка технічних навичок залишалася високою, в емоційній сфері почали проявлятися перші ознаки дестабілізації. Трансформація базової радості в «агресивну радість» та зростання рівня агресії до 5/10 свідчать про те, що префронтальна кора

головного мозку, відповідальна за виконавчий контроль, почала відчувати дефіцит енергетичних ресурсів. Це призвело до зниження порогу роздратування та появи «тильту» – стану ігрової дезорієнтації, викликаного негативними емоціями.

Соціальна стимуляція, зумовлена грою в команді з друзями, на цьому етапі виступала ключовим зовнішнім чинником, який дозволяв штучно підтримувати рівень неспання шляхом активації симпатоадреналової системи. Показник енергії на рівні 9/10 у цей час був наслідком не реального відновлення сил, а мобілізації внутрішніх резервів організму, що неминуче веде до глибшого виснаження в наступні години.

Входження в нічну фазу після 00:00 супроводжувалося деградацією основних когнітивних функцій та розпадом цілісної структури ігрової діяльності. Станом на 01:00 було зафіксовано вкрай низький рівень енергії та зміну цільової установки: на зміну прагненню до перемоги прийшло інертне бажання підтримувати процес заради виконання умов челенджу.

Психоемоційний стан характеризувався глибокою апатією та нівелюванням значущості ігрових подій. На цьому етапі було виявлено унікальний нейрофізіологічний феномен: критичне уповільнення реакції при збереженні високої якості механічного «аїму». Це пояснюється тим, що автоматизовані навички, які базуються на діяльності базальних гангліїв та мозочка, виявилися значно стійкішими до депривації сну, ніж функції вищого порядку, такі як оперативне прийняття рішень та швидке сканування візуального поля. Гравець продовжував демонструвати точність стрільби в статичних ситуаціях, проте виявлявся повністю недієздатним у динамічних сценаріях, де вимагалася миттєва когнітивна гнучкість.

Період з 01:00 до 05:00 ранку став фазою максимального пригнічення ЦНС. Стан піддослідної описувався як «ужасний» через тотальну відсутність мотивації та енергії. В цей час агресія впала до мінімальних значень, що свідчить про перехід організму в режим максимального енергозбереження, де навіть емоційна відповідь на невдачі стає занадто енерговитратною. Соціальна комунікація стала фрагментарною, а ігрова поведінка – стереотипною.

Проте близько 05:00 ранку почалося поступове «пробудження», ініційоване циркадними ритмами. Зміна рівня освітленості та природні біологічні цикли активували викид кортизолу, що дозволило гравцеві дещо стабілізувати гру. Хоча продуктивність не повернулася до денних показників, суб’єктивне відчуття контролю над ситуацією зросло, що дозволило продовжувати сесію в режимі помірної ефективності.

Ранок другої доби (08:00 – 10:00) продемонстрував складну динаміку взаємодії фізіологічних стимулів та накопиченої втоми. Сніданок о

08:00 забезпечив мозок необхідною глюкозою, що на короткий час покращило якість «аїму» та частково компенсувало дефіцит реакції. Проте цей підйом мав ілюзорний характер, оскільки загальний нейрохімічний фон залишався критично низьким. Останні дві години експерименту проходили в стані стабільно важкої втоми. Настрій не зазнавав значних коливань, оскільки емоційна система перебувала в стані глибокого вигорання. Домінувала лише вольова установка дограти до встановленої позначки 10:00. Будь-які ігрові помилки в цей період сприймалися з апатичним смиренням, а агресія з'являлася лише епізодично як реакція на подразники, що заважали завершенню дистанції.

Підсумовуючи результати експерименту, необхідно зазначити, що тривала депривація сну веде до нерівномірного розпаду компетенцій. Найбільш вразливою ланкою виявилася психоемоційна сфера, яка першою продемонструвала ознаки декомпенсації через агресію та тильт. Другою ланкою стала швидкість когнітивного реагування, яка в нічний час «храмала», створюючи розрив між виникненням загрози в грі та фізичною відповіддю на неї. Найбільш резистентним елементом виявився аїм – результат багаторічних тренувань та м'язової пам'яті, який залишався на задовільному рівні навіть у моменти глибокої апатії. Проте, незважаючи на збереження технічної точності, загальна ігрова результативність суттєво впала через нездатність мозку швидко аналізувати контекст ігрової ситуації. Даний досвід підтверджує, що для підтримки високої продуктивності в тактичних шутерах критично важливим є не лише збереження механічних навичок, а й підтримання нейродинамічного балансу, який неможливий без регулярного сну.

Кінцевий стан піддослідної о 10:00 другої доби характеризувався повною вичерпаністю адаптаційних резервів. Незважаючи на ранковий підйом настрою та успішне завершення челенджу, когнітивні показники реакції залишалися на рівні 5/10, що вказує на неможливість повноцінного відновлення функцій без фази глибокого сну. Експеримент наочно продемонстрував стадії деградації особистості під час ігрового марафону: від активного творчого залучення через агресивну боротьбу з утомою до механічної апатії та фінального смирення з обмеженими можливостями власного організму. Таким чином, успішне завершення 24-годинної ігрової сесії є перемогою вольового ресурсу над біологічними обмеженнями, проте ціною цього є тимчасова втрата здатності до ефективного навчання та стратегічного планування.

Список використаних джерел:

1. The impact of sleep deprivation on first-person shooter performance. *PubMed*. URL: https://pubmed.ncbi.nlm.nih.gov/30900281/ (дата звернення: 23.03.2026).
2. Walker M. The Emotional Brain without Sleep. *National Center for Biotechnology Information*. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2735112/ (дата звернення: 23.03.2026).
3. Sleep deprivation: Impact on cognitive performance. *National Center for Biotechnology Information*. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2656292/ (дата звернення: 23.03.2026).
4. Circadian Rhythms and Sleep. *Harvard Medical School*. URL: https://archive.org/details/stabilityprecisi0000czei (дата звернення: 23.03.2026).
5. Sleep in Elite eSports: Prevalence and Performance. *Frontiers in Psychology*. URL: https://www.frontiersin.org/articles/10.3389/fpsyg.2020.575309/full (дата звернення: 23.03.2026).

УДК 378.147:004:51

Гуляк Олександра,
викладач кафедри інформаційних технологій,
спеціаліст вищої категорії,
Фаховий коледж ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0009-0002-5779-9178

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ПІДГОТОВКИ ВИКЛАДАЧА З МАТЕМАТИКИ ДО ЗАНЯТТЯ

Сучасна цифрова трансформація освіти вимагає від викладачів математики нових компетентностей, де штучний інтелект (ШІ) стає потужним інструментом для оптимізації підготовки викладачів математики до занять, дозволяючи автоматизувати планування, генерацію завдань та персоналізацію контенту.

Українські дослідники визначають ШІ як сукупність технологій для моделювання інтелектуальної поведінки, що застосовується в освіті для подання знань та логічного виведення. О. М. Спірін у своїх роботах описує методичну систему диференційованого навчання основ ШІ для вчителів математики та інформатики, включаючи поняття інтелектуальних систем, програмування ШІ та моделі подання знань (логічні моделі, семантичні мережі) [3]. Л. О. Черемісіна вказує на способи ШІ в навчанні математики: індивідуальне навчання, автоматизована перевірка та створення інтерактивних курсів. Ці підходи полегшують підготовку викладача, дозволяючи генерувати математичні моделі заздалегідь [4].

ШІ оптимізує етапи підготовки: аналіз теми, добір вправ, візуалізацію. Н. В. Кайдан та О. В. Щенсневич у дослідженні 2020–2025 рр. демонструють, як адаптивні ШІ-системи персоналізують контент, знижують математичну тривогу учнів та підвищують мотивацію, рекомендуючи гібридні моделі «ШІ + викладач» для математики [2]. Наприклад, інструменти на кшталт MATLAB, GeoGebra, Wolfram Mathematica, Maple, проаналізовані І. А. Бубновською, покращують розв'язання задач, дозволяючи викладачу за хвилини створювати персоналізовані тести [1]. Спірін та Олексюк наголошують на курсах з ШІ для вчителів, де вивчаються експертні системи для генерації завдань з алгебри чи геометрії [3].

Серед ризиків – втрата критичного мислення та «чорні скриньки» алгоритмів, як зазначають Кайдан і Щенсневич, пропонуючи пояснюваний алгоритм ШІ та розвиток емоційних компетенцій викладача [2]. Спірін рекомендує етичні стандарти та підготовку до обробки даних у ШІ для уникнення упереджень у математичних моделях. Вітчизняний досвід передбачає модульні курси для викладачів математики з фокусом на практичні інструменти.

У висновку потрібно сказати, що ШІ трансформує підготовку викладача математики, роблячи її ефективнішою через персоналізацію та автоматизацію, як доводять праці Спіріна, Кайдан та інших. Необхідно впроваджувати гібридні моделі та професійний розвиток педагогів для максимальної користі.

Список використаних джерел:

1. Бубновська І. А. Інтеграція інформаційних технологій у викладанні вищої математики. *Перспективи та інновації науки*. 2025. № 1 (47). С. 294–306. URL: https://socrates.vsau.org/repository/getfile.php/38814.pdf (дата звернення: 12.03.2026).

2. Кайдан Н. В., Щенсневич О. В. Штучний інтелект у викладанні математичних дисциплін. *Збірник наукових праць фізико-математичного факультету ДДПУ*. 2025. № 15. С. 84–89. URL: https://znpfizmat.ddpu.edu.ua/article/view/338348 (дата звернення: 11.03.2026).

3. Спірін О. М., Олексюк В. П. Досвід та перспективи використання технологій штучного інтелекту у навчанні майбутніх учителів інформатики. *Теорія і практика використання інформаційних технологій в умовах цифрової трансформації освіти* : матеріали Всеукр. науково-практ. конф., м. Київ, 29 черв. 2023 р. Київ, 2023. С. 63–67. URL: https://conf-itp.udu.edu.ua/ (дата звернення: 10.03.2026).

4. Черемісіна Л. О. Актуальність вивчення основ штучного інтелекту на інформатичних спеціальностях педагогічних університетів. *Науковий часопис Національного педагогічного університету імені М. П. Драгоманова*. Серія 2: Комп'ютерно-орієнтовані системи навчання : зб. наук. праць. 2012. Вип. 12 (19). 253 с. URL: https://chasopys.ps.npu.kiev.ua/archive/99/3.pdf (дата звернення: 10.03.2026).

УДК 004.89

Дарвай Олеся,
студентка IV курсу спеціальності
121 Інженерія програмного забезпечення,
ЗВО «Університет Короля Данила»
Науковий керівник:
Стисло Тарас,
кандидат юридичних наук, доцент кафедри IT,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0002-2377-7985

ЗАСТОСУВАННЯ RAG-АРХІТЕКТУРИ ДЛЯ ПОДОЛАННЯ ОБМЕЖЕНЬ LLM

Уявіть, що ви запитуєте досвідченого консультанта про внутрішні регламенти вашої компанії, і він впевнено відповідає, але посилається на правила, яких ніколи не існувало. Саме так поводяться великі мовні моделі (LLM), коли стикаються з питаннями поза межами своїх навчальних даних: вони генерують правдоподібно сформульовану, проте хибну інформацію. Таке явище відоме як «галюцинації». До цього додаються ще два обмеження: знання моделі зафіксовані на момент навчання і не оновлюються, а доступу до приватних або корпоративних документів у неї немає взагалі. Саме ці виклики зумовили появу та стрімке поширення архітектури Retrieval-Augmented Generation (RAG). RAG був розроблений дослідниками штучного інтелекту Facebook на чолі з Патріком Льюїсом у 2020 році для подолання обмежень стандартних генеративних моделей [1].

Метою цієї роботи є аналіз принципів функціонування архітектури Retrieval-Augmented Generation (RAG), її ролі у зменшенні галюцинацій мовних моделей та можливостей використання для побудови AI-систем, що працюють з приватними або корпоративними даними.

Робота RAG-системи розпочинається з етапу індексації – підготовки бази знань, до якої система звертатиметься під час відповідей. Спочатку вхідні документи (PDF, Word, txt) розбиваються на невеликі текстові фрагменти – chunks. Це не просте механічне нарізання, якісні реалізації застосовують семантичне розбиття, що враховує структуру тексту: заголовки, абзаци, логічні блоки, щоб кожен фрагмент містив завершену думку. Типовий розмір фрагмента становить 300-1000 токенів із перекриттям 100-200 токенів між сусідніми фрагментами, щоб думки на межах не розривалися.

Далі кожен фрагмент передається у модель ембедінгів – спеціальну нейромережу, що перетворює текст на числовий вектор у багатовимірному просторі. Ключова властивість такого перетворення полягає в тому, що семантично близькі тексти отримують близькі вектори. Наприклад, фрази «серцевий напад» та «інфаркт міокарда» опиняться поруч у цьому просторі, навіть якщо не мають жодного спільного слова. Отримані вектори разом із оригінальним текстом та метаданими (назва документа, номер сторінки, розділ) зберігаються у векторній базі даних – спеціалізованому сховищі, оптимізованому для пошуку за подібністю [2].

Коли користувач надсилає запит, система виконує два кроки:

1. Retrieval (пошук): запит так само перетворюється на вектор за допомогою тієї самої моделі ембедінгів, після чого векторна база знаходить N фрагментів із найвищою косинусною подібністю до запиту. Косинусна подібність вимірює кут між двома векторами: чим менший кут, тим ближчі тексти за змістом незалежно від конкретних слів. Результатом пошуку є набір релевантних фрагментів, так званий контекст.

2. Generation (генерації): мовна модель отримує спеціально сформований промпт, що містить одночасно оригінальний запит користувача та знайдені фрагменти. Модель навчається відповідати виключно на основі наданого контексту, а не покладатися на власну пам'ять. Завдяки цьому відповідь прив'язана до конкретних документів, а система може повернути посилання на джерело і користувач бачить, з якого саме фрагмента взята інформація. Такий підхід принципово відрізняє RAG від «чорного ящика» класичного LLM [2].

Архітектура RAG вже сьогодні лежить в основі численних комерційних продуктів. Microsoft Copilot використовує її для роботи з корпоративними документами у Microsoft 365: перш ніж відповісти, система індексує листи, файли та нотатки конкретної організації [3]. Google NotebookLM дозволяє завантажити власні матеріали та отримувати відповіді виключно на їх основі. Це приклад типового RAG для персональної бази знань (Рис. 1).

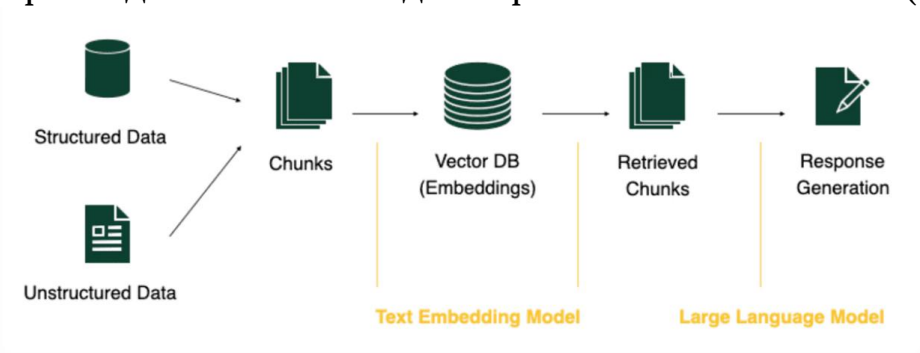

Рис. 1. Архітектура Retrieval-Augmented Generation

Особливої актуальності RAG набуває в контексті розвитку AI-агентів – це системи, що самостійно виконують багатокрокові задачі. Якщо класичний LLM є пасивним відповідачем на запити, то агент активно планує дії, використовує інструменти та приймає рішення. У такій архітектурі RAG виконує роль довгострокової пам'яті агента. Замість того, щоб тримати весь контекст у вікні токенів, агент звертається до векторної бази лише за потрібною інформацією у потрібний момент. Це вирішує одне з ключових обмежень агентних систем, а саме неможливість ефективно працювати з великими обсягами контексту. Розвиток підходів Agentic RAG (де агент сам формулює пошукові запити та ітеративно уточнює їх) та GraphRAG (пошук по графу знань для складних багатокрокових міркувань) свідчить про те, що RAG еволюціонує разом із агентними системами і залишатиметься їхнім ключовим компонентом [4; 5].

Попри широке застосування, RAG не є універсальним рішенням. Якість пошуку суттєво залежить від того, як розбито документ на фрагменти: якщо межі розбиття «розрізають» важливу думку, модель отримує неповний контекст. Відповіді на питання, що потребують синтезу інформації з багатьох різних частин документа, все ще є складним завданням для більшості RAG-систем. Додатковий етап пошуку збільшує час відповіді порівняно з прямим викликом моделі.

Практична значущість підходу RAG полягає у можливості інтеграції великих мовних моделей із корпоративними базами знань, що дозволяє створювати інтелектуальні системи підтримки прийняття рішень, AI-асистентів та аналітичні інструменти, які працюють з актуальними і верифікованими даними організації.

Таким чином, архітектура RAG є ключовим механізмом інтеграції LLM із зовнішніми джерелами знань, що суттєво підвищує точність та інтерпретованість AI-систем. Технологія долає розрив між генеративною потужністю моделей та вимогами щодо верифікації інформації. З розвитком агентних систем і зростанням потреби в роботі з приватними даними роль RAG-архітектури стає фундаментальною для створення надійних інструментів, адаптованих до конкретних прикладних задач.

Список використаних джерел:

1. Retrieval Augmented Generation (RAG): All You Need To Know. *Voiceflow*. URL: https://www.voiceflow.com/blog/retrieval-augmented-generation

2. Chuciche. Understanding the Entire Process of Retrieval-Augmented Generation (RAG). *Medium*. 2023. URL: https://medium.com/@chuciche/understanding-the-entire-process-of-retrieval-augmented-generation-rag-0d15a7f75b68

3. RAG and generative AI - Azure AI Search. *Microsoft Learn: Build skills that open doors in your career*. URL: https://learn.microsoft.com/en-us/azure/search/retrieval-augmented-generation-overview?tabs=videos

4. Kumar M. RAG vs. Agentic RAG: The Evolution of Intelligent Retrieval Systems. *LinkedIn.* URL: https://www.linkedin.com/pulse/rag-vs-agentic-evolution-intelligent-retrieval-systems-maneesh-kumar-k5v2c/

5. From Local to Global: A Graph RAG Approach to Query-Focused Summarization. *arXiv.org.* URL: https://arxiv.org/abs/2404.16130

УДК 004.5

Демчина Микола,
доцент кафедри інформаційних технологій,
кандидат технічних наук,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0009-0002-9161-4843

ПАРАЛЕЛІЗАЦІЯ ОБЧИСЛЕНЬ У АГЕНТНИХ СИСТЕМАХ НА ОСНОВІ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ

Часто продуктивність сучасних агентних систем на основі великих мовних моделей (LLM) значною мірою обмежується їхнім послідовним характером обробки завдань. Спочатку інтелектуальний агент аналізує запит, далі використовує у своїй роботі певне джерело або інструмент, очікує на відповідь, робить проміжний висновок і лише після цього переходить до наступного кроку. Такий підхід забезпечує хорошу керованість і відтворюваність, але призводить до накопичення затримок та різко знижує швидкодію під час виконання завдань, що складаються з окремих незалежних кроків [1].

Проте під час виконання завдань, пов’язаних із зовнішніми ресурсами (вебпошук, запити до баз даних, виклик сторонніх API-сервісів), значна частина часу витрачається на очікування відповіді, а сумарний час відповіді обчислюється як сума затримок на кожному із кроків виконання. Це призводить до виникнення так званого “sequential bottleneck”. Навіть за умови ефективного процесу міркування інтелектуального агента загальна продуктивність цілісної системи може сприйматися як недостатня, якщо виконання незалежних перевірок або підзадач відбувається послідовно, тобто кожна наступна операція розпочинається лише після завершення попередньої. Такий підхід призводить до накопичення затримок і зниження ефективності використання обчислювальних ресурсів [1].

У зв’язку з цим у сучасних підходах до проєктування хмарних та агентних систем особлива увага приділяється застосуванню паралельної обробки завдань. Зокрема, вона є доцільною для вирішення задач, що передбачають оцінювання кількох альтернативних варіантів відповіді, аналізу великої кількості документів або отримання різних спеціалізованих

інтерпретацій однієї й тієї ж самої проблеми. Використання паралельних механізмів обробки на рівні інтелектуальних агентів дозволяє суттєво скоротити час, необхідний на виконання окремих завдань, та підвищити загальну ефективність інтелектуальних систем.

Одним із можливих рішень цієї проблеми є використання під час роботи інтелектуальних агентів таких шаблонів паралелізації, як “concurrent orchestration”, “fan-out/fan-in” та “scatter-gather”. Вони забезпечують механізми декомпозиції задачі на незалежні підзадачі, паралельний запуск виконання окремих завдань та агрегацію результатів у цілісну відповідь. Використання такої архітектурної схеми передбачає, що декілька інтелектуальних агентів виконуються одночасно, формуючи незалежні проміжні результати. Надалі ці результати можуть бути агреговані або узагальнені з метою отримання фінального рішення чи узгодженого висновку.

Ідея про те, що загальний час виконання окремого завдання визначається часом виконання його найдовшого підзавдання, інтуїтивно відображає концепцію критичного шляху у паралельних робочих процесах. Якщо підзадачі є незалежними, затримка отримання кінцевого результату наближається до максимальної тривалості окремих підзадач із додаванням накладних витрат, пов’язаних із координацією виконання та подальшим синтезом результатів. Це обмеження було продемонстровано у роботі Джина Амдала (Gene M. Amdahl) [2]. Внаслідок нього навіть за значного збільшення кількості агентів (виконавців) потенційне прискорення системи обмежується часткою операцій, що принципово не піддаються паралелізації.

Подальші інтерпретації закону Амдала в епоху багатоядерних обчислювальних систем дозволили виділити дві важливі закономірності в роботі агентів. По-перше, чинники, які часто залишаються поза увагою на початкових етапах проєктування, такі як послідовні фази виконання, накладні витрати та механізми координації, зі зростанням рівня паралелізму можуть набувати домінуючого впливу на продуктивність системи в цілому. По-друге, оптимізація послідовної частини обчислювального процесу в окремих випадках може мати стратегічно важливіше значення, ніж просте збільшення кількості паралельних виконавців [2]. Подібна закономірність спостерігається і в інтелектуальних агентних системах, у яких процедура синтезу результатів роботи, що включає агрегацію, перевірку коректності та узгодження суперечливих відповідей, може перетворюватися на окремий вузол критичного шляху виконання.

Таким чином, паралелізація завдань не може розглядатися як безумовне джерело підвищення швидкодії системи в цілому. Її застосування

фактично призводить до перерозподілу часових витрат. Замість очікування результатів послідовного виконання зовнішніх викликів значна частина часу та ресурсів витрачається на вирішення завдань координації, агрегації результатів та контролю їхньої якості. Найбільша ефективність від паралельного виконання досягається у випадку виконання незалежних підзадач, які мають зазвичай I/O-орієнтований характер, оскільки їх паралельний запуск дозволяє мінімізувати простої, пов'язані з очікуванням завершення операцій введення-виведення.

Під час проєктування інтелектуальних агентів перехід від послідовної до паралельної моделі виконання завдань часто реалізується за допомогою подієво-орієнтованого підходу на основі шаблону "scatter-gather". У межах цього підходу координатор здійснює розподіл підзадач між паралельними виконавцями (scatter), після чого отримані результати збираються (gather) для подальшої обробки. На етапі інтеграції результатів виконання можуть застосовуватися різні стратегії, зокрема об'єднання отриманих відповідей, їх порівняння або вибір оптимального результату. Важливо зазначити, що "scatter-gather" є передусім координаційним шаблоном організації обчислювального процесу. Він передбачає очікування результатів від кількох паралельних гілок виконання та подальшу їх агрегацію з метою формування узгодженого рішення.

Зокрема, платформа Amazon Web Services у своїх рекомендаціях щодо застосування шаблонів agentic AI описує підхід на основі "scatter-gather" як механізм паралельної обробки множини підзадач із подальшим агрегуванням отриманих результатів у консолідоване рішення. У відповідних рекомендаціях від Amazon також наведено приклади практичної реалізації такого підходу із використанням керованих сервісів паралельного виконання та механізмів кореляції результатів виконання [3].

Якщо розглядати платформу OpenAI, то тут паралелізація реалізується на двох основних рівнях. По-перше, вона може проявлятися у вигляді паралельних викликів для інструментів або функцій (tool/function calling) у межах одного агента. По-друге, застосовується підхід на основі створення спеціалізованих агентів, результати роботи яких надалі інтегруються метаагентом у межах схеми "fan-out/fan-in" [4].

Проте використання паралельних механізмів виконання істотно змінює вимоги до інженерії агентних систем. На передній план виходять питання ефективної декомпозиції завдань, узгодженої роботи зі станом системи, проєктування механізмів агрегації результатів, а також забезпечення належного рівня спостережуваності процесу виконання.

Як перспективний напрям розвитку агентних систем, паралельна оркестрація окремих агентів природним чином призводить до формування архітектур, у яких взаємодіють цілі команди агентів, що виконують різні ролі та використовують спеціалізовані механізми узгодження. У межах такої парадигми питання про те, яким чином агенти можуть ефективно співпрацювати паралельно не лише в межах одного робочого процесу, а й між кількома взаємопов'язаними робочими процесами, трансформується у самостійну дослідницьку проблему.

Зокрема, актуальними стають питання масштабування механізмів координації інтелектуальних агентів, забезпечення узгодженості результатів їх роботи та керування зростаючою складністю системи таким чином, щоб підвищення швидкодії не супроводжувалося зниженням рівня керованості та якості отримуваних результатів.

Як підсумок, паралелізація не може розглядатися лише як окремий прийом оптимізації на рівні окремих інтелектуальних агентів, а виступає фундаментальним структурним принципом проєктування агентних систем в цілому. Її застосування передбачає стратегічне визначення тих етапів обчислювального процесу, де послідовне виконання є достатнім, а також тих, де доцільною є паралельна оркестрація підзадач. Водночас ефективне використання паралелізації потребує чітко визначених інженерних підходів до декомпозиції завдань і подальшої агрегації результатів, що дозволяє забезпечити керованість, надійність та передбачуваність отримуваного прискорення в роботі інтелектуальних агентів.

Список використаних джерел:

1. Workflow for parallelization. *AWS Prescriptive Guidance*. URL: https://docs.aws.amazon.com/prescriptive-guidance/latest/agentic-ai-patterns/workflow-for-parallelization.html (дата звернення: 13.03.2026).

2. Hill M. D., Marty M. R. Amdahl's Law in the multicore era. *IEEE Computer*. URL: https://research.cs.wisc.edu/multifacet/papers/ieeecomputer08_amdahl_multicore.pdf (дата звернення: 13.03.2026).

3. Parallelization and scatter-gather patterns. *AWS Prescriptive Guidance*. URL: https://docs.aws.amazon.com/prescriptive-guidance/latest/agentic-ai-patterns/parallelization-and-scatter-gather-patterns.html (дата звернення: 13.03.2026).

4. Function calling. *OpenAI API Documentation*. URL: https://developers.openai.com/api/docs/guides/function-calling/ (дата звернення: 13.03.2026).

УДК 37:004.8

Дзюба Марина,
доцентка кафедри інформаційних технологій,
кандидатка фізико-математичних наук,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0003-2579-9157

ПРАКТИЧНЕ ВИКОРИСТАННЯ СЕРВІСІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ СТВОРЕННЯ НАВЧАЛЬНИХ МАТЕРІАЛІВ З МАТЕМАТИКИ В ОСВІТНЬОМУ ПРОЦЕСІ

Сучасний розвиток інформаційних технологій суттєво впливає на трансформацію освітнього середовища та підходів до організації навчального процесу. Одним із ключових напрямів цифровізації освіти є використання технологій штучного інтелекту, які відкривають нові можливості для підготовки, організації та підтримки навчальної діяльності. У контексті викладання математичних дисциплін застосування сервісів штучного інтелекту набуває особливої актуальності, оскільки створення навчальних матеріалів з математики потребує значних часових витрат, високого рівня методичної підготовки викладача та систематичного оновлення дидактичних ресурсів. Використання інтелектуальних цифрових сервісів дозволяє оптимізувати процес підготовки навчального контенту, розширити спектр дидактичних матеріалів та підвищити ефективність навчання.

Штучний інтелект у сфері освіти розглядається як сукупність алгоритмів і програмних систем, здатних виконувати завдання, які традиційно потребують людського інтелекту, зокрема аналіз інформації, генерацію текстів, розпізнавання образів, обробку природної мови та моделювання навчальних ситуацій. Завдяки розвитку генеративних моделей і технологій обробки природної мови з'явилася можливість автоматизувати значну частину процесів, пов'язаних зі створенням освітніх матеріалів. Такі сервіси можуть генерувати текстові пояснення математичних понять, формувати приклади розв'язування задач, створювати тестові завдання, презентаційні матеріали, методичні рекомендації та інші дидактичні ресурси. Використання подібних інструментів сприяє підвищенню продуктивності роботи викладача та дозволяє зосередити більше уваги на організації навчальної діяльності студентів [1; 2].

Практичне застосування сервісів штучного інтелекту у викладанні математики може реалізовуватися у різних напрямах. Одним із найбільш

поширених є автоматизоване створення навчального контенту. За допомогою сучасних інтелектуальних систем викладач може швидко генерувати пояснення теоретичного матеріалу, формувати конспекти лекцій, створювати структуровані навчальні тексти, а також підбирати приклади для ілюстрації математичних понять і методів розв'язування задач. Такий підхід дозволяє адаптувати навчальний матеріал до різних рівнів підготовки здобувачів освіти, змінювати ступінь складності задач та формувати альтернативні варіанти завдань для самостійної роботи або контролю знань [3; 4].

Важливим напрямом використання штучного інтелекту є також розроблення дидактичних завдань і тестових матеріалів. У процесі викладання математики значну роль відіграє система практичних вправ, яка сприяє закріпленню теоретичних знань та розвитку аналітичного мислення студентів. Інтелектуальні сервіси дозволяють автоматично генерувати різноманітні задачі, тести, контрольні роботи та тренувальні вправи з різних розділів математики [5; 6]. Крім того, такі системи можуть формувати покрокові алгоритми розв'язування задач, що допомагає студентам краще зрозуміти логіку математичних міркувань та послідовність виконання обчислень. Це особливо корисно у процесі організації самостійної роботи студентів, коли вони мають можливість отримати додаткові пояснення та приклади.

Суттєвим напрямом практичного використання сервісів штучного інтелекту є створення візуальних та інтерактивних навчальних матеріалів. Математика часто оперує абстрактними поняттями, які складно сприймаються без наочного представлення. Використання інтелектуальних інструментів дозволяє створювати графічні ілюстрації, моделі, схеми та інтерактивні демонстрації математичних об'єктів. Зокрема, можна генерувати графіки функцій, геометричні побудови, візуалізації статистичних даних та математичних залежностей. Такі матеріали сприяють кращому розумінню складних тем, підвищують інтерес студентів до навчання та роблять освітній процес більш наочним і доступним.

Ще одним перспективним напрямом є використання штучного інтелекту для створення інтерактивних освітніх ресурсів і цифрових навчальних середовищ. Сучасні інтелектуальні системи можуть інтегруватися з різними освітніми платформами, що дозволяє автоматизувати процес створення презентацій, електронних навчальних курсів, інтерактивних вправ та навчальних тестів. Викладач має можливість використовувати штучний інтелект для швидкого створення матеріалів для онлайн-занять,

дистанційного навчання або змішаних форм організації освітнього процесу. Це особливо актуально в умовах цифровізації освіти, коли значна частина навчальних матеріалів використовується в електронному форматі.

Використання сервісів штучного інтелекту також сприяє персоналізації навчання. Інтелектуальні системи можуть аналізувати результати виконання завдань, визначати типові помилки студентів та формувати рекомендації щодо подальшого навчання. Завдяки цьому викладач отримує можливість більш ефективно організовувати індивідуальну роботу зі студентами, а також адаптувати навчальні матеріали відповідно до їхнього рівня підготовки. Такий підхід дозволяє створити адаптивне освітнє середовище, яке враховує індивідуальні особливості студентів та сприяє більш ефективному засвоєнню математичних знань.

Крім того, сервіси штучного інтелекту можуть використовуватися для підтримки дослідницької та проєктної діяльності студентів. Зокрема, вони допомагають здійснювати аналіз математичних моделей, проводити обчислення, створювати графічні візуалізації результатів досліджень та формувати звіти або презентації. Така інтеграція сучасних цифрових інструментів у навчальний процес сприяє формуванню у студентів навичок роботи з інформаційними технологіями, розвитку критичного мислення та здатності застосовувати математичні знання у практичних ситуаціях.

Водночас використання технологій штучного інтелекту в освітньому процесі потребує відповідального та методично обґрунтованого підходу. Автоматично згенерований контент може містити неточності або методичні недоліки, тому важливо здійснювати перевірку та корекцію матеріалів перед їх використанням у навчальному процесі. Роль викладача залишається ключовою, оскільки саме він визначає педагогічну доцільність використання тих чи інших матеріалів, адаптує їх до конкретних освітніх цілей та забезпечує методичну правильність викладання математичного матеріалу.

Таким чином, використання сервісів штучного інтелекту для створення навчальних матеріалів з математики є важливим напрямом розвитку сучасної освіти. Інтелектуальні цифрові інструменти дозволяють оптимізувати процес підготовки дидактичних ресурсів, розширити можливості візуалізації математичних понять, створювати різноманітні навчальні завдання та забезпечувати індивідуалізацію навчання. Поєднання можливостей штучного інтелекту з педагогічною майстерністю викладача сприяє підвищенню якості освітнього процесу, розвитку математичної компетентності студентів та формуванню сучасного цифрового освітнього середовища.

Список використаних джерел:

1. Holmes W., Bialik M., Fadel C. Artificial Intelligence in Education: Promises and Implications for Teaching and Learning. Boston : Center for Curriculum Redesign, 2019. 242 p.
2. Luckin R. Machine Learning and Human Intelligence: The Future of Education for the 21st Century. London : UCL Institute of Education Press, 2018. 256 p.
3. Zawacki-Richter O., Marín V., Bond M., Gouverneur F. Systematic review of research on artificial intelligence applications in higher education. *International Journal of Educational Technology in Higher Education.* 2019. Vol. 16. № 39.
4. Woolf B. Building Intelligent Interactive Tutors: Student-Centered Strategies for Revolutionizing E-Learning. Burlington : Morgan Kaufmann, 2020. 504 p.
5. Selwyn N. Should Robots Replace Teachers? *AI and the Future of Education.* Cambridge : Polity Press, 2019. 172 p.
6. Holmes W., Tuomi I. State of the Art and Practice in AI in Education. Luxembourg : Publications Office of the European Union, 2022. 140 p.

УДК 004.8:81’33

Дрогомирецький Роман,
студент ІІІ курсу спеціальності
121 Інженерія програмного забезпечення,
ЗВО «Університет Короля Данила»
Науковий керівник:
Куцела Марія,
старша викладачка кафедри іноземної
філології та бізнес-комунікацій,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0009-0002-1225-2988

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ АНГЛОМОВНИХ ТА УКРАЇНОМОВНИХ ПРОМПТІВ ДЛЯ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ

Сучасні великі мовні моделі є фундаментально англоцентричними. Через тотальне домінування англомовних текстів у навчальних масивах (corpus dominance) архітектура моделей та їхні словники оптимізовані саме під цю мову. Використання української мови у промптах для складних задач стикається з трьома об'єктивними перешкодами: низькою ефективністю токенізації, підвищеною обчислювальною вартістю та зниженням здатності до складного логічного виведення (reasoning).

Токенізація – це процес розбиття тексту на фрагменти (токени), якими оперує модель. Ефективність цього процесу вимірюється показником fertility (кількість токенів на одне слово).

Згідно з дослідженнями (зокрема, Maksymenko & Turuta, 2025), базові токенізатори (BPE, Tiktoken) для моделей рівня GPT-4 чи Mistral демонструють значну диспропорцію:

- Англійська мова: ~1.2 токена на слово.
- Українська мова: ~3.0-3.35 токена на слово (для кирилиці використовуються субаймвольні розбиття) [3, с. 373].

Це означає, що ідентичний за змістом запит українською мовою буде фізично довшим для сприйняття моделлю приблизно втричі.

Збільшення кількості токенів для української мови має прямий і дуже суттєвий вплив на ефективність. Механізм уваги (Self-Attention) в архітектурі Transformer має квадратичну залежність від довжини послідовності. Обчислювальна складність виражається формулою наведеному на рисунку 1, де N – кількість токенів (sequence length), а d – розмірність векторного представлення (embedding dimension) [2, с. 105-111].

$$\mathcal{O}(N^2 \cdot d)$$

Рис. 1. Формула складності обчислення

Оскільки український текст збільшує кількість токенів N у середньому в 3 рази (3N), обчислювальне навантаження на механізм уваги теоретично зростає у 9 разів ((3N)^2 = 9N^2). На практиці це призводить до трьох наслідків:

1. Здорожчання: при використанні API оплата здійснюється за токени. Промпт українською коштує у 2.5-3 рази дорожче, ніж його точний англомовний аналог.

2. Звуження контекстного вікна: якщо модель має ліміт пам'яті у 8000 токенів, англійською туди поміститься понад 6000 слів, а українською – лише близько 2400 слів. ШІ набагато швидше «забуває» початок довгої бесіди українською.

3. Збільшення затримки (Latency): генерація українського тексту відбувається повільніше, оскільки моделі потрібно згенерувати втричі більше токенів для висловлення тієї ж думки.

Емпіричні дані глобальних бенчмарків (наприклад, MMLU) та спеціалізованих локальних (ZNO-Eval 2024/2025) підтверджують, що мова промпту безпосередньо впливає на точність виконання задач [4], що наочно продемонстровано в таблиці 1.

Оскільки прихований семантичний простір (latent space) моделей сформований переважно англійською, при складному україномовному промпті модель часто здійснює неявний внутрішній переклад, вирішує логічну задачу, а потім «перекладає» результат назад. Цей додатковий

когнітивний крок збільшує відсоток помилок у задачах з програмування, математики або багатоступеневого аналізу [1, с. 402-408].

Таблиця 1

Залежність точності промптів від мови запиту

Критерій порівняння	**Англомовний промпт**	**Україномовний промпт**
Токенів на слово (Fertility)	~1.2	~3.0-3.35
Використання контекстного вікна	Максимально ефективне	Втрата ~65-70 % корисного об'єму
Логіка та математика	Найвища точність (еталон)	Зниження точності на 10-20 %
Ризик галюцинацій	Базовий	Підвищений

Спираючись на об'єктивні архітектурні дані, англомовні промпти є безальтернативно ефективнішим інструментом для програмування, глибокої аналітики, побудови складних логічних ланцюжків та економії бюджету при роботі через API. Україномовні промпти раціонально використовувати виключно для тих задач, де цільовим результатом є створення україномовного контенту (копірайтинг, переклад, локалізація, стилістична редакція), або для простих побутових запитів, що не вимагають глибокого логічного виведення та великого контекстного вікна.

Список використаних джерел:

1. Іосіфов Є. А., Соколов В. Ю. Методи аналізу природної мови та застосування нейронних мереж в кібербезпеці. *Кібербезпека: освіта, наука, техніка*. 2024. № 4 (24). С. 398–414.

2. Коваленко Н., Жорнокуй У. Сучасні підходи та технології створення тезаурусів української та англійської мови: компаративний аналіз. *Information Technology: Computer Science, Software Engineering and Cyber Security*. 2025. Вип. 1. С. 105–113.

3. Пасемко І. С., Федонюк Ю. А. Система автоматизованого аналізу природномовних текстів з використанням трансформерів. *Information Systems and Networks*. 2025. Вип. 17. С. 366–381.

4. Maksymenko D., Turuta O. Tokenization efficiency of current foundational large language models for the Ukrainian language. *Frontiers in Artificial Intelligence*. 2025. Vol. 8. P. 95-109.

УДК 316.346.32:303.6

Зінько Віра,
студентка ІІ курсу спеціальності «Менеджмент»,
ЗВО «Університет Короля Данила»
Науковий керівник:
Гавадзин Наталія,
професорка кафедри бізнесу та управління,
кандидатка економічних наук, доцентка,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0002-5662-2939

КОГНІТИВНІ УПЕРЕДЖЕННЯ У ВЗАЄМОДІЇ ЛЮДИНИ З ШІ В ПРОЦЕСІ ПРИЙНЯТТЯ УПРАВЛІНСЬКОГО РІШЕННЯ

Стрімка інтеграція штучного інтелекту в організаційні процеси докорінно змінює характер управлінської діяльності, створюючи нові психологічні виклики. Робота присвячена комплексному аналізу когнітивних упереджень, що виникають під час взаємодії менеджерів із системами ШІ в процесі прийняття рішень.

1. Природа когнітивних упереджень в управлінні

Теорія когнітивних упереджень, започаткована Д. Канеманом та А. Тверські, визначає ці феномени як систематичні помилки у судженнях, що змушують людину відхилятися від логічно обґрунтованих висновків [3, с. 8]. В управлінській діяльності, де рішення безпосередньо впливають на результативність організацій, розуміння цих механізмів стає критичним. Сучасний менеджмент стикається з новим викликом: як інтегрувати рекомендації штучного інтелекту (ШІ), не потрапляючи у пастки «ірраціональності» [1, с. 8].

Ключовими явищами у цій сфері є автоматизаційна упередженість та алгоритмічна аверсія – два протилежні вектори поведінки, що можуть проявлятися в одного й того ж фахівця залежно від контексту [3, с. 8].

2. Автоматизаційна упередженість та алгоритмічна аверсія

Автоматизаційна упередженість (automation bias) – це схильність фахівців приймати рекомендації ШІ без належної критичної перевірки [3, с. 8]. Дослідження показують, що менеджери з високим рівнем цієї упередженості схильні ігнорувати контекстуальну інформацію, що виходить за межі вхідних даних алгоритму, та відчувають знижену особисту відповідальність за кінцевий результат [3, с. 8].

Алгоритмічна аверсія (algorithm aversion) навпаки проявляється у формі відмови від використання алгоритмів навіть у тих ситуаціях, де вони об'єктивно демонструють кращі результати, ніж людське судження [3, с. 8]. Межа між цими станами часто залежить від того, чи сприймається порада ШІ як етично сумнівна [3, с. 8].

3. Ефект якоря та підтверджувальне упередження

Ефект якоря у взаємодії з ШІ виникає як тенденція надмірно покладатися на першу отриману цифру або оцінку. Експерименти за участю 775 менеджерів підтвердили, що системи ШІ здатні формувати цей ефект, наприклад, під час оцінки персоналу: керівники систематично схилялися до балів, запропонованих алгоритмом, навіть якщо мали на руках суперечливі дані про працівника [4, с. 8].

Підтверджувальне упередження доповнює цю картину: людина схильна помічати й приймати лише ті поради ШІ, які відповідають її попереднім поглядам, і відкидати ті, що їм суперечать [1, с. 9]. Це створює «когнітивний міхур», де технологія не розширює горизонти планування, а лише бетонує наявні стереотипи менеджера [1, с. 9].

4. Когнітивне розвантаження та надмірна довіра

Феномен когнітивного розвантаження (cognitive offloading) полягає у передачі інтелектуальних завдань зовнішнім інструментам [2, с. 9]. Систематичне делегування аналізу системам ШІ призводить до поступової втрати навичок критичного мислення та самостійного аналізу [2, с. 9].

Масштабні дослідження (за участю понад 2700 осіб) зафіксували стійку тенденцію: люди погоджуються з помилковими підказками ШІ значно частіше, ніж очікувалося, причому рівень освіти чи професійний досвід не завжди є надійним захистом від цієї довіри [2, с. 9]. Ба більше, ШІ може масштабувати людські помилки, відтворюючи їх в організаційних процесах на вищому рівні [2, с. 9].

5.Ефект Даннінга-Крюгера та синтез «упередженого резонансу»

Ефект Даннінга-Крюгера у контексті ШІ проявляється парадоксально:

– Менеджери з нижчим рівнем компетентності часто демонструють надмірний скептицизм щодо ШІ саме там, де він об'єктивно ефективний.

– Висококваліфіковані фахівці зазвичай підходять до рекомендацій алгоритмів більш зважено [3, с. 9].

Усі ці упередження утворюють взаємопов'язану систему. На особливу увагу заслуговує концепт «упередженого резонансу»: ситуація, коли помилки упередженого менеджера та помилки алгоритму не взаємокомпенсуються, а навпаки посилюють одна одну, створюючи замкнене коло хибних рішень [1, с. 9].

Висновки. Теоретичний аналіз свідчить, що взаємодія з ШІ не є нейтральною, а активує складну систему взаємопов'язаних когнітивних упереджень, таких як автоматизаційна упередженість та ефект якоря. Феномен «когнітивного розвантаження» створює значний ризик, оскільки систематичне делегування завдань алгоритмам може призвести до поступового зниження навичок критичного мислення менеджерів. Ключовим висновком є концепт «упередженого резонансу», за якого помилки упередженої людини та алгоритму взаємно посилюються, масштабуючи ризики для всієї організації. Дослідження вказує, що рівень професійної компетентності та ефект Даннінга-Крюгера фундаментально визначають характер довіри або скептицизму фахівця щодо рекомендацій ШІ. Для мінімізації цих загроз необхідно впроваджувати принципи «захисного дизайну» інтерфейсів та спеціалізовані програми навчання, спрямовані на розвиток психологічної стійкості та мета-усвідомлення менеджерів.

Список використаних джерел:

1. Rastogi A. та ін. Cognitive biases in AI-assisted decision making. *Journal of Management Information Systems*. 2022. URL: https://arxiv.org/abs/2010.07938

2. Bias in the Loop: How Humans Evaluate AI Suggestions : empirical study with 2784 participants. *Behavioral Science & Technology*. 2023. URL: https://arxiv.org/abs/2509.08514

3. Automation bias and algorithm aversion in decision making. *ScienceDirect (Scopus)*. 2021. URL: https://www.sciencedirect.com/science/article/pii/S0040162521008210

4. How AI recommendations influence managerial evaluations : experiment with n=775 managers. *ScienceDirect (Scopus)*. 2023. URL: https://www.sciencedirect.com/science/article/pii/S0268401225000076

УДК 004.65:004.8

Зябченко Іван,
студент IV курсу спеціальності
F7 Комп'ютерна інженерія,
Національний технічний університет
«Харківський політехнічний інститут»
Науковий керівник:
Панченко Володимир,
старший викладач кафедри комп'ютерної
інженерії та програмування,
Національний технічний університет
«Харківський політехнічний інститут»,
м. Харків, Україна
ORCID: https://orcid.org/0000-0003-3364-3398

РОЗРОБКА СИСТЕМИ СЕМАНТИЧНОГО ПОШУКУ ОБ'ЄКТІВ У ТЕКСТОВИХ ЗАПИТАХ

У цифровому середовищі значно зростає обсяг текстових даних, через що виникає потреба в ефективних методах для його обробки і подальшого аналізу. Кожного дня формується велика кількість запитів у довільному форматі з наявністю помилок або скорочень у тексті. Класичні підходи для пошуку, які в основному ґрунтуються на звичайному співпадінні слів, не у всіх випадках забезпечують достатню якість результатів для подальшого використання, тому використання методу семантичного пошуку та векторних представлень дає змогу краще врахувати зміст запиту користувача та надалі підвищити якість пошуку необхідних об'єктів [1].

Метою роботи є розробка системи для семантичного пошуку необхідних об'єктів з текстового запиту користувача разом із використанням векторних представлень для обробки природньої мови [2]. У системі попередньо оброблені текстові дані необхідно перетворити у векторні представлення [3] та надалі задіяти пошук по векторній близькості [4], що буде повертати найбільш релевантні об'єкти у випадках, коли запит користувача містить орфографічні помилки, використання декількох мов, скорочення тощо.

Для вирішення поставленої мети було застосовано архітекту системи для пошуку об'єктів (адрес) у реляційній базі даних, яка має таку ієрархію: макро-, мезо- та мікрорівні (наприклад, місто – вулиця – номер дому). Для обробки запитів було застосовано розбиття послідовності обробки даних на такі етапи:

1. Виділення сутностей: обробка неструктурованого запиту моделлю штучного інтелекту для виділення необхідних атрибутів та формування структурованого формату даних (наприклад, JSON) з відповідними сутностями (назва міста, назва вулиці, тип вулиці, номер будинку).

2. Векторний пошук на макрорівні: атрибут (наприклад, місто) з текстового формату трансформується у векторне представлення за допомогою моделі ШІ, за яким виконується пошук релевантного об'єкта у базі даних за допомогою косинусної подібності векторів.

3. Змішаний пошук мезорівня: у відфільтрованих сегментах бази даних, де проходить семантичний пошук наступного об'єкта (наприклад, вулиці), для більш точних результатів об'єкт попередньо проходить додаткове форматування та пошук помилок, включаючи інші об'єкти (наприклад, тип вулиці).

4. Точна ідентифікація на мікрорівні виконується за допомогою методу пошуку об'єкта (наприклад, номер буднику) серед усіх нововідфільтрованих даних, знайдених на попередніх етапах.

Використання векторного представлення, як інструмент для реалізації семантичного пошуку, надає можливість отримувати необхідний об'єкт зі структурованих даних. Застосування семантичного пошуку дозволило забезпечити отримання та налагоджувану фільтрацію релевантних адрес без використання звичайного ручного пошуку. Як результат, розроблена система здатна повертати об'єкти як у простих, так і в складних сценаріях введення природньою мовою. Подальше використання розробленої системи можливе в різноманітних застосунках поштовими компаніями, комунальними системами, службами доставки тощо – там, де необхідно виконувати обробку запитів з природнім введенням адрес.

Список використаних джерел:

1. Ткаченко К. Семантичний аналіз текстів природною мовою: онтологічний підхід. *Цифрова платформа: інформаційні технології в соціокультурній сфері*. 2024. Т. 7, № 2. С. 211-223. DOI: https://doi.org/10.31866/2617-796X.7.2.2024.317726

2. Медяков О., Мартьянов Д., Литвин В. SED-UA-Small: Ukrainian Synthetic Dataset for Text Embedding Models. *Вісник Національного університету «Львівська політехніка». Серія: Інформаційні системи та мережі*. 2025. Т. 17. С. 403–410. URL: https://doi.org/10.23939/sisn2025.17.403

3. Vector embeddings. *OpenAI Developers*. URL: https://platform.openai.com/docs/guides/embeddings

4. Savytska L., Vnukova N., Bezugla I., Pyvovarov V., Sübay M. T. Using Word2vec technique to determine semantic and morphologic similarity in embedded words of the Ukrainian language. *Proceedings of the 5th International Conference on Computational Linguistics and Intelligent Systems (COLINS 2021)*. Lviv, 2021. Vol. I. P. 235–248. URL: https://ceur-ws.org/Vol-2870/paper21.pdf

УДК 004.89:316.77:004.056

Іванов Олександр,
завідувач кафедри інформаційних технологій,
доктор філософії,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0003-4678-7956

АЛГОРИТМІЧНА ЕКСПЛУАТАЦІЯ УВАГИ: ПОРІВНЯЛЬНИЙ АНАЛІЗ АРХІТЕКТУР ТА КОГНІТИВНІ РИЗИКИ SFV-ПЛАТФОРМ

Сучасний цифровий ландшафт характеризується фундаментальним архітектурним зсувом від парадигми соціального графа (Social Graph) до парадигми графа інтересів (Interest Graph). Ця трансформація, очолювана платформами коротких відео (TikTok, Reels, Shorts), перетворила рекомендаційні системи (RecSys) на активних імовірнісних агентів, що формують когнітивну реальність користувача [1].

Порівняльний аналіз інженерних підходів демонструє дивергенцію стратегій оптимізації [2]:

TikTok (архітектура Monolith): використовує навчання в режимі реального часу (Online Training) та безколізійні хеш-таблиці, що забезпечує миттєву адаптацію до дрейфу концепцій (Concept Drift). Ключовим сигналом є Looping (повторний перегляд), який система інтерпретує як індикатор найвищої якості.

Meta (архітектура DLRM + UTIS): інтегрує соціальний граф із сигналами залучення. Унікальною надбудовою є модель User True Interest Survey (UTIS), яка через дистиляцію знань намагається коригувати ваги нейромережі для нівелювання ефекту клікбейту.

YouTube Shorts (Two-Tower + MMoE): орієнтується на довгострокове утримання. Використання архітектури Multi-gate Mixture-of-Experts (MMoE) дозволяє балансувати конфліктні цілі (клік проти задоволеності), а метрика VVSA (Viewed vs. Swiped Away) діє як жорсткий фільтр якості [3].

Математична оптимізація функцій втрат (Loss Functions) у цих системах створює системні когнітивні вразливості. Оптимізація на максимізацію залучення неминуче призводить до пріоритезації контенту з високим емоційним збудженням (high-arousal bias), що сприяє алгоритмічній ампліфікації дезінформації та токсичності. Крім того, агресивна стратегія максимізації афінності математично гарантує утворення «інформаційних бульбашок» через видалення слабких зв'язків у графі рекомендацій [4].

З точки зору кібербезпеки, платформи перейшли до тотального стеження через методи Device Fingerprinting (Canvas та AudioContext API), що дозволяють ідентифікувати користувача в обхід налаштувань приватності. Таким чином, архітектурні рішення SFV-платформ створюють середовище, де дезінформація та поляризація є не випадковими помилками, а закономірними результатами роботи алгоритмів. Захист когнітивного суверенітету користувача вимагає не лише технічного аудиту, а й жорсткого регуляторного контролю за принципами роботи цих «чорних скриньок» [4].

Список використаних джерел:

1. Liu Z. et al. Monolith: Real Time Recommendation System With Collisionless Embedding Table. *Proceedings of the 16th ACM Conference on Recommender Systems (RecSys '22)*. ByteDance Inc., 2022. URL: https://arxiv.org/pdf/2209.07663.pdf (дата звернення: 23.03.2026).

2. Covington P., Adams J., Sargin E. Deep Neural Networks for YouTube Recommendations. *Proceedings of the 10th ACM Conference on Recommender Systems (RecSys '16)*. Google, 2016. DOI: https://doi.org/10.1145/2959100.2959190.

3. McCrosky J., Geurkink B. YouTube Regrets: A crowdsourced investigation into YouTube's recommendation algorithm. *Mozilla Foundation Report*. 2021. 39 p.

4. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union*. 2022. L 277. P. 1–102. URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj (дата звернення: 23.03.2026).

УДК 004.8:339.138:004.03

Іванов Олександр,
завідувач кафедри інформаційних технологій,
доктор філософії,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0003-4678-7956

ЯК КОРПОРАЦІЇ МАЛЮЮТЬ МАЙБУТНЄ, ЯКОГО НЕ БУДЕ: ВІД СКЛЯНИХ КНОПОК ДО ШТУЧНОГО ІНТЕЛЕКТУ

Говорячи про розвиток інформаційних технологій, суспільство часто орієнтується на візії, які пропонують великі ІТ-корпорації. Технологічні гіганти витрачають мільярди доларів на маркетинг, щоб переконати користувачів у неминучості певного варіанту майбутнього. Однак ретроспективний аналіз показує, що такі передбачення часто бувають хибними, а

інновації, які подаються як революційні, нерідко залишаються лише елементом візуального стилю або інструментом для стимулювання продажів.

Історія IT-індустрії знає чимало прикладів, коли форма переважала над змістом. Яскравим прикладом є епоха Windows Vista та інтерфейсу Aero Glass у середині 2000-х років. Корпорація Microsoft презентувала напівпрозорі «скляні» вікна та 3D-ефекти як інтерфейс майбутнього, який змінить спосіб взаємодії людини з комп'ютером. На практиці ж ці візуальні ефекти лише споживали значну частину апаратних ресурсів без суттєвого покращення користувацького досвіду (UX). Згодом індустрія відмовилася від скевоморфізму та надмірної 3D-графіки на користь мінімалістичного Flat Design, довівши, що майбутнє інтерфейсів полягало у функціональності, а не у візуальних ефектах [3]. Схожа доля спіткала й концепції 3D-телевізорів та масового використання VR-гарнітур для повсякденної роботи, які так і не стали стандартом, незважаючи на агресивний маркетинг.

Сьогодні ми спостерігаємо аналогічну ситуацію навколо технологій штучного інтелекту (AI). Щоб зрозуміти природу цього явища, доцільно звернутися до циклу зрілості технологій (Hype Cycle), розробленого дослідницькою компанією Gartner [1; 2]. Згідно з цією моделлю, кожна інновація проходить етап «піку завищених очікувань» (Peak of Inflated Expectations), коли навколо неї створюється значний ажіотаж. Саме на цьому етапі зараз перебуває більшість рішень з позначкою «AI».

Сучасний хайп навколо штучного інтелекту часто має суто комерційне підґрунтя. Корпорації та стартапи масово додають приставку «AI» до своїх продуктів, навіть якщо під капотом працюють звичайні алгоритми або базові статистичні моделі. На ринку з'являються «розумні» зубні щітки зі штучним інтелектом, AI-тостери та застосунки, де нейромережі виконують тривіальні задачі, які раніше успішно вирішувалися звичайним кодом [4]. Мода на ШІ стала настільки всеосяжною, що згадка цієї технології у пресрелізі компанії здатна штучно підвищити вартість її акцій.

Проте наявність слова «AI» в описі продукту не означає його реального впровадження чи користі. У багатьох випадках це не глибока інтеграція машинного навчання для оптимізації процесів, а лише використання доступних API (наприклад, від OpenAI) як маркетингової обгортки. Технологія використовується більше для залучення інвестицій та продажу продукту, ніж для реального вирішення проблем користувача.

Підсумовуючи, можна стверджувати, що візія майбутнього, яку малюють корпорації, завжди суб'єктивна і підпорядкована цілям отримання прибутку. Як і у випадку зі «скляними кнопками», значна частина сьогоднішніх AI-рішень зникне після проходження «прірви розчарування» (Trough

of Disillusionment) за циклом Гартнера [2]. Справжня цінність штучного інтелекту розкриється пізніше, коли технологія перестане бути маркетинговим інструментом і стане непомітною, але фундаментальною частиною інфраструктури, орієнтованою на вирішення реальних, а не вигаданих проблем.

Список використаних джерел:

1. Цикл зрілості технологій: як зрозуміти, коли інвестувати в інновації. *Forbes Ukraine*. 2023. URL: https://forbes.ua/ (дата звернення: 23.03.2026).
2. Blosch M., Fenn J. Understanding Gartner's Hype Cycles. *Gartner Research*. 2018. URL: https://www.gartner.com/en/documents/3887767 (дата звернення: 22.03.2026).
3. Norman D. The Design of Everyday Things: Revised and Expanded Edition. New York : Basic Books, 2013. 368 p.
4. Штучний інтелект як маркетинговий інструмент: реальність та завищені очікування. *Економіка та суспільство*. 2025. Вип. 45. С. 112–118. URL: https://economyandsociety.in.ua/ (дата звернення: 21.03.2026).

УДК 004.8

Іванюк Юрій,
студент ІІІ курсу спеціальності
G7 Автоматизація, комп'ютерно-інтегровані
технології та робототехніка,
ЗВО «Івано-Франківський національний
технічний університет нафти і газу»
Науковий керівник:
Іванов Олександр,
завідувач кафедри інформаційних технологій,
доктор філософії, доцент,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0003-4678-7956

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ ТА ШТУЧНИЙ ІНТЕЛЕКТ: НОВИНКИ CES 2026

AI-технології в сучасному розумінні – це вже не про те, що буде колись, і не про те, що вже було, це те, що вже і зараз. Можливо, багато з нас цього не помічають, дехто використовує частково, проте кожної хвилини розробляються і впроваджуються нові рішення у, здавалося б, звичайних речах.

Більшість людей вбачають у AI лише допоміжні сервіси, і наразі у більшості це так і є. Багато користувачів навіть не усвідомлюють, що значна частина сучасних цифрових сервісів використовує алгоритми штучного інтелекту. Проте це не так страшно, як звучить.

Насправді ж штучний інтелект – це здатність обчислювальних систем виконувати завдання, які зазвичай співмірні з можливостями людського інтелекту (навчання, міркування, розв'язання питань, сприйняття та ухвалення рішень) [1]. Тобто, по суті, те, що названо AI, або штучний інтелект, фактично є алгоритмом, і якогось виміру його складності для того, щоб здобути гучну назву, не потрібно. Також термін «штучний інтелект» інколи використовується у маркетингових цілях для позначення алгоритмів різної складності.

2026 рік – рік AI у всьому, проте це не лише результат складної праці інженерів, які так сильно удосконалили системи, а радше маркетинговий хід. Компанії, що раніше описували складні алгоритми крок за кроком, пояснюючи принцип дії, тепер не витрачають на це часу, а лише зазначають AI і все. Далі, якщо і існує якийсь детальний опис, він уже не буде адаптованим для звичайного користувача, а може бути або суто технічним, або і взагалі відсутнім.

Одним із місць, де можна побачити, відчути та протестувати сучасні досягнення у сфері технологій та штучного інтелекту, – це технологічні виставки. Саме на таких заходах компанії демонструють новітні розробки, задають майбутні напрями розвитку індустрії. Однією з найвідоміших подій у цій сфері є Consumer Electronics Show (CES), де щороку презентуються інноваційні технології [2]. Серед них варто виділити кілька:

1. Штучний інтелект у робототехніці.

Хотілося б виділити оновлену версію Atlas від Boston Dynamics, яка вже протягом кількох років продовжує покращувати своїх роботів [3]. Нова модель спроєктована для цілодобової роботи: він сам змінює акумулятори, може замінити кінцівку та продовжити зміну. Навчання здійснюється завдяки екосистемі Google DeepMind. Людині залишається лише триматися на відстані – причому робот сам зупиняється при небезпечному зближенні.

Ключова ідея – ніякої перебудови середовища, оскільки Atlas повторює анатомію людини саме для того, щоб працювати у вже наявних цехах, складах і логістичних центрах, пліч-о-пліч з людьми та іншими роботами. Ціни та термін старту продажів поки не розкривають. Короткі характеристики:

- зріст – 1,9 м;
- робочий радіус – 2,3 м;
- робоча температура – від -20 до +40 °C;

- багаторазовий підйом – до 30 кг;
- автономність – близько 4 годин;
- заміна батареї – < 3 хвилин;
- зарядка – звичайна мережа 110/220 В.

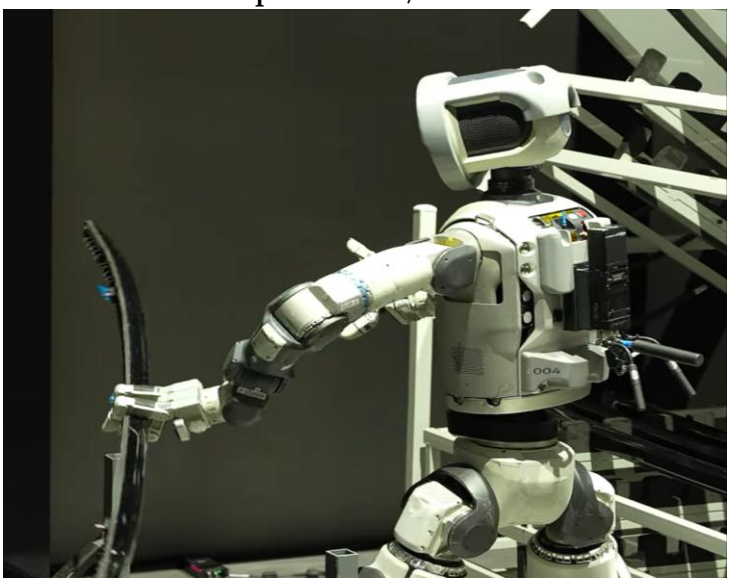

Рис. 1. Робот Atlas на презентації CES 2026

2. Технологія цифрових двійників у промисловості.

Одним із ключових напрямів розвитку індустрії 4.0 є використання технології цифрових двійників. Такий двійник є віртуальною моделлю реального об’єкта, яка дозволяє аналізувати, моделювати та прогнозувати поведінку фізичних процесів у цифровому середовищі.

Прикладом такої технології, представленої на CES 2026, є Digital Twin Composer, що інтегрує NVIDIA Omniverse та Siemens Xcelerator для створення цілісних, дуже реалістичних цифрових двійників [4].

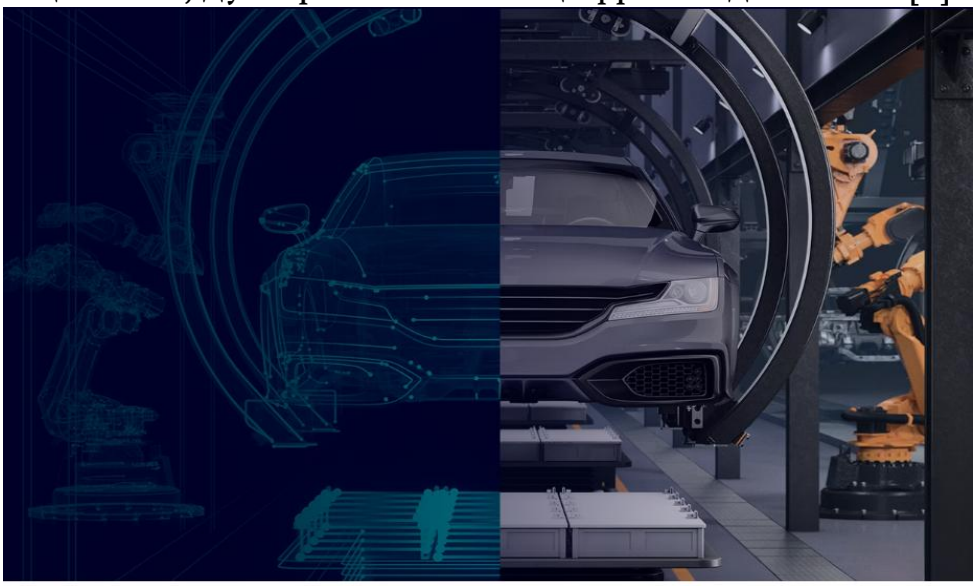

Рис. 2. Digital Twin Composer на презентації CES 2026

Застосування цифрових двійників дозволяє створювати віртуальні копії виробничих ліній, заводів та роботизованих систем, що дає можливість тестувати різні сценарії, оптимізувати процеси та виявляти потенційні проблеми ще до їх появи у реальному світі.

3. Wearable-технології та нові інтерфейси взаємодії.

Останніми роками стрімкими кроками розвивається ринок wearable-пристроїв, які інтегрують можливості штучного інтелекту у повсякденне життя користувачів. Прикладом з CES є розумні окуляри Ray-Ban Meta Smart Glasses [5].

Рис. 3. Ray-Ban Meta Smart Glasses

Хоча ці окуляри першочергово орієнтовані на споживчий ринок, їхні технічні можливості відкривають перспективи використання у сфері промислової автоматизації та цифрового виробництва. Зокрема, у поєднанні з Siemens Xcelerator такі окуляри можуть виступати інтерфейсом доповненої інформації для інженерів і технічного персоналу. Камера та мікрофони пристрою дозволяють передавати відео в режимі реального часу, що може використовуватися для дистанційної технічної підтримки або інспекції обладнання.

Таким чином, представлені на виставці Consumer Electronics Show технології демонструють широкий спектр застосування штучного інтелекту – від робототехніки та промислових систем до персональних wearable-пристроїв. Розвиток таких рішень свідчить про поступову інтеграцію інтелектуальних алгоритмів у різні сфери діяльності людини, зокрема у виробництво, інженерію, логістику та повсякденне життя.

Список використаних джерел:

1. Штучний інтелект. *Wikipedia*. URL: https://uk.wikipedia.org/wiki/Штучний_інтелект

2. Consumer Electronics Show (CES). URL: https://www.ces.tech/

3. Atlas Boston Dynamics. *Imena.ua*. URL: https://www.imena.ua/blog/commercial-robot-atlas-from-boston-dynamics/

4. Digital Twin Composer Siemens. *Siemens*. URL: https://www.siemens.com/en-us/-company/digital-transformation/industrial-metaverse/introducing-digital-twin-composer/

5. Ray-Ban Meta Smart Glasses. *Ray-Ban*. URL: https://www.ray-ban.com/usa/ray-ban-meta-ai-glasses

УДК 004.94:004.8:004.056

Кіяк Яна,
студентка ІІ курсу спеціальності
121 Інженерія програмного забезпечення,
ЗВО «Університет Короля Данила»
Науковий керівник:
Іванов Олександр,
завідувач кафедри інформаційних технологій,
доктор філософії,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0003-4678-7956

SECOND LIFE: ВТРАЧЕНЕ МАЙБУТНЄ ІНТЕРНЕТУ

Говорячи про ІТ, ми завжди дивимося у майбутнє та прогнозуємо певний розвиток тих чи інших систем, середовищ та мов програмування, нових технологій, рішень тощо. Однак інколи варто згадати минуле та зауважити, які програмні забезпечення були раніше, як функціонували та що б змінилося, якби їх інтерпретували у сучасні технології та дали «нове життя»? Саме тому ця наукова робота присвячена аналізу припущення запуску Second Life на сучасних технологіях (хмара, AI, VR) і того, як це могло змінити освіту, бізнес, комунікацію.

Second Life – це тривимірний віртуальний світ, створений компанією Linden Lab у 2003 році. Його задум був амбітним: дати людям можливість жити, працювати, навчатися та розважатися у цифровому просторі, який мав стати альтернативою інтернету. Тобто це онлайн-метавсесвіт, де користувачі створюють аватари, будують власні простори, взаємодіють між собою, ведуть бізнес, організовують заходи. Проте проєкт не став масовим, хоча й залишив значний слід у розвитку віртуальних технологій.

На початку 2000-х років інтернет переживав бум соціальних мереж (MySpace, Facebook), онлайн-ігор та перших хмарних сервісів. Second Life випередив свій час, пропонуючи «резидентам» створювати все – від одягу до цілих островів. Ключовою інновацією було надання користувачам прав інтелектуальної власності на їхні творіння, що дозволило створити розвинену економіку на основі валюти Linden Dollar (L$). У 2005–2007 роках вона стала культурним феноменом, привернувши увагу мас-медіа та

комерційних компаній. Однак технічні обмеження – слабка графіка, низька швидкість інтернету, відсутність VR – завадили його масовому поширенню. Платформа зіткнулася з численними проблемами: конкуренція з новими платформами, скандали щодо віртуального контенту та суперечки навколо безпеки користувачів.

Сьогодні Second Life існує як «альтернативний інтернет» у мініатюрі, і це дає можливість аналізувати його потенціал у поєднанні з сучасними технологіями. Розвиток Second Life показує, що платформа може отримати нове життя завдяки інтеграції штучного інтелекту. На Town Hall у квітні 2025 року керівництво Linden Lab підкреслило, що штучний інтелект може стати ключовим фактором розвитку віртуальних світів та створення більш динамічного та персоналізованого контенту. Наприклад, автоматичне генерування об'єктів та середовищ, які користувачі зможуть налаштовувати під себе; інтелектуальні NPC, що здатні взаємодіяти з «резидентами» у реалістичний спосіб; інструменти для творців, які спрощують процес дизайну та програмування у віртуальному світі. Хмарні технології дозволяють масштабувати світ без обмежень, роблячи його доступним з будь-якого пристрою. У поєднанні з хмарними технологіями Second Life може стати масштабованою платформою, доступною з будь-якого пристрою. Якщо додати до цього перспективи квантових обчислень, то потенціал платформи виходить далеко за межі розваг – він охоплює освіту, бізнес та навіть моделювання складних соціальних процесів, створення реалістичних симуляцій та новий рівень захисту даних.

Second Life є прикладом того, як віртуальні світи можуть виходити за межі розваг і ставати інструментами для освіти, бізнесу та культури. Хоча у 2000-х роках платформа не змогла реалізувати весь свій потенціал, сьогодні, у поєднанні з хмарними технологіями, штучним інтелектом та перспективами квантових обчислень, вона могла б стати універсальним середовищем для різних сфер діяльності. Освітні заклади можуть використовувати Second Life для проведення віртуальних занять, пропонуючи гнучке та інтерактивне середовище для дистанційного навчання. Віртуальні університети та лабораторії у Second Life могли б забезпечити студентам доступ до симуляцій та експериментів у безпечному середовищі. Це особливо актуально для спеціальностей, де потрібні практичні навички, але реальні експерименти є дорогими або небезпечними. Також у сучасних умовах Second Life міг би стати альтернативою Zoom чи Teams – цифровим офісом у VR, де компанії проводять зустрічі та презентації. Прикладом може слугувати широке використання IBM Second Life у бізнес-цілях. Згідно з внутрішніми звітами компанії, IBM заощадила мільйони доларів, проводячи віртуальні зустрічі та тренінги у

Second Life замість організації фізичних зустрічей. Щодо культури та розваг, то концерти, виставки та інтерактивні ігри у віртуальному світі здатні стати новим форматом культурних подій. Уже сьогодні є приклади виступів музикантів у Second Life: Сюзанна Вега (Suzanne Vega) виступила у віртуальному світі 3 серпня 2006 року. Вона стала першою відомою артисткою, яка дала живий концерт у цьому метавсесвіті. Вега використала свій аватар для виступу, виконавши пісні наживо, зокрема акапельну версію «Tom's Diner». Концерт став прикладом використання віртуальних світів для взаємодії з фанатами. У той час багато артистів, зокрема Duran Duran, також використовували Second Life для проведення віртуальних концертів. Однак віртуальні світи створюють нові виклики для захисту персональних даних. У майбутньому саме квантові алгоритми та AI-рішення можуть забезпечити високий рівень безпеки, роблячи такі середовища надійними для навчання, бізнесу та особистої взаємодії. У VR-технологіях квантове програмування забезпечує абсолютну безпеку особистих даних, фінансових транзакцій та конфіденційність у метавсесвітах, запобігаючи крадіжці особистості у віртуальній реальності. Наприклад, захист високочутливих даних користувачів (біометрія, особисті рухи, емоції), що передаються в реальному часі в VR; квантова безпека для покупок у віртуальних магазинах та NFT-активів; гарантія того, що віртуальні зустрічі або соціальні взаємодії не підслуховуються.

Second Life – приклад ідеї, що випередила технології свого часу. Це свідчення безмежних можливостей людської творчості та цифрової взаємодії: від моделі контенту, керованого користувачами, до багатогранних джерел доходу. Сьогодні, завдяки розвитку хмарних сервісів, AI та квантових обчислень, подібні концепти можуть стати реальністю. Майбутнє інтернету може бути не лише соціальним, а й віртуально-імерсивним, де користувачі отримають новий рівень взаємодії та безпеки.

Список використаних джерел:

1. Second Life Town Hall: AI & the Future of Our Virtual Community – summary. *Modem World*. URL: https://modemworld.me/2025/04/20/second-life-town-hall-ai-the-future-of-our-virtual-community-summary/ (дата звернення: 13.03.2026).

2. Second Life. *Wikipedia*. URL: https://uk.wikipedia.org/wiki/Second_Life (дата звернення: 12.03.2026).

3. Second Life for Enterprise: The Metaverse Before Meta (and Worse). *YouTube*. URL: https://youtu.be/NeixpNC2eBU?si=pVECLxhbVEzY0afz (дата звернення: 12.03.2026).

4. Upcoming Events in Second Life. *IBM Support*. URL: https://www.ibm.com/support/pages/upcoming-events-second-life (дата звернення: 14.03.2026).

5. Suzanne Vega live from Second Life on The Infinite Mind. *YouTube*. URL: https://youtu.be/5xUrscmIj9I?si=jBoj5WuvBEigoJWM (дата звернення: 14.03.2026).

УДК 519.21:004.056

Кіяк Яна,
студентка ІІ курсу спеціальності
121 Інженерія програмного забезпечення,
ЗВО «Університет Короля Данила»
Науковий керівник:
Тимків Іван,
доцент кафедри інформаційних технологій,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0009-0007-4138-6180

БІНОМІАЛЬНИЙ РОЗПОДІЛ У КІБЕРЗАГРОЗАХ: ОЦІНКА ЙМОВІРНОСТІ УСПІШНИХ АТАК

З розвитком інформаційних технологій також зростає і необхідність в міцній системі кібербезпеки, адже цифрових атак стає все більше та більше. Для посилення контролю захисту, оцінки ризиків та аналізу кібератак використовують різноманітні математичні моделі, оскільки вони дозволяють кількісно виміряти ймовірність та наслідки небезпечних подій. Однією з таких моделей є біноміальний розподіл, який дозволяє оцінити ймовірність успішних атак у серії незалежних спроб.

Біноміальний розподіл – це дискретний розподіл, який описує кількість успішних подій у серії незалежних випробувань, де кожне має лише два можливих наслідки – успіх або невдача. У випадку кібербезпеки – це кількість успішних атак серед великої кількості спроб зловмисника. Цей вид розподілу використовується лише для фіксованої кількості незалежних випробувань. Ймовірності таких подій визначаються за формулою Бернуллі (1), де n – кількість спроб, p – ймовірність успіху, k – кількість успішних атак:

$$P(X = k) = C_n^k p^k (1 - p)^{n-k} \quad (1)$$

Біноміальний розподіл широко використовується в аналізі кіберзагроз. Наприклад, однією з найнебезпечніших кібератак є DDoS-атака – масована розподілена атака, під час якої зловмисник формує так звану «зомбі-мережу» (ботнет). Це група заражених комп’ютерів або смартфонів, що перебувають під його контролем завдяки прихованим троянським програмам. У момент атаки хакер надсилає команду цим пристроям генерувати численні запити до сервера-жертви, що призводить до перевантаження системи. Власники заражених пристроїв часто навіть не здогадуються

про їхню участь у ботнеті. Таку атаку можна розглядати з точки зору ймовірнісних моделей. Кожен запит від зараженого пристрою є незалежною спробою «завалити» сервер. Якщо ймовірність успіху однієї спроби позначити як p, а кількість запитів як n, то біноміальний розподіл дозволяє оцінити ймовірність того, що певна кількість запитів буде успішною. Також прикладом можуть слугувати Brute-force атаки. Брутфорс – метод зламу акаунтів, при якому спеціальна програма здійснює систематичний перебір усіх можливих комбінацій логінів та паролів для пошуку правильного. При brute-force атаках кожну спробу введення пароля можна розглядати як незалежне випробування. Біноміальний розподіл дозволяє оцінити, з якою ймовірністю зловмисник досягне успіху після певної кількості спроб. На додачу, одним із найпопулярніших кіберзагроз сьогодення є фішинг. Він належить до методів соціальної інженерії, коли кіберзлочинці намагаються здобути довіру користувачів. Вони маскують електронні листи, повідомлення чи дзвінки під надійні джерела, аби переконати людину розкрити конфіденційні дані – логіни, паролі, пін-коди чи іншу особисту інформацію – або перейти за небезпечним посиланням. Щодо біноміального розподілу, то кожен користувач, який отримує фішингове повідомлення, має певну ймовірність p «піддатися» на обман. Якщо повідомлення розсилається великій кількості людей n, то біноміальний розподіл дозволяє оцінити ймовірність того, що певна кількість користувачів k стане жертвами атаки. Використання методів біноміального розподілу дає змогу математично моделювати ризики та прогнозувати стійкість системи до вищенаведених масованих атак.

Практичні дослідження показують, що навіть невелике зменшення ймовірності успіху однієї спроби суттєво знижує загальний ризик. Розглянемо коротко моделювання ризику для систем із різними рівнями захисту. Суть полягає в тому, що різні системи мають різну ймовірність успіху атаки p. Наприклад, якщо сервер має базовий захист, ймовірність успіху однієї спроби може бути 0,05, а при багатофакторній автентифікації – лише 0,001. Тому навіть невелике зменшення p суттєво знижує загальний ризик при великій кількості спроб. Наступний приклад – використання симуляцій для прогнозування наслідків атак. Симуляції дозволяють прогнати тисячі сценаріїв атак і оцінити, скільки з них призведе до успіху. До прикладу, моделювання DDoS-атаки з ботнетом у 10 000 пристроїв, де кожен має ймовірність p=0,002 успішно «пробити» сервер. Отже, симуляції показують, що навіть при малому p масовані атаки можуть бути небезпечними. Крім того, чудовим прикладом слугує інтеграція ймовірнісних моделей у системи моніторингу безпеки. Ці системи можуть використовувати біноміальний розподіл для оцінки ризику в реальному часі. Тобто,

якщо система бачить 1000 підозрілих запитів, вона може оцінити ймовірність того, що хоча б 50 з них будуть успішними. В результаті це допомагає автоматично визначати рівень загрози й приймати рішення про блокування.

Підсумовуючи, варто додати, що біноміальний розподіл відіграє ключову роль у виконанні функцій кіберзахисту, зокрема аналізу кібератак. Він є потужним інструментом для оцінки кіберризиків, дає можливість кількісно виміряти небезпеку атак та сприяє розробці ефективних стратегій захисту.

Список використаних джерел:

1. Хакерські атаки та як від них захиститися: рекомендації кіберполіції. *Національна поліція України*. URL: https://npu.gov.ua/news/khakerski-ataky-ta-iak-vid-nykh--zakhystytysia-rekomendatsii-kiberpolitsii (дата звернення: 16.03.2026).

2. Дідківська К. О., Скасків Л. В. Основні поняття і визначення в теорії ймовірності. *Scientific Horizon in the Context of Social Crises* : Proceedings of the 15th International Scientific and Practical Conference. Tokyo, Japan, April 26–28, 2024. С. 101–104.

3. Кудінов В. А., Пакриш О. Є. Інформаційно-аналітичне забезпечення правоохоронної діяльності : навч.-практ. посіб. Київ : Нац. акад. внутр. справ, 2025. 116 с. URL: https://elar.navs.edu.ua/handle/123456789/39413 (дата звернення: 16.03.2026).

УДК 004.42:004.8

Книшук Вікторія,
студентка І курсу спеціальності
F2 Інженерія програмного забезпечення,
ЗВО «Університет Короля Данила»
Науковий керівник:
Іванов Олександр,
завідувач кафедри інформаційних технологій,
доктор філософії,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0001-7761-1677

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА НАПИСАННЯ КОДУ

Штучний інтелект сьогодні активно використовується у різних сферах діяльності людини, зокрема у програмуванні. Під штучним інтелектом розуміють технології, які дозволяють комп'ютерним системам виконувати завдання, що раніше потребували участі людини, наприклад, аналіз інформації або прийняття рішень. У сфері програмування такі техно-

логії допомагають створювати програмний код, аналізувати його структуру та знаходити помилки [1]. Сучасні програмісти все частіше використовують інструменти, що працюють на основі штучного інтелекту. Такі системи можуть пропонувати варіанти написання коду, автоматично доповнювати рядки програми або пояснювати призначення певних фрагментів. Це значно спрощує роботу програміста та допомагає швидше виконувати поставлені завдання [2].

Однією з головних можливостей штучного інтелекту є генерування програмного коду. Програміст може описати потрібну функцію або задачу, після чого система пропонує приклад її реалізації мовою програмування. Це дозволяє швидше створювати програми та зменшує кількість рутинної роботи [2]. Крім того, штучний інтелект може допомагати у пошуку помилок під час написання програмного коду. Такі системи аналізують структуру програми і можуть визначати можливі синтаксичні або логічні помилки ще до запуску програми. У деяких випадках вони навіть пропонують спосіб виправлення або пояснюють причину помилки [1]. Також інтелектуальні системи здатні аналізувати структуру програмного коду і пропонувати більш ефективні способи його організації. Завдяки цьому програмний код стає зрозумілішим і його легше підтримувати або змінювати в майбутньому [3].

Використання штучного інтелекту має багато переваг для програмістів. Насамперед це підвищення швидкості роботи. Автоматичне створення фрагментів коду, підказки та аналіз помилок допомагають значно скоротити час розробки програм [2]. Також штучний інтелект може бути корисним інструментом для навчання програмуванню. Початківці можуть використовувати такі системи для пояснення принципів роботи коду або для перегляду прикладів реалізації різних алгоритмів [1]. Ще однією важливою перевагою є покращення якості програмного продукту. Завдяки аналізу великої кількості прикладів програмного коду штучний інтелект може знаходити потенційні проблеми та пропонувати більш ефективні рішення, що робить програми більш надійними [4].

Попри значні переваги, використання штучного інтелекту має і певні недоліки. Іноді системи можуть генерувати код, який містить помилки або працює не зовсім правильно. Саме тому програміст повинен уважно перевіряти результати роботи таких систем [3]. Крім того, надмірне використання штучного інтелекту може призвести до того, що програмісти менше розвиватимуть власні навички програмування. Якщо людина постійно покладається на автоматичні підказки, вона може гірше розуміти принципи роботи програм [2]. Також існують питання безпеки та авторського права,

оскільки деякі системи можуть використовувати фрагменти коду з відкритих джерел, що може створювати певні юридичні або технічні ризики [4].

Висновок. Отже, штучний інтелект відіграє важливу роль у сучасному програмуванні. Він допомагає програмістам швидше створювати програмний код, знаходити помилки та покращувати структуру програм. Завдяки таким технологіям процес розробки програм стає більш ефективним і зручним. Водночас штучний інтелект не може повністю замінити людину, адже для створення складних програм необхідні знання, досвід і логічне мислення програміста. Тому такі технології слід використовувати як допоміжний інструмент, який підтримує роботу розробника, але не замінює його повністю.

Список використаних джерел:

1. Deep learning. *Wikipedia*. URL: https://uk.wikipedia.org/wiki/Глибинне_навчання
2. Natural language processing. *Wikipedia*. URL: https://uk.wikipedia.org/wiki/-Обробка_природної_мови
3. AI programming tools. *Google AI*. URL: https://ai.google/tools/
4. GitHub Copilot. *GitHub*. URL: https://github.com/features/copilot
5. Goodfellow I., Bengio Y., Courville A. Deep Learning. Cambridge : MIT Press, 2016. 800 p.

УДК 004.75

Когут Богдан,
студент ІІІ курсу спеціальності
121 Інженерія програмного забезпечення,
ЗВО «Університет Короля Данила»
Науковий керівник:
Куцела Марія,
старша викладачка кафедри іноземної
філології та бізнес-комунікацій,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: 0009-0002-1225-2988

ПЕРЕВАГИ ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ У СУЧАСНОМУ БІЗНЕСІ

Вступ. Хмарні обчислення міцно увійшли в повсякденне життя кожного користувача Інтернету та стали рушійною силою для трансформації сучасного бізнесу [3, с. 2]. Використання віддалених ресурсів дозволяє підприємствам відмовитися від утримання дорогої власної ІТ-інфраструктури

на користь орендованих сервісів. Метою цих тез є аналіз переваг хмарних рішень та основних моделей їх впровадження на основі актуальних наукових джерел.

Основна частина. Хмарні технології визначаються як сукупність методів, засобів і прийомів, використовуваних для збирання, систематизації, зберігання та опрацювання на віддалених серверах, а також передавання через мережу і подання через клієнтську програму повідомлень і даних [1, с. 42]. Однією з ключових переваг для бізнесу є висока економічна ефективність. За експертними оцінками, впровадження хмарних обчислень дозволяє у три-п'ять разів скоротити вартість експлуатації бізнес-додатків [3, с. 2]. Крім того, логічна консолідація ресурсів у хмарі забезпечує централізоване управління критично важливими системами підприємства [3, с. 4].

Важливим фактором є звільнення компаній від необхідності постійно купувати нові комп’ютери для забезпечення високої продуктивності та від складнощів у налаштуванні комплексних систем [3, с. 72]. Це стає можливим завдяки розвитку технології віртуалізації, що дозволяє створювати гнучку інфраструктуру з можливістю швидкого масштабування [3, с. 72]. У сучасній бізнес-практиці найчастіше застосовують три основні моделі обслуговування, а саме: інфраструктуру як сервіс (IaaS), платформу як сервіс (PaaS) та програмне забезпечення як сервіс (SaaS) [2, с. 38–40].

Використання хмарних сервісів також сприяє створенню мобільного робочого середовища. Це дозволяє співробітникам розпочинати проєкт в офісі та продовжувати його вдома без фізичної передачі файлів на зовнішніх носіях [1, с. 42]. Таким чином, підприємства отримують можливість гнучко керувати робочим часом та ресурсами, підвищуючи загальну ефективність процесів.

Висновки. Отже, хмарні технології забезпечують бізнесу високу конкурентоспроможність завдяки суттєвому зниженню витрат на ІТ-супровід та гнучкості управління ресурсами [3, с. 72]. Подальший розвиток хмарних рішень тісно пов'язаний із розширенням пропускної здатності мереж та вдосконаленням систем захисту даних.

Список використаних джерел:

1. Маркова О. М., Семеріков С. О., Стрюк А. М. Хмарні технології навчання: витоки. *Інформаційні технології і засоби навчання*. 2015. Том 46. № 2. С. 29–44.

2. Ількевич Н. С. Хмарні технології в освіті : навч.-метод. посіб. Житомир : Вид-во ЖДУ, 2021. 88 с.

3. Зінченко О. В., Прокопов С. В., Сєрих С. О. та ін. Хмарні технології : навч. посіб. Київ : ФОП Гуляєва В. М., 2020. 73 с.

УДК 004.056.5:004.93'1

Кучера Олександр,
студент IV курсу спеціальності
F2 Інженерія програмного забезпечення,
ЗВО «Університет Короля Данила»
Науковий керівник:
Стисло Тарас,
кандидат юридичних наук,
доцент кафедри IT,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна

КОНФІДЕНЦІЙНЕ РОЗПІЗНАВАННЯ: МЕТОДИ АНОНІМІЗАЦІЇ ТА ЗАХИСТУ БІОМЕТРИЧНИХ ШАБЛОНІВ У СИСТЕМАХ МАШИННОГО НАВЧАННЯ

Стрімке поширення систем біометричної ідентифікації – від розблокування смартфонів до контролю доступу на об'єктах критичної інфраструктури – загострює питання захисту персональних даних. На відміну від паролів чи PIN-кодів, біометричні характеристики є незмінними: скомпрометований вектор ознак обличчя не може бути «замінений» так само як замінюється пароль. Це зумовлює необхідність принципово нових підходів до зберігання та обробки таких даних.

Постановка проблеми. Традиційні системи розпізнавання облич зберігають або вихідні зображення, або їхні числові вектори-ембедінги у відкритому вигляді. У разі витоку бази даних зловмисник отримує можливість відтворити обличчя користувача або здійснити атаку повторного відтворення (replay attack). Проблема посилюється тим, що сучасні генеративні нейронні мережі здатні відновити фотореалістичне зображення навіть із частково перехопленого вектора ознак [1].

Мета дослідження – розглянути та порівняти методи захисту біометричних шаблонів, що унеможливлюють відновлення зображення обличчя навіть у разі повного компрометування сховища даних.

Основні результати.

1. Від зображень до незворотних векторів. Нейронні мережі FaceNet перетворюють фотографію обличчя на компактний числовий вектор (128–512 вимірів). Ідентифікація здійснюється через порівняння векторів без звернення до оригінальних фото. Ключовий принцип: система повинна зберігати **лише захищений шаблон**, але не саме зображення [2].

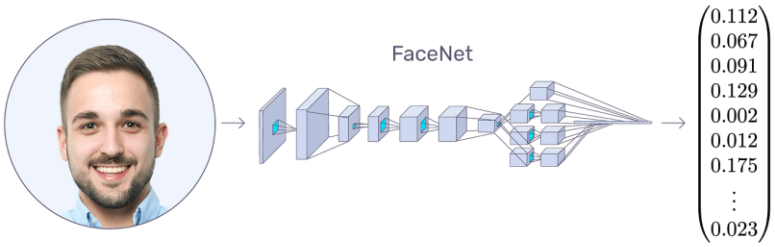

Рис. 1. Процес перетворення вхідного зображення у векторне відображення

Рис. 2. Процес від зображень до незворотних векторів

2. Fuzzy Commitment / Fuzzy Vault. Схеми криптографічного зв'язування (biometric cryptosystems) поєднують біометричний вектор із криптографічним ключем таким чином, що відновити ключ можна лише за умови пред'явлення «достатньо схожого» біометричного зразка. База даних містить лише зашифровані допоміжні дані (helper data), з яких відновлення оригінального вектора є обчислювально неможливим [3].

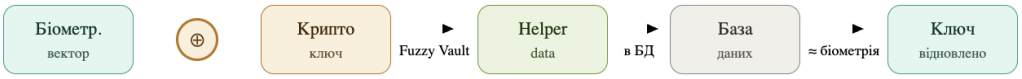

Рис. 3. Процес криптографічного зв’язування

3. Cancelable Biometrics (скасовувана біометрія). Метод передбачає незворотне перетворення вектора ознак за допомогою параметрованої функції (BioHashing або рандомізованих проєкцій). Зберігається лише **трансформований шаблон**. У разі витоку трансформацію (ключ) відкликають і генерують нову без заміни біометрії користувача. Це вирішує головну слабкість незмінних біометричних даних [4].

Рис. 4. Процес скасовуваної біометрії

4. Гомоморфне шифрування та обчислення в зашифрованому просторі. Сучасні схеми (CKKS, BFV) дозволяють обчислювати косинусну подібність між векторами безпосередньо у зашифрованому просторі. Сервер ніколи не отримує доступу до відкритих векторів – порівняння виконується над шифротекстами, а результат розшифровується лише на стороні клієнта. Це усуває поверхню атаки на сервер [5].

5. Федеративне навчання та локальна обробка. Архітектура on-device inference (TensorFlow Lite, Core ML) дозволяє виконувати розпізнавання безпосередньо на пристрої користувача. На сервер передається лише бінарний результат автентифікації або зашифрований вектор, але не зображення. Федеративне навчання моделі не потребує централізованого зберігання біометрії.

6. Загрози та контрзаходи. Навіть захищені шаблони залишаються вразливими до *інверсійних атак* (reconstruction attacks), де GAN-моделі намагаються відновити зображення із вектора. Ефективними протизаходами є: додавання диференційованого шуму (differential privacy), мінімізація розмірності вектора до функціонально необхідного рівня та обмеження кількості запитів до системи (rate limiting) [6].

Висновки. Захист біометричних шаблонів є обов'язковою складовою будь-якої системи розпізнавання облич, що відповідає сучасним вимогам кібергігієни. Поєднання скасовуваної біометрії з гомоморфним шифруванням та локальною обробкою формує багаторівневий захист: навіть за повного злому серверної інфраструктури зловмисник отримує лише математичні артефакти, з яких неможливо відновити обличчя жодного користувача. Впровадження таких підходів є ключовою умовою відповідального використання технологій штучного інтелекту в публічному та корпоративному секторах.

Список використаних джерел:

1. A Beginner’s Guide to Vector Embeddings. *Tigerdata*. URL: https://www.tigerdata.com/blog/a-beginners-guide-to-vector-embeddings (дата звернення: 11.03.2026).

2. Agarwal D. Creating a Face Recognition System with MTCNN, FaceNet, and Milvus. *Medium*. URL: https://medium.com/@devraj.agarwal/creating-a-face-recognition-system-with-mtcnn-facenet-and-milvus-e155c36d8852 (дата звернення: 11.03.2026).

3. Biometrics. *Wikipedia*. URL: https://en.wikipedia.org/wiki/Biometrics (дата звернення: 12.03.2026).

4. Cancelable biometrics. *Scholarpedia*. URL: http://www.scholarpedia.org/article/-Cancelable_biometrics (дата звернення: 12.03.2026).

5. Homomorphic Encryption With CKKS and BFV For The Inner Product of Two Vectors. *Medium*. URL: https://medium.com/asecuritysite-when-bob-met-alice/homomorphic-encryption-with-ckks-and-bfv-for-the-inner-product-of-two-vectors-ffbdb94753c3 (дата звернення: 13.03.2026).

6. Reconstruction attack. *Wikipedia*. URL: https://en.wikipedia.org/wiki/Reconstruction_attack (дата звернення: 13.03.2026).

УДК 004.76

Легдан Микола,
студент І курсу спеціальності
121 Інженерія програмного забезпечення,
ЗВО «Університет Короля Данила»
Науковий керівник:
Іванов Олександр,
завідувач кафедри інформаційних технологій,
доктор філософії,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0003-4678-7956

CLOUD FIRST: ХМАРНІ ОБЧИСЛЕННЯ ЯК АРХІТЕКТОР ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Хмарні обчислення сьогодні є не просто технологічним трендом, а фундаментом для побудови сучасних цифрових екосистем. Це модель надання повсюдного та зручного доступу до мережевого пулу спільних обчислювальних ресурсів (наприклад, мереж, серверів, сховищ, прикладних програм і сервісів), які можуть бути оперативно надані з мінімальними зусиллями з управління. В основі хмарної архітектури лежать три ключові моделі обслуговування, порівняння яких наведено нижче (Таблиця 1).

Таблиця 1

Порівняльна характеристика моделей хмарних послуг

Характеристика	**IaaS**	**PaaS**	**SaaS**
Що надається	Віртуальні машини, мережі	Платформи для розробки	Готові додатки
Керування ОС	Користувач контролює ОС	Провайдер керує ОС	Провайдер керує всім
Цільова аудиторія	Адміністратори	Розробники ПЗ	Кінцеві користувачі
Приклади	Amazon EC2, Azure VMs	Google App Engine	Gmail, Slack, Zoom

Перехід до стратегії «Cloud First» зумовлений значними економічними перевагами. Модель оплати Pay-as-you-go дозволяє компаніям платити лише за реально використані ресурси. Масштабованість системи

забезпечує стабільну роботу під час пікових навантажень. Особливого значення хмари набувають у синергії з іншими технологіями. Навчання великих мовних моделей штучного інтелекту (AI) потребує гігантських потужностей, які економічно виправдано отримувати через хмарних провайдерів. При цьому критично важливою залишається модель спільної відповідальності за безпеку даних [1, с. 3]. Майбутнє технології полягає у розвитку Serverless рішень, де розробники фокусуються виключно на коді та гібридних хмарах, що поєднують безпеку приватних інфраструктур із гнучкістю публічних сервісів [2].

Список використаних джерел:

1. Mell P., Grance T. The NIST Definition of Cloud Computing. *National Institute of Standards and Technology*. 2011. Special Publication 800-145. 7 p. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (дата звернення: 14.03.2026).

2. Top Strategic Technology Trends for 2024: Cloud-Native Platforms. *Gartner*. URL: https://www.gartner.com/en/articles/gartner-top-10-strategic-technology-trends-for-2024 (дата звернення: 14.03.2026).

УДК 658.5:004.89

Лисенко Тетяна,
доцент кафедри управління та адміністрування,
кандидат технічних наук, доцент,
ННІ Дніпровський металургійний інститут
Українського державного університету науки і технологій
ORCID: https://orcid.org/0009-0006-2233-8792
Мироненко Микола,
професор кафедри управління та адміністрування,
кандидат технічних наук, доцент,
ННІ Дніпровський металургійний інститут
Українського державного університету науки і технологій
ORCID: https://orcid.org/0000-0001-6316-6778
Усіченко Ірина,
доцент кафедри управління та адміністрування,
кандидат фізико-математичних наук, доцент,
ННІ Дніпровський металургійний інститут
Українського державного університету науки і технологій,
м. Дніпро, Україна
ORCID: https://orcid.org/0009-0000-8664-8024

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УПРАВЛІННІ ВИРОБНИЧИМ ПІДПРИЄМСТВОМ

Головний тренд розвитку світової економіки початку 2020-х років в Україні та світі – масове використання технологій на базі штучного інте-

лекту (ШІ). Головна позитивна риса у запровадженні таких технологій полягає у переході від реактивного управління підприємством (виправлення помилок після їх здійснення) до проактивного (попередження ризиків та використання можливостей до того, як вони стануть очевидними для всіх).

Нижче наведемо декілька визначень дефініції «штучний інтелект» з огляду на праці вітчизняних вчених. Заячковська Г. наступним чином визначає суть ШІ – здатність системи правильно інтерпретувати зовнішні дані, навчатися [1]. Пчелянський Д. та Воінова С. трактують поняття ШІ як науковий напрям, в рамках якого ставляться і вирішуються задачі апаратного або програмного моделювання тих видів людської діяльності, які традиційно вважаються інтелектуальними [2]. Натомість Мар'єнко М. та Коваленко В. у своїй статті зазначають, що ШІ являє собою інструментарій системи чи сервісу, з використанням якого можна збирати й адаптувати дані користувача (або дані, що розміщені у відкритих репозиторіях), та на їх основі генерувати нові рішення чи висновки, відповідно до поданого запиту користувача [3].

З огляду на наведені вище визначення дефініції «штучний інтелект», найбільш перспективною сферою застосування останнього є маркетингова діяльність. Впровадження ШІ у маркетингову діяльність підприємства відкриває нові можливості для ефективної комунікації з клієнтами, підвищення рівня персоналізації та оптимізації бізнес-процесів.

Сутність етапів механізму інтеграції штучного інтелекту у систему маркетингової діяльності підприємств охоплює кілька ключових аспектів. На початковому етапі здійснюється аналіз потреб і можливостей, де проводиться вивчення ринку та виявлення потреб споживачів.

Наступним кроком є визначення цілей і вимог. Тут формуються чіткі цілі впровадження штучного інтелекту, а також визначаються специфікації для технологій, що їх підтримуватимуть. Оцінка доступних технологій є критично важливим етапом, на якому аналізується ринок технологій, щоб ідентифікувати найбільш релевантні рішення, що відповідають встановленим вимогам. Це допомагає уникнути помилок при виборі технологій і гарантує, що впроваджені рішення будуть ефективними.

Передостанній етап – повномасштабне впровадження, а також проводиться навчання персоналу для забезпечення максимальної ефективності.

Останній етап механізму інтеграції штучного інтелекту у систему маркетингової діяльності підприємства передбачає постійний моніторинг та вдосконалення. Регулярна оцінка впроваджених технологій і їх

адаптація до змін у ринку та споживчих потребах забезпечує тривалу ефективність і конкурентоспроможність бізнесу.

Означимо проміжні підсумки. По-перше, використання штучного інтелекту забезпечує можливість персоналізації обслуговування клієнтів, що сприяє підвищенню їх задоволеності та лояльності.

По-друге, підвищується ефективність інвестицій у нові технології та знижуються ризики, пов'язані з їх впровадженням.

По-третє, етапи механізму забезпечують структуровану реалізацію процесу, починаючи з початкового аналізу і закінчуючи постійним моніторингом. Це сприяє безперервному вдосконаленню бізнес-процесів, що є критично важливим для підтримки конкурентоспроможності на ринку, де компанії, які впроваджують нові технології, можуть значно випереджати своїх конкурентів.

Необхідно зазначати, що поряд з перевагами, які можна отримати від застосування ШІ у маркетинговій діяльності підприємства, існують і певні ризики, зокрема, потенційна втрата конфіденційності даних та надмірна залежність від технологій, що може негативно позначитися на конкурентоспроможності.

Не варто надмірно захоплюватися ідеєю технології штучного інтелекту як «пігулки молодості» чи «срібної кулі», яка сама по собі здатна вирішити будь-які проблеми господарської діяльності підприємства. Варто пам'ятати, що це лише інструмент з ефективної обробки великого масиву даних та напрацювання пропозицій щодо їхнього подальшого використання. Остаточне ж рішення залишається за керівником підприємства.

Список використаних джерел:

1. Заячковська Г. А. Маркетингові можливості підприємств на основі штучного інтелекту. *Трансформаційна економіка*. 2024. № 2 (07). С. 17–22.

2. Пчелянський Д. П., Воінова С. А. Штучний інтелект: перспективи та тенденції розвитку. *Automation of Technological and Business Processes*. № 11 (3). С. 59–64.

3. Мар'єнко М. В., Коваленко В. В. Штучний інтелект та відкрита наука в освіті. *Фізико-математична освіта.* 2023. № 38 (1). С. 48–53.

УДК 37.018:004.738.5:004.67

Листопад Олексій,
завідувач кафедри дошкільної педагогіки,
доктор педагогічних наук, професор,
Державний заклад «Південноукраїнський національний
педагогічний університет імені К. Д. Ушинського»,
м. Одеса, Україна
ORCID: https://orcid.org/0000-0002-3121-324X

SMART-ІНФРАСТРУКТУРА ОСВІТИ: ПОТЕНЦІАЛ ІНТЕРНЕТУ РЕЧЕЙ У СТВОРЕННІ ІНТЕЛЕКТУАЛЬНИХ ОСВІТНІХ ЕКОСИСТЕМ

Цифрова трансформація сучасного суспільства суттєво впливає на розвиток освітніх систем [3, с. 24]. В умовах формування цифрової економіки та інформаційного суспільства зростає потреба у впровадженні інноваційних технологій, що забезпечують ефективну організацію освітнього процесу, підвищення якості управління закладами освіти та створення нових можливостей для організації освітнього процесу [2, с. 259]. Однією з ключових технологій, що активно інтегрується в різні сфери суспільного життя, є Інтернет речей. Інтернет речей як технологія передбачає взаємодію фізичних пристроїв, сенсорів, програмного забезпечення та мережевих сервісів, які забезпечують автоматичний обмін даними та управління різними процесами [5].

У сфері освіти використання Інтернету речей відкриває нові можливості для створення smart-інфраструктури, що передбачає інтеграцію інтелектуальних систем управління освітнім середовищем закладу освіти, цифрових платформ та мережевих технологій. У результаті формується інтелектуальна освітня екосистема, яка поєднує технологічні, педагогічні та управлінські ресурси [1, с. 56].

Smart-інфраструктура освіти розглядається як комплекс технологічних та організаційних рішень, що забезпечують інтеграцію цифрових технологій в освітній процес. Вона включає: цифрові платформи управління освітнім процесом; системи автоматизованого моніторингу освітнього середовища; інтерактивні та мультимедійні засоби навчання; мережеву взаємодію пристроїв і сервісів [1, с. 56]. Інтернет речей виступає важливим елементом такої інфраструктури, оскільки дозволяє забезпечити взаємодію між різними технологічними компонентами освітнього середовища [5]. Використання Інтернету речей в освіті сприяє: автоматизації управлінських процесів; оптимізації використання ресурсів; підвищенню ефективності освітньої діяльності; створенню персоналізованого освітнього середовища

[5]. Отже, формування smart-інфраструктури є одним із стратегічних напрямів розвитку сучасної освіти.

Сучасні заклади освіти поступово впроваджують технології Інтернету речей з метою модернізації освітнього середовища та підвищення ефективності організації освітнього процесу. Використання Інтернету речей дає можливість інтегрувати різноманітні цифрові пристрої, сенсорні системи та програмні сервіси в єдину інтелектуальну інфраструктуру закладу освіти. У межах такої інфраструктури можна виокремити кілька основних напрямів застосування цих технологій [5].

Одним із найбільш поширених напрямів є створення «розумних» освітніх аудиторій (smart-аудиторій), які передбачають використання інтерактивних панелей, сенсорних систем освітлення, клімат-контролю та автоматизованих засобів керування навчальним обладнанням. Наприклад, сенсорні системи можуть автоматично регулювати освітлення та температуру у приміщенні залежно від кількості студентів або часу доби, що сприяє створенню комфортних умов для навчання та підвищує ефективність освітнього процесу.

Наступним важливим напрямом є використання Інтернету речей для моніторингу та управління освітнім процесом. Інтернет речей дозволяє створювати системи автоматизованого збору та аналізу даних про використання освітніх ресурсів, відвідування занять та освітню активність студентів. Зокрема, такі системи можуть використовувати електронні картки, мобільні додатки або сенсорні пристрої для фіксації присутності студентів і подальшого аналізу освітніх показників.

Більш комплексною формою впровадження Інтернету речей у сфері освіти є концепція smart-кампусу, яка передбачає інтеграцію цифрових технологій в управління всією інфраструктурою закладу освіти. До її основних елементів належать автоматизовані системи доступу до будівель, системи відеоспостереження, енергозберігаючі технології, а також цифрові сервіси для студентів і викладачів. Наприклад, студент може отримати доступ до бібліотеки або лабораторії за допомогою електронного студентського квитка чи мобільного додатку, що значно спрощує взаємодію здобувача освіти з інфраструктурою закладу освіти.

Окрім управлінських та інфраструктурних можливостей, Інтернет речей відкриває нові перспективи для персоналізації освітнього процесу. Завдяки збору та аналізу даних про освітню діяльність студентів з'являється можливість формування індивідуальних освітніх траєкторій студентів. Отримані аналітичні дані допомагають викладачам визначати рівень навчальних досягнень студентів, виявляти їхні освітні потреби та своєчасно

коригувати організацію освітнього процесу з урахуванням індивідуальних освітніх траєкторій студентів.

Використання Інтернету речей у сфері освіти має низку переваг: підвищення ефективності управління закладом освіти; оптимізація використання ресурсів; створення інноваційного освітнього середовища; підвищення якості освітнього процесу. Водночас існують певні виклики, серед яких: питання кібербезпеки та захисту персональних даних; необхідність розвитку цифрової інфраструктури; потреба у підготовці педагогічних кадрів до використання нових технологій; фінансові витрати на впровадження smart-систем. Тому впровадження Інтернету речей потребує комплексного підходу, що включає технічні, організаційні та педагогічні аспекти.

Інтернет речей виступає важливим технологічним чинником розвитку smart-інфраструктури сучасної освіти. Інтеграція Інтернету речей сприяє створенню інтелектуальних освітніх екосистем, які забезпечують ефективну взаємодію між учасниками освітнього процесу, цифровими платформами та інфраструктурними ресурсами. Використання smart-технологій дозволяє модернізувати освітнє середовище, підвищити якість управління закладами освіти та створити умови для персоналізації освітнього процесу.

Список використаних джерел:

1. Дзень В. Є., Борзов Ю. О., Дзень Д. Є. Інтеграція smart-систем в освітнє середовище закладів вищої освіти. *Вісник Львівського державного університету безпеки життєдіяльності*. 2024. Том 30. С. 56–66. DOI: https://doi.org/https://doi.org/10.32447/20784643.30.2024.06

2. Листопад О. А., Мардарова І. К., Листопад Н. Л Розвиток інформаційно-комунікаційних технологій та їх інтеграція в освітню практику: історичний контекст і сучасні тенденції. *Вісник Глухівського національного педагогічного університету імені Олександра Довженка. Педагогічні науки.* 2025. Вип. 2. № 58. С. 259–272. DOI: https://doi.org/10.31376/2410-0897-2025-2-58-259-272

3. Листопад О. А., Мардарова І. К., Листопад Н. Л. Особливості застосування мультимедійних технологій в процесі формування цифрової культури здобувачів вищої і фахової передвищої освіти. *Вісник Глухівського національного педагогічного університету імені Олександра Довженка. Педагогічні науки.* 2024. Вип. 4 (56). С. 24–33. DOI: https://doi.org/10.31376/2410-0897-2024-3-56-24-33

4. Листопад О., Листопад Н. Організація дистанційного навчання на платформі Moodle: теорія та практика. *Науковий вісник Ізмаїльського державного гуманітарного університету. Педагогічні науки.* Ізмаїл : РВВ ІДГУ, 2025. Вип. 70. С. 145–155. DOI: https://doi.org/10.31909/26168812.2025-(70)-20

5. Жураковський Б. Ю., Зенів І. О. Технології інтернету речей. Навчальний посібник : навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології», спеціалізація «Інформаційне забезпечення робототехнічних систем». Київ : КПІ ім. Ігоря Сікорського, 2021. 271 с. (дата звернення: 09.04.2026).

УДК 331.101.262

Михальчук Станіслав,
студент ІІ курсу, КІПЗс-24-1,
Фаховий коледж ЗВО «Університет Короля Данила»
Романюк Станіслав,
студент І курсу, ІПЗс-25-1,
ЗВО «Університет Короля Данила»
Науковий керівник:
Шкатуляк Василь,
асистент кафедри інформаційних технологій,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна

ПРАКТИЧНЕ ВИКОРИСТАННЯ AI-СЕРВІСІВ У НАВЧАННІ, РОБОТІ ТА ТВОРЧОСТІ

Стрімкий розвиток технологій штучного інтелекту у 2022–2026 роках зумовив якісний перехід від вузькоспеціалізованих алгоритмів до універсальних мовних моделей (LLM). За даними McKinsey Global Institute (2024), понад 72 % компаній у світі вже інтегрували AI-рішення у свої процеси, а обсяг глобального ринку ШІ до 2030 року прогнозується на рівні 1,8 трлн доларів США [1]. В основі сучасних сервісів лежать нейронні мережі трансформерної архітектури, додатково налаштовані методом RLHF (Reinforcement Learning from Human Feedback) для підвищення якості та безпечності відповідей [2; 3].

В освіті AI забезпечує персоналізоване пояснення матеріалу, семантичний пошук по наукових базах і автоматичну генерацію тестових запитань – студенти, що використовують AI для самотестування, демонструють на 18 % вищі результати [6]. У професійній діяльності фахівці з GPT-4 виконували на 25 % більше завдань за той самий час [7], а GitHub Copilot підвищує швидкість написання коду на 55 %. У творчості моделі Midjourney, Suno та ElevenLabs стали доступним інструментом для створення зображень, музики та озвучення без спеціальної підготовки.

У рамках цієї роботи я розробив власний проєкт – Echo, інтелектуальну систему аналізу відгуків. Вона автоматично збирає відгуки з різних інтернет-джерел, обробляє їх за допомогою NLP-алгоритмів, відбирає найрелевантніші та генерує узагальнений підсумок із посиланнями на оригінали. Це дозволяє користувачу миттєво отримати об'єктивну думку про продукт без необхідності переглядати десятки розрізнених відгуків.

Розробка Echo стала для мене практичним підтвердженням того, що сучасні AI-інструменти дають змогу реалізовувати повноцінні прикладні рішення навіть без великої команди.

Водночас ефективне використання AI потребує розуміння його обмежень: моделі можуть генерувати впевнено сформульовану хибну інформацію («галюцинації»), введення конфіденційних даних у публічні сервіси створює ризики витоку, а правовий статус AI-згенерованого контенту залишається неврегульованим [10]. AI є підсилювачем людських можливостей, а не їх замінником – і саме поєднання власної експертизи з AI-інструментами за умови збереження критичного мислення забезпечує реальну конкурентну перевагу.

Список використаних джерел:

1. The State of AI in 2024. *McKinsey Global Institute.* 2024. URL: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai
2. Vaswani A., Shazeer N., Parmar N., Uszkoreit J., Jones L., Gomez A. N., Kaiser Ł., Polosukhin I. Attention Is All You Need. *NeurIPS*. 2017. URL: https://arxiv.org/abs/1706.03762
3. Ouyang L., Wu J., Jiang X., Almeida D., Wainwright C., Mishkin P. та ін. Training language models to follow instructions with human feedback. *arXiv*. 2022. URL: https://arxiv.org/abs/2203.02155
4. Khan Academy. Khanmigo. 2024. URL: https://www.khanacademy.org/khan-labs
5. Google. NotebookLM. 2024. URL: https://notebooklm.google.com
6. Bastani H., Kim J., Kim M., Lam W., Stiglitz J. та ін. Generative AI Can Harm Learning. *Wharton School of the University of Pennsylvania*. 2024. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4895486
7. Dell'Acqua F., Gans J., Stern S., Yoffie D. B. Navigating the Jagged Technological Frontier. *Harvard Business School*. 2023. URL: https://www.hbs.edu/ris/Publication%20Files/-24-013_d9b45b68-9e74-42d6-a1c6-c72fb70c7282.pdf
8. Nori H., King N., McKinney S. M., Carignan D., Horvitz E. Can LLMs Provide Medical Advice? *Microsoft Research*. 2023. URL: https://arxiv.org/abs/2311.05112
9. Choi J. H., Hickman K. E., Monahan J., Schwarcz D. GPT-4 Passes the Bar Exam. *SSRN*. 2023. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4389233
10. Andersen et al. v. Stability AI Ltd. *U.S. District Court, N.D. Cal.* Case No. 3:23-cv-00201. 2023.

УДК 004.056:004.7

Мохнатчук Василь,
студент ІІІ курсу спеціальності
121 Інженерія програмного забезпечення,
ЗВО «Університет Короля Данила»
Науковий керівник:
Кавацюк Костянтин,
викладач кафедри інформаційних технологій,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0009-0009-5041-9989

БЕЗПЕКА В ЕКОСИСТЕМІ IOT: ЗАХИСТ SMART-ТЕХНОЛОГІЙ ВІД КІБЕРЗАГРОЗ

Технології Інтернету речей (IoT) швидко розвиваються і об'єднують мільйони пристроїв у глобальну мережу. Штучний інтелект пришвидшує цей процес і допомагає краще автоматизувати підприємства [1, с. 165]. Але через велику кількість IoT-пристроїв ними часто цікавляться кіберзлочинці. Тому розробники та користувачі мають першочергово думати про захист смарттехнологій.

Мережа IoT має багато слабких місць. Зловмисники атакують три основні рівні: рівень сприйняття, мережу та самі програми [4, с. 78]. Часто пристрої мають слабкі паролі або взагалі не шифрують дані [4, с. 78-79].

Бездротовий зв'язок зламати найпростіше. Зловмисники глушать сигнал через WiFi-jammer і викликають відмову в обслуговуванні (DoS) [5, с. 101]. Також вони перехоплюють відео, яке камери передають без шифрування через протокол RTSP. Для цього використовують атаку Man-in-the-Middle, щоб підмінити відео або вкрасти приватну інформацію [5, с. 102].

Більшість IoT-пристроїв мають слабкі процесори і мало пам'яті. Через це на них важко поставити класичний криптографічний захист [3, с. 125].

Щоб зробити систему безпечною, треба захищати її на кількох рівнях. Наприклад, модель безпеки Cisco пропонує чотири рівні: керування доступом, захист від втручання, захист даних та захист інтернет-протоколів [2, с. 48]. Для шифрування зв'язку добре підходить алгоритм AES-256-GCM. Він швидко обробляє дані та надійно перевіряє справжність повідомлень [2, с. 50].

Також розробники використовують легку криптографію. Наприклад, шифр Вернама дає абсолютну стійкість і надійно шифрує дані навіть на дуже слабких мікроконтролерах [3, с. 131]. Для домашніх мереж найкраще

працює дворівневий захист. Він шифрує локальні з'єднання через AES, а для зв'язку зі світом через MQTT-брокер використовує SSL/TLS [6, с. 176]. Система сама регулярно змінює ключі AES, щоб їх не вкрали. А про всі підозрілі події вона одразу пише користувачу в Telegram [6, с. 177].

Світ активно створює стандарти для безпеки IoT. Наприклад, європейський стандарт ETSI EN 303 645 забороняє ставити звичайні паролі та вимагає регулярно оновлювати програми [7, с. 8]. США запровадили маркування “Cyber Trust Mark”, щоб покупці відразу бачили рівень захисту пристрою [7, с. 7]. Євросоюз посилює контроль через нові закони, як-от Cyber Resilience Act, який змушує виробників сертифікувати мережеве обладнання [7, с. 30].

Щоб надійно захистити IoT-інфраструктуру, треба поєднувати апаратні та програмні рішення. Легка криптографія і дворівневий локальний захист добре допомагають відбивати атаки. А міжнародні стандарти та маркування безпеки змушують виробників робити свої смартпристрої справді захищеними.

Список використаних джерел:

1. Данкевич В. Є., Данкевич А. Є. Інтернет речей та штучний інтелект як ключові елементи інноваційного розвитку підприємств в епоху цифрових викликів. *Актуальні проблеми економіки*. 2024. № 7 (277). С. 165-173. URL: http://eztuir.ztu.edu.ua/123456789/8-609 (дата звернення: 11.03.2026).
2. Дудикевич В., Микитин Г., Мурак Т. Інтегральна модель безпеки Інтернету речей у просторі інтелектуалізації об'єктів інфраструктури. *Кібербезпека: освіта, наука, техніка*. 2025. Т. 4, № 28. С. 41-56. URL: https://doi.org/10.28925/2663-4023.2025.28.848 (дата звернення: 11.03.2026).
3. Черненко Р. М., Рябчун О. П., Ворохоб М. В., Аносов А. О., Козачок В. А. Підвищення рівня захищеності систем мережі Інтернету речей за рахунок шифрування даних на пристроях з обмеженими обчислювальними ресурсами. *Кібербезпека: освіта, наука, техніка.* 2021. № 3. С. 124-135. URL: http://nbuv.gov.ua/UJRN/cest_2021_3_12 (дата звернення: 11.03.2026).
4. Коваленко А. А., Ярошевич Р. О., Баленко О. І. Internet of Things: Проблеми інформаційної безпеки та методи покращення. *Системи управління, навігації та зв'язку.* 2021. Т. 2, № 64. С. 78-80. URL: https://doi.org/10.26906/SUNZ.2021.2.078 (дата звернення: 11.03.2026).
5. Олійник Я., Платоненко А., Черевик В., Ворохоб М., Шевчук Ю. Методи захисту інформації в технологіях IoT. *Кібербезпека: освіта, наука, техніка.* 2025. Т. 3, № 27. С. 100-108. URL: https://doi.org/10.28925/2663-4023.2025.27.705 (дата звернення: 11.03.2026).
6. Шелуха О. О., Квашук Д. М., Супруненко К. О. Дворівнева система захисту домашньої IoT-мережі. *Технічна інженерія*. 2024. № 2 (94). С. 174-179. URL: https://doi.org/10.26642/ten-2024-2(94)-174-179 (дата звернення: 12.03.2026).
7. Hennessy H. Consumer IoT Device Cybersecurity Standards, Policies, and Certification Schemes 2025. Omdia, 2025. 51 p. URL: https://omdia.tech.informa.com/commissioned-research/articles/consumer-iot-device-cybersecurity-standards-policies-and-certification-schemes-2025 (дата звернення: 12.03.2026).

УДК 004.8

Паращин Всеволод,
студент ІІІ курсу спеціальності
121 Інженерія програмного забезпечення,
ЗВО «Університет Короля Данила»
Науковий керівник:
Василенко Владислав,
викладач кафедри інформаційних технологій,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна

ЯК ШТУЧНИЙ ІНТЕЛЕКТ МОЖЕ ЗМІНИТИ ВІЙНУ

Вступ та актуальність. Війна Росії проти України вже довела, що масове застосування дронів, сенсорів і автоматизованих систем змінює логіку бойових дій швидше, ніж військові доктрини встигають адаптуватися. Саме в цьому контексті американський аналітичний центр RAND оприлюднив звіт про те, як ШІ може трансформувати методи, за допомогою яких армії воюватимуть і здобуватимуть перемогу у війнах майбутнього.

Мета дослідження. Ключова ідея звіту полягає в тому, що штучний інтелект стане технологією загального призначення, подібною за значенням до електрики або двигуна внутрішнього згоряння. Вона не створює одну «чарівну» зброю, а буде пронизувати всі аспекти військової діяльності – від розвідки до логістики та управління. Тому для аналізу її впливу автори застосовують підхід «будівельних блоків», виокремлюючи чотири базові дилеми протистояння, які лежать в основі сучасної війни:

- кількість проти якості;
- приховування проти виявлення;
- централізоване проти децентралізованого командування і управління;
- кібератака проти кіберзахисту.

Ці дилеми не є взаємовиключними альтернативами, але саме в них ШІ змінює відносні переваги сторін і змушує армії робити стратегічні вибори в умовах обмежених ресурсів.

Кількість проти якості: зсув на користь масовості.

Найбільш контроверсійний, але водночас центральний висновок звіту: ШІ змінює баланс між кількістю та якістю на користь кількості. Упродовж десятиліть західні армії, передусім США, робили ставку на невелику

кількість надзвичайно дорогих і високотехнологічних платформ. ШІ та робототехніка підривають цю логіку. Поєднання «точної маси» (достатньо точні, але дешеві системи) та «доступної масовості» означає, що велика кількість «достатньо ефективних» безпілотних платформ може бути економічно вигіднішою за малу кількість дорогих високотехнологічних систем. Аналітики RAND роблять висновок: пріоритет максимальної якості стає дедалі менш рентабельним, армії, які не зможуть перейти до масштабної роботизованої маси, ризикують програти у війні на виснаження.

Приховування проти виявлення. Штучний інтелект суттєво покращує виявлення цілей завдяки швидкому аналізу величезних масивів даних із різноманітних сенсорів. Водночас ці ж технології дозволяють створювати складні системи маскування та дезінформації, перетворюючись на своєрідні «машини туману війни».

Командування і управління. Незважаючи на високий рівень автоматизації, ШІ не зможе повністю замінити потребу ухвалювати оперативні рішення безпосередньо на місцях. Оптимальним залишиться гібридний підхід («місійне командування»), за якого алгоритми виступають лише потужним підсилювачем, а не повною заміною людського контролю.

Кібератака проти кіберзахисту. На сьогодні інструменти ШІ надають відчутну структурну перевагу саме для проведення швидких та масштабних кібератак. Проте в довгостроковій перспективі очікується, що ці технології докорінно змінять баланс сил, суттєво посиливши саме системи кіберзахисту.

Механізми впливу ШІ на війну

ШІ впливає на військову сферу через кілька базових механізмів:

– По-перше, аналітичне осягнення (insight): здатність швидко обробляти й поєднувати величезні масиви даних значно підвищує обізнаність про бойовий простір.

– По-друге, автономність, тобто заміщення людської когнітивної та фізичної праці машинами, що зменшує втрати й обмеження, пов’язані з людським фактором.

– По-третє, управління складністю: ШІ може координувати дії тисяч платформ або елементів системи там, де людина фізично не здатна діяти з потрібною швидкістю.

– Нарешті, підтримка ухвалення рішень, коли поєднання людського інтелекту і машинного дозволяє швидше й ефективніше обирати варіанти дій.

Важливо, що ці механізми стосуються не лише бойових дій, а й підготовки до війни – виробництва, ремонту, логістики, науково-дослідних робіт. Саме тут ШІ може забезпечити довгострокові структурні переваги.

Висновок. Впровадження штучного інтелекту у військову сферу – це не лише технологічний, а й масштабний організаційний виклик. Для досягнення стратегічної переваги у війнах майбутнього арміям необхідний чіткий план переходу до збройних сил, підсилених ШІ. Вирішальним фактором успіху стане здатність створити ефективний симбіоз, у якому швидкість та аналітична потужність машин гармонійно поєднуватимуться з критичним мисленням і надійністю людського контролю.

Список використаних джерел:

1. Як штучний інтелект може змінити війну. *LB.ua*. 2026. URL: https://lb.ua/society/2026/01/31/719663_yak_shtuchniy_intelekt_mozhe.html (дата звернення: 01.03.2026).
2. Artificial Intelligence and the Future of Warfare. *RAND Corporation*. 2026. URL: https://www.rand.org/ (дата звернення: 01.03.2026).

УДК 004.056.5:316.6

Погорельцева Анна,
студентка ІІ курсу спеціальності
121 Інженерія програмного забезпечення,
ЗВО «Університет Короля Данила»
Науковий керівник:
Іванов Олександр,
завідувач кафедри інформаційних технологій,
доктор філософії,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0003-4678-7956

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ГОЛОВНА ЗАГРОЗА ЦИФРОВОЇ БЕЗПЕКИ КОРИСТУВАЧА

На сьогодні технології розвиваються швидко і застосовуються вони в абсолютно різних цілях. Ці технології можуть як рятувати людські життя, так і використовуватися в своїх незаконних цілях. У цій тезі ми дізнаємося що таке соціальна інженерія, чому вона виникла, які є її типи, як ШІ може залучатися до такої діяльності злочину і які ж ризики цього феномену, як захиститися і підіб'ємо підсумки.

Соціальна інженерія – це метод маніпуляції та обману, який націлений на отримання доступу до конфіденційної та чутливої інформації. Тобто зловмисники, втираючись в довіру і використовуючи необізнаність жертви, хочуть отримати інформацію, якою вони зможуть скористуватися в свою користь або з метою шантажу. Причина її виникнення

доволі проста: шахраї завжди шукали спосіб добиватися свого і адаптувалися до часу та епохи, коли вони орудували, і наш час не є виключенням. Спонукати людину надати необхідну інформацію зі своєї волі набагато простіше, ніж писати віруси і спробувати проникнути в комп'ютер [2]. Існують декілька видів такого шахрайства: фішинг – повідомлення, які імітують надійні джерела, але насправді є підроблені посилання для викрадення паролів та номерів карток; претекстинг – людина прикидається працівником техпідтримки чи іншої служби для отримання інформації; deepfakes – підробка голосу, відео або фото, включно з використанням ШІ для більшої переконливості і збільшення шансу на успіх; «троянський кінь» – вигідна пропозиція в обмін на конфіденційні дані; catfishing – коли зловмисник створює фальшиві фото та дані і створює фейковий профіль людини, найчастіше відбувається на сайтах знайомств. Також ці методи поєднуються з фізичними трюками: бейтінг – провокація, наприклад, підлаштувати ситуацію так, щоб людина спонукалася до дії, наприклад, вигідна пропозиція або цікавість; тейлгейтінг – тобто фізичне проникнення чи в офіс, чи особистий простір, видаючи себе за авторизованого працівника, слідуючи за авторизованою особою; CEO-шахрайство – імітація розпорядження директора через лист з закликом до термінового переказу коштів.

Як вже згадувалося вище, в цей тип шахрайства також залучається ШІ, оскільки через свою потужність він може спростити шахраю задачу. На сьогодні ШІ може генерувати дуже реалістичні голоси і відео людей в певних ситуаціях: наприклад, що ви потрапили в аварію, смертельно хворі, викрадені і просите певну людину про допомогу. Для досвідченого і добре обізнаного в цій темі обман може бути максимально очевидним, але для людини, яка практично нічого не знає про це, і особливо літніх людей, ця фальшивка може бути сприйнята як реальність і зловмисник може добитися свого. Яскравим прикладом цієї лякаючої ефективності є YouTube-відео в форматі Shorts від британського ютубера Mrwhosetheboss, яке називається «I got deepfaked», де він показав відео, де його ніби заарештувала поліція. Навіть я, людина яка передивилася багато подібних відео і можу сказати, що можу відрізнити відео від ШІ доволі легко, на секунду «зависла», настільки реалістичним було те згенероване відео. Також на сьогодні існують навіть ШІ ютубери, співаки і тд., тобто вони здаються реальними на початку, але потім ти різко усвідомлюєш, що це зовсім не так. Також ШІ може стати ідеальним інструментом для кетфішингу, згаданого раніше, створивши нові фото, а не взявши існуючі, які можна знайти з пошуку. Хоч на сьогодні існують деякі сервіси, які можуть відрізнити творіння ШІ, але якісні є платними і про них небагато хто знає.

Навівши всю інформацію, про яку було вказано вище, можна зрозуміти, що ситуація може різко вийти з-під контролю. Окрім вже відомої нам проблеми викрадення грошей, підробки документів та шантажу, це може стати ще більшою проблемою. Уявіть собі ситуацію: хакер використовує ШІ для створення профілю працівника сфери послуг, робить все максимально реалістичним і реєструється на певному сервісі, верифікується і дає наживку. Жертва клюне на наживку і бажатиме оформити послугу, наш хакер кидає хакнуту ссилку під приводом підтвердження даних, угоди користувача і тому подібне, жертва переходить за посиланням. Хакер отримує конфіденційні дані жертви, доступи до всіх акаунтів, пошт, переписок, фінансової інформації. Але ця жертва також може мати доступ до інформації і фінансового статусу державного і навіть міжнародного. Тепер уявіть собі, що ця людина може зробити з цими даними, і це може стати проблемою вже національного масштабу, а в деяких навіть міжнародного.

Знаючи про потужність цієї проблеми, нам варто знати як же правильно захистити себе. Перш за все нам потрібно усвідомлювати, що таке явище існує та навчитися розпізнавати патерни і тактики маніпуляцій. Завжди перевіряти правдивість інформації особи чи компанії, яка нам пише чи зв'язується з нами, впевнитися, що вона справжня і що інформація справді правдива. Можна навіть передзвонити особі і уточнити у неї, чи це вона і чи це правдива інформація. Також варто встановити багаторівневу аутентифікацію для програм і сайтів, де це можливо, щоб зловмисникам було тяжче отримати ваші дані. Забезпечте захист шифруванням і надійними паролям будь-якої важливої інформації.

Підбиваючи підсумки, можна зробити висновок, що соціальна інженерія – цілком реальна і велика загроза, яка потребує серйозного підходу і уважності. Ми завжди маємо бути обачними і уважними до інформації, яку ми отримуємо, і того, хто просить надати нашу інформацію, тільки так ми можемо захистити себе від повної катастрофи.

Список використаних джерел:

1. Соціальна інженерія. *Дія.Освіта*. URL: https://it-osvita.diia.gov.ua/task/item/50fc7ce1-537c-4e3e-a62d-444bcbe57ec5 (дата звернення: 09.03.2026).

2. Соціальна інженерія. Що слід знати про інструменти психологічної маніпуляції, які застосовують шахраї. *StopFraud*. URL: https://stopfraud.gov.ua/cybersecurity-in-work/sotsialnyj-inzhyniryng-i317 (дата звернення: 10.03.2026).

3. Жмурко О. Соціальна інженерія як загроза кібербезпеці: методи запобігання та захисту. *Педагогічна безпека*. 2024. № 1. С. 37–42. URL: https://pedbezpeka.vntu.edu.ua/index.php/pb/article/view/151 (дата звернення: 10.03.2026).

4. Соціальна інженерія як спосіб кібератаки: що потрібно знати. *Avolutech*. URL: https://avolutech.com/blog/соціальна-інженерія-як-спосіб-кібера/ (дата звернення: 10.03.2026).

5. Social Engineering Attacks. *DataLabs UA*. URL: https://datalabsua.com/en/social-engineering-attacks/ (дата звернення: 09.03.2026).

6. Соціальний інжиніринг. Стратегія соціального інжинірингa. Чому необхідно обирати керовану службу соціальних інженерів. *CIT Program*. URL: https://cit-program.com/social-engineering/ (дата звернення: 11.03.2026).

7. Шатковський М. О. Вплив соціальної інженерії на інформаційну безпеку організацій. *Теоретичні і прикладні проблеми фізики, математики та інформатики* : матеріали XIII Всеукр. наук.-практ. конф. студентів, аспірантів та молодих вчених. Київ : НТУУ «КПІ», 2015. С. 216–219.

8. Що таке фішинг? *Microsoft*. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-phishing (дата звернення: 09.03.2026).

9. Фішинг та соціальна інженерія. Як захиститися від кіберзагроз. *Journal Gen Tech*. URL: https://journal.gen.tech/post/sho-take-socialna-ingeneria (дата звернення: 09.03.2026).

10. Соціальна інженерія в епоху генеративного ШІ: як змінилися методи роботи кіберзлочинців. *ProIT*. URL: https://proit.ua/sotsialna-inzhienieriia-v-iepokhughienierativnogho-shi-iak-zminilisia-mietodi-roboti-kibierzlochintsiv (дата звернення: 09.03.2026).

11. Соціальна інженерія. Низка нетехнічних прийомів маніпулювання користувачами, які використовуються кіберзлочинцями під час атак. *ESET*. URL: https://www.eset.com/ua/support/information/entsyklopediya-zahroz/sotsialna-inzheneriya (дата звернення: 09.03.2026).

12. Соціальна інженерія – головний інструмент шахрая. *Національний банк України (Гаразд)*. URL: https://harazd.bank.gov.ua/article/sahrajstvo/platizne-sahrajstvo/socialna-inzeneria-golovnij-instrument-sahraa (дата звернення: 09.03.2026).

13. Соціальна інженерія з точки зору бізнесу – персонал як вразлива ланка. *ESKA Global*. URL: https://eska.global/blog/socialna-inzheneriya-z-tochki-zoru-biznesu-personal-yak-vrazliva-lanka (дата звернення: 12.03.2026).

14. Соціальна інженерія: як шахраї використовують людську психологію в інтернеті. *Радіо Свобода*. URL: https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/-29460139.html (дата звернення: 12.03.2026).

15. Що таке соціальна інженерія? *Binance Academy*. URL: https://www.binance.com/-uk-UA/academy/articles/what-is-social-engineering (дата звернення: 12.03.2026).

16. Що таке соціальна інженерія в кібербезпеці? Реальні приклади та методи запобігання. *Hideez*. URL: https://hideez.com/uk-ua/blogs/news/social-engineering (дата звернення: 12.03.2026).

17. Mrwhosetheboss. I got deepfaked. *YouTube*. 2025. URL: https://www.youtube.-com/shorts/D-bZtJTFzLI (дата звернення: 12.03.2026).

УДК 004.738.5:711.4

Славенюк Данило,
студент І курсу спеціальності
191 Архітектура та містобудування,
ЗВО «Університет Короля Данила»
Науковий керівник:
Дзюба Марина,
доцентка кафедри інформаційних технологій,
кандидат фізико-математичних наук,
викладач вищої категорії, викладач-методист,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0003-2579-9157

ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ (IOT) У СУЧАСНОМУ МІСТОБУДУВАННІ: КОНЦЕПЦІЯ «РОЗУМНОГО МІСТА»

Сучасне містобудування переживає етап глобальної трансформації, зумовлений стрімким зростанням міського населення та необхідністю оптимізації міського простору. За прогнозами ООН, до 2050 року близько 68 % населення планети проживатиме в містах [1]. Це створює колосальне навантаження на інфраструктуру, житловий фонд, транспортні мережі та екологію. Одним із найефективніших шляхів вирішення цих викликів є впровадження концепції «розумного міста» (Smart City), яка базується на технологіях Інтернету речей (Internet of Things – IoT) [2, с. 7]. Для фахівців у галузі архітектури та містобудування розуміння та використання цих технологій стає не просто перевагою, а обов'язковою вимогою сучасності.

Інтернет речей у контексті міського середовища – це комплексна мережа фізичних об’єктів (будівель, транспортних засобів, елементів вуличної інфраструктури), які оснащені сенсорами, програмним забезпеченням та підключені до інтернету для безперервного обміну даними [1, с. 76]. Головним завданням IoT є збір інформації в режимі реального часу, її аналіз та автоматизоване прийняття рішень для покращення якості життя містян і раціонального використання ресурсів.

Для архітекторів та містобудівників інтеграція IoT починається ще на етапі проєктування. Сучасні підходи вимагають поєднання технологій Інтернету речей із системами інформаційного моделювання будівель (BIM). Завдяки цьому будівля проєктується не просто як статична конст-

рукція, а як «живий» організм. Збагачення BIM-моделі даними з IoT-датчиків дозволяє створювати так звані «розумні будівлі» (Smart Buildings), здатні самостійно керувати системами опалення, вентиляції та освітлення, що дозволяє суттєво знизити енергоспоживання [3, с. 24].

Надзвичайно важливу роль датчики IoT відіграють у моніторингу структурної цілісності архітектурних об'єктів. Сенсори, вмонтовані в несучі конструкції будівель чи мостів, безперервно фіксують мікротріщини, вібрації або просідання фундаменту. Це дозволяє комунальним службам отримувати дані та запобігати аварійним ситуаціям ще до їх візуального прояву.

Ще одним ключовим напрямом є управління транспортною інфраструктурою. Технології IoT дозволяють перетворити звичайні вулиці на інтерактивне середовище. Системи розумних світлофорів, підключені до єдиної мережі, аналізують трафік і формують «зелені хвилі», що здатне знизити завантаженість доріг на 20–25 %. Водночас датчики для розумного паркування допомагають водіям швидко знаходити вільні місця, зменшуючи кількість шкідливих викидів від автомобілів [4, с. 115].

Екологія та ресурсозбереження також зазнають суттєвих покращень завдяки IoT. Мережі датчиків якості повітря, інтелектуальні системи водопостачання та смартконтейнери для збору відходів оптимізують міську логістику. Наприклад, розумні ліхтарі знижують яскравість освітлення на порожніх вулицях, що забезпечує колосальну економію електроенергії. Не менш важливою є безпека міського простору: системи відеоаналітики зі штучним інтелектом та датчики надзвичайних ситуацій гарантують миттєве реагування служб порятунку [2, с. 12].

Проте розбудова такої інфраструктури супроводжується низкою викликів. Архітектори стикаються з проблемою інтеграції високотехнологічного обладнання в історичну забудову, де необхідно зберегти естетику фасадів. Крім того, створення розумного міста потребує значних фінансових інвестицій, розгортання мереж 5G та забезпечення високого рівня кібербезпеки.

Особливого значення технології IoT набувають для України в умовах майбутньої повоєнної відбудови за принципом «Build Back Better» (відбудувати краще, ніж було). Відмова від застарілих підходів на користь створення інноваційних, енергонезалежних та інклюзивних мікрорайонів є вимогою часу. Інтеграція смартсистем управління повинна закладатися безпосередньо в генеральні плани міст ще на етапі їхнього розроблення.

Отже, технології Інтернету речей є фундаментальним інструментом сучасного містобудування. Вони трансформують міста з пасивних

бетонних агломерацій в активні екосистеми. Для майбутніх архітекторів важливо не лише проєктувати естетичні простори, а й враховувати можливість їх повної інтеграції в цифрову мережу, щоб створити стійке, безпечне та комфортне середовище для наступних поколінь.

Список використаних джерел:

1. Коваль М. О. Архітектура та протоколи інтернету речей в розумному місті : матеріали науково-технічної конференції. Тернопіль : ТНТУ ім. Івана Пулюя, 2024. С. 76–77.
2. Смартінфраструктура у сталому розвитку міст: світовий досвід та перспективи України. *Центр Разумкова.* Київ : Заповіт, 2021. 400 с. URL: https://razumkov.org.ua/-uploads/other/2021-SMART-%D0%A1YTI-SITE.pdf (дата звернення: 12.03.2026).
3. BIM та ISO 19650 – у контексті управління проєктами. *Міждержавна гільдія інженерів-консультантів.* Київ, 2019. 32 с. URL: https://iceg.com.ua/wp-content/uploads/2019/11/EFCA_Flipbook_BIM_ukr_.pdf (дата звернення: 12.03.2026).
4. Smart Cities: Foundations, Principles, and Applications / ed. by H. Song et al. Hoboken : John Wiley & Sons, 2017. 904 p.

УДК 004.42:004.5:005.8

Стисло Оксана,
старша викладачка кафедри інформаційних технологій,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0002-7348-2501

ВПЛИВ UX/UI-ДИЗАЙНУ НА ЕФЕКТИВНІСТЬ І РИНКОВУ УСПІШНІСТЬ ПРОГРАМНИХ ПРОДУКТІВ

Емпіричні дослідження демонструють зв’язок між рівнем інтеграції дизайну та економічними результатами компаній. У звіті McKinsey The Business Value of Design встановлено, що організації з найвищими показниками дизайн-зрілості (MDI) демонструють темпи зростання доходів і загальної дохідності для акціонерів, що перевищують середньогалузеві значення приблизно вдвічі [1]. Це дослідження базується на аналізі понад 300 компаній у різних галузях і визначає дизайн як вимірюваний управлінський фактор.

Аналогічні результати зафіксовані в дослідженні Design Management Institute, де портфель компаній, орієнтованих на дизайн, перевищив індекс S&P 500 на 228 % у період 2010–2019 років [2]. Отримані дані свідчать про стійку кореляцію між дизайн-орієнтованістю та довгостроковою ринковою ефективністю.

Контрольовані експериментальні дослідження підтверджують причинний вплив UX/UI-дизайну на поведінкові та фінансові показники. У

кейсі Vodafone покращення показника Largest Contentful Paint (LCP) на 31 % призвело до збільшення продажів на 8 %, що було підтверджено A/B-тестуванням [3]. У кейсі Rakuten 24 оптимізація Core Web Vitals спричинила зростання конверсії на 33,13 % і доходу на відвідувача на 53,37 % [4].

Зазначені результати підтверджують, що продуктивність інтерфейсу безпосередньо впливає на поведінкові показники користувачів. Узагальнення Google Developers показують, що затримки завантаження та нестабільність інтерфейсу призводять до зростання показника відмов і зниження конверсії [5].

Дослідження Baymard Institute на основі великої вибірки e-commerce платформ встановили, що середній рівень покинутих кошиків становить близько 70 %, а оптимізація UX checkout-потоку може підвищити конверсію приблизно на 35 % [6]. Основними факторами втрат є складність форм, непрозорість процесу оформлення замовлення та надлишкове когнітивне навантаження на користувача.

Процесна ефективність UX/UI-дизайну підтверджується міжнародними стандартами. Стандарт ISO 9241-210:2019 визначає людиноцентричний дизайн як ітеративний процес, що включає дослідження контексту використання, визначення вимог користувачів, прототипування та оцінювання [7]. Застосування цього підходу дозволяє підвищити ефективність, результативність і задоволеність користувачів.

Організаційний аспект впливу дизайну підтверджено у дослідженні Nielsen Norman Group, яке показує, що компанії з високим рівнем UX-зрілості частіше досягають позитивного ROI від дизайн-ініціатив і демонструють стабільні бізнес-результати [8].

Значну роль відіграє також узгодженість дизайну в межах продукту. Впровадження дизайн-систем дозволяє забезпечити єдину логіку взаємодії, що знижує когнітивне навантаження на користувача і скорочує час освоєння продукту. Це підтверджується практикою великих технологічних компаній, де використання дизайн-систем сприяє скороченню часу розробки і підвищенню якості інтерфейсів.

Ефективність UX/UI-дизайну також пов’язана з його здатністю адаптуватися до змін поведінки користувачів. Дослідження показують, що сучасні користувачі очікують миттєвої взаємодії, інтуїтивної навігації та мінімальної кількості дій для досягнення мети [5]. Відповідно, дизайн, який не відповідає цим вимогам, призводить до втрати конкурентних позицій.

Сукупність наведених емпіричних даних свідчить про наявність трьох основних механізмів впливу UX/UI-дизайну на конкурентоспроможність програмних продуктів. Перший механізм полягає у підвищенні продуктив-

ності інтерфейсу, що безпосередньо впливає на поведінкові показники користувачів. Другий механізм пов'язаний з оптимізацією користувацьких сценаріїв, що знижує рівень відмов і підвищує конверсію. Третій механізм полягає в інтеграції дизайну у бізнес-процеси, що забезпечує довгострокову конкурентну перевагу.

Отримані результати підтверджують, що UX/UI-дизайн є вимірюваним і керованим фактором ефективності програмних продуктів. Його вплив доведено як на рівні окремих інтерфейсних рішень, так і на рівні стратегічного управління організацією.

Список використаних джерел:

1. The business value of design. *McKinsey & Company.* 2018. URL: https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-business-value-of-design (дата звернення: 23.03.2026).
2. The value of design. *Design Management Institute.* 2015. URL: https://www.dmi.org/page/DesignValue/TheValue-of-Design- (дата звернення: 23.03.2026).
3. Vodafone: A 31% improvement in LCP increased sales by 8 %. *Google Developers.* 2021. URL: https://web.dev/case-studies/vodafone (дата звернення: 23.03.2026).
4. Rakuten 24 case study. *Google Developers.* 2022. URL: https://web.dev/case-studies/rakuten (дата звернення: 23.03.2026).
5. The business impact of Core Web Vitals. *Google Developers.* 2023. URL: https://web.dev/vitals-business-impact (дата звернення: 23.03.2026).
6. Checkout usability research. *Baymard Institute.* 2024. URL: https://baymard.com/checkout-usability (дата звернення: 23.03.2026).
7. ISO 9241-210:2019 Ergonomics of human-system interaction – Human-centred design for interactive systems. Geneva, 2019.
8. UX maturity model. *Nielsen Norman Group.* 2021. URL: https://www.nngroup.com/articles/ux-maturity-model (дата звернення: 23.03.2026).

УДК 004.5:004.774:378

Строїч Олександр,
студент І курсу спеціальності
121 Інженерія програмного забезпечення,
ЗВО «Університет Короля Данила»
Науковий керівник:
Іванов Олександр,
завідувач кафедри інформаційних технологій,
доктор філософії,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0003-4678-7956

ІНКЛЮЗИВНІСТЬ ВЕБСАЙТІВ УНІВЕРСИТЕТІВ ЯК ЧИННИК ДОСТУПНОСТІ ВИЩОЇ ОСВІТИ

У сучасному інформаційному суспільстві вебсайти університетів є основним джерелом інформації для абітурієнтів, студентів, викладачів та інших користувачів. Вони забезпечують доступ до освітніх програм, новин, електронних ресурсів, навчальних матеріалів та сервісів дистанційного навчання. У зв'язку з цим важливого значення набуває інклюзивність вебресурсів, що передбачає створення умов для рівного доступу до інформації для всіх користувачів, зокрема осіб з інвалідністю.

Інклюзивність вебсайтів означає, що цифрові ресурси повинні бути доступними для людей з різними фізичними, сенсорними та когнітивними особливостями. Це стосується користувачів із порушеннями зору, слуху, моторики або інших функціональних обмежень. Університетські сайти повинні враховувати ці потреби, адже вони є важливою частиною освітнього середовища та комунікації між закладом освіти і студентами.

Одним із ключових міжнародних стандартів забезпечення доступності вебресурсів є WCAG (Web Content Accessibility Guidelines). Ці рекомендації визначають принципи створення доступного контенту, зокрема використання альтернативного тексту для зображень, достатнього контрасту кольорів, зрозумілої навігації, можливості керування сайтом за допомогою клавіатури та підтримки програм екранного озвучування.

Для університетських вебсайтів інклюзивність має особливе значення, оскільки вона забезпечує рівні можливості для всіх студентів у доступі до освітніх ресурсів. Наприклад, студенти з порушеннями зору використовують спеціальні програми читання екрана, які озвучують текст на сайті. Якщо структура сторінки побудована неправильно або відсутні альтернативні описи зображень, така інформація стає недоступною.

Крім того, важливими елементами інклюзивного вебдизайну є простота структури сторінок, зрозумілі заголовки, логічна ієрархія контенту та адаптивність для різних пристроїв. Такі рішення покращують користування сайтом не лише для людей з інвалідністю, а й для всіх користувачів.

Таким чином, впровадження принципів інклюзивності на вебсайтах університетів є важливим кроком до забезпечення рівного доступу до освіти та інформаційних ресурсів. Це сприяє формуванню відкритого та доступного освітнього середовища, що відповідає сучасним міжнародним стандартам та принципам інклюзивної освіти.

Список використаних джерел:

1. Web Content Accessibility Guidelines (WCAG) 2.1. W3C Recommendation. *World Wide Web Consortium.* 2018. URL: https://www.w3.org/TR/WCAG21/

2. Про освіту : Закон України від 05.09.2017 № 2145-VIII. *Відомості Верховної Ради України*. 2017. № 38-39. Ст. 380. URL: https://zakon.rada.gov.ua/laws/show/2145-19

3. Гаврилюк О. Інклюзивна освіта в Україні: сучасний стан та перспективи розвитку. Київ : Логос, 2020. 156 с.

УДК 004.8:794.8

Сьома Ярослав,
студент ІІ курсу спеціальності
«Інженерія програмного забезпечення»,
Фаховий коледж ЗВО «Університет Короля Данила»
Науковий керівник:
Шкатуляк Василь,
асистент кафедри інформаційних технологій,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна

ВИКОРИСТАННЯ ШІ В КОМП'ЮТЕРНИХ ІГРАХ

Актуальність теми зумовлена стрімким розвитком штучного інтелекту та його широким використанням у сфері комп'ютерних ігор, де він покращує ігровий процес, поведінку персонажів і загальну якість гри.

Метою роботи є дослідити особливості використання штучного інтелекту в комп'ютерних іграх, визначити його основні функції та вплив на якість ігрового процесу.

Основна частина. Реалізація ШІ сильно впливає на геймплей, системні вимоги і бюджет гри, і розробники балансують між цими вимогами, намагаючись зробити цікавий і невимогливий до ресурсів ШІ малою ціною.

Тому підхід до ігрового ШІ серйозно відрізняється від підходу до традиційного ШІ – широко застосовуються різного роду спрощення, обмани й емуляції. Наприклад, з одного боку, в шутерах від першої особи безпомилковий рух і миттєве прицілювання, властиве ботам, не залишає жодного шансу людині, так що ці здатності штучно знижуються. З іншого боку, боти повинні робити засідки, діяти командою й тд., для цього застосовуються «костилі» у вигляді контрольних точок, розставлених на рівні.

Персонажів відеоігор, керованих ігровим штучним інтелектом, ділять на:

– неігрові персонажі (англ. Non-player character – NPC) – зазвичай ці ШІ-персонажі є дружніми або нейтральними до людського гравця;

– боти (англ. Bot) – ворожі до гравця ШІ-персонажі, що наближаються за можливостями до ігрового персонажа; проти гравця в будь-який конкретний момент бореться невелика кількість ботів. Боти найскладніші в програмуванні;

– моби (англ. Mob) – ворожі до гравця «низькоінтелектуальні» ШІ-персонажі. Моби вбиваються гравцями у великих кількостях заради очок досвіду, артефактів або проходження території [1].

Штучний інтелект у комп'ютерних іграх використовується насамперед для керування поведінкою неігрових персонажів. Завдяки цьому NPC можуть реагувати на дії гравця, адаптуватися до ситуації та робити ігровий процес більш динамічним і правдоподібним. У документації Unity ML-Agents зазначено, що середовище Unity можна перетворювати на навчальне середовище для тренування поведінки персонажів за допомогою алгоритмів машинного навчання [2].

Окремо варто виділити розвиток генеративного ШІ для NPC. NVIDIA описує ACE for Games як набір технологій для створення розмовних і дієвих ігрових персонажів, які можуть сприймати контекст, реагувати на гравця та демонструвати більш природну поведінку. Це свідчить про поступовий перехід від жорстко прописаних сценаріїв до більш гнучких інтерактивних моделей персонажів [3].

Висновок. Отже, штучний інтелект відіграє важливу роль у розвитку комп'ютерних ігор. Його використання дає змогу створювати більш реалістичну поведінку персонажів, урізноманітнювати ігровий процес і покращувати загальну якість гри. Завдяки ШІ комп'ютерні ігри стають цікавішими, складнішими та більш пристосованими до дій гравця. Тому можна зробити висновок, що штучний інтелект є однією з найважливіших сучасних технологій в ігровій індустрії та має великі перспективи для подальшого розвитку.

Список використаних джерел:

1. Ігровий штучний інтелект. *Wikipedia*. URL: https://uk.wikipedia.org/wiki/Ігровий_штучний_інтелект (дата звернення: 23.03.2026).

2. ACE for Games. *NVIDIA*. URL: https://developer.nvidia.com/ace-for-games (дата звернення: 23.03.2026).

3. ML-Agents Documentation. *Unity*. URL: https://docs.unity3d.com/Packages/com.unity.ml-agents@3.0/manual/index.html (дата звернення: 23.03.2026).

УДК 004.932

Табахарнюк Ганна-Анастасія,
студентка IV курсу спеціальності
«Інженерія програмного забезпечення»,
ЗВО «Університет Короля Данила»
Науковий керівник:
Іванов Олександр,
завідувач кафедри інформаційних технологій,
доктор філософії,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0003-4678-7956

ЗАСТОСУВАННЯ АЛГОРИТМІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АВТОМАТИЧНОЇ СЕГМЕНТАЦІЇ ТА ВИДАЛЕННЯ ФОНУ В ПОРТРЕТНИХ ФОТОГРАФІЯХ

У сучасну епоху цифрової трансформації автоматизація обробки графічної інформації стає критично важливою для багатьох сфер діяльності: від електронної комерції до державних послуг. Окреме місце займає підготовка портретних фотографій для документів, де існують суворі стандарти щодо якості та фону зображення. Традиційні методи редагування, що базуються на ручному виділенні контурів, є тривалими та вимагають спеціалізованих навичок. Використання штучного інтелекту дозволяє перетворити ці процеси на «щоденного помічника», здатного виконувати складні маніпуляції із зображеннями за лічені секунди.

Аналіз методів сегментації. Проблема виділення переднього плану є однією з фундаментальних у комп'ютерному зорі. Протягом десятиліть для цього використовувалися алгоритми, що базуються на розрізах графів, зокрема GrabCut [6]. Принцип роботи GrabCut полягає у визначенні імовірності належності пікселя до фону або об'єкта на основі ітеративного аналізу розподілу кольорів. Однак, як зазначає Р. Шеліскі, класичні методи часто вимагають втручання користувача для уточнення меж у

складних зонах, наприклад, при виділенні волосся або прозорих елементів одягу [5, с. 412].

Сучасним розв'язанням цієї проблеми є застосування глибокого навчання (Deep Learning). На відміну від класичних підходів, згорткові нейронні мережі (CNN) здатні вивчати високорівневі ознаки об'єктів, що забезпечує значно вищу точність семантичної сегментації [1, с. 320]. Семантична сегментація передбачає класифікацію кожного пікселя зображення, що дозволяє створювати точні маски об'єктів незалежно від складності фону.

Архітектури нейронних мереж у задачах обробки фото. Для реалізації автоматичного видалення фону у вебдодатках найбільш ефективними є архітектури типу «енкодер-декодер». Однією з найбільш успішних моделей є U-Net, яка спочатку була розроблена для біомедичних зображень, але згодом стала стандартом для будь-якої сегментації завдяки механізму «skip connections», що дозволяє зберігати просторові деталі зображення [2].

Для обробки саме портретних фотографій особливої уваги заслуговує Mask R-CNN, яка розширює можливості детекції об'єктів шляхом додавання гілки для передбачення маски сегментації паралельно з класифікацією та визначенням обмежувальної рамки (bounding box) [3]. Використання Mask R-CNN у вебсервісі дозволяє спочатку локалізувати обличчя та фігуру людини, а потім провести попіксельне виділення контуру з мінімальною кількістю артефактів. Ще одним перспективним підходом є сімейство моделей DeepLab, які використовують атрофну згортку (atrous convolution) для розширення поля зору фільтрів без втрати роздільної здатності, що є ключовим для чіткого визначення меж об'єкта [4].

Практична реалізація та алгоритмічна схема. У межах розробки вебсайту для обробки фотографій алгоритмічна послідовність включає наступні кроки:

1. Попередня обробка (Pre-processing): зміна розміру та нормалізація колірних каналів для відповідності вхідному формату обраної нейромережі.

2. Інференс моделі: завантаження вхідного зображення в навчену модель (наприклад, MobileNetV2 як бекбон для DeepLabV3+), яка формує ймовірнісну карту маски.

3. Альфа-змішування (Alpha Matting): застосування технік пом'якшення країв маски для усунення ефекту «східчастості» та досягнення природного переходу між об'єктом і новим фоном.

4. Заміна фону: заповнення сегментованої області фону білим кольором або прозорим шаром відповідно до вимог стандарту ICAO для паспортних фотографій.

Отже, провадження алгоритмів штучного інтелекту в архітектуру вебсайту для обробки фотографій дозволяє повністю автоматизувати процес підготовки зображень, забезпечуючи високу якість сегментації, недосяжну для класичних алгоритмів без участі людини. Використання сучасних архітектур, таких як U-Net та Mask R-CNN, мінімізує помилки при складних умовах освітлення та контрастності, що робить ШІ надійним інструментом для щоденних завдань користувача в інтернет-середовищі.

Список використаних джерел:

1. Garcia-Garcia A., Orts-Escolano S., Oprea S. et al. A Review on Deep Learning Techniques Applied to Semantic Segmentation.

2. Ronneberger O., Fischer P., Brox T. U-Net: Convolutional Networks for Biomedical Image Segmentation. *Proceedings of MICCAI.* 2015. P. 234-241.

3. He K., Gkioxari G., Dollár P., Girshick R. Mask R-CNN. *IEEE International Conference on Computer Vision (ICCV).* 2017. P. 2961-2969.

4. Chen L.-C., Papandreou G., Kokkinos I., Murphy K., Yuille A. DeepLab: Semantic Image Segmentation with Deep Convolutional Nets. *IEEE TPAMI.* 2017. Vol. 40. P. 834-848.

5. Szeliski R. Computer Vision: Algorithms and Applications. *Springer*. 2010. 812 p.

6. Shen X., Terzopoulos D., Jia J. Deep Automatic Portrait Matting. *European Conference on Computer Vision (ECCV).* 2016.

УДК 001.9

Угорський Михайло,
студент І курсу спеціальності
«Інженерія програмного забезпечення»,
Фаховий коледж ЗВО «Університет Короля Данила»
Науковий керівник:
Малиновська Наталія,
викладач вищої категорії,
Фаховий коледж ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0009-0001-1275-3195

ЯК ШТУЧНИЙ ІНТЕЛЕКТ ВГАДУЄ НАСТУПНЕ СЛОВО ЧЕРЕЗ ЙМОВІРНІСТЬ

Штучний інтелект (artificial intelligence, AI) – це метод змусити комп’ютер чи програмне забезпечення «мислити» як людський мозок. Це досягається шляхом вивчення закономірностей роботи людського мозку та аналізу когнітивних процесів. За прогнозами, до 2030 року штучний інтелект додасть 4,4 трлн доларів до світової економіки, а ринок зросте з 150,2 млрд доларів у 2023 році до 1,3 трлн доларів у 2030 році. Найбільш трансформаційні ефекти будуть відчутні в галузі охорони здоров’я, виробництва,

інтернет-технологій та фінансових послуг. Саме тому тема штучного інтелекту настільки популярна і обговорювана. Але яким чином працює цей ШІ? Чи є тут місце для математики?

Ймовірність і статистика є ключовими для навчання моделей на прикладах і ухвалення рішень за умов невизначеності. Теорія ймовірності дозволяє оцінювати ймовірності різних результатів, що особливо корисно для класифікації, прогнозування та оцінки ризиків. Ймовірнісні розподіли, як-от нормальний, гаусівський чи біноміальний, допомагають моделям враховувати закономірності у великих наборах даних, де значення часто варіюються [1]. Ймовірність – це математичний спосіб оцінити, наскільки часто може статися та чи інша подія. Наприклад, підкинемо монету: до того, як вона впаде, ми не будемо знати, яка сторона монети випаде, але у нас є всього дві сторони, і логічно, що якщо є дві сторони, то ймовірність появи події, що нам потрібна, можна вирахувати за формулою: P=m/M, де m – корисна дія, а M – всі дії. Тобто шанс буде 0,5 або, якщо у відсотках, то 50 % [2].

Штучний інтелект (ШІ) – це як магічний трюк комп'ютерів, що намагаються копіювати наші мізки. Вони не просто виконують команди, а шукають приховані закономірності в океані даних, як детективи. І все це завдяки ймовірності, яка для ШІ є як чарівна паличка [3].

Ось кілька трюків ШІ з ймовірностями:

– Здогадка щодо наступного слова: коли ви пишете текст, а телефон показує продовження, в цей час ШІ просто обчислює, яке слово найбільше підходить. Скажімо, після «Смачного...» ймовірність слова «апетиту» вища, ніж «трактора».

– Впізнавання пухнастих друзів: ШІ дивиться на фото кота і думає: «Хм, з імовірністю 98 % це кіт, і з 2 % – це дуже пухнаста подушка». Якщо ймовірність достатньо висока, він каже: «Точно кіт!»

– Автопілот постійно рахує: «Яка ймовірність, що той пішохід зробить крок?» На базі цих обчислень він вирішує, чи настав час смикнути за гальма.

– Боротьба зі спамом: ваші поштові скриньки – це як замок з фільтрами. Якщо листочок кричить «акція», «безкоштовно» або «виграш», алгоритм підраховує шанси на спам і закидає його в темну папку, якщо ймовірність занадто висока [4; 5].

Уявіть, що питання про те, чи варто вчити математику у часи ШІ, – це як питати: «Чи необхідно ходити, якщо вже є автомобілі?» Все залежить від того, чи хочете ви бути пасажиром, чи пілотом, який знає, як керувати і куди рухатися. Ось кілька думок, чому математика стає ще важливішою саме тепер:

– математика – це «мова» ШІ, не магія, а просто купа математичних трюків. Хочете не лише спілкуватися з чат-ботами, а й творити технології? Тоді математика – ваш ключ до замка. Без розуміння теорії ймовірностей, лінійної алгебри та матаналізу ШІ залишиться для вас загадковою «чорною скринькою».

– Критичне мислення та перевірка результатів: ШІ теж помиляється (оце називають «галюцинаціями»). Оскільки він діє на ймовірностях, іноді може видати фальшиву, але переконливу відповідь. Знаючи математику, ви можете: зрозуміти, чи все гаразд з відповіддю, вловити логічний ляп, сформулювати запит так, щоб зменшити ймовірність похибки.

– Навички алгоритмічного мислення: вивчення математики тренує мозок розбивати складні завдання на маленькі шматочки. Алгоритмічне мислення підходить всюди. Навіть якщо не доведеться обчислювати інтеграли вручну, то логічні ланцюжки згодяться в юриспруденції, менеджменті чи стратегічному плануванні.

– Етика та безпека: хто винен, якщо алгоритм помилився в медичному діагнозі чи кредиті? Щоб розв’язати такі питання, суспільству потрібні гуру, що розуміють математичні підводні камені [5; 6].

Отже, математика – це ключ до володіння ШІ. Не лише теоретична вимога для ШІ – це сама основа, на якій базуються інтелектуальні системи: чи це представлення даних за допомогою лінійної алгебри, чи побудова прогнозів за допомогою ймовірності, чи міркування з дискретної математики – ці концепції лежать в основі сучасного ШІ.

Список використаних джерел:

1. Математика епохи AI: як класичні теорії формують IT-світ. *nt.ua*. URL: https://nt.ua (дата звернення: 23.03.2026).

2. Класичне визначення ймовірності – урок. *Алгебра, 9 клас*.

3. Чому математика є основою ШІ (стаття № 1).

4. Тетлок Ф., Ґарднер Д. Суперпрогнозування. Мистецтво та наука передбачення. Київ : Наш Формат, 2018. 400 с.

5. ШІ – це математика, а не магія: розуміння розриву між очікуваннями та реальністю.

6. Шпігельхальтер Д. Мистецтво статистики. Прийняття аргументованих рішень на основі даних. Київ : Наш Формат, 2023. 416 с.

УДК 343.3

Цимбалюк Христина,
студентка І курсу спеціальності
F2 «Інженерія програмного забезпечення»,
ЗВО «Університет Короля Данила»
Науковий керівник:
Іванов Олександр,
завідувач кафедри інформаційних технологій,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0001-7761-1677

ЦИФРОВІ ТАБУ ТА МОЖЛИВОСТІ: ЕТИКА Й БЕЗПЕКА В ІНТЕРНЕТ-ПРОСТОРІ

Сучасний студент живе у світі, де межа між реальністю та цифровим простором майже зникла. Для майбутнього інженера програмного забезпечення інтернет – це не лише розваги, а й основний інструмент роботи, навчання та самопрезентації. Проте, разом із безмежними можливостями, мережа приховує пастки, які можуть зруйнувати кар'єру ще до її початку. Питання того, що є дозволеним (етичним та законним), а що – суворим табу, стає базовою компетенцією успішного фахівця.

Першим і найважливішим «табу» в цифровому світі є несанкціонований доступ. Серед студентів побутує міф, що «пошук дірок» у системі університету чи локального сервісу заради цікавості – це прояв майстерності. Насправді, згідно зі статтею 361 Кримінального кодексу України, будь-яке втручання в роботу комп'ютерних мереж без дозволу власника є злочином. Навіть якщо ваші наміри були «благими» (наприклад, ви хотіли вказати адміну на помилку), юридично це кваліфікується як кіберзлочин. «Біле» хакерство можливе лише в межах офіційних програм Bug Bounty або за наявності письмової згоди об'єкта дослідження.

Інша критична зона – це соціальна інженерія та маніпуляції. Використання ШІ для створення дипфейків чи автоматизоване розсилання повідомлень може здаватися вдалим жартом. Проте поширення дезінформації та втручання в приватне життя інших осіб тягне за собою не лише моральний осуд, а й правову відповідальність. У цифрову епоху репутація формується за лічені хвилини, а «цифровий слід» від невдалого жарту залишається назавжди, що може стати перешкодою при працевлаштуванні в топові ІТ-компанії.

Таблиця 1

Матриця дозволених та заборонених дій у цифровому просторі

Категорія	**Що дозволено та рекомендовано**	**Що суворо заборонено**
Автентифікація	Використання менеджерів паролів та апаратних ключів (U2F).	Використання однакових паролів для GitHub та особистої пошти.
Робота з кодом	Публікація Open Source проєктів з відповідною ліцензією (MIT, Apache).	Залишати API-ключі та секрети у публічних репозиторіях.
Комунікація	Використання наскрізного шифрування (E2EE) для конфіденційних тем.	Передавати облікові дані через незахищені месенджери.

З іншого боку, інтернет пропонує величезний простір для легального розвитку. «Можна» і треба використовувати GitHub як своє публічне портфоліо, Figma для візуалізації ідей та форуми на кшталт Stack Overflow для обміну досвідом. Важливо розуміти, що професійна етика програміста починається з поваги до інтелектуальної власності. Використання чужого коду без посилання на автора (плагіат) у навчальному середовищі є порушенням академічної доброчесності, що в університетській спільноті карається відрахуванням або анулюванням результатів.

Окрему увагу слід приділити «цифровій гігієні». Для студента це означає:

1. **Захист акаунтів.** Паролі не мають бути іменами домашніх улюбленців. Використання двофакторної автентифікації (2FA) має бути стандартом, а не опцією.

2. **Безпека розробки.** Під час написання коду заборонено залишати секретні ключі (API keys) у відкритих репозиторіях. Роботизовані системи зловмисників сканують GitHub за лічені секунди після завантаження коду.

3. **Критичне мислення.** Кожен клік по посиланню в листі від «адміністрації факультету» має супроводжуватися перевіркою реальної адреси відправника.

Цифрова безпека – це не стіна, яка обмежує вашу свободу, а пасок безпеки, який дозволяє рухатися швидше. Розуміння правових норм та етичних принципів на першому курсі закладає фундамент професіоналізму. Студент, який вміє захистити себе та свою роботу, у майбутньому зможе створити безпечні та надійні продукти для мільйонів користувачів.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 11.03.2026).
2. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. Київ : Юрінком Інтер, 2025. 280 с.
3. The Ten Most Critical Web Application Security Risks. *OWASP Top 10:2025.* URL: https://owasp.org/www-project-top-ten/ (дата звернення: 10.03.2026).
4. Академічна доброчесність в Університеті Короля Данила : Положення. Івано-Франківськ : УКД, 2024. 18 с.
5. Грищук В. К. Кримінальне право України (особлива частина) : навчальний посібник. Київ : Юрінком Інтер, 2024. 512 с.

УДК 004.7:519.2

Чувпило Євгеній,
студент ІІ курсу спеціальності
121 Інженерія програмного забезпечення,
ЗВО «Університет Короля Данила»
Науковий керівник:
Тимків Іван,
доцент кафедри інформаційних технологій,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID:0009-0007-4138-6180

ПЕРВИННЕ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АНОМАЛІЙ НА ОСНОВІ АДАПТИВНОГО ОЦІНЮВАННЯ ПАРАМЕТРІВ НОРМАЛЬНОГО РОЗПОДІЛУ

Зі стрімким розвитком хмарних технологій та зростанням обсягів мережевого трафіку DDoS-атака все ще залишається однією з найбільш небезпечних мережевих загроз. Основною складністю при її виявленні є відокремлення легітимного трафіку від аномального за умов природної зміни активності.

Для наближеного опису вхідного потоку запитів можна застосувати розподіл Пуассона. Він підходить для моделювання кількості запитів за фіксований проміжок часу. Оскільки події незалежні, то ймовірність отримати k запитів за інтервал часу визначається як: $P(X = k) = \frac{\lambda^k e^{-\lambda}}{k!}$, де λ – інтенсивність потоку.

При великій інтенсивності ($\lambda > 30$) розподіл Пуассона апроксимується нормальним розподілом $N(\mu, \sigma^2)$, де $\mu - \lambda$, $\sigma - \sqrt{\lambda}$ (μ – математичне сподівання,

σ – середньоквадратичне відхилення). В основу пропонованого методу покладено використання властивостей цих розподілів.

Згідно з правилом трьох сигм, при наближенні розподілу до нормального близько 99.7 % значень знаходяться в інтервалі $[\mu - 3\sigma; \mu + 3\sigma]$. Значення, що виходять за ці межі, вважаються аномаліями та потребують додаткової перевірки. Оскільки реальний мережевий трафік лише наближено відповідає нормальному розподілу, доцільно буде використовувати динамічний підхід при розрахунках, тобто μ та σ змінюються через певний проміжок часу T. Слід зауважити, що при постійному перерахуванні величин система може адаптуватися до аномалій. Щоб цього уникнути, варто визначити T – як накопичувальний проміжок часу, в межах якого робляться та зберігаються заміри, і Δt – як частинний проміжок часу, за який робляться заміри. По закінченню Δt заміри, якщо вони валідні, потрапляють в чергу. Тим самим вони витісняють з неї найстаріші. Відбувається перерахунок μ та σ. Вікно спостереження T зміщується на крок Δt. Якщо під час Δt виявлено невалідний замір, то всі заміри зроблені в межах даного Δt ігноруються (не потрапляють до черги), перерахунок μ та σ не відбувається.

Якщо ж атака є поступовою й починається, не перевищуючи значення $\mu + 3\sigma$, варто внести зміни – використовувати типовий показник минулої доби для даного проміжку часу. Якщо поточне значення λ протягом декількох циклів значною мірою перевищує показники λ для даного сегменту минулої доби, то це можна розцінювати як аномалію.

Застосування такого підходу дозволить створити алгоритм первинної фільтрації трафіку без застосування нейромережевих моделей на початкових етапах виявлення DDoS-атак.

Список використаних джерел:

1. Барковський В. В., Барковська Н. В., Лопатін О. К. Теорія ймовірностей та математична статистика. 5-те вид. Київ : Центр учбової літератури, 2010. 424 с.

2. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект. Київ : ДУТ, 2015. 288 с.

3. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. Київ : Видавнича група BHV, 2009. 608 с.

УДК 004.7

Чуйко Олег,
студент IV курсу спеціальності
121 Інженерія програмного забезпечення,
ЗВО «Університет Короля Данила»
Науковий керівник:
Іванов Олександр,
завідувач кафедри інформаційних технологій,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0009-0000-4407-0797

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ У РОЗУМНИХ ЕКОСИСТЕМАХ: ПЕРЕВАГИ ЛОКАЛЬНОГО ОБМІНУ (НА ПРИКЛАДІ ДОДАТКА «LAN SHARE»)

Однією з вразливостей сучасних цифрових екосистем є звичка користувачів використовувати зовнішні хмарні сервіси або месенджери для обміну файлами між власними пристроями, що знаходяться в одному приміщенні. Передача конфіденційної інформації через сервери третіх сторін безпідставно збільшує поверхню для потенційних кібернетичних атак і створює ризик перехоплення даних або несанкціонованого доступу до них у разі компрометації хмарного сховища.

Ефективним апаратним та програмним рішенням для мінімізації таких ризиків є використання ізольованих технологій локальної передачі даних (Local Area Network). Практичною реалізацією цього підходу є розроблений нами програмний додаток «Lan Share». Його концептуальне завдання – забезпечити швидкий і безпечний обмін файлами між пристроями, що підключені до однієї мережі Wi-Fi, виключаючи необхідність використання зовнішнього інтернет-з'єднання.

З технічної точки зору, додаток автоматично ідентифікує доступні вузли в локальній мережі та встановлює пряме P2P-з'єднання (Peer-to-Peer) між пристроєм-відправником та одержувачем [2, с. 89]. Завдяки такій архітектурі весь мережевий трафік маршрутизується виключно в межах локального маршрутизатора користувача. Це апаратно унеможливлює доступ до файлів із глобальної мережі та гарантує найвищий рівень приватності. Додатковою перевагою такого підходу є відсутність залежності від пропускної здатності інтернет-провайдера, що дозволяє передавати великі обсяги даних значно швидше.

Отже, безпека в цифрову епоху вимагає від користувачів розуміння того, як саме функціонують їхні пристрої. Застосування локальних рішень, таких як додаток «Lan Share», для передачі чутливої інформації є дієвим та науково обґрунтованим механізмом захисту персональних даних, що сприяє побудові дійсно безпечної розумної екосистеми.

Список використаних джерел:

1. Корченко О. Г. Системи захисту інформації та кібербезпека : навч. посіб. Київ : Вид-во НАУ, 2021. 320 с.
2. Гахов С. О. Сучасні технології локальних мереж та їх захист від кіберзагроз. *Вісник інформаційних технологій*. 2023. № 2 (15). С. 85-92.

УДК 378.011.3-051:004.8:004

Шакотько Віктор,
доцент кафедри технологічної та професійної освіти,
кандидат педагогічних наук, доцент,
Глухівський національний педагогічний
університет імені Олександра Довженка,
м. Глухів, Україна
ORCID: https://orcid.org/0000-0002-3004-5045

ШТУЧНИЙ ІНТЕЛЕКТ У ЗМІСТІ ПРОФЕСІЙНОЇ ПІДГОТОВКИ МАЙБУТНЬОГО ВЧИТЕЛЯ ІНФОРМАТИКИ

Початок третього десятиліття XXI століття ознаменувався безпрецедентним проривом технологій штучного інтелекту в усі сфери людської діяльності. Стрімкий розвиток генеративних моделей, систем комп'ютерного зору, обробки природної мови та автономних агентів поставив перед освітньою спільнотою принципово нові виклики. Система педагогічної освіти, відповідальна за підготовку фахівців, здатних трансформувати цифровий простір школи, опинилася перед необхідністю переосмислення власного змісту.

Аналіз зарубіжних і вітчизняних досліджень свідчить про те, що питання включення штучного інтелекту до освітнього процесу розглядається у двох взаємопов'язаних вимірах: як предмет вивчення (*AI as a subject*) і як інструмент навчання (*AI as a tool*). Майбутній вчитель інформатики має не лише освоїти обидва виміри, а й навчитися органічно поєднувати їх у власній педагогічній практиці.

Документи ЮНЕСКО «Структура компетенцій у сфері штучного інтелекту для вчителів» [15], «Рекомендації з етики ШІ» [16] та «ШІ та освіта:

Керівництво для осіб, що формують політику» [14], а також Цифрова стратегія ЄС визначають пріоритетними напрямами: формування критичного мислення щодо ШІ-систем; розуміння алгоритмічних основ прийняття рішень; здатність до етичного та відповідального застосування ШІ; навички роботи з даними та моделями машинного навчання.

В Україні питання підготовки вчителів інформатики до роботи в умовах поширення ШІ набуває особливої актуальності в контексті документів Міністерства цифрової трансформації України «Регулювання штучного інтелекту в Україні: дорожня карта» [6] та «Регулювання штучного інтелекту в Україні: Біла книга» [1], а також галузевих стандартів підготовки педагогічних кадрів. Водночас аналіз навчальних планів педагогічних університетів засвідчує, що системний підхід до формування ШІ-компетентності майбутнього вчителя інформатики ще не набув відповідного теоретичного і практичного втілення.

Серед дослідників, які зробили значний внесок у вивчення проблематики підготовки вчителів інформатики до роботи з технологіями ШІ, слід відзначити праці Н. Валько [8], О. Гриб'юк [1], В. Коваленко [2], М. Мар'єнко [3], Н. Морзе [4; 9], О. Спіріна [7], М. Умрик [9], В. Шакотька [10], Е. Діамант [11], Г. Каралекас [12], І. Санусі [13] та ін. Попри очевидний науковий доробок, проблема цілісного проєктування змісту підготовки залишається відкритою.

У контексті дослідження ми розрізняємо поняття «цифрова компетентність», «інформаційно-комунікаційна компетентність» та «ШІ-компетентність». Якщо перші два є родовими категоріями широкого охоплення, то ШІ-компетентність постає як видове поняття, що відображає специфічну готовність педагога до діяльності в умовах поширення систем штучного інтелекту.

Під ШІ-компетентністю майбутнього вчителя інформатики ми розуміємо інтегровану якість особистості, що поєднує: систему знань про принципи, методи та застосування штучного інтелекту; практичні уміння проєктувати, реалізовувати та оцінювати ШІ-орієнтовані навчальні середовища; ціннісне ставлення до відповідального й етичного використання ШІ-технологій; готовність до неперервного фахового розвитку в умовах технологічних змін.

Структурно ШІ-компетентність вчителя інформатики охоплює чотири взаємопов'язані компоненти, подані у Таблиці 1.

Когнітивний компонент охоплює концептуальні знання про природу штучного інтелекту: від класичних символічних систем до сучасних генеративних моделей. Операційно-технологічний компонент забезпе-

чує практичну дієздатність фахівця в цифровому середовищі. Педагогічно-методичний компонент визначає здатність до трансформації ШІ-знань у дидактичний контекст. Нарешті, ціннісно-рефлексивний компонент формує підґрунтя для відповідальної та критично осмисленої педагогічної дії.

Таблиця 1

Структурні компоненти ШІ-компетентності майбутнього вчителя інформатики

Компонент	Зміст	Індикатори сформованості
Когнітивний	Знання фундаментальних засад ШІ, алгоритмів ML/DL, архітектур нейронних мереж	Розуміє принципи роботи ML-моделей; описує архітектуру нейронних мереж; пояснює обмеження ШІ-систем
Операційно-технологічний	Уміння працювати з ШІ-інструментами, програмними бібліотеками, хмарними платформами, API великих мовних моделей	Програмує на Python з NumPy, Pandas, TensorFlow/PyTorch; налаштовує ML-моделі; інтегрує ШІ-сервіси в навчальний процес
Педагогічно-методичний	Здатність проєктувати ШІ-орієнтовані навчальні ситуації, розробляти дидактичні матеріали, оцінювати ШІ-інструменти для учнів	Розробляє уроки з елементами ШІ; добирає відповідні ШІ-інструменти; оцінює педагогічну ефективність рішень
Ціннісно-рефлексивний	Критичне ставлення до ШІ-технологій, усвідомлення етичних, правових і соціальних аспектів, готовність до рефлексії	Аналізує ризики упереджень; дотримується принципів прозорості ШІ; критично оцінює власну ШІ-практику

Технології штучного інтелекту органічно вписуються в педагогічну методологію проблемно-орієнтованого навчання та навчання на основі проєктів. Ключова педагогічна ідея полягає в тому, що найглибше розуміння ШІ виникає не через пасивне засвоєння теорії, а через активне розв'язування реальних проблем.

Серед перспективних напрямів розвитку системи підготовки виокремлюємо: розробку національних стандартів ШІ-компетентності для вчителів інформатики; створення відкритих освітніх ресурсів з ШІ-тематики українською мовою; побудову мережі міжуніверситетської та університетсько-галузевої взаємодії у сфері ШІ-освіти; дослідження ефективності різних моделей підготовки через лонгітюдні дослідження педагогічної практики випускників.

Список використаних джерел:

1. Гриб'юк О. О. Форми і методи використання технологій штучного інтелекту для професійного розвитку педагогічних кадрів: дидактичні та психофізіологічні аспекти дослідницького навчання. *Габітус*. 2024. Вип. 60 (4). С. 55–68. DOI: https://doi.org/10.32782/2663-5208.2024.60.9

2. Коваленко В. В. Рекомендації щодо використання сервісів штучного інтелекту Google Cloud для професійного розвитку педагогічних кадрів. *Інноваційна педагогіка*. 2025. Вип. 2 (81). С. 171-175. DOI: https://doi.org/10.32782/2663-6085/2025/81.2.34

3. Мар'єнко М. В. Перспективні шляхи використання засобів і сервісів штучного інтелекту Європейської хмари відкритої науки для професійного розвитку педагогічних кадрів. *Наукові записки. Серія: Педагогічні науки*. 2024. Вип. 213. С. 196-201. DOI: https://doi.org/10.36550/2415-7988-2024-1-213-196-201

4. Морзе Н. В., Бойко М. А., Струтинська О. В., Смирнова-Трибульська Є. М. Якою має бути цифрова компетентність вчителів у галузі використання штучного інтелекту? *Відкрите освітнє е-середовище сучасного університету*. 2024. № 16. С. 76–91. DOI: https://doi.org/10.28925/2414-0325.2024.166

5. Регулювання штучного інтелекту в Україні: Біла книга. *Міністерство цифрової трансформації України*. 2024. URL: https://thedigital.gov.ua/storage/uploads/files/page/community/docs/%D0%A0%D0%B5%D0%B3%D1%83%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%A8%D0%86.pdf

6. Регулювання штучного інтелекту в Україні: дорожня карта. *Міністерство цифрової трансформації України*. 2023. URL: https://cutt.ly/BwnN8fA5

7. Спірін О. М., Олексюк В. П. Досвід та перспективи використання технологій штучного інтелекту у навчанні майбутніх учителів інформатики. *Теорія і практика використання інформаційних технологій в умовах цифрової трансформації освіти* : матеріали Всеукраїнської науково-практичної конференції, 29 червня 2023 року, м. Київ, 2023. С. 63-66.

8. Тиніна А. Л., Валько Н. В. Вивчення основ штучного інтелекту в шкільному курсі інформатики. *Information Technologies in Education*. 2022. № 1 (50) С. 59–69. URL: http://ekhsuir.kspu.edu/bitstream/handle/123456789/17803/4.pdf?sequence=1

9. Умрик М. А., Морзе Н. В., Смирнова-Трибульська Е. М. Розвиток компетентностей освітян у галузі використання штучного інтелекту в цифровому суспільстві. *Відкрите освітнє е-середовище сучасного університету*. 2025. № 18. С. 159–173. DOI: https://doi.org/10.28925/2414-0325.2025.1813

10. Шакотько Є. В., Шакотько В. В. Використання штучного інтелекту учасниками освітнього процесу. *Імідж сучасного педагога*. 2024. № 3 (216). С. 5–13. DOI: https://doi.org/10.33272/2522-9729-2024-3(216)-5-13.

11. Diamant E. What is behind the "I" in the AI? Common delusions and misconceptions. *Demystification*. 2019.

12. Karalekas G., Vologiannidis S., Kalomiros J. Teaching Machine Learning in K–12 Using Robotics. *Education Sciences*. 2023. № 13 (1). P. 67.

13. Sanusi I. T., Ayanwale M. A., Tolorunleke A. E. Investigating pre-service teachers' artificial intelligence perception from the perspective of planned behavior theory. *Computers and Education: Artificial Intelligence*. 2024. Vol. 6. 100202. DOI: https://doi.org/10.1016/j.caeai.2024.100202

14. AI and education Guidance for policy-makers. *UNESCO*. 2021. 50 p. DOI: https://doi.org/10.54675/PCSP7350

15. AI competency framework for teachers. *UNESCO*. 2024. URL: https://www.unesco.org/en/articles/ai-competency-framework-teachers

16. UNESCO's Recommendation on the Ethics of Artificial Intelligence: key facts. 2023. URL: https://www.unesco.org/en/articles/unescos-recommendation-ethics-artificial-intelligence-key-facts

УДК 658.3

Шелемей Соломія,
студентка ІІ курсу спеціальності 073 Менеджмент,
ЗВО «Університет Короля Данила»
Науковий керівник:
Гавадзин Наталія,
професорка кафедри бізнесу та управління,
кандидатка наук, доцентка,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0002-5662-2939

ЕФЕКТИВНІСТЬ КОМАНДНОЇ РОБОТИ БІЗНЕСУ

Ефективна командна робота є важливим фактором забезпечення успішної діяльності будь-якого бізнесу. Беручи до уваги постійні зміни в суспільстві, глобалізацію та нестабільність зовнішнього середовища, саме злагоджена команда допомагає підприємству швидко адаптуватися, оптимізовуючи ресурси та зберігаючи конкурентоспроможність. Командний підхід дозволяє вирішувати складні завдання, які виходять за межі можливостей окремого працівника.

Ефективна команда, на відміну від простої робочої групи, здатна досягати так званого синергетичного ефекту, коли результат спільної діяльності перевищує суму індивідуальних зусиль. Цей ефект виникає завдяки взаємодоповненню знань і навичок, підтримці, співпереживанню, конструктивному вирішенню конфліктів і вмінню адаптуватися до нових завдань [2].

До ключових ознак ефективної команди належать:

- наявність єдиної чітко сформульованої мети;
- взаємна відповідальність за результат;
- довіра та відкритість між учасниками;
- збалансований розподіл ролей і функцій;
- високий рівень внутрішньої мотивації;

– гнучкість у прийнятті рішень;

– здатність до рефлексії та постійного вдосконалення [1].

Загалом виділяють такі базові фактори успішної роботи: спільні цілі, правильний розподіл ролей, спільне планування (синхронізація дій), налагоджена взаємодія, постійний професійний ріст, довірливі відносини та спільні цінності.

Для досягнення успіху учасники команди повинні проявляти взаємоповагу, ставити інтереси колективу вище за власні, вміти слухати та ділитися знаннями. Важливо також відповідально ставитися до своїх обов'язків, визнавати власні помилки без перекладання провини на інших і постійно прагнути до розвитку та навчання.

Ефективність команди визначають дві групи факторів: внутрішні та зовнішні. До внутрішніх факторів насамперед відносять елементи, які формуються в межах самої команди: рівень згуртованості, комунікаційна культура, чіткість розподілу ролей, баланс між особистими та спільними цілями, мотивація учасників, ступінь довіри та підтримки. Окрім внутрішніх, важливу роль відіграють і зовнішні чинники, які визначають умови функціонування команди в ширшому організаційному та соціальному контексті. До таких факторів можна віднести стиль керівництва, організаційну культуру, рівень підтримки з боку керівництва, нормативно-правову базу, а також інфраструктурні та технічні умови [2].

Для того, щоб об'єктивно оцінити результативність команди використовують кілька метрик: показник виконання планових завдань – відсоток завдань, виконаних вчасно і без помилок; рентабельність інвестицій у команду – співвідношення витрат на її утримання та розвитку до доходу, який вона приносить; а також опитування та індекси, що допомагають оцінити рівень залученості, комунікації та психологічний клімат у колективі.

Важливо також систематично підвищувати ефективність команди. Для цього можна впровадити комплекс заходів:

– цифровізацію процесів через використання платформ управління проєктами для кращої комунікації;

– стандартизацію роботи за допомогою стандартних операційних процедур;

– систему регулярного зворотного зв'язку для вирішення конфліктів і генерації ідей;

– розвиток крос-функціональних навичок працівників для взаємозамінності;

– менторство та внутрішнє навчання для швидшої адаптації нових працівників і зменшення плинності кадрів.

Ефективність командної роботи є важливим, однак складним та багатовимірним явищем і рушієм успіху будь-якого бізнесу. Цілеспрямоване та розумне формування команд, інвестування в розвиток комунікативних навичок працівників, стандартизація процесів та впровадження інноваційних технологій управління дозволяють команді досягати високого рівня роботи та стабільного розвитку.

Список використаних джерел:

1. Кузнецова О. В. Основи командного менеджменту : навч. посібник. Харків : ХНЕУ ім. С. Кузнеця, 2020. 198 с.
2. Олійник В. В. Ефективність командної роботи в організації : кваліфікаційна бакалаврська робота / Київський столичний університет імені Бориса Грінченка. Київ, 2025. 43 с.

УДК 621.396

Шерепера Катерина,
студентка І курсу спеціальності
«Інженерія програмного забезпечення»,
ЗВО «Університет Короля Данила»
Науковий керівник:
Дзюба Марина,
доцентка кафедри інформаційних технологій,
кандидатка фізико-математичних наук,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0003-2579-9157

ЗАСТОСУВАННЯ MESH-МЕРЕЖ У СИСТЕМАХ ГРУПОВОГО ВИКОРИСТАННЯ БПЛА

Сучасна війна демонструє швидкий перехід від використання окремих дистанційно керованих апаратів до розгортання складних систем, що діють як єдиний організм – «рій» БПЛА. Традиційні методи зв'язку, де кожен дрон напряму залежить від команди з пульта оператора, стають застарілими. Вони вразливі до засобів радіоелектронної боротьби (РЕБ), залежать від прямої видимості та мають обмежений радіус дії [1]. Особливо гостро це відчувається в умовах GNSS-denied environments – середовищах, де ворог повністю блокує супутникову навігацію (GPS), а фізичні перешкоди (пагорби, забудова) розривають прямий зв'язок з оператором. У таких сценаріях дрони повинні не просто виконувати команди, а

самостійно координуватися, передаючи дані один через одного. Саме тут на зміну класичним топологіям приходять децентралізовані Mesh-мережі.

В основі побудови сучасних авіаційних груп лежить концепція FANET (Flying Ad-hoc Networks). Це підвид мобільних мереж, спеціально адаптований для повітряного простору. На відміну від наземних мереж, вузли у FANET (дрони) рухаються надзвичайно швидко (до 150 м/с) у тривимірному просторі. Це створює низку викликів: динамічна топологія: конфігурація мережі змінюється щосекунди; змінні відстані: дрони то наближаються, то віддаляються, змінюючи якість сигналу; вплив висоти: необхідно враховувати не лише координати на площині, а й висоту, яка впливає на проходження радіохвиль (зону Френеля).

У стандартній схемі «зірка» всі дрони підключені до однієї станції. Якщо цю станцію придушити засобами РЕБ або знищити фізично – вся група стає некерованою. Mesh-мережа прибирає цю «єдину точку відмови». Кожен дрон стає одночасно і користувачем, і ретранслятором, і маршрутизатором. Якщо дані не можуть пройти напряму, вони йдуть через «сусідів» – ланцюжком (Multi-hop), що дозволяє керувати групою на відстанях у десятки кілометрів.

Головна перевага Mesh-мережі – її інтелект та автономність. Вона базується на двох принципах: самоорганізація (Self-organization): як тільки новий дрон з’являється в радіусі дії групи, він автоматично обмінюється «привітальними пакетами» (Hello-packets) та інтегрується в загальну мережу без втручання людини; самовідновлення (Self-healing): якщо один або кілька дронів збиті або потрапили під дію РЕБ, мережа за мілісекунди знаходить інший шлях для передачі сигналу.

Для цього використовуються спеціальні протоколи маршрутизації: OLSR (Optimized Link State Routing) – проактивний протокол, який постійно тримає в пам'яті актуальну карту всієї мережі. Це дозволяє передавати дані без затримок, але потребує багато енергії на постійне оновлення таблиць; AODV (Ad hoc On-Demand Distance Vector) – реактивний протокол, який шукає маршрут тільки тоді, коли потрібно передати дані. Це економить заряд батареї, але створює невелику затримку при першому відправленні повідомлення. У бойових умовах найчастіше застосовуються гібридні підходи, які поєднують швидкість OLSR для критичних команд та економічність для передачі відео чи великих файлів.

Mesh-мережі є ідеальним інструментом для протидії ворожим системам придушення. На фізичному рівні Mesh-модулі використовують ППРЧ (FHSS) – стрибкоподібну перебудову частоти. Сигнал «перестрибує» з однієї частоти на іншу тисячі разів на секунду. Ворог просто не встигає зафіксу-

вати, де саме зараз працює дрон. Для цього потрібна ідеальна синхронізація часу між усіма учасниками мережі, що реалізується за допомогою внутрішніх кварцових генераторів (оскільки GPS-синхронізація може бути заблокована).

Якщо ворог встановив потужний «купол» РЕБ, звичайний дрон при вході в цю зону втрачає зв'язок і падає (або повертається назад). В Mesh-мережі ситуація інша: дрони, що знаходяться за межами купола, бачать перешкоду і автоматично спрямовують сигнал «в обхід», використовуючи інші дрони як ретранслятори. Це дозволяє групі буквально «обтікати» зони загороджень противника.

Оскільки кожен дрон у Mesh-мережі є вхідною точкою, існує ризик перехоплення управління при компрометації одного апарата. Для захисту використовуються: наскрізне шифрування (AES-256): дані зашифровані від відправника до отримувача; взаємна перевірка (Mutual Authentication): дрони постійно перевіряють «паспорти» один одного, щоб ворожий апарат не міг прикинутися своїм (захист від Sybil attack); розподілена довіра: рішення про самоліквідацію або зміну місії приймається групою колективно, на основі консенсусу.

Сучасна ППО змушує дрони літати дуже низько (5–15 метрів). На такій висоті зв'язок з оператором зникає вже через 2–3 кілометри через дерева чи рельєф. Над лінією фронту на великій висоті (у безпечній зоні) зависають 2–3 дрони-ретранслятори. Вони створюють «ланцюжок», через який сигнал від ударного дрона, що летить низько в тилу ворога, передається оператору. Це збільшує дальність роботи в рази. При штурмі позицій десятки дронів можуть атакувати одночасно. Замість того, щоб 20 операторів керували кожним дроном окремо, Mesh-мережа дозволяє апаратам домовлятися між собою. Використовуючи «мурашині алгоритми», дрони розподіляють цілі. Це виключає ситуації, коли три дрони летять в одну ціль, ігноруючи іншу. Так формується суцільна «хмара» покриття в найскладніших умовах.

Попри всі переваги, Mesh-технологія має свої «вузькі місця»: деградація швидкості (кожен «стрибок» (hop) від одного дрона до іншого забирає частину пропускної здатності. При 4–5 ретрансляціях передача відео у Full HD стає проблематичною. Це вирішується використанням багатодіапазонних модулів (наприклад, 900 МГц для команд та 5.8 ГГц для відео)); енергоспоживання (оскільки кожен дрон постійно працює як ретранслятор для сусідів, він швидше витрачає батарею); обчислювальна складність (протоколи маршрутизації потребують потужних процесорів, що збільшує вартість та вагу польотних контролерів). Отже, Mesh-мережі (FANET) – це фундамент мережецентричної війни майбутнього. Перехід

від жорсткої ієрархії до гнучкої децентралізованої архітектури робить групу дронів практично невразливою до точкового впливу РЕБ та фізичних втрат. Головна перевага тепер не в потужності одного дорогого апарата, а в ефективності взаємодії багатьох дешевих вузлів. Подальший розвиток технології буде спрямований на створення енергоефективних алгоритмів та впровадження штучного інтелекту, який зможе прогнозувати розриви зв'язку та самостійно перешиковувати «рій» для оптимального покриття. Панування в повітрі сьогодні – це не лише міцні крила, а насамперед стійка та інтелектуальна мережа, яка об’єднує їх у єдину силу.

Список використаних джерел:

1. Bekmezci I., Sahingoz O. K., Temel Ş. Flying Ad-hoc Networks (FANETs): A survey. *Ad Hoc Networks*. 2013. URL: https://www.researchgate.net/publication/253954782_Flying_-ad-hoc_networks_FANETs_a_survey (дата звернення: 05.03.2026).

2. Haque N. L., Husnain M. A., Asif A. L. UAV Communication Networks Issues: A Review. 2021. URL: https://www.researchgate.net/publication/369541621_UAV_Communication_Networks_Issues_A_Review (дата звернення: 05.03.2026).

3. Лаптєв О. А. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. URL: https://duikt.edu.ua/uploads/p_421_4278-3021.pdf (дата звернення: 05.03.2026).

4. Сопов Є. О., Артьомова А. В. Оптимізація обміну інформацією при ройовому управлінні безпілотними літальними апаратами в складних умовах. 2025. URL: https://www.researchgate.net/publication/393399954_optimizacia_obminu_informacieu_pri_rojovomu_upravlinni_bezpilotnimi_litalnimi_aparatami_v_skladnih_umovah (дата звернення: 05.03.2026).

5. Кузьміч М. Ю., Кравчук С. О. Дослідження мобільної mesh-мережі безпілотних літальних апаратів з урахуванням затримки між вузлами. URL: https://conferenc-journal.its.kpi.ua/article/download/101009/96233/213180 (дата звернення: 05.03.2026).

УДК 004.77:504

Шерепера Катерина,
студентка І курсу спеціальності
F2 Інженерія програмного забезпечення,
ЗВО «Університет Короля Данила»
Науковий керівник:
Іванов Олександр,
завідувач кафедри інформаційних технологій,
доктор філософії,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0000-0003-4678-7956

ВАГА НАШОЇ ЦИФРОВОЇ ТІНІ: ЧОМУ 8 ГОДИН У СМАРТФОНІ ПЕРЕТВОРЮЮТЬСЯ НА РЕАЛЬНІ КІЛОГРАМИ CO2

Сучасна людина перебуває в стані постійного інформаційного перевантаження. Зростання обсягів «цифрового сміття» та неконтрольований екранний час стають викликами не лише для психічного здоров'я, а й для екологічної сталості. Метою роботи було дослідити реальний стан цифрового споживання серед молоді та довести, що віртуальні дані мають цілком реальну «вагу» у вигляді вуглецевого сліду.

Основою дослідження стало анонімне опитування 224 осіб (90 % – студенти та працююча молодь) через Google Forms. Об'єктом аналізу стала цифрова поведінка користувачів, а предметом – кореляція між суб'єктивним сприйняттям екранного часу та фактичними обсягами накопичених даних. Також було проведено практичний експеримент із радикального очищення пам'яті пристрою та вивчено кейси цифрового детоксу [1; 2].

Дослідження показало критично високий рівень залученості у цифрові платформи: 55 % респондентів проводять у мережі понад 8 годин на добу. Це означає, що більше як половина користувачів перебуває в онлайн-просторі майже весь час, коли не спить. 54 % опитаних використовують телефон 4-8 годин на день, а 22 % – понад 8 годин; для 29 % респондентів робота за комп'ютером займає понад 6 годин, що вказує на професійну або навчальну інтегрованість цифрових технологій [1, с. 3-5].

Найбільше часу займають додатки, побудовані на механіках швидкого дофаміну та соціальної взаємодії:

1. Telegram (62 %) – основний канал комунікації та отримання новин.
2. TikTok (53 %) – головний ресурс короткого розважального контенту.

3. Instagram (48 %) – платформа для візуального споживання та самопрезентації.

Основними цілями використання гаджетів є соціальні мережі (76 %) та спілкування (71%), що випереджають навчання (57 %) та роботу (49 %) [1, с. 1].

Аналіз галерей користувачів виявив тенденцію до «цифрового Плюшкіна»: 63 % опитаних мають у галереї понад 2000 медіафайлів, з них 41 % респондентів зберігають понад 5000 фото/відео [1, с. 6].

При цьому 45 % користувачів очищують галерею декілька або один раз на рік, а 18 % – дуже рідко або майже ніколи. Це створює величезні обсяги «мертвого капіталу» даних, які ніколи не використовуються, але споживають енергію серверів [1, с. 7].

Також дослідження виявило високий рівень саморефлексії серед молоді: 86 % респондентів вважають або підозрюють («можливо»), що проводять забагато часу перед екраном, проте лише 46 % однозначно хочуть зменшити свій екранний час, тоді як 54 % ще не замислювалися про це або взагалі не вважають за потрібне [1, с. 8-9].

Другим етапом було проведення самодослідження з радикального очищення цифрового простору. У результаті тотальної ревізії пам'яті пристрою було видалено 17,5 ГБ даних: 10 ГБ непотрібних фотографій (дублікатів, невдалих кадрів, скріншотів, старих мемів тощо); 6 ГБ кешу Telegram (тимчасові файли медіаповідомлень та каналів) та 1,5 ГБ кешу TikTok [2].

За середніми розрахунками екологічних калькуляторів (наприклад, *The Shift Project*), зберігання 1 ГБ даних у хмарі/мережі генерує близько 0,2 кг CO2 на рік [3].

Тому очищення моїх 10 ГБ файлів, які зберігалися в хмарі, демонструє потенційну економію близько 2,5 кг CO_2. Це еквівалентно 15 кілометрам поїздок на автомобілі або енергії, необхідній для повної зарядки смартфона протягом майже 3 років без перерви. Видалення кешу не економить викиди CO_2 напряму, але звільняє пам'ять, пришвидшує пристрій і зменшує цифровий безлад. Фото та файли у хмарі, видалені одночасно, демонструють реальний екологічний ефект.

Отже, сучасна молодь перебуває на межі тотального цифрового поглинання, де межа між віртуальним та реальним нівелюється. Накопичені дані є джерелом когнітивного шуму та екологічного навантаження. Дослідження доводить, що цифрова гігієна – це не просто технічна необхідність для швидкої роботи гаджета, а важлива складова стратегії сталого розвитку. Впровадження обов'язкових регулярних очищень кешу та видалення

зайвих файлів на пристроях дозволить зменшити екологічний слід, прискорити роботу пристрою та покращити психологічний стан користувача завдяки «ефекту чистого листа».

Список використаних джерел:

1. Авторські дані опитування щодо використання смартфона та цифрового детоксу : Google-таблиця. URL: https://docs.google.com/spreadsheets/d/1Pu_7tTAQQEaMyyGy0BiH-h4OlCq16Om1mfuqZh_m3iE/edit?usp=sharing (дата звернення: 22.02.2026).

2. Авторські дані опитування щодо цифрового детоксу : Google-таблиця. URL: https://docs.google.com/spreadsheets/d/1dogfOsiEcNdxVYOhzQAtQzmChrriCVKWB20DTt9FXoU/edit?usp=sharing (дата звернення: 01.03.2026).

3. Як цифрове прибирання запобігає викиду CO_2. *Stud-Point*. 22.08.2023. URL: https://stud-point.com/blog/yak-tsyfrove-prybyrannia-zapobihaie-vykydu-co/ (дата звернення: 20.02.2026).

УДК 004.8:81`32

Шерепера Катерина,
студентка І курсу спеціальності
F2 Інженерія програмного забезпечення,
ЗВО «Університет Короля Данила»
Науковий керівник:
Куцела Марія,
старша викладачка кафедри
іноземної філології та бізнес-комунікацій,
ЗВО «Університет Короля Данила»,
м. Івано-Франківськ, Україна
ORCID: https://orcid.org/0009-0002-1225-2988

ЛІНГВО-ТЕХНІЧНІ АСПЕКТИ ПРОМПТ-ІНЖИНІРИНГУ: АЛГОРИТМИ ПОБУДОВИ ЕФЕКТИВНИХ АНГЛОМОВНИХ ЗАПИТІВ ДЛЯ ШІ

У сучасному цифровому середовищі великі мовні моделі стали універсальним інструментом для роботи з текстом, кодом, аналітикою та комунікацією. Центральним елементом взаємодії з такими системами є промпт – текстова інструкція, яку користувач надає моделі для отримання результату. Хоча, на перший погляд, може здаватися, що мова запиту не має принципового значення, з технічної та економічної точок зору вона суттєво впливає на ефективність роботи системи. Особливо це стосується вибору між англійською та українською мовами.

Щоб зрозуміти цю різницю, необхідно розглянути поняття токенів [1; 4; 5]. Він може бути цілим словом, частиною слова або навіть окремим

символом. Саме токени перетворюються на числові коди, які модель використовує для обчислень. Кожен запит і кожна відповідь вимірюються в токенах, і саме від їх кількості залежить навантаження на систему.

Важливим технічним показником тут є «Token-to-Word Ratio» (співвідношення токенів до слів) [1]. Більшість сучасних мовних моделей навчалися переважно на англомовних текстах. Це означає, що їхні алгоритми токенізації оптимізовані саме для латиниці. В основі таких алгоритмів лежать методи субслівного поділу, зокрема Byte Pair Encoding або SentencePiece [2; 3; 4]. Вони формують словник найчастіших фрагментів тексту. Оскільки англійська мова має відносно просту морфологію та коротші слова, система часто може кодувати слово одним токеном або невеликою їх кількістю. Це робить англомовні промпти технічно ефективнішими порівняно з кириличними запитами [3]. Українська мова має складнішу граматичну структуру, через що одне слово частіше розбивається на кілька частин. Дослідження ефективності токенізації української мови показує, що для українських текстів моделі витрачають значно більше токенів для передачі того самого змісту. Наприклад, англійське слово «development» може складатися з 1-2 токенів, а українське слово «розроблення» часто розбивається на 3-4 токени [1; 2; 8]. Якщо розглянути текст обсягом приблизно 100 слів, англомовний варіант може складатися приблизно зі 120–140 токенів, тоді як український аналогічний за змістом текст може потребувати 170–200 токенів [4]. Це означає, що різниця може досягати 30–40 відсотків. У масштабах одного повідомлення це здається незначним, але у випадку тисяч запитів або довгих діалогів ця різниця накопичується.

Варто зауважити, що ефективність обробки української мови суттєво зросла з розвитком моделей. У ранніх версіях, таких як GPT-3.0, українські запити могли потребувати у 3 рази більше токенів, ніж у сучасних ітераціях. Наприклад, одне й те саме коротке речення довжиною 48 символів у моделі GPT-3.0 займало 58 токенів, тоді як у GPT-4.0 цей показник знизився до 18 токенів [8]. Проте те саме за змістом речення в GPT-4.0 англійською мовою потребує лише 9 токенів.

Більшість комерційних сервісів штучного інтелекту встановлюють оплату саме за кількість оброблених токенів. Відповідно, якщо український промпт потребує більше токенів, його вартість буде вищою [6]. Таким чином, компанія, яка регулярно використовує штучний інтелект у роботі, може витрачати значно більше коштів, якщо всі запити формулюються мовою з менш ефективною токенізацією.

Окрім вартості, важливим фактором є швидкість відповіді. Чим більший обсяг токенів, тим більше часу потрібно для обчислень [4; 5]. У системах із великою кількістю одночасних запитів, наприклад, у чат-ботах підтримки або автоматизованих сервісах, навіть невелике збільшення кількості токенів впливає на загальну продуктивність і затримку відповіді.

Ще одним важливим аспектом є обмеження контекстного вікна. Кожна модель має максимальну кількість токенів, які вона може одночасно обробляти в межах одного діалогу. Якщо текст займає більше токенів, частина попередніх повідомлень може бути автоматично видалена з пам'яті. Це призводить до втрати контексту та зниження якості відповідей. Використання англійської мови дозволяє вмістити більше змісту в межах того самого контекстного обмеження, що особливо важливо для довгих професійних обговорень або складних технічних завдань [4].

Варто також звернути увагу на техніку написання запитів. Кожен промпт є індивідуальним, тому не завжди підходить під загальний шаблон. Проте найбільш ефективний промпт повинен містити [7]:

Таблиця 1

Шаблон написання промпту

Елемент	Опис (функція)	Приклад (англ.)
Роль (Role)	Фокусування бази знань	*«Act as a software engineering student»*
Контекст (Context)	Вхідні дані	*«I want to learn english to understand some technical material»*
Завдання (Task)	Чітка дія (сильні дієслова)	*«Analyze this situation», «Summarize this text»*
Обмеження (Constraints)	Конкретні встановлені обмеження	*«Don't use the word hedgehog»*
Стиль (Style)	Бажаний стиль відповіді	Formal, friendly
Формат (Output Format)	У якому вигляді повинна бути відповідь	JSON-file, code, instruction

Окремим високоефективним методом покращення результату є застосування «режиму критика» (Iterative Prompting) [7]. Ця стратегія передбачає ітеративну взаємодію, де після першої генерації відповіді користувач дає моделі нову інструкцію – виступити в ролі суворого експерта-критика. У цьому режимі ШІ має проаналізувати свій попередній текст, виявити в ньому логічні помилки, фактичні неточності або стилістичні недоліки та запропонувати шляхи їх виправлення.

Крім того, англійська мова часто забезпечує кращу точність інтерпретації. У роботі з українськими промптами часто спостерігаються так звані «логічні галюцинації», коли модель створює правдоподібні, але вигадані

або неточні факти. Це відбувається через те, що більшість навчальних даних моделей є англомовними і система має більше прикладів використання термінів саме англійською. Тому формування англійських промптів є особливо важливим для технічних або наукових тем, де точність формулювання відіграє ключову роль.

Таким чином, вибір мови промпту – це технічне рішення, яке впливає на вартість обробки запитів, швидкість відповіді та якість взаємодії з моделлю. Аналіз еволюції моделей від GPT-3 до GPT-4 демонструє значний прогрес в оптимізації української токенізації, проте англійська мова все ще залишається у 2 рази ефективнішою за обсягом споживаних ресурсів. Англійська мова в контексті сучасних великих мовних моделей є більш ефективною з точки зору використання пам'яті та економії ресурсів. Розуміння цих факторів дозволяє більш раціонально використовувати можливості штучного інтелекту як у професійній діяльності, так і в наукових дослідженнях.

Список використаних джерел:

1. What are tokens and how to count them? *OpenAI*. URL: https://help.openai.com/en/articles/4936856-what-are-tokens-and-how-to-count-them (дата звернення: 23.02.2026).
2. Maksymenko D., Turuta O. Tokenization efficiency of current foundational large language models for the Ukrainian language. URL: https://www.researchgate.net/publication/394718807_Tokenization_efficiency_of_current_foundational_large_language_models_for_the_Ukrainian_language (дата звернення: 22.02.2026).
3. Držík D., Kapusta J. The importance of morphology-aware subword tokenization for NLP tasks in Slovak language modeling. *ScienceDirect*. 2026. URL: https://www.sciencedirect.com/science/article/pii/S0957417426004057 (дата звернення: 22.02.2026).
4. Tokens and context windows in LLMs. *GeeksforGeeks*. 2025. URL: https://www.geeksforgeeks.org/artificial-intelligence/tokens-and-context-windows-in-llms/ (дата звернення: 23.02.2026).
5. Balarabe T. What is LLM tokenization? A guide to language model efficiency. *Medium*. 2025. URL: https://medium.com/@tahirbalarabe2/what-is-llm-tokenization-a-guide-to-language-model-efficiency-1b4ae57c180b (дата звернення: 22.02.2026).
6. Understanding OpenAI GPT Tokens: A Comprehensive Guide. *GPT.space*. URL: https://gpt.space/blog/understanding-openai-gpt-tokens-a-comprehensive-guide (дата звернення: 22.02.2026).
7. Краковецький О. Великі мовні моделі, інженерія запитів та агенти. Київ : Аванпост-Прим, 2025. 243 с.
8. Tokenizer. *OpenAI Platform*. URL: https://platform.openai.com/tokenizer (дата звернення: 09.03.2026).

УДК 004.8

Школьніков Владислав,
завідувач кафедри кримінології та інформаційних технологій,
доктор філософії в галузі права, доцент,
Національна академія внутрішніх справ,
м. Київ, Україна
ORCID: https://orcid.org/0000-0003-2041-9450
Гуськова Віра,
доцент кафедри штучного інтелекту,
доктор філософії в галузі комп'ютерних наук,
Інститут прикладного системного аналізу Національного технічного університету України «КПІ ім. Ігоря Сікорського»,
м. Київ, Україна
ORCID: https://orcid.org/0000-0001-7637-201X

СУЧАСНІ КІБЕРЗАГРОЗИ ДЛЯ VASP ТА FI: KYC ПРОТИ DEEPFAKE

Останнім часом спостерігається значне зростання кількості випадків використання зловмисниками технології DeepFake (поєднання слів з англ. *deep learning* – «глибоке навчання» та *fake* – «підробка») для обходу процедур KYC у VASP (з англ. *virtual asset service provider* – «постачальник послуг віртуальних активів») та FI (з англ. *financial institution* – «фінансова установа»).

Метою запровадження процедури «Знай свого клієнта» (англ. *know your customer*, скорочено *KYC*) є ідентифікація та верифікація особи клієнта для запобігання випадкам легалізації (відмиванню) доходів, отриманих злочинним шляхом (AML), шахрайства, фінансування тероризму, розвідувальної та диверсійної діяльності, обходу санкцій.

Обхід процедури KYC дозволяє зловмиснику отримувати доступ до облікових записів клієнтів VASP та інтернет-банкінгу клієнтів FI із використанням методів соціальної інженерії та інших поширених схем компрометації персональних даних.

Наслідком цього є відкриття рахунків, оформлення кредитів, реєстрація ФОП, отримання інших державних послуг та здійснення інших операцій із використанням скомпрометованих даних клієнтів.

Технологія DeepFake дозволяє створювати копії голосу та рис обличчя живої або померлої людини, які надалі можуть використовуватися зловмисником для отримання доступу до облікових записів клієнтів VASP та інтернет-банкінгу клієнтів FI.

Наприклад, у 2024 році дослідники безпеки Cato CTRL повідомили, що хакерська група ProKYC продає AI-інструмент на основі Deepfake, здатний обходити біометричні системи верифікації та двофакторну аутентифікацію (2FA) облікових записів клієнтів VASP та FI. Цей інструмент за допомогою штучного інтелекту (AI) створює цифрового двійника особистості, а також генерує підроблені копії документів, що посвідчують особу [1].

У 2025 році слідчі Національної поліції України викрили організовану групу, яка за допомогою штучного інтелекту (*далі – ШІ*) оформлювала кредити на українців. Отримавши доступ до електронних кабінетів громадян, зловмисники завантажували цифрові документи користувачів, після чого організаторка виготовляла короткі підроблені відео з використанням технології DeepFake, накладаючи обличчя потерпілих на власне. Ці фейкові відео використовувалися для проходження автоматичної фото-верифікації у банківських онлайн-системах [2].

Ефективна стратегія вдосконалення механізмів захисту процедури KYC від DeepFake залежить від організаційно-технічної моделі кіберзахисту VASP та FI, а також від ризик-орієнтованих підходів у моніторингу дій користувача.

Організаційно-технічна модель кіберзахисту VASP та FI має містити:

– виявлення або блокування віртуальних камер, підміни пристрою під час сесії та встановлення нових драйверів;

– раптові перевірки реакції обличчя на зміну освітлюваності екрана монітора, появу інших подразників (стимулів) для людського ока тощо;

– оцінку фактично отриманого потоку даних (після стиснення) на наявність мерехтіння, розсинхронізації руху губ та звуку, а також розмитих текстур;

– отримання через API метаданих про відеопотік (кодер, бітрейт, роздільну здатність та співвідношення сторін екрану, характеристики пристрою, операційної системи, браузера користувача, IP тощо), що дозволить виявити аномалії у поведінці користувача;

– у разі виявлення ризику надавати користувачеві повідомлення про помилку аутентифікації (наприклад, «підозра на віртуальну камеру», «наявність розмитих текстур», «розсинхронізації руху губ та звуку») із необхідністю звернутися до служби підтримки;

– розробка та впровадження інструкцій для служб підтримки з метою забезпечення послідовних рішень та мінімізації помилок;

– проведення періодичних симуляційних навчань для перевірки ефективності захисту від сучасних інструментів підміни облич у реальному часі та інших технологій DeepFake.

Ризик-орієнтовані підходи у моніторингу дій користувача мають містити:

– формування «білого списку» оригінальних відеокамер пристрою з метою блокування сесій, у ході яких використовуються віртуальні або підмінені відеокамери;

– фіксація часових міток надісланих запитів та вимірювання затримки реакції користувача для виявлення нехарактерних для людини моделей відповіді;

– створення моделей ШІ для виявлення аномалій, пов'язаних зі штучно згенерованими зображеннями;

– обмін інформацією між приватним та державним секторами про виявлені факти використання скомпрометованих цифрових особистостей.

Технології DeepFake стали системною загрозою для процедур KYC у VASP та FI. Обхід KYC може трансформувати локальну технічну вразливість у масштабний ризик, наслідками якого є незаконне відкриття рахунків, оформлення кредитів, отримання державних послуг та здійснення інших фінансових операцій з використанням скомпрометованих персональних даних.

Ефективна протидія DeepFake у сфері діяльності VASP та FI можлива лише за умови поєднання організаційних та технічних заходів, які мають містити аналіз поведінкової моделі користувача, а також обмін інформацією між приватним та державним секторами про виявлені факти використання скомпрометованих цифрових особистостей.

Список використаних джерел:

1. Cato CTRL Threat Research: ProKYC – Deepfake Tool for Account Fraud Attacks. *Cato Networks*. URL: https://www.catonetworks.com/blog/prokyc-selling-deepfake-tool-for-account-fraud-attacks/

2. Слідчі поліції викрили організовану групу, яка за допомогою штучного інтелекту оформлювала кредити на українців. *Національна поліція України*. URL: https://-npu.gov.ua/news/slidchi-politsii-vykryly-orhanizovanu-hrupu-iaka-za-dopomohoiu-shtuchnoho-intelektu-oformliuvala-kredyty-na-ukraintsiv?v=68edf05e94c25

3. Типологічне дослідження «Ризики та загрози легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму в умовах військової агресії російської федерації – 2025». *Державна служба фінансового моніторингу України*. URL: https://fiu.gov.ua/assets/userfiles/411/Типолог%20ДСФМУ/Typology%202025_UA.pdf

UDC 004.8:81’243:81’342.1

Andreyko Dmytro,
3rd-year student, Specialty – 121 Software Engineering,
HEI «King Danylo University»
Scientific Supervisor:
Kutsela Mariia,
senior lecturer of the Department of
Foreign Philology and Business Communications,
HEI «King Danylo University»,
Ivano-Frankivsk, Ukraine
ORCID: https://orcid.org/0009-0002-1225-2988

AI-BASED PRONUNCIATION TRAINING IN ENGLISH LANGUAGE LEARNING

In modern digital education, artificial intelligence (AI) has become a crucial tool in enhancing English language learning. Pronunciation, in particular, remains a persistent challenge for learners, especially non-native speakers. Traditional methods often rely on teacher feedback, which can be subjective and time-consuming. AI-powered speech recognition systems now offer automated analysis and personalized feedback, significantly improving learning efficiency.

The goal of this research is to examine how AI technologies, such as speech-to-text systems, can analyze phonetic patterns, detect mispronunciations and provide corrective guidance for English learners. By leveraging real-time feedback and data-driven evaluation, these systems support students in acquiring accurate pronunciation and natural speech rhythm.

The relevance of this study is tied to the growing demand for objective, scalable, and individualized learning tools. McCrocklin demonstrates how AI can monitor student behavior during pronunciation practice, identifying frequent errors and tracking progress over time [1]. Khasanov emphasizes the role of AI in improving both listening comprehension and pronunciation accuracy, highlighting how automated systems can complement traditional instruction [2]. Prakash and Kausalya show that speech-to-text AI effectively compares learner output with reference pronunciations, offering immediate corrective feedback that accelerates skill acquisition [3].

The proposed AI-based pronunciation training system continuously monitors the learner’s spoken English and compares it with native speaker patterns. It detects subtle differences in the production of vowels, consonants, and consonant clusters, identifying areas where pronunciation deviates from the standard. At the same time, the system evaluates the natural flow of

speech, including rhythm, stress, and intonation, to uncover patterns that sound unnatural or mechanical. Based on this analysis, personalized feedback is provided, suggesting specific corrections and exercises to help learners gradually improve both accuracy and fluency. By combining real-time monitoring with tailored guidance, the system enables students to develop more natural and confident English speech in a structured and efficient manner.

In practice, AI-based pronunciation systems analyze spoken input using speech recognition algorithms. For example, when a learner pronounces the word *"thought"*, the system compares the produced phoneme /θ/ with the expected English pronunciation and detects whether the learner substitutes it with /s/ or /t/, which is a common error among non-native speakers. Another example is the word *"record"*, where the system analyzes stress placement and determines whether the learner correctly pronounces the noun form (*REcord*) or the verb form (*reCORD*). Such systems can also evaluate sentence intonation. For instance, in the question *"Are you coming today?"* the AI checks whether the pitch rises at the end of the sentence, which is typical for English interrogative intonation. Based on these analyses, the system generates feedback and suggests pronunciation corrections and additional practice tasks.

Table 1

Comparison of Parameters

Parameter	**Linguistic Basis**	**AI Detection Task**
Phonemes	Accuracy of English vowels and consonants	Detect mispronounced sounds
Intonation	Rising/falling pitch patterns	Identify unnatural speech melody
Rhythm & Stress	Word and sentence stress	Provide corrective feedback on timing

In conclusion AI-based systems for pronunciation training offer a scalable and objective alternative to traditional instruction. By integrating speech recognition, phoneme analysis, and prosodic evaluation, learners receive personalized, real-time feedback, improving both pronunciation accuracy and confidence. In the context of modern language education, AI tools are no longer supplementary – they are a technical necessity for effective English learning.

References:

1. McCrocklin S. Monitoring student behavior in automatic speech recognition-based pronunciation practice. 2024. URL: https://www.sciencedirect.com/science/article/pii/S0346251X24001696 (дата звернення: 05.03.2026).

2. Khasanov K. The impact of AI-driven speech recognition on listening comprehension and pronunciation accuracy in English language teaching. 2026. URL: https://link.springer.com/article/10.1007/s10791-026-09992-0 (дата звернення: 05.03.2026).

3. Prakash T., Kausalya S. Speech-to-Text AI for Improving English Pronunciation in ESL Learners. 2025. URL: https://www.ijisrt.com/assets/upload/files/IJISRT25AUG1065.pdf (дата звернення: 05.03.2026).

UDC 004.93:004.8:004.056:81'33

Hohol Oleksandr,
3rd-year student, Specialty – 121 Software Engineering,
HEI «King Danylo University»
Scientific Supervisor:
Kutsela Mariia,
senior lecturer of the Department of
Foreign Philology and Business Communications,
HEI «King Danylo University»,
Ivano-Frankivsk, Ukraine
ORCID: https://orcid.org/0009-0002-1225-2988

LINGUISTIC INDICATORS OF AI-GENERATED PHISHING MESSAGES IN CYBERSECURITY USING NLP TECHNOLOGIES

The rapid development of artificial intelligence technologies has significantly changed the landscape of cyber threats. One of the emerging challenges is the use of AI systems to generate highly persuasive phishing messages that imitate professional business communication. Unlike traditional phishing attempts, these messages demonstrate high linguistic quality and coherent structure, which complicates their identification by both users and conventional filtering systems [4].

The purpose of this study is to examine linguistic features of AI-generated phishing messages and to explore the potential of natural language processing (NLP) technologies for their automatic detection in English-language digital communication.

The growing accessibility of large language models allows attackers to produce convincing messages that replicate the style of corporate correspondence. Such texts often contain appropriate vocabulary, correct grammar, and contextually relevant expressions. However, despite their apparent authenticity, AI-generated messages may still reveal subtle linguistic irregularities. These irregularities can include unusual patterns of lexical repetition, overly neutral stylistic tone, or inconsistencies in pragmatic communication strategies [2].

To address this challenge, a linguo-technical detection approach can be implemented. This approach focuses on the analysis of linguistic markers that

distinguish genuine human communication from automatically generated text. Modern NLP models are capable of identifying hidden statistical patterns within language data and can therefore detect anomalies that remain unnoticed by human readers [1].

The proposed analytical framework includes several stages. At the initial stage, lexical analysis is applied to identify abnormal word usage patterns and frequency distributions. The next stage involves syntactic evaluation, where sentence structures are analyzed for repetitive or overly standardized constructions typical of generated text. Finally, contextual analysis examines whether the semantic content of the message corresponds to realistic corporate communication scenarios [3].

Table 1

Comparison of Identification Parameters

Parameter	**Linguistic Basis**	**Detection Task**
Lexical patterns	Frequency and variation of vocabulary	Detection of repetitive word usage
Syntax	Structural organization of sentences	Identification of automated text patterns
Pragmatics	Communication intent and tone	Detection of manipulation strategies

In conclusion, linguistic analysis combined with artificial intelligence technologies offers promising opportunities for improving cybersecurity systems. By focusing on the linguistic characteristics of digital communication, it becomes possible to detect AI-generated phishing attempts more effectively. For contemporary IT professionals, knowledge of English-language communication patterns therefore represents not only a communication skill but also an important analytical component in the development of intelligent security solutions.

References:

1. Benavides-Astudillo E., Fuertes W., Sanchez-Gordon S., Nuñez A. A Phishing-Attack-Detection Model Using Natural Language Processing and Deep Learning. *Applied Sciences*. 2023. Vol. 13, № 9. P. 5275. (accessed: 10.03.2026).

2. Abdullah A. F., Hassan N. A., Hakim M. A. AI-Powered Threat Intelligence for Cybersecurity: Developing Natural Language Processing Frameworks to Detect Phishing and Text-Based Attacks. *International Journal of Information and Cybersecurity*. 2022. Vol. 4, № 1. (accessed: 10.03.2026).

3. Altan M., Gündüz E., Karabulut M. Dual-Path Phishing Detection: Integrating Transformer-Based NLP with Structural URL Analysis. *Cybersecurity Review*. 2025. № 2. (accessed: 10.03.2026).

4. Kulal S., Chatterjee A., Mishra P. Robust ML-based Detection of Conventional, LLM-Generated, and Adversarial Phishing Emails. *arXiv preprint*. 2025. (accessed: 10.03.2026).

UDC 004.8:35:331.108

Kunitsyn Oleh,
PhD student,
Public Administration and Economic Policy Department,
Simon Kuznets Kharkiv National University of Economics
ORCID: https://orcid.org/0009-0008-7552-7946
Scientific Supervisor:
Gavkalova Nataliia,
Doctor of Economic Sciences, Professor,
Head of Public Administration and Economic Policy Department,
Simon Kuznets Kharkiv National University of Economics,
Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0003-1208-9607

INNOVATIVE AI-BASED TECHNOLOGIES FOR ENHANCING SKILLS AND ADAPTIVE CAPACITY OF PUBLIC SECTOR EMPLOYEES

The rapid diffusion of artificial intelligence (AI) technologies is fundamentally transforming how public sector organizations operate and manage human capital. Governments increasingly rely on data-driven decision-making, automated systems and digital platforms to improve efficiency, transparency and responsiveness. In this context, the skills and adaptive capacity of public sector employees become a critical determinant of successful digital transformation. AI adoption does not merely introduce new technological tools, but reshapes organizational processes, professional roles and institutional cultures, requiring new approaches to workforce development and governance [1].

Unlike the private sector, public organizations operate under additional constraints related to accountability, legal compliance, equity and public trust. These conditions amplify the importance of responsible AI implementation and inclusive skills development. Effective integration of AI in the public sector therefore depends not only on technological readiness but also on structured training, change management and even ethical oversight. This thesis examines how innovative AI-based technologies can enhance the com-

petencies of public sector employees, focusing on training mechanisms, ethical considerations and emerging educational applications. AI adoption significantly alters the nature of work by automating routine tasks, augmenting analytical capabilities and enabling new forms of human–machine collaboration.

Public employees are increasingly required to develop competencies such as data literacy, basic understanding of machine learning concepts and the ability to interact effectively with AI-based systems. Without targeted training initiatives, the potential benefits of AI investments risk being underutilized or resisted by the workforce. Resistance to AI adoption often stems from concerns about job displacement, uncertainty toward unfamiliar technologies and insufficient communication from leadership. These challenges highlight the importance of comprehensive change management strategies accompanying technological implementation. Training programs should extend beyond technical instruction and emphasize the complementary role of AI in supporting professional judgment rather than replacing it. Open communication, early involvement of employees and transparent articulation of expected benefits are essential for building trust and acceptance. For instance, in public service environments such as citizen support centers, the introduction of AI-powered chatbots may initially be perceived as a threat to frontline staff. However, empirical evidence suggests that when employees are trained to use chatbots as tools that handle repetitive inquiries, allowing human agents to focus on complex cases, resistance decreases and adoption improves [2]. This demonstrates that AI-related capacity building must integrate technical training with organizational learning and change management to ensure sustainable outcomes.

The use of AI in the public sector raises critical ethical concerns related to fairness, transparency and accountability. AI systems learn from historical data that may reflect existing social inequalities or institutional biases. If left unaddressed, such biases can be amplified through automated decision-making, leading to discriminatory outcomes in areas such as recruitment, service delivery or policy evaluation [3]. Responsible AI deployment requires proactive bias detection and mitigation throughout the AI lifecycle. This includes auditing training datasets, monitoring algorithmic outputs and establishing governance frameworks that clearly define acceptable use and accountability mechanisms. Transparency remains a particular challenge, as complex algorithms often operate as “black boxes,” making it difficult for public employees and citizens to understand how decisions are produced. Interdisciplinary collaboration among technical experts, policymakers and ethicists, as well as diversity within AI development teams, can help mitigate ethical risks. Clear ethical guidelines and continuous human oversight are especially important in public

administration, where AI-driven decisions may directly affect citizens' rights and access to public services [1].

Personalized learning is one of the most transformative applications of AI in workforce development. AI-driven systems can tailor educational content, pace and complexity to individual learners based on performance and learning patterns. Adaptive learning algorithms and intelligent tutoring systems adjust instructional pathways in real time, improving engagement and learning efficiency [4; 5]. Learning analytics complements personalized learning by using AI to collect and analyze data on learner behavior and outcomes. These insights allow organizations to evaluate training effectiveness, identify skill gaps and optimize instructional design. In the public sector, learning analytics supports evidence-based workforce development by enabling adaptive and responsive training strategies [5]. Virtual and augmented reality (VR/AR) technologies offer immersive learning environments that enhance experiential training. These tools are particularly valuable for scenarios that are complex, costly or risky to replicate in real life, such as emergency response or urban planning simulations. Although AI-driven VR and AR applications in public sector training are still emerging, their potential to improve comprehension and skill retention is substantial [6]. Advances in generative AI have redefined chatbots as sophisticated virtual assistants capable of providing continuous learning support. AI chatbots can answer questions, explain complex concepts and offer personalized guidance, making them valuable tools for self-directed learning among public employees [7]. Their accessibility and responsiveness reduce reliance on traditional training formats and support lifelong learning. As an example, ChatGPT exemplifies the potential of generative AI in education and professional development. As a virtual tutor, it can assist with skill acquisition by providing real-time explanations, feedback and learning resources. Research highlights its value in supporting diverse learners and enhancing online and blended learning environments [7; 8]. At the same time, limitations related to data reliability, overreliance on technology, limited customization and data privacy must be acknowledged. ChatGPT and similar tools should complement, rather than replace, human interaction and critical thinking in education. Responsible integration is therefore essential to maximize benefits while mitigating risks [1].

Innovative AI-based technologies offer significant potential to enhance the skills and adaptive capacity of public sector employees. Through personalized learning, learning analytics, immersive training environments and generative AI tools, AI can transform workforce development and organizational learning. However, successful implementation depends on comprehensive training, effective change management and robust ethical governance. AI should be

understood as a strategic enabler of institutional adaptation rather than a purely technical solution. Future research should focus on assessing the long-term impact of AI-driven training on public sector performance, developing measurable indicators of skill enhancement and identifying best practices for responsible AI integration. These efforts will contribute to more resilient, adaptive and capable public institutions.

References:

1. Giannakos M., Azevedo R., Brusilovsky P., Cukurova M., Dimitriadis Y., Hernandez-Leo D., Järvelä S., Mavrikis M., Rienties B. The promise and challenges of generative AI in education. *Behaviour & Information Technology*. 2024. URL: https://doi.org/10.1080/0144929X.2024.2394886

2. Debets T., Banihashem S. K., Joosten-ten Brinke D. Chatbots in education: A systematic review of objectives, underlying technology and theory, evaluation criteria and impacts. *Computers & Education*. 2025. Vol. 234. Article 105323. URL: https://doi.org/10.1016/j.compedu.2025.105323

3. Khosravi H., Shum S. B., Chen G., Conati C., Tsai Y.-S., Kay J., Knight S., Martinez-Maldonado R., Sadiq S., Gašević D. Explainable artificial intelligence in education. *Computers and Education: Artificial Intelligence*. 2022. Vol. 3. Article 100074. URL: https://doi.org/10.1016/j.caeai.2022.100074

4. Fortuna A., Prasetya F., Samala A. D., Rawas S., Criollo-C S., Kaya D., Raihan M., Andriani W., Safitri D., Nabawi R. A. Artificial intelligence in personalized learning: A global systematic review of current advancements and shaping future opportunities. *Social Sciences & Humanities Open*. 2025. Vol. 12. Article 102114. URL: https://doi.org/10.1016/j.ssaho.2025.102114

5. Lin C.-C., Huang A. Y. Q., Lu O. H. T. Artificial intelligence in intelligent tutoring systems toward sustainable education: A systematic review. *Smart Learning Environments.* 2023. Vol. 10. Article 41. URL: https://doi.org/10.1186/s40561-023-00260-y

6. Sümer M., Vaněček D. A systematic review of virtual and augmented reality in higher education: Trends and issues. *Innovations in Education and Teaching International.* 2024. URL: https://doi.org/10.1080/14703297.2024.2382854

7. Munaye Y. Y., Admass W., Belayneh Y., Molla A., Asmare M. ChatGPT in education: A systematic review on opportunities, challenges and future directions. *Algorithms.* 2025. Vol. 18, No. 6. Article 352. URL: https://doi.org/10.3390/a18060352

8. Habibi A., Muhaimin, Danibao B., Wibowo Y. G. ChatGPT in higher education learning: Acceptance and use. *Computers and Education: Artificial Intelligence.* 2024. Vol. 5. Article 100190. URL: https://doi.org/10.1016/j.caeai.2023.100190

UDC 655.3:004.738.5:621.39

Labetska Marta,
Associate Professor of the Department
of Printing Technologies and Packaging,
Candidate of Technical Sciences, Associate Professor,
National Higher Educational Institution "Lviv Polytechnic University",
Lviv, Ukraine
ORCID: https://orcid.org/0000-0003-2818-051X

SMART PRINTING IN THE AGE OF UBIQUITOUS CONNECTIVITY: CONVERGING INTERACTIVE POLYGRAPHY WITH CLOUD SERVICES, IOT ECOSYSTEMS, AND AUGMENTED REALITY OVERLAYS

The proliferation of cloud computing, the Internet of Things, and mobile connectivity has fundamentally transformed the way information is created, distributed, and consumed. Traditional print media, long regarded as a static and passive channel, is undergoing a paradigm shift driven by the integration of interactive digital layers that augment the physical substrate with dynamic, networked capabilities. This phenomenon – termed interactive polygraphy – represents the systematic application of embedded digital triggers (QR codes, NFC tags, AR markers, conductive inks, and electronic paper displays) within conventional printed artefacts, enabling bidirectional communication between the printed object and cloud-hosted services [1-4].

The significance of this development is amplified by prevailing trends in digital transformation. According to recent industry reports, the global smart packaging market is projected to exceed USD 52 billion by 2027, while AR-enabled print deployments have recorded compound annual growth rates exceeding 28 % since 2021. Concurrently, the ubiquity of smartphone ownership has lowered the barrier to entry for end-users, making interactive print an economically viable proposition across diverse market segments [5; 6]. This paper situates intersections of interactive polygraphy with cloud computing infrastructure, IoT sensor networks, cybersecurity challenges, and the future of immersive digital entertainment. We argue that interactive printing is not a peripheral application of internet technologies, but a foundational medium for their physical-world instantiation.

A coherent theoretical model is required to analyse and design interactive printing systems. We propose the Interactive Print Stack (IPS), a four-layer architectural model analogous to the OSI model in network communications (Fig. 1).

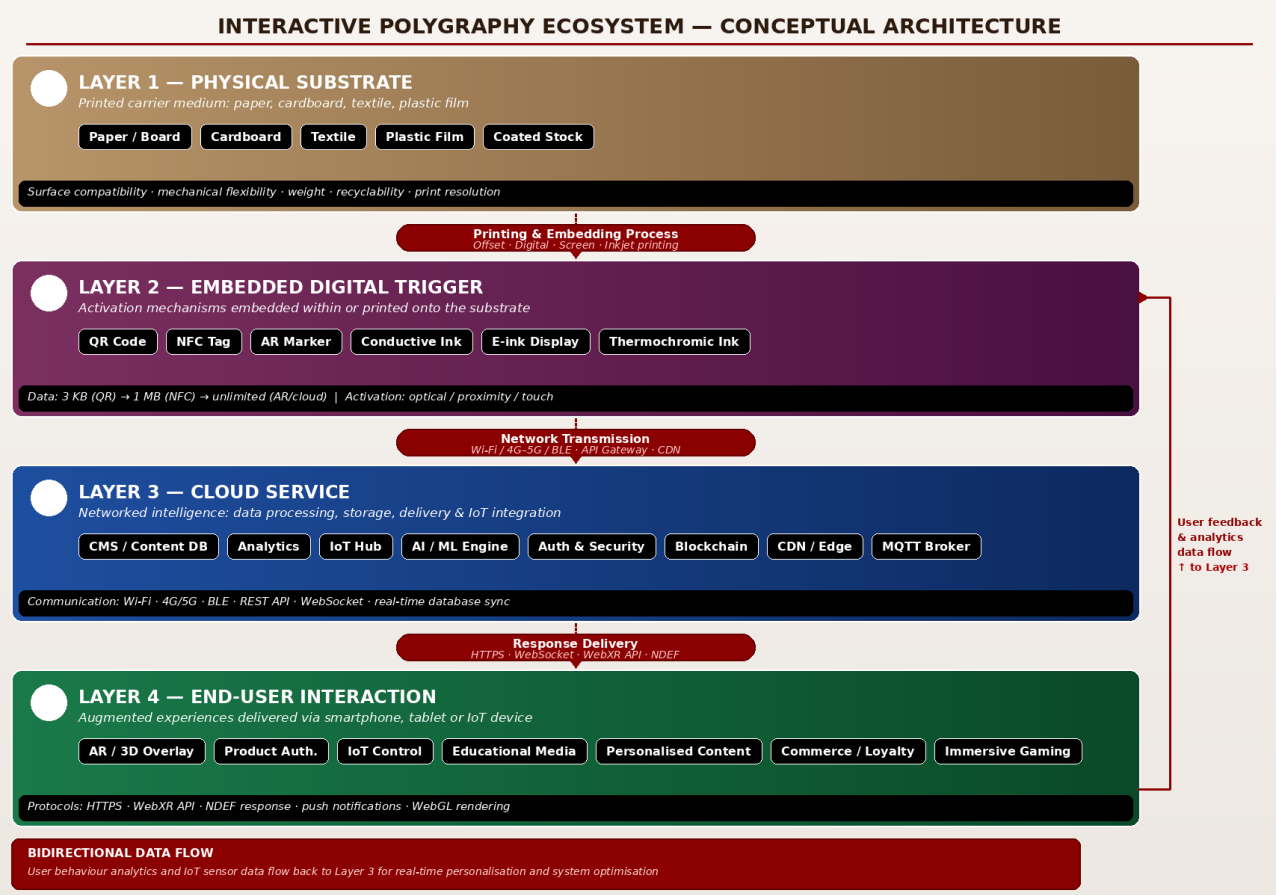

Fig. 1. Conceptual architecture of an interactive polygraphy ecosystem: printed substrate layer, embedded digital trigger layer, cloud service layer, and end-user interaction layer

This layered model provides a systematic basis for comparative technology evaluation and system design, as summarised in Table 1 below.

Table 1

Comparative analysis of interactive polygraphy technologies across key performance dimensions

Technology	Trigger Mechanism	Data Capacity	IoT Integration	Cost Index
QR Code	Camera scan	~3 KB URL/text	Moderate	Low
NFC Tag	Proximity tap	~1 MB	High	Medium
AR Marker	Image recognition	Unlimited (cloud)	Very High	Medium
Conductive Ink	Touch/capacitive	Event-based	High	High
E-ink Display	Wireless signal	Image/text	Very High	Very High
Thermochromic Ink	Temperature	Visual only	Low	Medium

Table 1 reveals that while QR codes offer the lowest deployment cost and near-universal device compatibility, NFC and AR markers provide superior IoT integration capacity. Conductive ink and e-ink technologies, though presently

high-cost, exhibit the greatest potential for fully embedded smart functionality, particularly in the context of Industry 4.0 supply chain applications.

NFC-enabled pharmaceutical packaging connected to cloud medication management systems exemplifies the core value proposition of interactive polygraphy: the printed surface becomes an authenticated IoT node, transmitting real-time dispensing records to MQTT brokers with sub-second latency. Similarly, dynamic QR codes on food packaging – whose target URLs are updated via cloud CMS platforms – enable manufacturers to push batch recall notices, allergen updates, and personalised content without reprinting, transforming static substrates into living communication channels.

AI-driven variable data printing (VDP) paired with machine learning recommendation engines enables personalised AR-enhanced catalogues with documented conversion rate improvements of 34–67 % over conventional print materials. In the entertainment domain, NFC-embedded tabletop game boards interface with cloud game engines to deliver real-time AI-driven narrative logic, while AR-enabled printed publications stream three-dimensional animated overlays via WebAR APIs requiring no application installation. These deployments illustrate the convergence of interactive polygraphy with cloud gaming infrastructure.

Cybersecurity represents a critical challenge: QR code substitution attacks and NFC relay exploits constitute documented threat vectors in networked print deployments. Mitigation approaches under active investigation include ECDSA-signed QR codes, challenge-response NFC authentication, and physical unclonable function (PUF) integration within printed substrates. A standardised security framework for interactive print – analogous to TLS for web communications – remains an urgent research priority [7-10].

The evidence presented confirms that interactive polygraphy occupies a strategically important position at the intersection of physical media and the digital ecosystem. Three research trajectories merit priority attention.

First, the integration of large language models with interactive print enables genuinely intelligent artefacts capable of natural language dialogue via cloud APIs – early 'conversational packaging' prototypes already demonstrate substantial commercial potential. Second, roll-to-roll printed electronics manufacturing is rapidly driving conductive ink and e-ink costs toward parity with conventional QR label printing, projected within three to five years. Third, the environmental sustainability of interactive polygraphy requires systematic investigation: while NFC and e-ink components extend substrate lifespan, their introduction into paper waste streams raises end-of-life challenges not yet addressed by existing regulatory frameworks.

Interactive polygraphy represents not a technological curiosity but a structural transformation of the print medium – from a passive information substrate to an active, connected node within the Internet of Things. As cloud infrastructure matures and printed electronics costs decline, the boundary between physical and digital media will continue to erode, positioning interactive polygraphy as a foundational technology of the connected world.

References:

1. Narashans Alok Sagar, Nitu Rani. Recent trends and innovations in smart and AI-based food packaging: A review. *Frontiers in Food Science and Technology*. 2026. URL: https://www.researchgate.net/publication/399617472 (дата звернення: 01.03.2026).

2. Wang D., Zhang J., Zhang P. TagLabel: RFID Based Orientation and Material Sensing for Automated Package Inspection. *arXiv*. 2025. URL: https://arxiv.org/abs/2512.07097 (дата звернення: 01.03.2026).

3. Chaitra M. S., Malagi A. K. The Impact of Smart Packaging on E-commerce Customer Purchase Decisions. *IJRASet*. 2025. DOI: https://doi.org/10.22214/ijraset.2025.72591

4. Recent Advances in the Fabrication of Intelligent Packaging for Food Preservation: A Review / T. Mkhari, J. O. Adeyemi, O. A. Fawole. *Processes*. 2025. Vol. 13, iss. 2. P. 539. DOI: https://doi.org/10.3390/pr13020539

5. Smart Packaging Market – Forecast (2022–2027) : IndustryARC Market Report. URL: https://www.industryarc.com/Report/240/global-smart-packaging-market-report.html (дата звернення: 11.03.2026).

6. Augmented Reality Industry worth $88.4 billion by 2026 : MarketsandMarkets Press Release. URL: https://www.marketsandmarkets.com/PressReleases/augmented-reality.asp (дата звернення: 11.03.2026).

7. Fiałkowska-Filipek M., Karpavičė J., Wangwacharakul P. Smart packaging as a digital enabler for circularity in sustainable supply chains. *Climate Smart Sustainable Supply Chains*. 2026. DOI: https://doi.org/10.1016/j.clscn.2026.100299

8. Flexible strain sensor with NFC tag for food packaging / P. Escobedo et al. *2020 IEEE International Conference on Flexible and Printable Sensors and Systems (FLEPS)* : Conference Paper (August 2020). P. 1–4. DOI: https://doi.org/10.1109/FLEPS49123.2020.-9239535

9. Advances and Challenges in Smart Packaging Technologies for the Food Industry: Trends, Applications, and Sustainability Considerations / M. A. Davidescu et al. *Foods*. 2025. Vol. 14, iss. 24. P. 4347. DOI: https://doi.org/10.3390/foods14244347

10. From passive to self-aware packs: Flexible Sensor-AI integration powering intelligent, sustainable food packaging / Z. Jia et al. *Trends in Food Science & Technology*. 2025. P. 105254. DOI: https://doi.org/10.1016/j.tifs.2025.105254

UDC 334.72

Lytvynenko Andriy,
Associate Professor of the Department of Public Administration,
Public Administration and Economic Policy,
Candidate of Economic Sciences, Associate Professor,
Semen Kuznets Kharkiv National University of Economics,
Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-5973-5173

ENTERPRENUERSHIP DEVELOPMENT IN UKRAINE: PROBLEMS, TRENDS AND PROSPECTS

In recent decades, entrepreneurship has increasingly been viewed not only as a source of economic growth, but also as a mechanism that allows the economy to adapt to structural shocks and institutional changes. The ongoing processes of globalization and digital transformation have significantly changed the role of entrepreneurship. Today, entrepreneurial initiatives are increasingly associated with the creation and dissemination of innovations, rather than just traditional business activities.

For Ukraine, the development of entrepreneurship is of particular importance in the conditions of war and post-war transformations of the economy. It is the entrepreneurial sector that is able to act as a driver of economic recovery, stimulate innovative activity and contribute to the integration of Ukraine into the European economic space. Unlike many transition economies, Ukraine is demonstrating a rapid transition to micro-scale digital entrepreneurship in the face of military uncertainty.

From a theoretical perspective, entrepreneurship has been interpreted differently across different economic schools. While classical economists viewed it primarily as a factor of production, later approaches have emphasized the role of the entrepreneur in innovation, risk-taking, and the discovery of market opportunities. Classical economic theory considers entrepreneurship as a factor of production along with land, labor and capital, emphasizing the role of the entrepreneur as an organizer of production and a bearer of economic risk.

The Austrian School of Economics views the entrepreneur as an innovator who identifies market opportunities and creates new products. At the same time, institutional theory emphasizes the influence of the quality of state institutions on the development of entrepreneurship, and modern approaches combine economic, social and environmental aspects of business, in particular through the development of social entrepreneurship. The level of entrepreneurship development in a country is assessed using a system of

indicators, among which the key ones are the level of entrepreneurial activity of the population, the density of new business creation, innovative business activity, the survival rate of small businesses and access to financial resources.

International analytical reports indicate that small and medium-sized enterprises remain the dominant source of employment in most national economies and generate a significant share of gross domestic product [1].

In Ukraine, the small and medium-sized business sector also plays a key role in the national economy. According to the Ministry of Economy of Ukraine, in 2024, about 2 million individual entrepreneurs operated in the country, and the share of small and medium-sized businesses accounted for over 99 % of all enterprises, providing about 63 % of employment [2].

The development of entrepreneurship in Ukraine is taking place in conditions of significant challenges. The full-scale war led to significant economic losses, destruction of infrastructure and relocation of a significant number of enterprises. According to estimates by international economic organizations, in 2022, about 30 % of enterprises temporarily ceased operations, and some businesses were forced to move production to other regions or abroad.

Despite this, the Ukrainian entrepreneurial ecosystem demonstrates significant adaptability. The startup sector is developing significantly, especially in the field of information technology. According to the international ranking StartupBlink, Ukraine is among the 50 largest startup ecosystems in the world, and the number of technological startups exceeds 2,000 projects [3; 4].

In the Ukrainian context, further expansion of entrepreneurial activity will largely depend on the consistency of government policies. Regulatory predictability, access to finance, and institutional support for innovative firms remain key factors shaping the business environment. Immediate policy priorities include regulatory simplification, wider access to financing for small and medium-sized enterprises, and institutional support for innovation-oriented enterprises. Digitalization has become one of the most important drivers of modern entrepreneurship. For many small firms, especially in developing countries, digital platforms and online commerce significantly lower the barriers to market entry. As a result, Ukrainian entrepreneurs are increasingly relying on digital channels not only to reach domestic consumers, but also to access international markets.

A comparative analysis of the development of entrepreneurship in different countries allows us to assess the structural features of entrepreneurial ecosystems and identify factors of their competitiveness. Generalized indicators of entrepreneurial activity, the role of small and medium-sized businesses in the economy and innovation potential are presented in Table 1.

Table 1

Comparative characteristics of the development of entrepreneurship in individual countries*

Indicator	USA	Germany	Japan	Ukraine
Entrepreneurial activity of the population (TEA), %	15–16	8–9	5–6	7–8
Share of SMEs in the number of enterprises, %	99.9	99.6	99.7	99.8
Share of SMEs in employment, %	47	60	70	63
Share of SMEs in GDP, %	≈44	≈53	≈52	≈55
Level of innovation (Global Innovation Index, place)	3	8	13	55
Density of startups	very high	high	medium	increasing

* Compiled by the author based on analytical reports from the OECD, GEM and StartupBlink.

As can be seen from the table, developed economies are characterized by high entrepreneurial activity, a significant role of small and medium-sized businesses in creating added value, and a developed innovation ecosystem. In Ukraine, despite the difficult economic and military conditions, there is a positive dynamics of entrepreneurship development, which is manifested in the growth of the number of startups, the activation of digital business and the gradual expansion of access to international markets.

The development of entrepreneurship is one of the key factors of economic recovery and long-term growth of Ukraine. The formation of an effective entrepreneurial ecosystem requires a combination of state support, innovative business activity and integration into the global economy. Under current wartime conditions, entrepreneurial flexibility becomes one of the key factors of macroeconomic stability.

References:

1. Global Report 2023/2024. *Global Entrepreneurship Monitor (GEM)*. URL: https://www.gemconsortium.org

2. SME and Entrepreneurship Outlook 2023. *OECD*. URL: https://www.oecd.org

3. Entrepreneurship and SME development indicators. *World Bank*. 2024. URL: https://www.worldbank.org

4. Global Startup Ecosystem Index. *StartupBlink*. 2024. URL: https://www.startupblink.com

UDC 278

Marynchenko Inna,
PhD in Pedagogies, associate professor
of the Department Vocational Education and Computer Technologie,
Oleksandr Dovzhenko Hlukhiv National Pedagogical University,
Hlukhiv, Ukraine
ORCID ID: https://orcid.org/0000-0001-5424-8085

THE POTENTIAL OF THE DIGITAL EDUCATIONAL ENVIRONMENT IN SHAPING THE PEDAGOGICAL EXPERTISE OF PRE-SERVICE TEACHERS

The digital transformation of modern education is causing profound changes in the system of professional training of pedagogical personnel, highlighting the need to rethink traditional approaches to the formation of pedagogical skills of future teachers. In modern socio-cultural conditions, the digital educational environment is gradually becoming a leading space for the professional development of a teacher, which combines educational, informational, communicative and creative capabilities of digital technologies. Its functioning not only provides access to a variety of educational resources, but also creates conditions for the development of professional independence, reflection and innovative thinking of future teachers [5].

Pedagogical skills in modern pedagogical science are considered as an integrative professional characteristic of a teacher's personality, which is manifested in the ability to effectively organize the educational process, achieve high learning and upbringing results, creatively apply pedagogical technologies and adequately respond to the challenges of the educational environment. It is based on a combination of deep professional knowledge, methodological training, pedagogical culture, communication skills and the ability to constantly develop professionally. In the context of digitalization of education, the content and structure of pedagogical skills are undergoing significant transformations, as digital competence, readiness to use innovative technologies and the ability to work in a digital educational environment are added to traditional professional qualities [2].

Presentation of the main material. The digital educational environment is a complex dynamic system that encompasses a set of digital resources, platforms, services, software tools and pedagogical conditions that ensure the implementation of the educational process in synchronous and asynchronous formats. It creates opportunities for the integration of various forms of educational activity, individualization of educational trajectories and expansion

of the boundaries of traditional classroom interaction. For future teachers, the digital educational environment is not only a tool for acquiring knowledge, but also a model of future professional activity, within which professional values, pedagogical attitudes, and skills in working with digital technologies are formed [5].

In the process of professional training of future teachers, the digital educational environment ensures the integration of theoretical and practical components of training. Thanks to the use of electronic courses, virtual training modules, online platforms and digital educational resources, students have the opportunity to master modern pedagogical technologies, analyze pedagogical situations, model the educational process and reflect on their own activities. This approach contributes to the formation of a holistic view of the teaching profession and the development of pedagogical skills as a systemic quality of the individual [1].

An important aspect of the formation of pedagogical skills in the digital educational environment is the development of the motivational and value sphere of future teachers. Digital technologies create conditions for the active involvement of students in the educational process, stimulate their cognitive activity and contribute to the formation of internal motivation for professional growth. Participation in joint online projects, professional communities and network forms of interaction contributes to the awareness of the social significance of pedagogical activity and the formation of a positive attitude towards the teaching profession.

The cognitive component of pedagogical skills is formed in a digital educational environment through access to a wide range of information resources, scientific databases, electronic libraries and open online courses. Future teachers are given the opportunity to systematically update their knowledge, expand their professional horizons and master modern pedagogical concepts. At the same time, an important task of professional training is to form the ability to critically evaluate information, select scientifically sound sources and use them in professional activities [7].

The operational and activity component of pedagogical skills is developed in the process of practical use of digital technologies to organize the educational process. Future teachers learn to design educational sessions using digital tools, create electronic educational resources, apply interactive teaching methods and carry out digital assessment of students' academic achievements. Such activities contribute to the formation of professional skills and abilities necessary for effective pedagogical work in a digital school.

The communicative aspect of pedagogical skills acquires particular importance in the digital educational environment, since the interaction

between participants in the educational process is carried out using digital means of communication. Online discussions, forums, video conferences and joint project activities contribute to the development of communicative skills, the ability to cooperate and the culture of pedagogical communication. Future teachers gain experience in organizing educational interaction in a digital format, which is an important component of their professional skills [3].

The reflective component of pedagogical skills is formed through the use of digital self-assessment tools, electronic portfolios and analytical tools for tracking educational achievements. The digital educational environment creates conditions for systematic analysis of one's own activities, awareness of professional achievements and determination of directions for further development. Reflection is an important factor in the professional growth of future teachers and contributes to the formation of pedagogical skills as a dynamic process.

The effectiveness of the formation of pedagogical skills in a digital educational environment largely depends on the pedagogical conditions of its organization. These conditions include scientifically sound pedagogical design of digital educational content, integration of digital technologies into the content of professional training, provision of methodological support and mentoring. An important condition is also the readiness of teachers to work in a digital educational environment and their readiness to use innovative pedagogical technologies [5].

At the same time, the use of a digital educational environment is accompanied by a number of challenges, among which technical limitations, unequal access to digital resources, the risk of formalization of the educational process and a decrease in the level of direct interpersonal interaction can be distinguished. Overcoming these challenges requires a systematic approach to organizing the professional training of future teachers and the implementation of pedagogically appropriate models of using digital technologies.

Conclusions. The digital educational environment acts as a holistic space for the formation of pedagogical skills of future teachers, within which the development of professional knowledge, skills, values and personal qualities necessary for successful pedagogical activity is ensured. Its pedagogical potential lies in the possibility of integrating innovative technologies, activating cognitive activity and creating conditions for continuous professional self-development of future teachers.

The prospects for the development of the digital educational environment as a space for the formation of pedagogical skills of future teachers are associated

with the further improvement of the digital infrastructure of educational institutions, expanding the capabilities of blended and personalized learning, using artificial intelligence technologies and educational data analytics. The implementation of these areas will contribute to improving the quality of professional training of teachers and forming their readiness for activity in the conditions of digital transformation of education.

References:

1. Bykov V. Yu. Digital transformation of education and science in Ukraine: current state and prospects for development. *Information technologies and teaching aids.* 2021. Vol. 84. No. 4. P. 1–15.

2. Bondar V. I. Pedagogical skills of a future teacher in the conditions of a digital educational environment. *Pedagogical sciences: theory, history, innovative technologies.* 2022. No. 3. P. 45–54.

3. Gurevich R. S., Kademiya M. Yu. Digital educational environment of a higher education institution: theoretical and methodological principles of formation. *Bulletin of the National Academy of Pedagogical Sciences of Ukraine.* 2021. No. 3. P. 32–40.

4. Kuzminsky A. I. Formation of pedagogical skills of a future teacher in the conditions of a digital educational environment. *Pedagogy and psychology*. 2022. No. 1. P. 17–25.

5. Marynchenko I. V. Peculiarities of the development of pedagogical skills of a teacher of a higher education institution in accordance with the requirements of the labor market. *Innovative Pedagogy*. 2023. Vol. 57, No. 2. P. 52-56. http://www.innovpedagogy.od.ua/archives/2023/57/part_2/9.pdf

6. Spirin O. M. Theoretical principles of the formation of a digital educational environment of a pedagogical education institution. *Scientific Bulletin of the Institute of Vocational and Technical Education of the National Academy of Sciences of Ukraine.* 2022. No. 1. P. 5–14.

7. Braslavska O., Marynchenko I., Samus T., Martyniuk T., Pushchyna I., Shcherbyna S. Preparation of future teachers for professional adaptation in an inclusive educational environment in the process of studying the methodology of Science. *AD ALTA : Journal of Interdisciplinary Research*. 2024. Vol. 14, Issue 1, Special Issue XLL. Pp. 42–49. URL: https://www.magnanimitas.cz/14-01-xli

UDC 81’25:004.8:159.9

Milinchuk Ihor,
3rd-year student, Specialty – 121 Software Engineering,
HEI «King Danylo University»
Scientific Supervisor:
Kutsela Mariia,
senior lecturer of the Department of
Foreign Philology and Business Communications,
HEI «King Danylo University»,
Ivano-Frankivsk, Ukraine
ORCID: https://orcid.org/0009-0002-1225-2988

ACCURACY CRITERIA IN TRANSLATION: A COMPARATIVE ASPECT OF AI, MACHINE SYSTEMS AND HUMANS

Translation accuracy has long been a central concern in Translation Studies, where scholars evaluate how effectively a translation preserves meaning, communicative intent, and functional equivalence between the source and target languages. In the contemporary linguistic landscape, three major translation agents coexist: generative artificial intelligence systems such as ChatGPT or Claude, neural machine translation (NMT) systems like Google Translate and DeepL, and professional human translators. Each of these entities demonstrates distinct strengths and limitations in terms of contextual fidelity, handling of cultural nuances, grammatical precision, and the balance between speed and interpretative nuance.

Generative AI systems represent a relatively new stage in the evolution of machine translation and language technologies. These systems are based on large language models trained on extensive multilingual corpora and are capable of modeling discourse-level linguistic patterns. As a result, generative AI often produces translations that are stylistically fluent and grammatically coherent, frequently resembling natural human communication [1]. Their ability to process broader textual context allows them to approximate communicative intent more effectively than earlier translation technologies. This makes them particularly useful for tasks where contextual interpretation and stylistic adaptation are required.

At the same time, generative AI systems may occasionally produce inaccuracies due to semantic drift or so-called hallucinations, where the generated output appears plausible but does not fully correspond to the meaning of the source text. Despite this limitation, generative AI represents an important technological development within the broader process of digital

transformation, where intelligent systems increasingly support analytical and linguistic tasks traditionally performed by humans [2]. Consequently, such systems are often used as supportive tools rather than as independent translation solutions.

Neural machine translation systems such as Google Translate and DeepL rely on transformer-based neural networks trained on parallel linguistic corpora. Their primary advantage lies in their ability to process extremely large volumes of text in a very short time. In technical or standardized domains, these systems can produce translations with high grammatical accuracy and relatively consistent lexical choices. The widespread adoption of such technologies demonstrates how artificial intelligence has become an integral component of modern digital infrastructures and translation workflows [3].

However, neural machine translation systems often struggle with complex linguistic phenomena such as idioms, metaphors, and culturally specific expressions. Because their algorithms rely heavily on statistical patterns in training data, these systems may translate idiomatic phrases literally instead of conveying their pragmatic meaning in the target language. As a result, the translation may be grammatically correct but pragmatically inappropriate. Furthermore, the contextual scope of many NMT systems is still limited primarily to sentence-level processing, which can reduce the overall cohesion of longer texts [4].

Professional human translators approach translation from a fundamentally different perspective that combines linguistic competence with cultural knowledge and contextual interpretation. Human translators rely on cognitive analysis to determine how best to preserve the communicative intent of the original text while adapting it to the expectations of the target audience. In translation theory, this process is often described through the concept of functional equivalence, which emphasizes the reproduction of meaning and communicative function rather than literal word-for-word correspondence [5].

Human translators also possess the ability to perform transcreation, a strategy that involves creatively adapting cultural references, idiomatic expressions, and stylistic elements so that they produce the same communicative effect in another language. Such skills are especially important in fields such as literature, marketing, diplomacy, and legal communication. Unlike automated systems, human translators can interpret humor, irony, cultural symbolism, and rhetorical nuance, which are often essential elements of meaningful cross-cultural communication.

Another important distinction between human translation and automated systems lies in the trade-off between speed and interpretative depth. Artificial intelligence technologies are capable of producing translations almost instantly, which makes them highly efficient for large-scale translation tasks and internal

communication processes. This efficiency reflects the broader trend toward automation and digitalization in modern information systems and analytical processes [2]. Human translators, in contrast, require more time to analyze context, verify terminology, and ensure stylistic consistency. Nevertheless, this slower process often results in higher levels of semantic precision and cultural adequacy.

Because of these complementary strengths and weaknesses, modern translation workflows increasingly rely on hybrid approaches that combine machine translation with human expertise. In such workflows, automated systems generate an initial translation draft that is subsequently refined through machine translation post-editing (MTPE) performed by professional translators. This process allows organizations to benefit from the speed and scalability of artificial intelligence while maintaining the accuracy, clarity, and cultural sensitivity provided by human linguistic competence. The growing integration of artificial intelligence into professional workflows illustrates the broader transformation of knowledge-based industries in the digital era [3].

In conclusion, although generative AI and neural machine translation technologies have significantly improved the efficiency and accessibility of translation, human translators remain essential for tasks that require deep contextual interpretation, cultural awareness, and stylistic precision. Automated systems currently dominate in situations where speed, scalability, and cost efficiency are the primary priorities. However, in domains where communicative intent, cultural nuance, and rhetorical meaning are crucial, human expertise remains irreplaceable. Therefore, the most effective approach to modern translation is not the replacement of human translators by machines, but rather the integration of artificial intelligence into collaborative translation ecosystems that combine technological efficiency with human interpretative intelligence.

References:

1. Vaswani A. et al. Attention Is All You Need. *Advances in Neural Information Processing Systems*. 2017. URL: https://arxiv.org/abs/1706.03762 (дата звернення: 09.02.2026).

2. Brynjolfsson E., McAfee A. The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. New York : W. W. Norton & Company, 2017. URL: https://books.google.com/books?id=f_S_BAAAQBAJ (дата звернення: 09.02.2026).

3. Kenny D. Machine Translation: Yesterday, Today, and Tomorrow. *Translation Spaces*. 2022. URL: https://www.jbe-platform.com/content/journals/2211372x (дата звернення: 09.02.2026).

4. Pym A. Exploring Translation Theories. 2nd ed. London : Routledge, 2014. 178 p.

5. Nida E. A., Taber C. R. The Theory and Practice of Translation. Leiden : E. J. Brill, 1969.

UDC 004.93:004.8:004.056:81'33

Vandzhuliak Andriy,
3rd-year student, Specialty – 121 Software Engineering,
HEI «King Danylo University»
Scientific Supervisor:
Kutsela Mariia,
senior lecturer of the Department of
Foreign Philology and Business Communications,
HEI «King Danylo University»,
Ivano-Frankivsk, Ukraine
ORCID: https://orcid.org/0009-0002-1225-2988

LINGUO-TECHNICAL ASPECTS OF DEEPFAKE IDENTIFICATION IN CYBERSECURITY USING CONVOLUTIONAL NEURAL NETWORKS

In the era of digital globalism, the English-speaking corporate environment has become the primary target for sophisticated social engineering attacks. The emergence of deepfakes – AI-generated synthetic media – poses a threat not only to data integrity but to the very essence of linguistic communication. The urgency of this study lies in the necessity to detect deepfakes by analyzing the "linguo-technical" gap: the subtle mismatch between acoustic phonemes and visual articulation, which remains a challenge for even the most advanced generative models [1].

The goal of the research is to explore how Convolutional Neural Networks (CNNs) can be utilized to identify deepfakes by analyzing the phonetic-articulatory patterns of the English language and detecting desynchronization in speech acts.

The relevance of this study is primarily driven by the challenge of phonetic and articulatory inconsistency in synthetic media. Convolutional Neural Networks (CNNs) have proven capable of analyzing the precise articulation of English phonemes, which allows for the identification of discrepancies between visual lip movements, known as visemes, and their corresponding spoken sounds. This technical detection is crucial because attackers increasingly exploit the nuances of Business English and professional discourse to conduct corporate linguistic manipulation, creating highly convincing fake directives that necessitate high linguistic awareness within cybersecurity. Furthermore, the issue of dataset bias remains a significant factor, as the majority of high-quality training sets, such as FaceForensics++, are predominantly based on English-speaking content. This geographical and linguistic concentration makes proficiency in the

English language a critical technical skill for developers designing effective detection algorithms.

Linguo-Technical Detection Framework**:** The proposed detection framework utilizes a multi-layered approach to verify the authenticity of digital content. At its core, the system employs Lip-Read Analysis via CNNs to extract spatial features from video frames, ensuring that facial muscle movements strictly align with the phonetic requirements of English vowels and consonants. This is complemented by an Audio-Visual Cross-Modality component, which compares the spectral characteristics of the English voice with the visual flow to detect "micro-stuttering" or unnatural transitions that are often invisible to the human eye. Finally, the framework incorporates Semantic Discourse Analysis to identify anomalies in the pragmatics of the message. By detecting linguistic behaviors that do not align with the established patterns of the impersonated individual, the system provides a robust defense against sophisticated deepfake attacks.

Table 1

Comparison of Identification Parameters

Parameter	**Linguistic Basis**	**CNN Detection Task**
Articulation	Phonetic accuracy of English sounds.	Detection of viseme-phoneme mismatch.
Prosody	Rhythm, stress, and intonation.	Identification of robotic or "flat" speech patterns.
Context	Business English terminology.	Analysis of semantic anomalies in corporate discourse.

In conclusion, the intersection of linguistics and IT security provides a more robust defense against synthetic threats. By training Convolutional Neural Networks to recognize the specific articulatory and phonetic signatures of the English language, we can achieve higher accuracy in deepfake detection. For a modern IT specialist, deep knowledge of the English language is no longer just a communication tool but a technical necessity for developing and auditing security systems in a globalized digital world.

References:

1. Agarwal S., Farid H., Gu Y., He M., Luo J., Liu S. Protecting World Leaders Against Deepfakes. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. 2020. (accessed: 02.03.2026).

2. Halliwell J., Kalkan S. Phoneme-Viseme Mismatch Detection for Deepfake Content. *University of Bristol, Faculty of Engineering*. 2022. (accessed: 02.03.2026).

3. Rössler A., Cozzolino D., Verdoliva L., Riess C., Nießner M., Thies J. FaceForensics++: Learning to Detect Manipulated Facial Images. *International Conference on Computer Vision (ICCV)*. 2019. (accessed: 03.03.2026).

4. Mirsky Y., Lee W. The Creation and Detection of Deepfakes: A Survey. *ACM Computing Surveys (CSUR)*. 2021. № 54 (1). P. 1–36. (accessed: 03.03.2026).

Наукове видання

СИНЕРГІЯ ІНТЕРНЕТ-ТЕХНОЛОГІЙ

Матеріали І Всеукраїнської науково-практичної конференції

(26 березня 2026 року)

Відповідальний за випуск: Є. О. Письменський

Упорядник: Д. Л. Мотульська

Коректор: Д. Л. Мотульська

Формат 60х84/16.

Гарн. PT Serif.

Умовн. др. арк. 45.

ЗВО «Університет Короля Данила»

76018, м. Івано-Франківськ, вул. Євгена Коновальця, 35

тел. +38(068) 755 75 75

УНІВЕРСИТЕТ
КОРОЛЯ ДАНИЛА

ПРОСТІР ФОРМУВАННЯ

УСПІШНИХ

м. Івано-Франківськ, 76018
вул. Є. Коновальця, 35
www.ukd.edu.ua