НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА

ІНСТИТУТ ПРОБЛЕМ РЕЄСТРАЦІЇ ІНФОРМАЦІЇ

ЗБІРНИК МАТЕРІАЛІВ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ «ШТУЧНИЙ ІНТЕЛЕКТ І БЕЗПЕКА»

19-21 листопада 2024 р.

Київ–2024

УДК 004(8+056+413.4)
ББК 32.813
Ш-94

Рекомендовано до друку Вченою радою Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (протокол № 12 від 28 листопада 2024 р.)

Ш-94 **Штучний інтелект і безпека,** науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Інституту проблем реєстрації інформації Національної академії наук України : матеріали, 19-21 листопада 2024 р. Київ : ІПМЕ ім. Г.Є.Пухова НАН України, ІПРІ НАН України, 2024. 115 с.

SH-94 **Artificial intelligence and security**, scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine, Institute for Information Recording of the National Academy of Sciences of Ukraine : materials, November 19-21, 2024. Kyiv: PIMEE NAS of Ukraine, IPRI NAS of Ukraine, 2024. 115 p.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
(м. Київ)
Інститут проблем реєстрації інформації
(м. Київ)

ПРОГРАМНИЙ КОМІТЕТ

Мохор Володимир Володимирович
член-кореспондент НАН України, доктор технічних наук, професор,
директор Інституту, голова програмного комітету

Чемерис Олександр Анатолійович
доктор технічних наук, старший науковий співробітник
заступник директора з наукової роботи

Чьочь Вікторія Володимирівна
кандидат технічних наук,
заступник директора з науково-технічної роботи

Артемчук Володимир Олександрвич
доктор технічних наук, старший науковий співробітник
заступник директора з науково-організаційної роботи

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Артемчук Володимир Олександрвич
доктор технічних наук, старший науковий співробітник
заступник директора з науково-організаційної роботи

Клименко Тетяна Михайлівна
Завідувачка науково-організаційного відділу

Цуркан Оксана Володимирівна
молодший науковий співробітник

Д.В. Ланде, В.І. Полуциганова, С.А. Смирнов

МЕТОДОЛОГІЯ РОЮ ВІРТУАЛЬНИХ ЕКСПЕРТІВ ДЛЯ ОЦІНКИ ВЗАЄМОЗВ'ЯЗКУ ЗАГРОЗ ТА УРАЗЛИВОСТЕЙ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У сучасних дослідженнях у сфері оцінки ризиків для об'єктів критичної інфраструктури важливим є методологічний підхід до оцінки взаємозв'язку між загрозами та уразливостями [1], [2]. Традиційно для цих цілей використовуються методи, засновані на експертних оцінках, однак такі підходи часто стикаються з проблемами суб'єктивності, обмеженого числа експертів і складності в інтеграції різноманітних знань.

Одним із підходів, який дозволяє ефективно вирішувати ці проблеми, є методологія «рою віртуальних експертів» [3], [4]. Термін «рій» у цьому контексті означає сукупність численних віртуальних агентів (експертів), які одночасно взаємодіють із системою штучного інтелекту (зокрема, великими мовними моделями - LLM), з метою отримання максимально точних і збалансованих оцінок. Кожен промпт, сформульований як запит до LLM, виступає як окремий "віртуальний експерт", що вносить свій внесок у загальний результат.

Метою роботи є створення та обґрунтування методології рою віртуальних експертів для оцінки взаємозв'язку між загрозами та уразливостями об'єктів критичної інфраструктури з використанням великих мовних моделей (LLM) та їх математичного моделювання для підвищення точності і надійності оцінок ризиків у сфері кібербезпеки.

Особливістю використання рою віртуальних експертів є те, що цей процес контролюється людиною, яка координує запити до системи, формує промпти і інтегрує відповіді, отримані від різних агентів. Це дозволяє зберігати певний рівень контролю над процесом, уникати системних помилок, що можуть виникати через відсутність нагляду.

Принцип роботи рою віртуальних експертів полягає у наступному:

- Кожен віртуальний експерт отримує запит у вигляді певного промпта, що містить інформацію про загрози, уразливості, або інші параметри системи.

- Після того, як кілька експертів надають свої оцінки, ці оцінки агрегуються. Агрегація може бути здійснена за допомогою зваженого середнього, або більш складних методів, таких як методи зліплення оцінок на основі ймовірності.

- Хоча кожен експерт є автономним, роль людини в цьому процесі полягає в тому, щоб здійснювати контроль за формулюванням запитів і корекцією відповідей, а також оцінювати консистентність отриманих результатів. Людина може коригувати промпти або вводити додаткові уточнення.

Використання рою віртуальних експертів для оцінки загроз та уразливостей має такі переваги, як урахування множинності точок зору, забезпечення точності оцінок, гнучкість і адаптивність, з ниження впливу людського фактора. Автоматизація процесу оцінки загроз та уразливостей знижує ймовірність помилок, які можуть бути пов'язані з людським фактором. Водночас, роль людини залишається важливою для контролю за коректністю результатів.

Загрози та уразливості є основними компонентами в аналізі безпеки критичних інфраструктур. Загроза визначається як можливість здійснення негативного впливу на систему, викликаного зловмисними діями або природними факторами. Уразливість — це слабкість системи, яка може бути використана для реалізації загрози. Взаємодія між цими двома поняттями є основою для прогнозування потенційних ризиків та побудови адекватних заходів безпеки.

Для коректного аналізу взаємозв'язків між загрозами та уразливостями пропонується використовувати матриці інцидентності, де кожен елемент матриці позначає наявність зв'язку між конкретною загрозою та уразливістю.

Нехай існує набір загроз $U = \{u_1, u_2, ..., u_m\}$ та набір уразливостей $B = \{b_1, b_2, ..., b_n\}$, де m — кількість загроз, а n — кількість уразливостей. Тепер можемо побудувати матрицю інцидентності M розміру $m \times n$, елементи якої m_{ij} показують наявність взаємозв'язку між загрозою u_i та уразливістю b_j:

$$M = \begin{pmatrix} m_{11}\ m_{12}\ \ldots m_{1n} \\ m_{21}\ m_{22}\ \ldots m_{2n} \\ . \\ . \\ . \\ m_{m1}\ m_{m2}\ \ldots m_{mn} \end{pmatrix},$$

де:

- $m_{ij} = 1$, якщо загроза u_i може бути реалізована через уразливість b_j;
- $m_{ij} = 0$, якщо зв'язку між загрозою та уразливістю немає.

Для зниження похибок та підвищення точності необхідно використовувати методи агрегації відповідей, отриманих від різних LLM. Одним із підходів є використання **методів зваженого середнього**, де кожній

відповіді від конкретної моделі надається вага в залежності від її надійності або точності. Ваги можуть бути визначені на основі досвіду моделей, їх специфікацій або попереднього тестування.

Щоб ефективно агрегувати відповіді від різних LLM у концепції «рою віртуальних експертів», метод зваженого середнього можна організувати із урахуванням:

- Кількості токенів у у кожній LLM. Цей параметр можна використати для надання вищої ваги таким моделям.
- Новіші релізи LLM можуть володіти більш актуальними знаннями, враховувати сучасні технології і методи, а також мати покращену архітектуру.
- Релевантності відповідей на тестових запитах, попередні результати тестування або експертні оцінки.

Після визначення вагових значень для кожної моделі (наприклад, $w_1, w_2, \ldots, w_n$), де w_i – вага відповідної LLM, можна розрахувати середню відповідь з урахуванням внеску кожної моделі. Якщо кожна модель видає оцінку або текстову відповідь a_i, тоді зважена середня відповідь A обчислюється як:

$$A = \frac{\sum_{i=1}^{n} w_i \cdot a_i}{\sum_{i=1}^{n} w_i}.$$

Таким чином, відповіді моделі з вищою вагою більше впливатимуть на кінцевий результат, підвищуючи точність і зменшуючи похибки.

Рій віртуальних експертів генерує числові оцінки на основі зазначених факторів. У таблиці інцидентності кожна клітинка відображає оцінку ймовірності зв'язку між конкретною загрозою та уразливістю. За допомогою методу "середнього" можна агрегувати оцінки рою для кожної клітинки таблиці. Середня оцінка для кожної пари загроза-уразливість визначається як середнє значення по всіх оцінках віртуальних експертів:

$$\hat{m}_{ij} = \frac{1}{K} \sum_{k=1}^{K} m_{ij}^{k}.$$

Така середня оцінка дає загальне уявлення про ймовірність наявності зв'язку між загрозою і уразливістю на основі оцінок рою.

Оскільки оцінки для кожної пари загроза-уразливість генеруються різними віртуальними експертами, важливо оцінити точність середніх оцінок. Можна ввести критерій точності для кожної пари загроза-уразливість, що дозволяє з'ясувати, наскільки точними є середні оцінки.

Для цього введемо функцію точності, що визначає різницю між середньою оцінкою та фактичною оцінкою, яку дають людські експерти або система автоматичної перевірки:

$$\delta_{ij} = \left| \hat{m}_{ij} - \hat{m}_{ij}^{true} \right|,$$

де $\hat{m}_{ij}^{true}$ — оцінка, отримана від людських експертів або іншої перевіреної системи.

Для оцінки ефективності рою віртуальних експертів можна використовувати критерії, такі як середня квадратична помилка (MSE), що дозволяє порівняти середні оцінки з реальними даними:

$$MSE = \frac{1}{N} \sum_{i=1}^{N} \sum_{j=1}^{M} \left(\hat{m}_{ij} - \hat{m}_{ij}^{true} \right)^2,$$

де N і M — кількість загроз та уразливостей відповідно.

Для практичного прикладу використовуємо звіт компанії Edgescan [5], де наведено статистика найбільш поширених уразливостей. За результатами проведеного експертного аналізу сформовано перелік загроз $\{u_i\}$ і уразливостей $\{b_j\}$, які позначають уразливості. Останні взаємопов’язано із потенційно вразливими компонентами, на які саме і можуть бути спрямовані кібератаки.

Для зазначеного об’єкта захисту сформовано наступний перелік елементів, які характеризують уразливості:

b_1 – уразливість вхідних драйверів вхідної інформації;

b_2 – уразливість драйверів інструментів обробки інформації;

b_3 – уразливість драйверів мікросхем BIOS; …

Визначений перелік загроз від кібератак наведено нижче:

u_1 – загроза завантаження шкідливого (вірусного) програмного забезпечення, використовуючи особливості альтернативної операційної системи з розширеними повноваженнями;

u_2 – загроза несанкціоноване копіювання інформації;

u_3 – загроза неавторизованої модифікації інформації; …

Для отримання оцінок від віртуальних експертів, які було реалізовано на базі застосування сервісів ChatGPT (https://chatgpt.com/), Groq (https://groq.com/, модель Llama-3), DeepSeec (https://www.deepseek.com/), застосовувався промпт:

Промпт: *Маємо: деякого об'єкта критичної інфраструктури сформовано наступний перелік елементів, які характеризують уразливості:*
b_1 – уразливість вхідних драйверів вхідної інформації;
b_2 – уразливість драйверів інструментів обробки інформації;
…
Визначений перелік загроз від кібератак на цей обєкт наведено нижче:
u_1 – загроза завантаження шкідливого (вірусного) програмного забезпечення, використовуючи особливості альтернативної операційної системи з розширеними повноваженнями;
u_2 – загроза несанкціоноване копіювання інформації;
…
Створить таблицю інцидентності, де рядки –(u), стовпці – (b).

Матриця інцидентності, яку було розглянуто у прикладі (Рис. 1), виглядає узгодженою та логічною, але для повної впевненості в її коректності бажано перевірити кожен зв'язок на відповідність конкретним технічним сценаріям та умовам об'єкта.

	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}
u_1	**1**										**1**		**1**
u_2				**1**					**1**	**1**	**1**		
u_3		**1**		**1**			**1**	**1**	**1**	**1**	**1**		
u_4				**1**		**1**	**1**						
u_5	**1**	**1**	**1**	**1**					**1**				
u_6					**1**	**1**	**1**	**1**	**1**				
u_7					**1**	**1**	**1**	**1**	**1**	**1**			
u_8												**1**	
u_9												**1**	
u_{10}										**1**			**1**
u_{11}											**1**		
u_{12}					**1**	**1**							
u_{13}					**1**	**1**		**1**					
u_{14}					**1**	**1**	**1**	**1**					

Рисунок 1 - Агрегована таблиця інцидентності

У наведеному прикладі людиною-експертом було підтверджено її логічність, при чому враховувалось декілька критеріїв для оцінки її коректності, а саме логічність зв'язків, повнота матриці, надмірність зв'язків, відповідність реальним практикам безпеки.

Висновки

Наукова новизна цієї роботи полягає в інтеграції рою віртуальних експертів із використанням LLM для автоматизованої, але контрольованої оцінки взаємозв'язків між загрозами і уразливостями в об'єктах критичної інфраструктури, а також у математичному моделюванні цього процесу. Цей підхід дозволяє підвищити точність і надійність оцінок, а також оптимізувати процес прийняття рішень у сфері кібербезпеки.

Метод рою віртуальних експертів є ефективним інструментом для оцінки таблиці інцидентності загроз та уразливостей у системах критичної інфраструктури. Використання таких методів дозволяє агрегувати численні оцінки і надавати середні значення, що відображають ймовірність виникнення конкретної загрози через певну уразливість.

Математичне моделювання процесу оцінки, а також перевірка коректності середніх оцінок через порівняння з оцінками людських експертів, дозволяє підтвердити ефективність і точність застосовуваного методу. Середні оцінки, отримані від рою віртуальних експертів, можуть використовуватись як основа для подальшої оцінки ризиків і планування заходів захисту для критичної інфраструктури.

Цей підхід також є адаптивним, оскільки можна змінювати параметри моделі та адаптувати її під конкретні потреби кожної інфраструктури. Тому метод рою віртуальних експертів може стати важливим інструментом у сфері кібербезпеки.

1. Aslan, Ömer, Semih Serkant Aktuğ, Merve Ozkan-Okay, Abdullah Asim Yilmaz, and Erdal Akin. "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions." Electronics 12, no. 6 (2023): 1333. DOI: 10.3390/electronics12061333.

2. Ghelani, Diptiben, Tan Kian Hua, and Surendra Kumar Reddy Koduru. "Cyber security threats, vulnerabilities, and security solutions models in banking." Authorea Preprints (2022). DOI: 10.22541/au.166385206.63311335/v1.

3. Lande D, Strashnoy L. GPT Semantic Networking: A Dream of the Semantic Web - The Time is Now. - Kyiv: Engineering, 2023. - 168 p. ISBN 978-966-2344-94-3.

4. Lande D, Strashnoy L. Swarm of Virtual Experts in the Implementation of Semantic Networking. ResearchGate Preprint, 2024. Access mode: https://doi.org/10.13140/RG.2.2.16686.11845.

5. Vulnerability Statistics Report 2023. Edgescan. URL: https://www.edgescan.com/intel-hub/stats-report/ (date of access: 22.06.2023).

В.В. Святко, І.О. Шахматов, А.Л. Юр'єв

СИСТЕМА ПЕРСОНАЛІЗОВАНИХ РЕКОМЕНДАЦІЙ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРОДАЖІВ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Вступ. Постановка задачі

Сучасний ринок телекомунікаційного обладнання стає все більш конкурентним і компанії шукають нові способи підвищення ефективності своїх продажів. Одним із найперспективніших рішень є впровадження систем персоналізованих рекомендацій на основі штучного інтелекту (ШІ). В умовах інформаційного перевантаження важливо забезпечити клієнтів релевантними пропозиціями, що відповідають їхнім потребам. Ці системи дозволяють аналізувати дані про клієнтів і їхні уподобання, що, в свою чергу, сприяє підвищенню рівня задоволеності клієнтів і збільшенню обсягу продажів. Таким чином, основною задачею даного дослідження є розробка системи (моделі) персоналізованих рекомендацій, яка використовує алгоритми штучного інтелекту для підвищення ефективності продажів телекомунікаційного обладнання, яку потрібно імплементувати в операційну діяльність у сфері продажів.

Мета дослідження.

Аналіз існуючих методів персоналізації рекомендацій у сфері продажів. Основні типи систем рекомендацій.

Розробка моделі, яка використовує дані про поведінку споживачів для формування рекомендацій на основі технологій машинного навчання. Впровадження системи рекомендацій.

Висновки та оцінка впливу впровадження системи рекомендацій на обсяги продажів та задоволеність клієнтів.

Результати дослідження

Етапи розробки моделі рекомендацій та її впровадження: аналіз даних, вивчення поведінки споживачів на основі історичних даних про покупки, перегляди товарів та відгуки, розробка моделі рекомендацій на основі алгоритмів машинного навчання, що дозволяє формувати персоналізовані пропозиції, проведення A/B тестування та оптимізації, яке дозволить виміряти % збільшення продажів та % підвищення задоволеності клієнтів.

Системи рекомендацій використовують алгоритми машинного навчання для аналізу поведінки користувачів і надання персоналізованих пропозицій. Основні типи систем рекомендацій: фільтрація на основі контенту, колаборативна фільтрація, гібридні системи.

Штучний інтелект, зокрема алгоритми машинного навчання, у системах персоналізованих рекомендацій може використовуватися на базі нейронних мереж, методів кластеризації та аналізу настроїв.

Таблиця 1 - Модель системи персоналізованих рекомендацій

Модель системи персоналізованих рекомендацій (алгоритм роботи)		
1. Збір даних	**2. Обробка даних**	**3. Алгоритми рекомендацій**
Дані про користувачів. Інформація про користувачів, така як: демографічні дані (вік, стать, місце проживання), історія покупок, перегляди товарів, рейтинги та відгуки. Дані про товари. Опис товарів, категорії, ціни, характеристики, а також метадані, такі як популярність та наявність. Контекстуальні дані Інформація про час, місце та пристрій, з якого користувач здійснює запит.	Попередня обробка. Очищення даних, заповнення пропусків, нормалізація та кодування категоріальних змінних. Аналіз даних. Використання статистичних методів для виявлення патернів у поведінці користувачів та характеристиках товарів. Алгоритми рекомендацій.	Колаборативна фільтрація. Оцінка поведінки інших користувачів. User-based. Рекомендації формуються на основі схожості між користувачами. Якщо два користувачі мають схожі вподобання, їм можуть бути рекомендовані товари, які сподобалися одному з них. tem-based. Рекомендації формуються на основі схожості між товарами. Якщо товар A подібний до товару B, користувачам, які купили товар A, можуть бути рекомендовані товар B. Контентна фільтрація. Рекомендації формуються на основі характеристик товарів. Якщо користувач раніше купував товари з певними характеристиками, йому можуть бути рекомендовані інші товари з подібними характеристиками. Гібридні методи. Комбінують колаборативну та контентну фільтрацію для покращення точності рекомендацій.

Кінець таблиці 1

4. Машинне навчання	5. Оцінка та вдосконалення	6. Інтерфейс користувача
Моделі машинного навчання. Використання алгоритмів, таких як регресія, дерева рішень, SVM, або нейронні мережі для навчання на основі історичних даних про користувачів і товари. Глибоке навчання. Використання нейронних мереж для виявлення складних патернів у даних, наприклад, за допомогою рекурентних нейронних мереж (RNN) або згорткових нейронних мереж (CNN) для обробки текстових або зображень товарів.	Метрики оцінки Використання метрик, таких як точність, відгук, F1-міра, AUC-ROC для оцінки якості рекомендацій. A/B тестування Проведення експериментів для порівняння різних моделей рекомендацій та вибору найефективнішої. Зворотний зв'язок. Збір зворотного зв'язку від користувачів для подальшого вдосконалення моделі.	Персоналізовані рекомендації. Відображення рекомендацій у зручному форматі на веб-сайті або в мобільному додатку. Можливість налаштування. Дозволити користувачам налаштовувати свої вподобання та отримувати рекомендації на основі їхніх інтересів.

Переваги у продажах телекомунікаційного обладнання після впровадження моделі персоналізованих рекомендацій: збільшення конверсії. (персоналізовані рекомендації можуть значно підвищити ймовірність покупки, оскільки вони пропонують продукти, які відповідають потребам клієнтів), покращення досвіду клієнтів (клієнти отримують релевантні пропозиції, що підвищує їхню задоволеність і лояльність до бренду), оптимізація маркетингових кампаній (збір даних про уподобання клієнтів дозволяє компаніям створювати більш цілеспрямовані та ефективні маркетингові стратегії)

Висновки та перспективи

Системи персоналізованих рекомендацій на основі штучного інтелекту мають великий потенціал для підвищення ефективності продажів телекомунікаційного обладнання. Вони дозволяють компаніям краще розуміти потреби своїх клієнтів і пропонувати їм релевантні рішення, що в свою чергу сприяє збільшенню обсягу продажів і покращенню клієнтського досвіду.

Перспективи подальшого розвитку включають: розширення функціоналу системи за рахунок інтеграції з CRM-системами, використання більш складних алгоритмів, проведення додаткових досліджень для вивчення впливу рекомендацій на різні сегменти ринку.

На етапі впровадження моделі персоналізованих рекомендацій та вже під час промислового використання компанії можуть стикатися із наступними викликами та ризиками: конфіденційність даних (необхідно дотримуватися норм захисту персональних даних), складність алгоритмів (розробка та впровадження складних алгоритмів може вимагати значних ресурсів), зміна поведінки споживачів. Постійні зміни в уподобаннях клієнтів можуть ускладнити точність рекомендацій.

1. Ricci, F., & Rokach, L. (2015). Recommender Systems Handbook. Springer. https://doi.org/10.1007/978-0-387-85820-3.

2. Zhang, Y., & Chen, L. (2013). A Survey on Recommendation Systems. Journal of Computer Science and Technology, 28(1), 1-20. https://doi.org/10.1145/356802.

3. Shani, G., & Gunawardana, A. (2011). Evaluating Recommendation Systems. In Recommender Systems Handbook (pp. 257-297). Springer. DOI:10.1007/978-0-387-85820-3_8.

4. Huang, Z., & Benyoucef, M. (2013). From e-commerce to social commerce: A close look at design features. Electronic Commerce Research and Applications, 12(1), 4-12. https://doi.org/10.1016/j.elerap.2012.12.003.

Ю.Г. Даник, В.І. Шестаков

ВАРІАНТИ КОНФЛІКТІВ ТА АНАЛІЗ РИЗИКІВ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНИ

На думку експертів, війна в Україні – це своєрідна «перша світова війна з використанням технологій штучного інтелекту(ШІ)» [1]. За аналізом перебігу протиборства у військових конфліктах сучасності можна стверджувати, що у сфері безпеки та оборони ШІ впроваджується для вирішення таких завдань:

аналізу і оцінки результатів та прогнозування варіантів дій і характеру протиборства, підтримка прийняття рішень із застосування військ (сил) та засобів на оперативному та стратегічному рівні військового та державного військового управління. Передбачається що за допомоги ШІ можна підвищити якість та ефективність управління. Однак сучасне протиборство є складним явищем, яке здійснюється кібер-фізичними системами у специфічному кіберінформаційному просторі, що у разі спрощених та неадекватних моделей, неповних даних навчання ШІ може призвести до неочікуваних, протилежних задуму результатів;

застосування автономних бойових комплексів (повітряних, надводних, підводних та наземних безпілотних комплексів). Самостійне визначення такою системою порядку дій на полі бою може призвести до отримання переваги над протидіючою стороною (знищення противника) з одночасним високим ризиком «дружніх» деструктивних впливів. Особливо за відсутності будь-якої системи розпізнавання «свій-чужий» в цій сфері. Це також порушує безліч вже існуючих етичних та правових питань, таких як дотримання міжнародного гуманітарного права та відповідальність за дії автономних систем тощо [2];

реалізації складних кібератак та здійснення кіберзахисту власних об’єктів критичної інформаційної інфраструктури від таких атак. На сьогодні складно спрогнозувати, як поведуть себе системи із ШІ протиборчих сторін, що вимагає постійного контролю з боку людини за діями таких систем.

Дослідження проблематики оцінювання та управління ризиками, які пов’язані із впровадження ШІ здійснюють відомі вітчизняні та закордонні наукові установи. Однак, незважаючи на значну кількість публікацій, на сьогодення відсутня єдина струнка система ідентифікації та оцінювання ризиків, пов’язаних із загрозами впровадження та використання, в тому числі бойового, ШІ. Тому, існує невирішене протиріччя між швидким впровадженням різноманітних технологій ШІ в сфері національної безпеки та оборони та необхідністю своєчасного передбачення небезпек і загроз, аналізу, оцінки та прогнозування ризиків, пов'язаних із збільшенням спроможностей та наслідків використання ШІ для подальшої мінімізації загроз його застосування у ході конфліктів сучасності і майбутнього.

Метою доповіді є оцінка можливих варіантів конфліктів та аналіз загроз і ризиків застосування протиборчими сторонами ШІ в сфері національної безпеки та оборони.

Для оцінювання ризику впливу ШІ запропоновано розглянути моделі взаємодії людини (Л), ШІ, кіберфізичної системи (КФС), які наведено на рис. 1, де елементи з індексом «n» та «i» вказують протиборчі сторони.

1. $Л_i \rightarrow ШІ_i \rightarrow КФС_i \leftrightarrow КФС_n \leftarrow Л_n$
2. $Л_i \rightarrow КФС_i \leftrightarrow КФС_n \leftarrow ШІ_n \leftarrow Л_n$
3. $Л_i \rightarrow ШІ_i \rightarrow КФС_i \leftrightarrow КФС_n \leftarrow ШІ_n \leftarrow Л_n$
4. $ШІ_i \rightarrow КФС_i \leftrightarrow КФС_n \leftarrow ШІ_n \leftarrow Л_n$

Рисунок 1 – Моделі взаємодії

У дослідженні авторів опис ризикової ситуації RS в рамках моделі «небезпека –ризик» формалізовано кортежем:

$$<RS>= <THR, PR,CON, Q, R, Rint >, \quad (1)$$

де THR – вектор загроз; PR – вектор ймовірностей реалізації загроз; CON – вектор наслідків; Q – вектор втрат/збитків; R – вектор ризиків; Rint – інтегральний ризик.

За такої моделі оцінювання ризиків впливу ШІ на хід та результати протиборства є багатокритеріальною задачею, яка потребує значних людських та обчислювальних ресурсів для її вирішення.

Авторами запропоновано для оцінювання впливу ризиків використати відомий підхід. Передбачається оцінювати: ймовірність реалізації загрози за чотирьох бальною шкалою від рідко до майже напевно можливого; наслідки ризику в декількох категоріях, таких як: наслідки, втрати, відповідальність за чотирьох бальною шкалою від незначних до критичних.

Вироблено пропозиції щодо усунення ризиків застосування ШІ в сфері кібербезпеки, а саме: здійснення суб’єктами сектору безпеки і оборони, які забезпечують кібербезпеку за координації Національного координаційного центру кібербезпеки, постійного моніторингу щодо розвитку спроможностей систем ШІ у сфері кібербезпеки; впровадження та розвиток ризик-орієнтованого підходу до забезпечення кібербезпеки; подальше поглиблення суб’єктами системи кібербезпеки співробітництва з міжнародними партнерами щодо обміном інформацією про кібератаки та кіберінциденти, а також досвідом та найкращими практиками запобігання загрозам неконтрольованого розвитку і використання ШІ.

1. Окопи зі штучним інтелектом: як під час війни в Україні використовуються старі й нові військові технології. – Foreign Ukraine, 17.07.2023. https://foreignukraines.com /2023/ 07/17/ how-old-and-new-military-technologies-are-used-during-the-war-in-ukraine/.

2. Коваленко Ю., Войнов М. Штучний інтелект та права людини: орієнтири та обмеження у контексті національної безпеки та оборони, 2024. https://www.helsinki.org.ua/wp-content/uploads/2024/05/Preview_AI_human_right_A4-1.pdf.

І.В. Басиста

ЧЕРГОВІ КРОКИ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

(продовження огляду)

До складових задекларованої проблематики вже неодноразово зверталися науковці [1; 2; 3], авторські узагальнення щодо позитивів та ризиків від штучного інтелекту, перспективності його використання у перебігу кримінального провадження, зокрема і для прийняття процесуальних рішень доповідалися на всеукраїнських науково-практичних заходах та оприлюднювалися на шпальтах фахових видань [4; 5; 6; 7].

За крайні кілька місяців можемо спостерігати такі тенденції у юридичній площині, як: ухвалення Радою Європи 17 травня під час щорічного засідання Комітету міністрів (міністри закордонних справ 46 країн-учасниць першої конвенції) РЄ у Страсбурзі Рамкової конвенція про штучний інтелект, права людини, демократію і верховенство права (два роки її розробляв спец. міжурядовий комітет, бізнесові кола та представники громадянського суспільства) [8]. Ця угода є відокремленою від закону ЄС про штучний інтелект, який набув чинності у Європейському Союзі з 1 серпня 2024 року [9] та, зі слів представника міністерства юстиції Британії, передбачає, щоб «нові технології можна було використовувати без руйнування найдавніших цінностей» [10].

Вже підкреслювалося, що це перша юридично зобов'язуюча угода, що з 5 вересня 2024 року відкрита для підписання також для країн за межами Європи (станом на 5.09.2024. її вже підписали Андорра, Грузія, Ісландія, Норвегія, Молдова, Сан-Марино, Велика Британія, а також Ізраїль, США та Європейський Союз [11]), яка охоплює, серед іншого, такі аспекти: ШІ у державній і недержавній сферах; обмеження чи заборону ШІ у тих випадках, коли його використання буде становити ризики для дотримання стандартів прав людини; вироблення країнами власних законодавчих механізми для захисту осіб, права яких будуть порушені через технології ШІ. Вказано про нагальність встановлення країнами процедурних запобіжників, як от: попередження осіб про те, що вони взаємодіють зі ШІ; запобіжники від зловживання ШІ для підриву демократичних інституцій і процесів тощо. Дотримання конвенції не є обов'язковим у питаннях, що виникають у зв'язку із захистом нацбезпеки, національної оборони, дослідницькій діяльності, але технології не можуть порушувати міжнародне право [12]. Фактично двома місяцями раніше 13 березня Європейський парламент ухвалив **перший у світі акт, який, як вже вище вказувалося набув чинності з 1 серпня та регулює розробку та використання штучного інтелекту** – Закон ЄС про штучний інтелект (AI Act). Згадувалося, що у планах– Офіс ШІ (AI Office), який і контролюватиме дотримання Закону, серед запобіжників – технології ШІ, які «заборонені» (розпізнавання емоцій та маніпулювання поведінкою, «соціального скорингу», прогнозування в правоохоронних цілях (predictive policing), а також більшість систем біометричної ідентифікації) та «високого ризику» [13]. Аналітики вже згадували, що значна кількість корпорацій та країн висловили своє занепокоєння і контраргументи [14; 15], ба навіть виголошували протести [16] такому категоричному «правовому» підходу. Поряд з цим, «країни-члени ЄС мають до 2 серпня 2025 року визначити національні компетентні органи, які контролюватимуть застосування правил для систем на основі штучного інтелекту та здійснюватимуть діяльність з нагляду за ринком» [9].

У окремих штатах, для прикладу у Каліфорнії, розроблений законопроєкт SB 1047, за допомогою якого намагаються покласти відповідальність на розробників та запобігти використанню великих моделей штучного інтелекту для заподіяння «критичної шкоди» (створення зброї задля масових жертв тощо) людству. Натомість, компанії OpenAI, Google та Meta виступила проти таких законодавчих ініціатив, як шкідливих для розвитку технологій [17].

Але ж варто розуміти, що не всі проєкти за участі ШІ є суспільно-корисними, адже хоча б взяти до уваги такі оприлюднені факти, які достатньо аргументовані (видання зі США під назвою The Conversation вивчало такі переконання), що акаунти-боти вже кілька років маніпулюють соціальними мережами, щоб вплинути на громадську думку за допомогою дезінформації (яка може бути очевидною, але штучно створена агентами-ботами велика кількість підписників моделює наше сприйняття в інший бік). Так, нейромережі створюють зображення, а боти, як «агенти штучного інтелекту», поширюють їх у соцмережах, залучаючи безліч реальних підписників, яким потім «промивають мізки». Є і «теорія мертвого інтернету», згідно з якою більшість контенту у Всесвітній павутині, включно з публікаціями в соціальних мережах, створюють і автоматизують системи штучного інтелекту. У міру зростання кількості підписників (справжніх або фейкових), акаунти, керовані штучним інтелектом, привертають все більше реальних користувачів. Це означає, що там створюється армія читачів і послідовників. Акаунти з великою кількістю підписників можуть бути використані в різних цілях тими, хто найбільше заплатить творцям. росія вправно із цим маніпулює, охоплюючи мільйони користувачів соціальних мереж [18]. Є й приклади використання **програмного забезпечення Stable Diffusion для** створення гіперреалістичних матеріали з сексуальним насильством над дітьми [19] тощо. Також соціальний скоринг із залученням ШІ викликає занепокоєння (як пише Дарина Бойко він поширений не лише у Китаї (Social Credit System, SCS), а й за оцінками фахівців ним користуються Affirm для прийняття рішення, чи повинні заявники отримувати кредити (сканують профілі людей в соціальних мережах, щоб зрозуміти спосіб їхнього життя). Також у цьому переліку британський брокер даних Experian, який відстежує, наскільки вчасно люди сплачують борги, надаючи оцінку кредиторам та постачальникам іпотечних кредитів.

Експерти зазначають, що діяльність схожих компаній порушує принципи захисту даних GDPR (General Data Protection Regulation)) [20].

Із крайніх законодавчих ініціатив варто виділити й таку, що «США, Велика Британія та Євросоюз підпишуть перший юридично обов'язковий міжнародний договір використання штучного інтелекту. Про це, із посиланням на Reuters, вказують кілька національних інформаційних ресурсів [10]. Раніше, ще у квітні цього року, «британський уряд оголосив про введення нового правопорушення, що робить незаконним створення сексуальних підробок …, а якщо зображення ще й поширять, порушників можуть посадити до в'язниці» [19].

Та й самі компанії-розробники, учені працюють над тестуванням ШІ-моделей задля усунення вже наявних проблем (для прикладу, «23 травня європейські користувачі нейромереж ChatGPT, Copilot, DuckDuckGo та інших пов'язаних із корпорацією Microsoft сервісів не могли ними скористатися» [21]) та щодо наявності «знань», які можна потенційно використовувати на шкоду [22]. Зокрема, поряд із тим, що американська OpenAI, розробник чат-бота ChatGPT, розпочавши навчання нової моделі ШІ –GPT-5, яка буде здатна міркувати і планувати, водночас заснувала комітет із безпеки, який даватиме рекомендації раді директорів щодо критично важливих рішень стосовно її проєктів і діяльності в цій сфері [23]. Відповідно появилися і аргументовані пересторогu, про що зазначали національні інформаційні видання із посиланням на те, що пише видання The Register, адже «…інструмент GPT-4 почав генерувати настільки природні текстові відповіді, що ефективно виконує різні мовні завдання, ставлячи під сумнів нашу здатність відрізнити машину від людського співрозмовника» [24]. Наявний перегук із відомим уявним експериментом Алана Тюрінга [24].

Також наявні випадки відповідної реакції суду, коли злочин вчинявся із використанням технологій ШІ. Так у рішенні суду, окрім накладання штрафу, суд зобов'язав Р. **«не використовувати, не відвідувати й не отримувати доступ»** до інструментів штучного інтелекту без попереднього дозволу поліції [19].

Отож очевидно, що перелічені та й інші правові кроки є на часі та мають належне підґрунтя, ба більше, вони є логічною відповіддю на невпинний розвиток технології ШІ, які вже глибинно інтегровані у наше повсякденне життя.

Так, ще, на початку травня МЗС України презентувало «представницю МЗС із консульських питань», яку назвали Вікторія ШІ [25]. Рекламні повідомлення сайтів рясніють інформацією, на кшталт: «Meta готує розумні навушники з камерами та ШІ» [26]; «Google Gemini дозволить користувачам Android вибирати свій улюблений сервіс для прослуховування музики в налаштуваннях застосунку» [27]; «Нова Circle to Copilot працює приблизно так само, як представлена раніше Google Circle to Search – користувач може обвести частину вмісту екрана, щоб обробити виділений фрагмент за допомогою ШІ»; Microsoft Edge у Windows 10 та 11 оновлює інтеграцію Copilot двома корисними функціями: додавання тегів і нове меню «Запитати Copilot», яке дозволяє швидко розширювати, пояснювати та підсумовувати вибрані тексти у довгому PDF-файлі або вебдодатку» [28]; «YouTube зробив доступним для власників підписки Premium новий інструмент Jump ahead, який дозволяє швидко перейти до фрагмента відео, який найбільше цікавив користувачів» [29]; «користувачі Stack Overflow отримають доступ до інформації для розробки нових генеративних інтеграцій ШІ, а OpenAI, разом з моделями платформи чат-ботів ChatGPT, – нові покращені відповіді на запитання, пов'язані з програмуванням» [30]; «Microsoft готує до запуску нову функцію Copilot в OneNote, яка дозволить ШІ розуміти рукописні нотатки користувачів і аналізувати їх…однак поки незрозуміло, як Copilot впорається з поганим почерком» [31]; «Голова Microsoft Сатья Наделла анонсував новий ШІ-інструмент під назвою «Recall AI». Це спеціальна версія нейромережі, яка на офіційному рівні за замовчуванням шпигуватиме за користувачами нових версій Windows…ШІ збирає метадані про активність, які може використовувати юзер для демонстрації того, чим він нещодавно займався на своєму гаджеті» [21].

У крайніх числах жовтня з'явилося повідомлення, що техногіганти OpenAI та Microsoft виділяють $10 мільйонів кільком американським засобам масової інформації на використання штучного інтелекту (для транскрипції, підсумовування, перекладу та розширення пропонованого вмісту; для аналізу, допомоги з маркетингом та продажами, а також з розширенням читацької бази) [32].

1. Карчевський М.В., Куковинець Д.О. (2023). Використання технологій штучного інтелекту правоохоронними та судовими органами: світовий досвід та напрями розвитку національного законодавства. Питання боротьби зі злочинністю: зб. наук. пр. / редкол.: В.С. Батиргареєва (голов. ред.) та ін. Харків: Право. 46. 21–31.

2. Торбас О.О. (2023). Способи використання штучного інтелекту при проведенні наукових досліджень в сфері кримінального процесу на прикладі функціоналу CHATGPT та аналізу категорії «розсуд» у кримінальному провадженні. Правові новели. 19. 368–377. http://legalnovels.in.ua/journal/19_2023/48.pdf. DOI https://doi.org/ 10.32782/ln.2023.19.48.

3. Vladyslav Teremetskyii, Yurii Burylo, Mykola Stefanchuk, Olha Zozuliak, Zhanna Udovenko, Dmitro Zhuravlov and Yevheniia Duliba (2024). Prospective regulation of artificial intelligence in the european union and its possible implications for Ukraine. International Journal of Applied Engineering & Technolog. Vol. 6 (1). 137–145.

4. Басиста І.В. (2024). Штучний інтелект: правила використання, перспективи, ризики та загрози, застосовність для кримінального провадження (продовження огляду). Кримінальне судочинство: сучасний стан та перспективи розвитку: матеріали Всеукр. наук.-практ. конф. (Київ, 2 трав. 2024 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ. (с. 16–24). Нац. акад. внутр. справ.

5. Басиста І.В. (2024). Використання можливостей штучного інтелекту у перебігу кримінального провадження та захист фундаментальних прав (продовження огляду). Актуальні питання забезпечення безпекового середовища в Україні : зб. тез наук. доп. Всеукр. наук.-практ. конф. (Київ, 19 квітн. 2024 р.) [Електронне видання] / упоряд.: М.Г. Вербенський, В.О. Рядінська, А.І. Хальота, В.А. Мацько. Київ. (с. 360–364). ДНДІ МВС України.

6. Басиста І.В., Удовенко Ж.В., Кулинич Марта-Марія А. (2024). Огляд тенденцій щодо штучного інтелекту та його перспективність для процесуальних рішень у перебігу кримінального провадження. Науковий вісник Ужгородського Національного Університету. Серія право. 81. Том (частина) 3. 19-38. https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/03/81_part-3.pdf.

7. Удовенко Ж.В., Басиста І.В. (2024). Використання штучного інтелекту у кримінальному провадженні: ілюзія чи реальність. Штучний інтелект у правовій практиці: межі та можливості : збірник тез Всеукраїнського круглого столу (15 березня 2024 року) / упор. О.О. Барабаш. Львів. (с. 188-197). Львівський державний університет внутрішніх справ file:///C:/Users/Ірина%20Володимирівна/Downloads/15_03_2024.pdf.

https://www.lvduvs.edu.ua/uk/library/materialy-naukovykh-konferentsii.html.

8. Рамкова конвенція про штучний інтелект, права людини, демократію і верховенство права/ з https://search.coe.int/cm#%7B"CoEObjectId":["0900001680afb11f"],"sort":["CoEValidationDate%20Descending"]%7D.

9. У Євросоюзі набув чинності перший у світі закон про штучний інтелект. (2024, 1 серпня). Ukrinform. https://www.ukrinform.ua/rubric-world/3891086-u-evrosouzi-nabuv-cinnosti-persij-u-sviti-zakon-pro-stucnij-intelekt.html

10. США, Велика Британія та ЄС підпишуть першу угоду у галузі штучного інтелекту. (2024, 5 вересня). Processer.media. https://processer.media/ua/ssha-velika-britaniya-ta-ies-pidpishut-pershu-ugodu-u-galuzi-shtuchnogo-intelektu/.

11. Рада Європи відкрила до підписання першу у світі конвенцію про штучний інтелект. (2024, 5 вересня). Ukrinform.

https://www.ukrinform.ua/rubric-world/3902460-rada-evropi-vidkrila-do-pidpisanna-persu-u-sviti-konvenciu-pro-stucnij-intelekt.html.

12. Марія Ємець (2024, 17 травня). Рада Європи ухвалила першу конвенцію щодо штучного інтелекту. https://www.eurointegration.com.ua/news/2024/05/17/7186177/.

13. Які ризики несе перший у світі закон про штучний інтелект і чому він потрібен ЄС. (2024, 1 квітня). https://www.eurointegration.com.ua/news/2024/04/1/7182827/.

14. Open Letter EU AI Act and Signatories.pdf - Google Диск.

15. Europe one step away from landmark AI rules after lawmakers' vote. (2024, 14 березня). Europe one step away from landmark AI rules after lawmakers' vote | Reuters.

16. World’s first major act to regulate AI passed by European lawmakers. (2024, 13 березня). World’s first major act to regulate AI passed by European lawmakers.

17. Ярослав Жахалов (2024, 22 серпня). OpenAI різко розкритикувала закон Каліфорнії відносно ШІ. Tech.liga.net. https://tech.liga.net/ua/technology/novosti/openai-rizko-rozkrytykuvala-zakon-kalifornii-vidnosno-shi.

18. «Мертвий інтернет»: штучний інтелект уже керує Мережею і людьми, – The Conversation. (2024, 21 травня). Internetua. com. https://internetua.com/-mertvii-internet-shtucsnii-intelekt-uje-keruye-merejeua-i-luadmi-the-conversation.

19. Генерував непристойні фото з дітьми: в Британії вперше заборонили користуватися ШІ злочинцю. (2024, 21 квітня). Rubryka.com. https://rubryka.com/2024/04/21/generuvav-neprystojni-foto-z-ditmy-v-brytaniyi-vpershe-zaboronyly-korystuvatysya-shi-zlochyntsyu/.

20. Дарина Бойко Соціальний скоринг та штучний інтелект: ризики для правосуддя. (2023, 28 грудня). Центр Дністрянського. https://dc.org.ua/news/socialnyy-skoryng-ta-shtuchnyy-intelekt-ryzyky-dlya-pravosuddya.

21. Microsoft розробляє штучний інтелект, що за замовчуванням шпигуватиме за всіма користувачами ОС Windows. (2024, 27 травня). Noworries. News. https://noworries.news/microsoft-rozroblyaye-shtuchnyj-intelekt-shho-za-zamovchuvannyam-shpyguvatyme-za-vsima-korystuvachamy-os-windows/.

22. Сем Альтман повернувся в OpenAI. (2024, 9 березня). Internetua. https://internetua.com/sem-altman-povernuvsya-v-openai.

23. Компанія OpenAI розпочала навчання нової ШІ-моделі. (2024, 28 травня). Elitexpert.ua. https://elitexpert.ua/nauka/kompaniya-openai-rozpochala-navchannya-novoi-shi-modeli/.

24. Михайло Митник Експерти попереджають про нові потенційні загрози використання ChatGPT. (2024, 23 червня). Itechua.com. https://itechua.com/news/261149.

25. Христина Бондарєва (2024, 1 травня). МЗС представило нову «речницю» з консульських питань, створену штучним інтелектом. https://www.eurointegration.com.ua/news/2024/05/1/7185016/

26. Meta готує розумні навушники з камерами та ШІ. (2024, 15 травня). Toneto.net. https://toneto.net/news/tehnologii/Meta-gotovit-umnie-naushniki-s-kamerami-i-ii.

27. Максим Шпирка (2024, 22 квітня). Gemini дозволить користувачам Android відтворювати музику за допомогою голосу. Vctr.media. https://vctr.media/ua/gemini-dozvolyt-korystuvacham-android-vidtvoryuvaty-muzyku-za-dopomogoyu-golosu-223669/.

28. Дарія Шуть (2024, 22 квітня). Microsoft додасть нові ШІ-функції до свого браузера. Psm7.com. https://psm7.com/uk/company/microsoft/microsoft-dodast-novi-shi-funkcziyi-do-svogo-brauzera.html.

29. jour12 (2024, 6 травня). Новий ШІ від YouTube дозволить перемотувати одразу до найцікавішої частини відео. https://ua.news/ua/technologies/novij-shi-vid-youtube-dozvolit-peremotuvati-odrazu-do-najtsikavishoyi-chastini-video.

30. Вікторія Рудзінська (2024, 6 травня). OpenAI став партнером Stack Overflow у розвитку генеративних моделей ШІ. Speka.media. https://speka.media/spivpracya-openai-ta-stack-overflow-v45e2k.

31. Microsoft навчила ШІ Copilot розуміти людський почерк. (2024, 12 липня). Internetua. https://internetua.com/microsoft-navcsila-shi-copilot-rozumiti-luadskii-pocserk.

32. Штучний інтелект допомагатиме ЗМІ у розслідуваннях – OpenAI та Microsoft виділять $10 мільйонів. (2024, 27 жовтня). Sud.ua/ https://sud.ua/uk/news/abroad/314079-iskusstvennyy-intellekt-pomozhet-smi-v-rassledovaniyakh-openai-i-microsoft-vydelyat-10-millionov.

О.М. Селезньова, С.М. Левaднюк

РИЗИКИ ТА ПЕРЕВАГИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СУЧАСНИХ УМОВАХ

Актуальність питання зростання ролі штучного інтелекту (далі – ШІ) викликає багато роздумів щодо інформаційної безпеки [1; 2]. Сучасний світ рухається в напрямку розробки безпечних стандартів та фреймворків для роботи з ШІ, однак надмірна регламентованість цієї сфери (якої так прагнуть, наприклад, країни Європейського Союзу) може певним чином їй зашкодити, хоча й вимагає контролю за використанням даних.

І. Ризики.

Основним ризиком, пов'язаним із застосуванням ШІ, є загроза зловживання його можливостями. У випадку кібербезпеки, ШІ може стати інструментом для автоматизації атак, розробки складних соціотехнічних обманів і створення алгоритмів, здатних обходити стандартні системи захисту. Шкідливе програмне забезпечення, підсилене ШІ, може швидше і точніше знаходити вразливості у системах, автоматично змінюючи свою поведінку для уникнення виявлення. Зокрема, ШІ здатний імітувати мовні шаблони і стиль письма, може використовуватися для соціальної інженерії та створення фішингових повідомлень, які важче виявити.

Крім кібербезпеки, ризики та вразливості ШІ торкаються також медицини, де алгоритми ШІ все частіше застосовуються для діагностики та надання медичних консультацій. Помилкові рішення, прийняті на основі ШІ, можуть мати критичні наслідки для здоров'я пацієнтів і призвести до втрати довіри медичної спільноти до таких систем.

У сфері правосуддя та державного управління ШІ застосовується для прийняття рішень, зокрема для прогнозування злочинності, оцінки кредитного ризику та управління містом. Ризик тут полягає в можливому обмеженні прав людей через використання алгоритмів, що можуть мати приховані упередження. Неправильне або несправедливе рішення, прийняте на основі таких алгоритмів, може підірвати довіру до державних інституцій і навіть призвести до соціальної нерівності. Це потребує посиленого нагляду і прозорості в тому, як саме працюють моделі ШІ, щоб забезпечити справедливе ставлення до всіх громадян.

ІІ. Переваги.

Незважаючи на ризики, ШІ пропонує значні переваги. Серед іншого, ШІ здатен зменшити людське втручання в рутинні та ризиковані процеси, що знижує ймовірність людських помилок. ШІ може автоматизувати моніторинг подій у системах, швидко реагуючи на підозрілі дії та допомагаючи виявляти кіберзагрози на ранніх стадіях. В області інформаційної безпеки ШІ може використовуватися для аналізу великих обсягів логів та виявлення аномалій, що сприяє швидкому реагуванню на потенційні інциденти.

У галузі охорони здоров'я ШІ може забезпечити революцію, пропонуючи автоматизовані діагностичні інструменти, що скорочують час на постановку діагнозу і дозволяють лікарям зосередитись на складніших завданнях. Наприклад, ШІ вже демонструє значні досягнення в ранньому виявленні онкологічних захворювань на основі аналізу зображень. Це також може бути корисним у віддалених регіонах, де доступ до кваліфікованих медичних спеціалістів обмежений. У сфері освіти ШІ може допомогти створити індивідуальні програми навчання, адаптовані до потреб кожного здобувача освіти, що зробить якісну освіту доступнішою (але чи більш сприйнятою людським розумом?) і підвищить її ефективність.

ІІІ. Прогнози.

Протягом наступних кількох років штучний інтелект, ймовірно, досягне ще більшого проникнення в медицину, освіту, державне управління, нормативно-правове регулювання та енергетику. Провідні спеціалісти прогнозують, що саме в цих сферах ШІ зможе зробити найбільший прорив завдяки масштабним обсягам даних і потенціалу для автоматизації процесів. Розвиток етичних стандартів і підвищення прозорості алгоритмів ШІ допоможуть мінімізувати ризики, сприяючи при цьому максимальному використанню переваг технології.

Крім того, технології ШІ розвиватимуться в напрямку підвищення автономності й обчислювальної потужності, що дозволить використовувати штучний інтелект у ще складніших і критичних сферах. Це також відкриє можливості для розвитку нових індустрій і робочих місць, орієнтованих на підтримку та управління штучним інтелектом, створюючи нові професії та зміцнюючи ринок праці в умовах швидких технологічних змін.

1. Інформаційне право: сучасні виклики і напрямки розвитку: матеріали Першої науково-практичної конференції (18 жовтня 2018 р., м.Київ) / Упоряд. В. М. Фурашев, С. Ю. Петряєв. К. : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2018. 196 с.
2. Мей К. Інформаційне суспільство. Скептичний погляд / Пер. з англ. К. : К. І. С., 2004. 220 с.

А.А. Омельченко

КОНФІДЕНЦІЙНІСТЬ ЦИФРОВИХ БІОМАРКЕРІВ ТА ШТУЧНИЙ ІНТЕЛЕКТ

Згідно [1] цифровий біомаркер (digital biomarkers) це цифрова форма біологічного маркеру, який є вимірним індикатором певного біологічного стану організму. Цифрові біомаркери відрізняє не тільки форма подання, але і спосіб отримання - непрямими вимірюваннями за допомогою безконтактних цифрових сенсорів. Наприклад частота серцевих скорочень, отримана на основі аналізу даних оптичного сенсора, кількість пройдених кроків тощо.

Однією із особливостей цифрових біомаркерів є також те, що вини можуть бути отримані в пацієнта (або користувача) дистанційно та приховано без його дозволу.

На даний момент на масовому споживчому ринку найбільш поширені дві групи пристроїв, які збирають цифрові біомаркери:

- пристрої, що надягаються, “натільні”, такі що мають контакт із тілом (wearables) - в першу чергу смартгодинники, фітнес браслети та навушники, рідше окуляри та спеціалізовані цифрові медичні прилади: цифрові ваги, термометри, тонометри, кардіомонітори тощо;
- пристрої, що носяться, “носимі”, такі які постійно перебувають із користувачем, але не мають контакту із тілом (portables) - в першу чергу смартфони та планшети,

До перспективних пристроїв збору цифрових біомаркерів слід віднеси імпланти та мікропристрої внутрішнього застосування (наприклад перорального).

Смартфони, розумні годинники та фітнес браслети стимулюють попит на використання цифрових біомаркерів: оптичне вимірювання частоти серцевих скорочень та насичення крові киснем (сатурація) є двома найпоширенішими цифровими біомаркерами споживчих носіїв а даний час. Все більше пристроїв використовують електричні контактні сенсори серцевої активності (які називаються в побуті ЕКГ).

Крім того, сучасні натільні та носимі пристрої обладнані інерційними вимірювальними пристроями (IMU) — акселерометром та гіроскопом, що потенційно надає можливості отримання даних фізичної активності користувача: кількість кроків та час. Також ці сенсори потенційно дозволяють отримати більш тонкі дані: частоту дихання або балістокардіограму.

Деякі натільні пристрої обладнані датчиками імпедансу шкіри, або навіть активними сенсорами складу тіла.

Використання радіоінтерфейсів, таких як WiFi або Bluetooth надає можливості як перехоплення високорівневих незашифрованих пакетів медичного обладнання або побутових приладів, так і використання радіомодулів як таких для дистанційного сканування біомаркерів.

Новіші сучасні пристрої обладнані радарами ультраширокого діапазону (ultra-wideband, UWB), які використовуються для передачі даних, але також можуть бути використані для безпосереднього визначення таких цифрових біомаркерів як частота серцевих скорочень та частота дихання [2].

Використання технології глобального позиціонування (GPS) дозволяє співставити зміни величин цифрових біомаркерів із конкретними місцями, які відвідав користувач.

Спільний інтелектуальний аналіз великого обсягу цифрових біомаркерів, якій можливий лише засобами штучного інтелекту дозволяє визначити “похідні” параметри, які оцінюють не тільки фізичний, але і психологічний стан користувача, наприклад “рівень стресу”, або його реакцію на події або власну поведінку.

В теперішній час майже 80% дорослого населення має смартфони тому, як мінімум проміжним, сховищем цифрових біомаркерів є смартфон, на якому типово встановлюється програмне забезпечення, яке управляє біометричним сенсором. Тому навіть ті цифрові біомаркери, які отримати приховано прямими вимірюваннями неможливо, наприклад результати аналізу глюкометра, можна спробувати отримати від смартфона. Більш того, в смартфонах здебільшого зберігаються не тільки результати поточних вимірювань, але й їхня історія, що надає додаткові можливості аналізу даних зловмисниками. Смартфон також може зберігати дані різних біосенсорів що надає ще більше можливостей оцінки фізичного або емоційного стану користувача.

Зростання використання цифрових біомаркерів, через легкість їх отримання та розповсюдження, супроводжується зростанням проблем конфіденційності та безпеки даних. Для їх захисту використовуються різні за природою та призначенням способи: зашумлення, деперсоналізація тощо, але це створює для кінцевих споживачів (наприклад, постачальників медичних послуг) певні проблеми, тому що наряду із захисту від неправомірного використання треба забезпечити гарантоване та ефективне їх використання. Тому найбільш ефективним є застосування засобі штучного інтелекту для визначення контексту отримання цифрових біомаркерів та блокування доступу до них в нехарактерних для цього випадках [3].

1. Biomarker. Digital. Електронний ресурс. Спосіб доступу: https://en.wikipedia.org/wiki/Biomarker#Digital.

2. A device for outputting simulated vital signs and method for operating the same Електронний ресурс. Спосіб доступу https://doi.org/10.8080/1020220121131?urlappend=en.

3. О. Скіцько, та ін. Загрози та ризики використання штучного інтелекту. Електронний ресурс. Спосіб доступу https://csecurity.kubg.edu.ua/index.php/journal/article/view/520/408.

V.P. Petrenko

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON ENTREPRENEURSHIP: INSIGHTS FROM A QUESTIONNAIRE STUDY AND A BRIEF LITERATURE REVIEW

In recent years, the integration of Artificial Intelligence (AI) has become a significant force across various industries, reshaping business operations and empowering entrepreneurs to address diverse tasks. The Strategic Program on Artificial Intelligence 2022-2024, developed in Rome, highlights the need for advanced research on AI, recognizing it as a key driver of digital transformation with the potential to enhance productivity, automate processes, and improve analytics (Ministry of University and Research, 2021). This study contributes to the field by exploring public perceptions of AI's impact on entrepreneurship, presenting findings from a questionnaire conducted in Ukraine and Italy, and reviewing relevant academic literature that underscores AI's transformative potential in business.

The literature identifies several ways in which AI transforms entrepreneurship. Giuggioli and Pellegrini (2023) outline four stages in an AI-enabled entrepreneurial journey: opportunity identification, decision-making, performance optimization, and research. Specifically, AI aids decision-making by analyzing extensive user data, uncovering latent needs, and providing valuable product feedback, as discussed by Li et al. (2022). Rao et al. (2024) suggest strategies for entrepreneurs to incorporate AI as a core component of their business strategies. Additionally, studies on AI's role in sustainable entrepreneurship have gained prominence, with Hossain (2024) and Abdus and colleagues (2024) emphasizing AI's importance in fostering sustainable business practices. Abdus et al. particularly highlight the integration of social and environmental responsibilities. Black et al. (2024) identify proactive leadership and a culture of innovation as key factors for successful AI-driven transformation, while Sohail et al. (2023) confirm that AI facilitates the development of innovative, sustainable business models.

In order to investigate public perceptions of AI's impact on entrepreneurship, a questionnaire was distributed among participants in Ukraine and Italy, targeting both entrepreneurs and non-entrepreneurs (Petrenko, 2024). The questionnaire included questions on various aspects of AI integration, including perceived utility, frequency of use, and opinions on AI's influence on business processes. Out of a total of 205 responses, 104 were from Ukraine and 101 from Italy. The results reveal that 85% of respondents use AI, and 93,7% consider it beneficial for entrepreneurial activities. Furthermore, 92,1% believe AI can streamline business operations. Among entrepreneurs, 84,2% have used AI for idea generation, and 73,7% actively use it in their business activities. Notably, 92,9% of entrepreneurs use AI regularly, ranging from daily to weekly. Regarding the value AI provides to their businesses, 92,9% rated its assistance between 3 and 5 on a scale of 1 to 5. AI was reported to be capable of managing up to 40% of business activities, depending on the industry. A notable finding from the survey is the split preference between hiring human workers and utilizing AI services, with 50% of respondents favoring each option. Additionally, 71,4% indicated they would find it challenging to stop using AI for business, and 92,9% expressed willingness to pay for AI services based on cost.

These findings underscore the substantial reliance on AI among entrepreneurs, particularly in generating ideas and enhancing productivity. The literature reviewed further supports these insights, demonstrating that AI impacts each stage of the entrepreneurial process, from identifying opportunities to supporting sustainable business practices. Giuggioli and Pellegrini's (2023) four-stage model offers a useful framework for understanding AI's role in entrepreneurship. Additionally, the survey results highlight interesting nuances in attitudes toward AI's integration, such as the balanced preference for human labor versus AI services and the anticipated challenges of discontinuing AI usage. This reflects AI's growing embedment in business operations and a shift toward data-driven, automated decision-making among entrepreneurs.

In conclusion, AI's integration into entrepreneurship is accelerating, presenting significant opportunities as well as challenges. This study underscores the need for continued research on AI's transformative role across sectors, as its applications continue to evolve. The findings reveal AI's capability to reshape business models, optimize decision-making, and foster sustainable development, echoing existing research that emphasizes AI's importance in contemporary entrepreneurship. Further investigation is required, especially with a focus on industry-specific impacts and the balance between human resources and AI-driven solutions. These insights could help shape policies and strategies to support entrepreneurs in harnessing AI's potential while addressing the ethical, social, and economic implications of its widespread adoption.

1. Ministry of University and Research. (2021). The National Strategic Program on AI (2022-2024): Alignment with the EU strategy on AI and Intervention Area 4 of the Italian PNR (2021-2027).

2. Giuggioli, G., Pellegrini, M.M. (2023). Artificial intelligence as an enabler for entrepreneurs: a systematic literature review and an agenda for future research. International Journal of Entrepreneurial Behavior & Research. Vol. 29 No. 4, pp. 816-837. https://doi.org/10.1108/IJEBR-05-2021-0426.

3. Li X., Zhang, X., Liu Y., Mi, Y., Chen, Y. (2022). The impact of artificial intelligence on users' entrepreneurial activities. Systems Research and Behavioral Science, Wiley Blackwell, vol. 39(3), pages 597-608.

4. Rao V.N.T., Vardhan G.H., Sushanth K. (2024). The future of entrepreneurship: employing artificial intelligence, pp. 134 - 151. https://doi.org/10.4018/979-8-3693-1842-3.ch009.

5. Hossain S.F.A. (2024). Utilizing AI and smart technology to improve sustainability in entrepreneurship. IGI Global, pp. 1 - 370. https://doi.org/10.4018/979-8-3693-1842-3.

6. Abdus, S., Rubaba, N., Hasanuzzaman, T., Nanta, S. (2024). Social and Environmental Responsibility in AI-Driven Entrepreneurship. https://doi.org/10.4018/979-8-3693-1842-3.ch012.

7. Black, S., Samson, D., Ellis, A. (2024). Moving beyond ‘proof points’: Factors underpinning AI-enabled business model transformation. International Journal of Information Management. Vol. 77. https://doi.org/10.1016/j.ijinfomgt.2024.102796.

8. Verma, Sohail. (2023). Sustainability in the Digital Age: Leveraging Artificial Intelligence for Organizational Transformation. https://www.researchgate.net/publication/376356595_Sustainability_in_the_Digital_Age_Leveraging_Artificial_Intelligence_for_Organizational_Transformation#full-text.

9. Petrenko, V. P. (2024). Impact Of Artificial Intelligence On Future Entrepreneurship: Survey Results And Trends Analysis. Review Of Transport Economics And Management, (11(27), 131–139. https://doi.org/10.15802/rtem2024/304822.

К.В. Бабій, О.А. Ворон

ВДОСКОНАЛЕННЯ РЕКУЛЬТИВАЦІЇ ТЕХНОГЕННО ПОРУШЕНИХ ЗЕМЕЛЬ ЗА ДОПОМОГОЮ РОБОТЕХНІКИ І ШТУЧНОГО ІНТЕЛЕКТУ

Процес діяльності гірничодобувних підприємств супроводжується порушенням не тільки масиву гірських порід, в якому знаходиться родовище корисних копалин, а й ґрунтового покриву на території гірничого відводу та прилежних землях. Крім того в оточуюче середовище і особливо в ґрунти, які законсервовані, потрапляють шкідливі речовини. Вони розповсюджуються під впливом зовнішніх факторів і псують стан ґрунтового покриття. З часом їх якісний стан погіршується за рахунок ерозії, ущільнення пористості, засолення, підвищення кислотності чи забруднення небезпечними речовинами тощо [1]. За законодавством техногенно порушенні території повинні бути рекультивовані згідно ст. 166 [2].

В Інституті геотехнічної механіки ім. М.С. Полякова НАН України розроблена технологія пошарової гірничотехнічної і біологічної рекультивації (ТПГБР) [3]. Технологія проведення пошарової рекультивації порушених техногенних середовищ забезпечує створення потенційно родючого шару необхідного для відновлення сільськогосподарських і лісогосподарських земель. Згідно [3] в цьому процесі послідовно укладаються різні прошарки за проектом рекультивації задля відновлення структури природного масиву. Особливістю технології є створення штучної пористості в прошарках за допомогою кореневої системи рослин, що сприяє покращенню його властивостей.

Технологічна схема робіт з рекультивації за ТПГБР включає наступні виробничі процеси: формування поверхні після гірничо-технічної рекультивації за проєктними кутами ландшафту, селективне транспортування осадових порід, формування першого шару насипного ґрунту визначеної потужності, вирівнювання його поверхні, підготовка під висадку рослин, висадка насіння, обробка паростків від шкідників за необхідністю, полив та скошування біомаси. Після цього комплексу робіт формується другий/наступний шар насипного ґрунту з тим самим переліком виробничих процесів. В результаті отримуємо пошарово-сформований масив з розвиненою щільною системою, яка необхідна для наступного використання земель в сільськогосподарському напрямку (рис. 1).

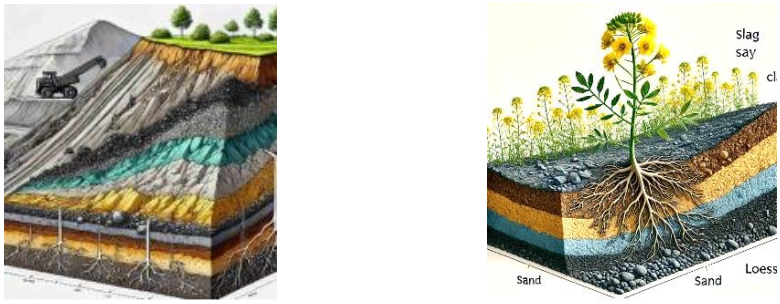


Рисунок 1 – Схема структури пошарово-сформованого масиву
для відновлення продуктивного шару ґрунту за технологією ТПГБР

Технологічний комплекс виконання ТПГБР включає: автосамоскид, бульдозер, навантажувач, екскаватор, сіяло, косарку тощо.

ТПГБР дозволяє відновити техногенно порушені землі та повернути їх до продуктивного сільськогосподарського фонду, але вона трудомістка і довготривала за часом виконання. Тому наступним етапом її розвитку запропоновано удосконалення процесу за рахунок застосування робототехніки і обладнання з штучним інтелектом (ШІ). Аналіз існуючого роботизованого гірничого транспорту і обладнання дозволив встановити можливість використання його за окремими технологічними процесами (рис. 2).

Рисунок 2 – Етапи проведення рекультивації за ТПГБР

Екскаватори з дистанційним керуванням забезпечують можливість виконання важких робіт у небезпечних зонах без участі оператора на місці. Це особливо важливо в кар'єрах при виконанні гірничотехнічної

рекультивації, де умови можуть бути небезпечними через нестабільні уступи, зсуви або наявність шкідливих речовин чи пилу. Завдяки такому підходу, оператори можуть контролювати роботу екскаватора з безпечної відстані, зменшуючи ризик травм. Дистанційно керовані навантажувачі забезпечують точне виконання операцій, таких як транспортування та укладання будівельних матеріалів у визначених зонах. Завдяки системам автоматичного управління вони можуть бути запрограмовані для виконання складних завдань, що підвищує ефективність роботи і знижує витрати на ресурси.

На перехідному етапі від гірничотехнічної до біологічної рекультивації необхідною ланкою є застосування автосамоскидів для селективного транспортування осадових порід. Запропоновано використовувати автосамоскиди з дистанційним керуванням і кластерами ШІ, що дозволить автономно виконувати завдання за заданими алгоритмами, відстежувати їх стан і ефективність у реальному часі, зменшити ризик помилок та підвищує продуктивність праці.

Дистанційні навантажувачі можуть бути використані для поступового укладання шарів під висадку фіто культур або енергетичних рослин. Технології дистанційного керування дозволяють проводити цю роботу з високою точністю. Автоматизація дозволяє швидше реагувати на зміни в умовах складного рельєфу, наприклад, у випадку необхідності коригування потужності насипного шару чи зміни кута нахилу для формування мезорельєфу [4].

Дрони рекомендовано використовувати для посадки насіння енергетичних культур, поливу та здобрювання проростих рослин. Вони забезпечують точне та ефективне внесення насіння, а також моніторинг стану рослинності.

Інноваційним впровадженням для вдосконалення ТПГБР є застосування методів зі ШІ, які допоможуть проаналізувати результати досліджень щодо стану ґрунту, рослинності і екологічних умов (на етапі перепроєктних рішень); планувати роботи та її організувати; оптимізувати маршрути для екскаваторів, самоскидів та навантажувачів, щоб забезпечити швидкий і безпечний транспорт, а також виконувати моніторинг і контроль.

Висновки. Використання робототехніки і штучного інтелекту в процесах рекультивації техногенно порушених земель відкриває нові можливості для підвищення ефективності та безпеки. Інтеграція ШІ в ці процеси є першим кроком у напрямку сталого розвитку гірничої промисловості.

1. Долгова Т.І. (2009). Екологічна безпека ґрунтів у гірничодобувних районах: Монографія. Днепропетровск: НГУ, 270 с.

2. Земельний Кодекс України від 25.10.2001 № 2768-III зі змінами від 16.07.2020 № 340-IX [Електронний ресурс]. Режим доступу http: zakon.rada.gov.ua/go/2768-14 /.

3. Четверик, М.С., & Ворон, О.А. (2011). Патент № 64879 Україна, спосіб рекультивації земель, порушених відкритими гірничими роботами, для створення потенційно родючого шару ґрунту. Отримано з https://ua.patents.su/364879-sposib-rekultivaci-zemel-porushenikh-vidkritimi-girnichimi-robotami-po-stvorennyu-potencijjnorodyuchogo-sharu-runtu.html.

4. Четверик, М.С., & Малєєв, Е.В. (2017). Обґрунтування технології відновлення мезорельєфу при використанні відвалоутворювача-метателя. Геотехнічна механіка: Міжвідомчий збірник наукових праць. Дніпро: ІГТМ НАНУ, Вип. 137, С. 202-212. Отримано з http://dspace.nbuv.gov.ua/handle/123456789/158651.

І.В. Дегтяренко

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ МОДЕЛЕЙ ГЛИБОКОГО НАВЧАННЯ НА EDGE-ПРИСТРОЯХ

Методи та моделі штучного інтелекту (ШІ) отримали стрімкий розвиток протягом останніх двох десятиріч [1,2] у таких сферах, як комп'ютерне бачення [3], обробка природної мови [4], розпізнавання образів та інші. Прогрес у цих напрямках дозволяє реалізовувати новітні сценарії обробки та витягу інформації з даних великих обсягів і складної структури завдяки використанню моделей глибокого навчання. Ці сценарії широко застосовуються в сучасних системах аналізу та розпізнавання різноманітних даних, що дозволяє значно підвищувати точність та ефективність сервісів, індустріальних і бізнесових операцій [5].

Паралельний стрімкий розвиток апаратних засобів відкрив можливість реалізації методів ШІ на так званих edge-пристроях, тобто на пристроях, максимально наближених до користувача. Вони виконують обробку даних безпосередньо на місці їх генерації, тобто на «краю» мережі, а не відправляють їх на центральний сервер або в хмару для подальшої обробки. Прикладами edge-пристроїв є смартфони, смарт-годинники, телевізори, розумні камери, автономні транспортні засоби та інші портативні або стаціонарні пристрої [6,7].

Основними перевагами імплементації ШІ на edge-пристроях у порівнянні з хмарними рішеннями є:

- значне зниження затримки на обробку за рахунок відсутності необхідності передачі даних на сервери або в хмару та чекання повернення результатів. Це критично для застосувань, де важлива швидка реакція в режимі реального часу, наприклад, в системах автономного керування автомобілем та системах взаємодії з користувачем (ідентифікація, розпізнавання або переклад текстових та аудіо даних);

- доступність сервісів у разі відсутності зовнішнього зв'язку. Це дозволяє зберігати функціональність пристрою навіть при тимчасових збоях у мережі або відсутності підключення до мережі, що особливо важливо для дронів, автомобілів, медичних пристроїв та ін.;

- зниження витрат на реалізацію рішень за рахунок зменшення або відсутності витрат на зовнішні канали зв'язку та сервери. Такі рішення є також значно більш енергоефективними в порівнянні з серверними рішеннями;

- покращення показників безпеки та конфіденційності даних користувача через те, що дані не покидають локальне середовище, що зменшує ризик їх витоку або несанкціонованого доступу під час передачі через мережу. Це має особливе значення для медичних пристроїв та пристроїв, що обробляють іншу персональну інформацію користувача;

- можливість персоналізації та адаптації сервісів за рахунок використання методів самонавчання. Це дозволяє пристроям вдосконалювати свої алгоритми та моделі на основі нових даних, отриманих у реальному часі, без потреби в постійній взаємодії з сервером.

Незважаючи на очевидні переваги, впровадження систем ШІ на edge-пристроях супроводжується низкою суттєвих проблем і викликів:

- обмеження пам'яті та процесорної потужності. Моделі ШІ, особливо глибокі нейронні мережі, можуть бути дуже великими і вимагати великих обсягів пам'яті для зберігання параметрів моделі, а також значної обчислювальної потужності для виконання розрахунків. Тому важливо адаптувати моделі для роботи в обмежених умовах;

- обмеження в енергоспоживанні. Ця проблема особливо актуальна для мобільних та інших автономних пристроїв. Високе енергоспоживання моделей ШІ може значно скоротити термін служби батарей або вимагати постійного підключення до джерел живлення;

- складність імплементації та оновлення моделей на edge-пристроях, особливо коли пристрої працюють в розподілених або ізольованих середовищах без постійного доступу до мережі;

- необхідність адаптації та оптимізації моделей ШІ для запуску на edge-пристроях. Це може бути дуже складним завданням, оскільки часто потрібно знаходити баланс між точністю моделі і ефективністю її роботи на пристрої. Архітектура нейронної мережі має бути узгоджена з можливостями певного edge-пристрою. Основні рекомендації щодо адаптації та оптимізації моделей глибокого навчання будуть наведені далі;

- підвищені вимоги до апаратних засобів edge-пристроїв та їх висока вартість. Як вже зазначалося, для запуску моделей глибокого навчання потрібні потужні обчислювальні модулі та великі обсяги пам'яті. Все це може обмежувати доступність таких пристроїв.

В сучасних обчислювальних системах, у тому числі і на edge-пристроях, використовуються три основні види процесорних модулів:

- центральний процесор (CPU) — універсальний процесор, який призначений для виконання загальних обчислювальних завдань. Він здатний виконувати широкий спектр операцій, включаючи логічні, арифметичні та управлінські функції;

- графічний процесор (GPU) — пристрій, спеціалізований на обробці графічних даних, але також має великий потенціал для обчислень, які можна паралелізувати;

- нейропроцесор (NPU) — спеціалізоване апаратне рішення, яке розроблене для прискорення обчислень, пов'язаних з нейронними мережами, особливо для виконання операцій, характерних для глибокого навчання (наприклад, матричні множення, активаційні функції тощо).

Імплементація моделей штучного інтелекту на NPU модулях є пріоритетною через його високу енергоефективність та швидкість обчислень. Але архітектури моделей глибокого навчання мають бути

адаптовані до можливостей та лімітів кожного конкретного NPU модуля. Перевага в архітектурі має бути віддана широко розповсюдженим конволюційним нейронним мережам (CNN) без використання специфічних перетворень. Рекурентні нейронні мережі (RNN) не підтримуються більшістю наявних NPU. При використанні комплексної або специфічної архітектури нейронної мережі вона має бути розбита на модулі з відокремленням частин, які можуть бути адаптовані для запуску на NPU [8]. Інші модулі мережі будуть запускатись на CPU або на GPU процесорах.

Окрім того, перед портуванням моделей глибокого навчання для запуску на edge-пристроях всі моделі мають бути оптимізовані з точки зору складності та розміру, оскільки, як вже зазначалося, edge-пристрої, як правило, мають суттєві обмеження в обчислювальних ресурсах та пам'яті [8,9]. Типовими техніками оптимізації моделей глибокого навчання є наступні:

- **Квантизація моделі.** Дана техніка націлена на зменшення точності представлення чисел (ваг) у моделі, що дозволяє значно зменшити її розмір і покращити швидкість виконання. Найбільш поширеними є 8- та 4-бітні квантизації, які в 4–8 разів зменшують моделі з 32-бітним представленням ваг. Квантизація особливо ефективна для прискорення виконання на спеціалізованих процесорах, таких як NPU або DSP, які оптимізовані для роботи з цілими числами замість чисел з плаваючою точкою.

- **Дистиляція моделі**. Це метод, при якому велика, складна модель (вчитель) навчає маленьку, спрощену модель (учень). Модель-учень намагається наблизитися до результатів моделі-вчителя, але має меншу кількість параметрів, що робить її швидшою та менш ресурсозатратною. Метод дистиляції можна реалізувати вручну або через спеціалізовані бібліотеки TensorFlow або PyTorch.

- **Прирізка моделі**. Ця техніка полягає в усуненні "неважливих" параметрів або нейронів із моделі. Це дозволяє зменшити її розмір і обчислювальну складність. Прирізка застосовується як для усунення нульових або малозначущих ваг, так і для усунення певних шарів в архітектурі нейронної мережі.

Існують також багато інших методів оптимізації мереж, які є комбінацією або розвитком вищевикладених технік [9]. Важливо зазначити, що при застосуванні цих методів оптимізації потрібно слідкувати за можливою деградацією якості роботи моделі. В кожному конкретному випадку потрібно визначити прийнятний компроміс між точністю, швидкістю та ресурсами моделі.

Для розгортання на edge-пристроях важливо використовувати фреймворки та інструменти, які дозволяють зберегти ефективність, при цьому забезпечуючи зручність інтеграції з пристроями. Найбільш популярними наразі є наступні засоби та формати:

- **TensorFlow Lite**: спеціалізована версія TensorFlow, яка оптимізована для виконання на мобільних та вбудованих системах;

- **ONNX**: стандарт для обміну моделями, який дозволяє виконувати моделі на різних пристроях, включаючи edge-пристрої;

- **OpenVINO**: набір інструментів для оптимізації виконання моделей на пристроях з Intel, таких як мобільні пристрої та вбудовані системи.

Висновки

Імплементація систем штучного інтелекту на edge-девайсах є важливим кроком у розвитку сучасних технологій, що відкриває нові можливості для реального часу обробки даних, зниження затримки та покращення безпеки. Водночас існують значні виклики, зокрема щодо обмежених ресурсів пристроїв, необхідності оптимізації моделей та інтеграції з іншими системами. В роботі представлено огляд особливостей застосування моделей глибокого навчання на edge-пристроях та надано практичні рекомендації щодо їх оптимізації та адаптації.

Інновації в області мікропроцесорних чіпів та методів ШІ створюють потужний фундамент для подальшого розвитку edge-комп'ютингу, відкриваючи нові можливості в автоматизації, безпеці, медицині, промисловості та багатьох інших сферах. У майбутньому ці пристрої відіграватимуть ключову роль у розвитку інтелектуальних, автономних та адаптивних систем, здатних працювати без необхідності постійного підключення до хмари або централізованих серверів.

1. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
2. Russell, S., & Norvig, P. (2020). Artificial intelligence: A modern approach (4th ed.). Pearson.
3. Shanmugamani, R. (2017). Deep learning for computer vision. Packt Publishing.
4. Jurafsky, D., & Martin, J. H. (2020). Speech and language processing (3rd ed.). Pearson.
5. Rose, D. (2019). Artificial intelligence for business: A roadmap for getting started with AI. O'Reilly Media.
6. Chen, S., & Zhang, J. (2021). Edge computing and AI: A survey on applications, opportunities, and challenges. IEEE Transactions on Industrial Informatics, 17(5), 3541-3553. https://doi.org/10.1109/TII.2020.3013371.
7. Degtyarenko, I., Deriuga, I., Grygoriev, A., Polotskyi, S., Melnyk, V., Zakharchuk, D., & Radyvonenko, O. (2021, June). Hierarchical recurrent neural network for handwritten strokes classification. In ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 2865–2869). IEEE. https://doi.org/10.1109/ICASSP39728.2021.9414269.
8. Degtyarenko, I., Tkach, N., Radyvonenko, O., Deriuga, I., Seliuk, K., Ivanov, O., ... & Hahm, C. H. (2023, June). SDRV: Real-time on-device subtitles detection, recognition and voicing. In 2023 IEEE International Conference on Acoustics, Speech, and Signal Processing Workshops (ICASSPW) (pp. 1–5). IEEE. https://doi.org/10.1109/ICASSPW59220.2023.10192952.
9. Zhang, S., & Xu, L. (2020). Optimizing deep learning models for deployment on edge devices. Proceedings of the IEEE International Conference on Edge Computing, 67-74. https://doi.org/10.1109/EDGE.2020.9052341.

Д.І. Симонов

ПРОГНОЗУВАННЯ ВПЛИВУ ЛІДЕРІВ ДУМОК НА ПОВЕДІНКУ СОЦІАЛЬНИХ ГРУПІ

Безпека держави та суспільства значною мірою залежить від здатності соціальних груп реагувати на внутрішні та зовнішні виклики. Лідери думок, що формують громадську думку, можуть сприяти як стабільності, так і дестабілізації суспільства. Нестача математичних моделей прогнозування їх впливу створює ризики для національної безпеки. Соціальні мережі та медіа платформи стають інструментами впливу, через які можна підтримувати або підривати суспільну стабільність. Це дослідження має на меті продемонструвати одну з моделей, що дозволяє ідентифікувати потенційні загрози та надати інформацію для зміцнення безпеки держави.

Узагальнена математична модель суспільства вимагає врахування її багаторівневої структури, що включає: індивідів, групи та лідерів думок (атракторів). Кожен індивід та група мають власні характеристики, які впливають на взаємодію і динаміку розвитку суспільства в цілому.

Припустимо, що суспільство можливо зобразити у вигляді графу $G = (V, E)$, де V – множина вершин (індивіди та групи), E – множина ребер $e_{ij} \in E$, що описує зв'язки між ними. Кожне ребро e_{ij} має вагу ω_{ij}, що характеризує силу зв'язку між індивідами або групами i та j (1):

$$\omega_{ij} = f\left(d_{ij}, p_{ij}\right), \tag{1}$$

де d_{ij} – відстань між індивідами i та j у просторі ідей чи інформаційних впливів; p_{ij} – параметр, що відображає інтенсивність взаємодії (наприклад, частоту контактів).

Для кожного індивіда $e_{ij} \in E$ визначено вектор стану $\vec{s_i}(t)$, який відображає його погляди, емоційний стан та сприйняття певних ідей у момент часу t. Нехай $\vec{s_i}(t)$ – це n-вимірний вектор, де кожна компонента $\vec{s_i^k}(t)$ відповідає конкретній характеристиці, наприклад, політичній або культурній орієнтації. Динаміка зміни стану індивіда описується рівнянням (2) [1]:

$$\frac{d\vec{s_i}(t)}{dt} = \sum_{j \in N(i)} \omega_{ij}\left(\vec{s}_j(t) - \vec{s}_i(t)\right) + \vec{I}_i(t), \tag{2}$$

де $N(i)$ – множина сусідів індивіда i; $\vec{I}_i(t)$ – зовнішній вплив, наприклад, від лідерів думок або інформаційних потоків.

Як було зазначено, лідери думок мають значний вплив на суспільство через широку аудиторію і сильний інформаційний вплив. Нехай $L \subset V$ – множина лідерів думок. Кожен лідер $l_k \in L$ має певну інтенсивність впливу $\alpha_k(t)$, що змінюється в часі. Вплив лідера на індивіда i описується як додатковий елемент у векторі зовнішнього впливу (3):

$$\vec{I}_i(t) = \sum_{k \in L} \alpha_k(t) \cdot \vec{s}_k(t) \cdot g(d_{ik}), \tag{3}$$

де $g(d_{ik})$ – функція зменшення впливу лідера l_k з віддаленням від індивіда i, яка може бути задана, наприклад, як $g(d_{ik}) = e^{-\beta d_{ik}}$ з деяким параметром β.

Інформаційні потоки формують загальний фон впливу на суспільство та мають широкий вплив на поведінку груп. Позначимо інформаційний потік як функцію $F(t, x)$, де x – просторові або тематичні координати. Кожен індивід взаємодіє з інформаційним полем, що впливає на його стан (4):

$$\vec{s}_i(t + \Delta t) = \vec{s}_i(t) + \gamma F\left(t, x_i\right) \cdot \Delta t, \tag{4}$$

де γ – коефіцієнт чутливості індивіда до інформаційного потоку; x_i – положення індивіда в просторі ідей чи інформації.

Рівновага в цій моделі досягається, коли зміна стану кожного індивіда стабілізується, тобто (5):

$$\frac{d\vec{s}_i(t)}{dt} \approx 0, \forall i \in V. \tag{5}$$

У моделюванні поведінки соціальних груп важливо враховувати як внутрішню динаміку групи, так і зовнішній вплив, що здійснюється лідерами думок. Модель поведінки груп описує, як настрої та погляди окремих індивідів трансформуються в колективні рішення та змінюються під впливом зовнішніх чинників.

Визначимо динамічну модель зміни групового стану під впливом лідерів думок та опишемо механізми взаємодії між групами та їх учасниками.

Нехай $G_i \subseteq G$ – соціальна група, що складається з індивідів $v_j \in V$, які мають вектори стану $\vec{s_j}(t)$. Стан групи можна описати середнім вектором, що відображає загальний настрій та позицію групи в момент часу t (6):

$$\vec{s}_j(t) = \frac{1}{|G_i|} \sum_{j \in G_i} \vec{s}_j(t), \tag{6}$$

де $|G_i|$ – кількість учасників у групі G_i.

Зв'язки між соціальними групами впливають на міжгрупову динаміку, де одні групи можуть посилювати або послаблювати вплив на іншу, а взаємодія між групами описується додатковою змінною в рівнянні (7) для $\vec{s}_{G_i}(t)$:

$$\frac{d\vec{s}_{G_i}(t)}{dt} = \sum_{k\in L} \alpha_k(t)\cdot\left(\vec{s}_k(t) - \vec{s}_{G_i}(t)\right)\cdot g(d_{ik}) + \sum_{G_i\in H,\, j\neq i} \beta_{ij}\cdot\left(\vec{s}_{G_j}(t) - \vec{s}_{G_i}(t)\right), \quad (7)$$

де H – множина груп; β_{ij} – коефіцієнт міжгрупової взаємодії.

Відповідно, рівноважний стан для групи $G_i \subseteq G$ досягається, коли зміни в груповому настрої припиняються, тобто (8):

$$\frac{d\vec{s}_{G_i}(t)}{dt} \approx 0, \forall i \in V. \quad (8)$$

Ця модель відображає, як вплив лідерів думок і внутрішня взаємодія учасників групи визначають динаміку колективних настроїв. Модель дозволяє виявити умови, за яких групи можуть стабілізуватися або змінити свої позиції під впливом зовнішніх інформаційних потоків та лідерів.

Прогнозування поведінки соціальних груп на основі математичної моделі та аналізу даних є важливим завданням у моделюванні соціальних систем. Використання алгоритму машинного навчання дозволяє адаптуватися до змін у поведінці груп та точніше передбачати зміни в їхніх настроях і позиціях. У цьому розділі розглянемо алгоритм машинного навчання, що базується на аналізі групових станів і зовнішніх впливів.

Для прогнозування групової поведінки можливо використовувати рекурентну нейронну мережу (RNN) або ж її покращені варіанти, наприклад, LSTM (Long Short-Term Memory) або GRU (Gated Recurrent Unit), які добре підходять для моделювання часових рядів та врахування попередніх станів групи.

Позначимо модель, яка прогнозує стан групи $\vec{s}_{G_i}$ на наступний момент часу $(t+\Delta t)$, як функцію M з параметрами θ, рівняння (9) [2]:

$$\vec{s}_{G_i}(t+\Delta t) = \mathrm{M}\left(X_{G_i}(t), \theta\right). \quad (9)$$

Навчання алгоритму виконується с використанням історичних даних про зміну станів соціальних груп і зовнішніх впливів, де $\left\{X_{G_i}(t), \vec{s}_{G_i}(t), \vec{s}_{G_i}(t+\Delta t)\right\}$ – навчальна вибірка.

Цільова функція для оптимізації параметрів θ моделі M може бути задана як середньоквадратична похибка (MSE) [3] між прогнозованим і реальним станом групи (10):

$$L(\theta) = \frac{1}{N}\sum_{i=1}^{N}\left\|\vec{s}^{\,\mathrm{pred}}_{G_i}(t+\Delta t) - \vec{s}_{G_i}(t+\Delta t)\right\|^2, \quad (10)$$

де N – кількість прикладів у навчальній вибірці; $\vec{s}^{\,\mathrm{pred}}_{G_i}(t+\Delta t)$ – прогнозований стан; $\vec{s}_{G_i}(t+\Delta t)$ – фактичний стан.

Для оцінювання точності моделі доцільно використовувати показник середньої абсолютної похибки (MAE) і коефіцієнт детермінації R^2, які показують, наскільки точно модель прогнозує зміни групового стану.

Оскільки поведінка групи може змінюватися під впливом непередбачуваних зовнішніх факторів, важливо, щоб модель була адаптивною [4]. Для цього застосовуються методи донавчання (fine-tuning) [5], що дозволяють регулярно оновлювати модель на основі нових даних. Наприклад, якщо група зазнала суттєвих змін, донавчання дозволяє моделі коригувати прогнози відповідно до нових умов.

Процес адаптації (adaptation) можна описати через оновлення параметрів θ після кожного нового спостереження або певного періоду часу. Це дозволяє алгоритму швидко адаптуватися до змін у соціальному середовищі, забезпечуючи більш точні прогнози.

Висновки

У цьому дослідженні ми запропонували математичну модель для прогнозування впливу змін, у тому числі через лідерів думок, на поведінку соціальних груп, яка враховує їхню багаторівневу структуру. Запропонований підхід дає змогу аналізувати та прогнозувати поведінку груп, враховуючи як внутрішню динаміку, так і зовнішні впливи через інформаційні потоки. Використання методів машинного навчання, таких як рекурентні нейронні мережі, забезпечує можливість адаптивного моделювання в умовах змінних соціальних параметрів. Результати дослідження можуть бути корисними для національної безпеки та управління суспільними настроями, дозволяючи виявляти та мінімізувати потенційні загрози стабільності держави.

1. Симонов, Д. І., Заіка, Б. Ю. (2024). Моделювання управління складними інформаційними багатокомпонентними системами. Науковий вісник Ужгородського університету. Серія «Математика і інформатика», 44(1), 168–174. https://doi.org/10.24144/2616-7700.2024.44(1).168-174.

2. Symonov, D., Symonov, Y. (2024). Methods for selecting models of functioning of multicomponent information and environmental systems. Scientific Journal «Mathematical Modeling», Vol. 1, No 50, P. 57-63. DOI: 10.31319/2519-8106.1(50)2024.304943.

3. Chicco, D., Warrens, M.J., & Jurman, G. (2021). The coefficient of determination R-squared is more informative than SMAPE, MAE, MAPE, MSE and RMSE in regression analysis evaluation. PeerJ Computer Science, 7. DOI:10.7717/peerj-cs.623.

4. Adnan, M., Alarood, A.A., Uddin, M.I., & Rehman, I.U. (2022). Utilizing grid search cross-validation with adaptive boosting for augmenting performance of machine learning models. PeerJ Computer Science, 8. DOI:10.7717/peerj-cs.803.

5. Black, K., Janner, M., Du, Y., Kostrikov, I., & Levine, S. (2023). Training Diffusion Models with Reinforcement Learning. ArXiv, abs/2305.13301. DOI:10.48550/arXiv.2305.13301.

С.О. Євдокимов

ВПЛИВ ТЕХНОЛОГІЇ «FINGERPRINTING» НА КІБЕРБЕЗПЕКУ СИГНАЛЬНИХ СИСТЕМ СУЧАСНОГО ЗАЛІЗНИЧНОГО ТРАНСПОРТУ

Сучасні залізничні системи мають величезну складність, зростаючі вимоги до безпеки та необхідність в адаптації до нових технологій. Серед новітніх рішень, що впроваджуються у залізничному транспорті, особливе місце займає технологія «Fingerprinting». Ця технологія може суттєво вплинути на підвищення рівня кібербезпеки сигналізаційних систем.

Фінгерпринтинг — це метод, який дозволяє ідентифікувати унікальні характеристики системи або пристрою на основі їхніх параметрів. В контексті залізничного транспорту, ця технологія може бути використана для ідентифікації різних компонентів сигналізації, забезпечуючи їх безперервний моніторинг та виявлення аномалій.

Діаграма на рис. 1 демонструє послідовність процесу автентифікації з використанням технології фінгерпринтингу у системі кібербезпеки залізничного транспорту. Показано взаємодію між пристроєм, модулем аналізу аномалій і контролером доступу, що дозволяє ідентифікувати пристрої за їх унікальними характеристиками, виявляти аномальні поведінки та забезпечувати безпечний доступ.

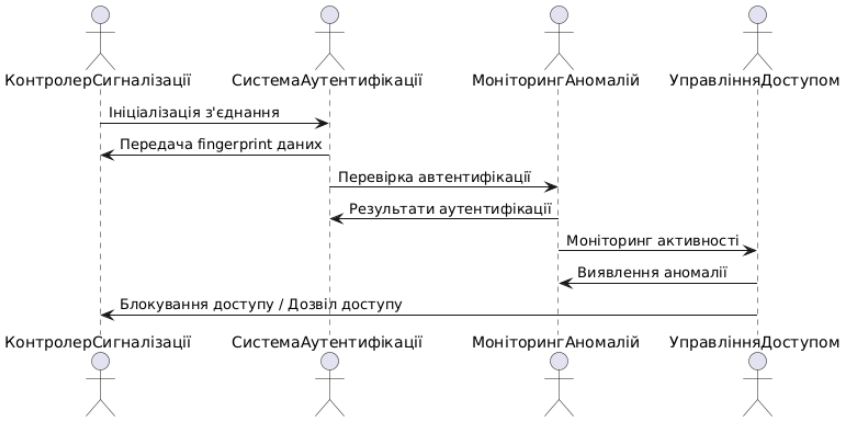


Рисунок 1 – Процес автентифікації з використанням Fingerprinting

У рамках дослідження було проведено детальний аналіз впливу технології фінгерпринтингу фінгерпринтингу на кібербезпеку сигналізаційних систем сучасного залізничного транспорту. Рівень несанкціонованого доступу:

$$U = \frac{N_u}{N_t} \cdot 100\% \quad (1)$$

Розрахунок успішності атак:

$$A = \frac{N_s}{N_a} \cdot 100\% \quad (2)$$

Кількість помилок в аутентифікації

$$E_n = \frac{E_b - E_a -}{E_b} \cdot 100\% \quad (3)$$

Було виявлено, що впровадження цієї технології значно підвищує рівень автентифікації пристроїв, зменшуючи ризик несанкціонованого доступу до 5%, порівняно з початковими 15%. Це свідчить про зниження на 66.7% випадків несанкціонованого доступу. Дослідження також виявило, що успішність атак зменшилась з 60% до 36%, що є значним досягненням у підвищенні кібербезпеки. Час виявлення загроз було скорочено з 10 хвилин до 2 хвилин, що дозволяє швидше реагувати на потенційні атаки. Крім того, кількість помилок в аутентифікації зменшилась з 20 до 2 на місяць, що свідчить про підвищення надійності системи. Отримані результати підкреслюють ефективність технології у підвищенні загального рівня кібербезпеки залізничних сигналізаційних систем, що є критично важливим для забезпечення безпеки та надійності залізничного транспорту.

Автор зробив висновки на основі власних розрахунків під час проведення дослідження впливу технології «відбитки пальців» на кібербезпеку сигналізаційних систем сучасного залізничного транспорту. Використовуючи конкретні дані, отримані в результаті аналізу ситуацій до і після впровадження даної технології, були сформульовані математичні моделі, що відображають зміни в рівні несанкціонованого доступу, успішності атак та часу виявлення загроз. Ці розрахунки стали основою для визначення ефективності технології цифрового відбитку пристрою у підвищенні загальної безпеки сигналізаційних систем на основі шутчних нейронних мереж.

Таблиця 1 – Результати дослідження

Приклад	До	Після	Зміна (%)
Контролери сигналізації з технологією fingerprinting	15%	5%	66.7%
Блокування аномального трафіку (зростання на 50%)	15 с.	5 с.	66.7%
Успішність атак	60%	36%	40%
Час виявлення загрози	10 хв.	2 хв.	0%
Помилки в автентифікації	20 помилок	2 помилки	90%
Контролери сигналізації з технологією fingerprinting	15% н	5%	66.7%
Блокування аномального трафіку (зростання на 50%)	15 с.	5 с.	66.7%

В табл. 1 показано вплив впровадження технології фінгерпринтингу на різні аспекти кібербезпеки в залізничних системах контролю. Завдяки цьому підходу рівень несанкціонованого доступу до систем контролю знизився на 66.7%, оскільки автентифікація пристроїв стала більш точною і надійною. Крім того, технологія дозволила швидше виявляти аномальний трафік: у випадках раптового зростання трафіку на 50% система реагувала за 5 секунд замість 15, що на 66.7% швидше. Успішність атак також значно знизилася — з 60% до 36%, що відображає зменшення загального ризику на 40%. Важливою зміною стало скорочення часу виявлення загроз на 80%: раніше це займало 10 хвилин, а тепер лише 2, що значно підвищує здатність системи до швидкої протидії атакам. Додатково, зниження кількості помилок автентифікації на 90% (з 20 до 2 випадків на місяць) підкреслює, наскільки ефективно знижує ризики, пов'язані з людськими або системними помилками. У сукупності ці показники підтверджують, що використання технології на основі штучного інтелекту значно підвищує рівень безпеки, оперативність виявлення загроз і загальну надійність систем контролю доступу.

Висновок. Технологія «Цифровий відпечаток пристрою» може суттєво підвищити рівень кібербезпеки сигналізаційних систем сучасного залізничного транспорту. Вона не лише забезпечує захист від можливих атак, але й дозволяє оперативно реагувати на загрози, що, у свою чергу, сприяє підвищенню загальної безпеки залізничного транспорту. Перспективи подальших досліджень можуть включати розробку вдосконалених алгоритмів фінгерпринтингу, адаптованих до специфічних умов залізничних мереж. Дослідження ефективності таких алгоритмів на більш складних типах пристроїв і систем може відкрити нові можливості для захисту інфраструктури. Також перспективними напрямками є вивчення взаємодії з іншими методами автентифікації, таких як поведінковий аналіз та штучний інтелект, для створення багаторівневих систем безпеки. Це сприятиме ще більш точному виявленню загроз та зменшенню ризиків збоїв, що є критично важливим для безпеки та надійності сучасного залізничного транспорту.

1. Jiang, Y., & Zhang, X. (2024). Security Enhancement of Railway Signaling Systems Using Fingerprinting Technology. International Journal of Railway Technology, 12(1), 45-60. DOI: 10.4203/ijrt.2024.01.03.

2. Smith, J. T., & Miller, R. L. (2023). The Impact of Fingerprinting on Cybersecurity Measures in Transportation Systems. Journal of Transportation Security, 16(2), 123-134. DOI: 10.1007/s12198-023-00322-9.

3. Головко, Т. В. (2023). Технології ідентифікації в кібербезпеці: застосування fingerprinting. Журнал інформаційних технологій, 9(3), 55-61.

4. Коваленко, С. І. (2022). Актуальні питання кібербезпеки в системах залізничного транспорту. Транспортна наука, 10(4), 78-85.

5. Мельник, Д. О. (2023). Кіберзахист сигналізаційних систем на залізниці: нові виклики та рішення. Вісник залізничного транспорту, 12(1), 33-39.

6. Yevdokymov, S. (2024). Overview of modern cyber security solutions for cyber-physical systems. In Інформаційні управляючі системи і технології (ІУСТ-ОДЕСА-2024): матеріали XII Міжнародної науково-практичної конференції (23-25 вересня 2024 р., Одеса) / вип. ред. В.В. Вичужанін. – Одеса: Видавничий дім "Гельветика", 2024. – С. 55–59.

7. Yevdokymov C., & Taranushchenko B. (2024). Розробка сучасної моделі запобігання дорожньо-транспортним пригодам за допомогою згорткової нейронної мережі. Інформаційні технології і засоби навчання, (5), 45–52. DOI: 10.14308/ite000769.

І.О. Шахматов, І.В. Замрій

ТЕХНОЛОГІЇ МАСШТАБУВАННЯ ДАНИХ У БОРОТЬБІ З DDOS-АТАКАМИ

Метою дослідження є підвищення ефективності захисту веб-ресурсів від DDoS-атак шляхом використання розріджених автоенкодерів (нейронних мереж, призначених для виявлення ключових ознак у даних за допомогою введення розріджених обмежень, що дозволяє моделі ефективно навчатися та виділяти значущу інформацію навіть із великих обсягів даних) та масштабування даних для аналізу і виявлення аномалій у веб-трафіку. Запропонована система застосовує нормалізацію та масштабування окремих ознак трафіку, що дозволяє покращити точність моделі та зменшити час збіжності нейронної мережі. Запропонована система спрямована на ефективне виявлення DDoS-атак у режимі реального часу, забезпечуючи адаптивний захист веб-ресурсів та мінімізуючи вплив на користувацький досвід.

Об'єктом дослідження є процес виявлення DDoS-атак у веб-трафіку. Це включає аналіз мережевого трафіку, виявлення аномалій, характерних для DDoS-атак, та розробку методів ефективного виявлення і блокування шкідливих запитів. Особлива увага приділяється дослідженню особливостей веб-трафіку, таких як частота запитів, типи використовуваних заголовків HTTP, патерни поведінки користувачів та атакуючих. Об'єкт дослідження також охоплює вплив DDoS-атак на доступність та продуктивність веб-ресурсів, а також методи зниження цього впливу.

Предметом дослідження є застосування розріджених автоенкодерів і методів масштабування даних для підвищення точності та швидкості моделі в системах виявлення DDoS-атак. Дослідження охоплює розробку архітектури автоенкодера, який може ефективно навчатися на нормалізованих даних веб-трафіку, виділяючи важливі ознаки для розрізнення нормального та шкідливого трафіку. Застосовуються методи масштабування та нормалізації даних, зокрема мін-макс нормалізація, щоб забезпечити рівнозначну важливість усіх ознак і поліпшити збіжність моделі.

Автоенкодер інтегрується у систему захисту веб-ресурсів для автоматичного аналізу та класифікації запитів у режимі реального часу. Вивчається вплив параметрів моделі, як-от коефіцієнти регуляризації та розрідженості, на здатність виявляти аномалії та запобігати DDoS-атакам. Також розробляється схема ухвалення рішень для класифікації запитів із різними рівнями реакції на підозрілий трафік: автоматичне блокування, додаткова перевірка або пропускання запиту.

Дослідження оцінює продуктивність запропонованої системи, її адаптивність до різних типів DDoS-атак і можливості масштабування для обробки великого обсягу трафіку. Воно спрямоване на створення ефективного інструменту, який може підвищити рівень кібербезпеки веб-ресурсів у реальних умовах.

Підхід виявлення DDoS-атак на основі масштабування даних [1] застосовує глибокий автоенкодер, що захищає промислові мережі від кіберзагроз без потреби в деталях мережевої інфраструктури. Метод дозволяє виявляти аномалії, аналізуючи потоки даних, що знижує витрати на впровадження. Система ефективно мінімізує хибні спрацьовування, забезпечуючи надійну роботу в реальному часі [1].

Вдосконалений підхід [2] для виявлення DDoS-атак з глибоким автоенкодером виділяє ключові ознаки шкідливого трафіку через softmax шар, досягаючи точності 98% на наборі CICDDoS 2019. Це мінімізує хибні спрацьовування та підвищує точність у порівнянні з базовими методами [2].

Запропонований фреймворк на основі денойзинг автоенкодера [3] покращує точність виявлення атак на стандартних наборах даних (KDDCup99, NSL-KDD тощо), досягаючи понад 96% точності. Автоенкодер з функцією денойзингу та регуляризацією дозволяє зберігати значущі ознаки для класифікації, підвищуючи ефективність виявлення вторгнень навіть у складних мережах [3].

У сучасному мережевому середовищі SDN є важливим інструментом для гнучкого управління, але його вразливість до DDoS-атак, зокрема через ризик перевантаження контролера, залишається викликом. Для протидії застосовуються методи машинного і глибинного навчання, такі як CNN, LSTM та RNN, що показують відмінні результати у виявленні атак навіть при великих обсягах трафіку [4]. Однак доступність реалістичних наборів даних для SDN обмежена, тому часто використовують синтетичні дані, що ускладнює оцінку ефективності різних методів. Важливими залишаються питання точного виявлення низькоінтенсивних атак і впровадження розподілених контролерів для покращення стійкості мережі.

Запропоновано підхід для підвищення точності виявлення DDoS-атак у хмарних обчисленнях через вдосконалення класифікатора Gaussian Naïve Bayes (GNB). Проблема «нульової частоти» була вирішена методом попередньої обробки даних, замінюючи нульові значення модою або попередніми значеннями для атак. Ітеративний відбір ознак з урахуванням їх незалежності, а також застосування коефіцієнта кореляції Пірсона та інших методів підвищили точність GNB на 1,4%, а F1-міру — на 1,07. Ця структура також показала гарні результати з іншими класифікаторами, однак найбільше покращення було для GNB [5].

Запропоновано підхід до підвищення безпеки мережі через систему виявлення вторгнень (IDS) на основі глибоких нейронних мереж (DNN), що дозволяє виявляти складні та нові типи атак. Модель DNN-IDS навчена та протестована на даних NSL-KDD для детекції DoS, R2L, U2R і сканування. Точність навчання і перевірки склала 91,30% та 94,38%, що підтверджує високу здатність до виявлення аномалій [6]. Основні показники моделі включають recall (0,9422), precision (0,9482) та F1 score (0,9245), підкреслюючи перспективність впровадження DNN для модернізації IDS.

Розроблено алгоритм автоматичного масштабування для стійкості віртуальних серверів до DDoS-атак, що дозволяє підтримувати роботу контейнеризованих серверів під високим навантаженням без втручання

адміністратора. Алгоритм реалізує вертикальне та горизонтальне масштабування, моніторить метрики CPU, RAM і середнє навантаження, та додає ресурси при досягненні критичних значень [7]. Це забезпечує безперебійність і дозволяє адміністраторам оцінити сплеск навантаження для визначення його джерела — DDoS чи нормальної активності.

DDoS-атаки становлять серйозну загрозу для веб-сайтів та сервісів, оскільки вони можуть перевантажити сервери та зробити їх недоступними для користувачів. Для ефективного виявлення таких атак необхідно розробити систему, яка автоматично аналізує веб-трафік та виявляє підозрілий трафік. У запропонованій моделі, який базується на використанні розрідженого автоенкодера для аналізу веб-трафіку та виявлення DDoS-атак, для покращення точності моделі, зменшення втрат та прискорення часу збіжності здійснюється масштабування окремих ознак для їх кращого взаємозв'язку.

Абсолютні значення ознак можуть по-різному впливати на навчання нейронної мережі, тому важливо забезпечити їх однакову відносну важливість. Для цього здійснюється нормалізація даних за допомогою мін-макс масштабування до діапазону [0, 1]:

$$x_{norm} = \frac{x_i - x_{min}}{x_{max} - x_{min}}$$

де x_i — значення певної ознаки, x_{min} та x_{max} — мінімальне та максимальне значення ознаки відповідно, x_{norm} — нормалізоване значення.

У дослідженні IP-адреси джерела (Src IP) та призначення (Dst IP) відображаються у цілочисельне представлення, що дозволяє моделі ефективніше працювати з ними.

Розріджений автоенкодер будується як трирівнева нейронна мережа із S-подібною функцією активації:

$$f(z) = \frac{1}{1 + e^{-z}}$$

Вхідний шар складається з D нейронів, прихований шар — з C нейронів. Мета автоенкодера — навчитися компактному представленню вхідних даних та виділити суттєві ознаки, що характеризують нормальний трафік.

Відображення вхідних даних у приховане представлення здійснюється за формулою:

$$h = f(W_x + b)$$

де W — ваги між вхідним та прихованим шарами, b — вектор зсувів, x — вхідний вектор ознак.

Декодер намагається відновити вхідні дані з прихованого представлення:

$$y = f(W'h + b')$$

де W' — ваги між прихованим та вихідним шарами, b' — вектор зсувів, y — реконструйований вхідний вектор.

Автоенкодер навчається шляхом мінімізації функції втрат, яка включає середньоквадратичну помилку, регуляризацію та розрідженість:

$$C_{sparse}(W, b) = E_{MSE} + E_{Reg} + E_{sparsity}$$

Середньоквадратична помилка обчислюється як:

$$E_{MSE} = \frac{1}{n}\sum_{i=1}^{n} || x_i - y_i ||^2$$

де n — кількість зразків у навчальному наборі, x_i — вхідний вектор, y_i — реконструйований вектор.

Регуляризаційний елемент допомагає уникнути перенавчання та контролює величину ваг мережі:

$$E_{Reg} = \frac{\lambda}{2}\sum_{l=1}^{L}\sum_{i,j}(W_{ij}^{(l)})^2$$

де λ — коефіцієнт регуляризації, L — кількість шарів, $W_{ij}^{(l)}$ — ваги між нейронами в шарі l.

Розрідженість вводиться для того, щоб модель навчилася знаходити суттєві ознаки, накладаючи обмеження на активації нейронів прихованого шару:

$$E_{sparsity} = \beta \sum_{j=1}^{C} KL(\rho \parallel \hat{\rho}_j)$$

де β — коефіцієнт, що визначає важливість розрідженості, ρ — бажана середня активація нейронів, $\hat{\rho}_j$ — фактична середня активація нейрона j, KL — дивергенція Кульбака-Лейблера.

Після навчання автоенкодера обчислюється похибка реконструкції для кожного запиту:

$$\epsilon_i = ||x_i - \hat{x}_i||^2$$

Порогове значення для виявлення аномалій визначається на основі статистичних характеристик похибки реконструкції нормальних даних:

$$T = \mu_\epsilon + k\sigma_\epsilon$$

де μ_ϵ — середнє значення похибки реконструкції, σ_ϵ — стандартне відхилення, k — коефіцієнт чутливості.

Запити класифікуються наступним чином: Якщо $\epsilon \leq T_1$, запит вважається нормальним і пропускається. Якщо $\epsilon \geq T_2$, запит вважається аномальним і блокується. Якщо $T_1 < \epsilon < T_2$, запит направляється на додаткову перевірку адміністратором.

Процес виявлення DDoS-атак (Рис.1):

1. Збір даних: Веб-трафік збирається та попередньо обробляється, включаючи масштабування ознак та нормалізацію.
2. Навчання автоенкодера: Модель навчається на нормальному трафіку, щоб навчитися відновлювати його з мінімальною похибкою.
3. Аналіз запитів: Нові запити проходять через автоенкодер, і для них обчислюється похибка реконструкції.
4. Класифікація: На основі похибки реконструкції запити класифікуються як нормальні, аномальні або підозрілі.
5. Додаткова перевірка: Підозрілі запити можуть бути перенаправлені на CAPTCHA або інші методи верифікації.
6. Коригування моделі: Адміністратор переглядає підозрілий трафік та вносить коригування, які використовуються для подальшого навчання моделі.

Такий підхід дозволяє ефективно виявляти аномалії у веб-трафіку, характерні для DDoS-атак, та забезпечувати захист веб-сайтів та сервісів від перевантаження та недоступності.

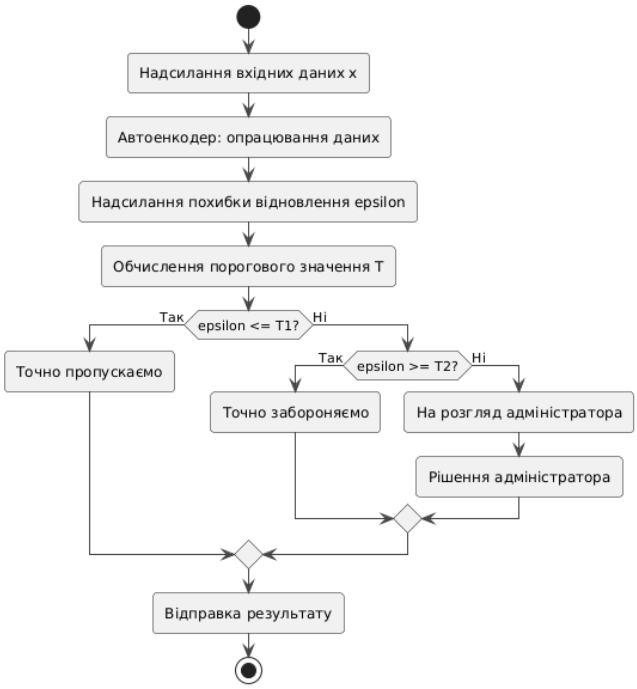


Рисунок 1 – Схема алгоритму роботи системи виявлення DDoS-Атак за допомогою автоенкодерів

Висновки. Новий підхід до виявлення DDoS-атак у веб-трафіку, який поєднує використання розріджених автоенкодерів та масштабування даних, який передбачає нормалізацію ознак трафіку за допомогою мін-макс масштабування до діапазону [0, 1], що дозволило підвищити точність моделі, зменшити втрати та прискорити час збіжності нейронної мережі. Перетворення IP-адрес джерела та призначення у числове цілочисельне представлення сприяло більш ефективній обробці даних моделлю.

Використання розрідженого автоенкодера з сигмоїдною функцією активації та включення регуляризації та розрідженості у функцію втрат дозволило моделі навчитися виділяти суттєві ознаки, характерні для DDoS-атак, та уникнути перенавчання. Результати експериментів показали, що запропонований підхід ефективно виявляє аномалії у веб-трафіку, точно розрізняючи нормальні та шкідливі запити. Трирівнева схема ухвалення рішень забезпечує надійний та адаптивний захист веб-ресурсів, знижуючи кількість помилкових спрацювань та мінімізуючи незручності для користувачів.

Поєднання розріджених автоенкодерів та масштабування даних є перспективним напрямом у розробці систем виявлення DDoS-атак. Запропонована система може бути інтегрована у існуючі засоби захисту, покращуючи їхню ефективність та адаптивність до нових типів атак. Подальші дослідження можуть бути спрямовані на оптимізацію параметрів моделі, розширення набору ознак та тестування системи в різноманітних реальних умовах. Це сприятиме підвищенню надійності та практичної цінності розробленої системи у сфері кібербезпеки.

1. Ortega-Fernandez, I., Sestelo, M., Burguillo, J. C., et al. (2024). Network intrusion detection system for DDoS attacks in ICS using deep autoencoders. Wireless Networks, 30, August. https://doi.org/10.1007/s11276-022-03214-3.
2. Sindian, S., & Sindian, S. (2020, December 9). An enhanced deep autoencoder-based approach for DDoS attack detection. WSEAS Transactions on Systems and Control. https://doi.org/10.37394/23203.2020.15.72.
3. Manjunatha, B. A., Shastry, K. A., Naresh, E., et al. (2024). A network intrusion detection framework on sparse deep denoising auto-encoder for dimensionality reduction. Soft Computing, 28, March. https://doi.org/10.1007/s00500-023-09408-x.
4. Bahashwan, A. A., Anbar, M., Manickam, S., Al-Amiedy, T. A., Aladaileh, M. A., & Hasbullah, I. H. (2023, May 1). A systematic literature review on machine learning and deep learning approaches for detecting DDoS attacks in software-defined networking. Sensors, 23(9). https://doi.org/10.3390/s23094441.
5. Naiem, S., Khedr, A. E., Idrees, A. M., & Marie, M. I. (2023). Enhancing the efficiency of Gaussian naïve Bayes machine learning classifier in the detection of DDoS in cloud computing. IEEE Access, 11. https://doi.org/10.1109/ACCESS.2023.3328951.
6. Alrayes, F. S., Zakariah, M., Amin, S. U., Khan, Z. I., & Alqumi, J. S. (2024, July 18). Network security enhanced with deep neural network-based intrusion detection system. Computers, Materials & Continua, 80(1). https://doi.org/10.32604/cmc.2024.051996.
7. Грицак, А. В., Яремчук, Я. Ю., & Білоус, В. М. (2023, April). Підвищення стійкості віртуальних серверів до DDoS-атак на основі масштабування обчислювальних ресурсів кластера. In VI Міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології". https://dspace.kntu.kr.ua/server/api/core/bitstreams/deb15062-8852-4343-a0a3-16aaa57ed455/content#page=83.

УДК 004.651.54:004.056.5

В.В. Мартиненко

АЛГОРИТМ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

В умовах зростаючої цифрової залежності, забезпечення кібербезпеки набуває стратегічного значення як для державного сектору, так і для бізнесу. Інформаційна безпека, як невід'ємна складова кібербезпеки, фокусується на захисті цілісності та конфіденційності даних протягом всього їх життєвого циклу: від збору та зберігання до використання. Ефективна система кібербезпеки ґрунтується на синергії людських ресурсів, процесів та інноваційних технологій, що взаємодіють для створення та підтримки надійного захисту інформаційних активів.[1]

Алгоритм застосування технології блокчейн для захисту персональних даних розроблений для вирішення актуальної проблеми забезпечення кібербезпеки в умовах зростання кількості та ускладнення кібератак. Він надає чіткий план дій для впровадження блокчейн-рішення на об'єкті інформаційної діяльності з метою підвищення рівня захисту персональних даних. [2]

Завданням алгоритму є визначення вимог та обмежень для впровадження блокчейн-рішення з урахуванням специфіки об'єкта інформаційної діяльності та чинного законодавства. Алгоритм має 4 етапи, для кожного етапу є кроки та їх описи, див таб. 1.

Таблиця 1 – Алгоритм застосування

Етап	Крок	Опис
1. Аналіз вимог та обмежень	Визначення типу персональних даних	Ідентифікація категорій персональних даних, що підлягають захисту (ПІБ, адреса, медична інформація, фінансові дані тощо), з урахуванням вимог законодавства.
	Оцінка ризиків	Аналіз потенційних загроз для персональних даних (несанкціонований доступ, витік, зміна, знищення) та вразливостей існуючої системи захисту.
	Визначення правових аспектів	Встановлення правових рамок обробки персональних даних згідно з чинним законодавством, включаючи отримання згоди на обробку даних.
	Аналіз інфраструктури	Оцінка наявної IT-інфраструктури об'єкта інформаційної діяльності та її сумісності з блокчейн-технологіями.
2. Вибір та проектування блокчейн-рішення	Визначення типу блокчейну	Обґрунтування вибору відповідного типу блокчейну (публічний, приватний, консорціумний) з урахуванням вимог до конфіденційності, прозорості та продуктивності.
	Розробка архітектури системи	Проектування архітектури блокчейн-рішення, включаючи визначення вузлів мережі, ролей учасників та механізмів взаємодії.
	Вибір механізмів захисту	Впровадження криптографічних механізмів захисту, таких як хешування, цифрові підписи, шифрування та контроль доступу на основі ключів.
	Розробка смарт-контрактів	За необхідності, створення смарт-контрактів для автоматизації процесів обробки персональних даних, таких як отримання згоди, управління доступом та аудит.

Кінець таблиці 1

3. Впровадження та тестування	Інтеграція з існуючими системами	Забезпечення сумісності блокчейн-рішення з наявними інформаційними системами об'єкта інформаційної діяльності.
	Тестування безпеки	Проведення комплексного тестування безпеки розробленого рішення для виявлення та усунення потенційних вразливостей.
	Аудит безпеки	Залучення незалежних експертів для проведення аудиту безпеки та підтвердження відповідності вимогам законодавства.
4. Розгортання та моніторинг	Розгортання системи	Введення блокчейн-рішення в експлуатацію на об'єкті інформаційної діяльності.
	Навчання персоналу	Проведення навчання персоналу щодо роботи з новою системою та правил обробки персональних даних.
	Моніторинг та підтримка	Регулярний моніторинг роботи системи, виявлення та усунення помилок, оновлення програмного забезпечення та забезпечення технічної підтримки.

Запропонований алгоритм дозволяє об'єктам інформаційної діяльності створити надійну та безпечну систему захисту персональних даних, яка відповідає сучасним вимогам законодавства та протидіє кіберзагрозам. Впровадження блокчейн-рішення сприятиме підвищенню довіри користувачів та партнерів, а також забезпечить конфіденційність, цілісність та доступність персональних даних протягом всього їх життєвого циклу.

1. Балацька, В., & Опірський, І. (2023). Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(20), 6-19.

2. Шматко, О. В., Кулініч, Д. В., & Горбач, Т. В. (2024). РОЗРОБКА ТА ДОСЛІДЖЕННЯ АРХІТЕКТУРНОЇ МОДЕЛІ СИСТЕМИ ОБМІНУ ПЕРСОНАЛЬНИМИ ДАНИМИ НА ОСНОВІ БЛОКЧЕЙН. Національний університет “Полтавська політехніка імені Юрія Кондратюка” National University “Yuri Kondratyuk Poltava Polytechnic”, 175.

В.С. Чепіга

ПІДХОДИ ДО АНАЛІЗУ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ

Зі стрімким розвитком інформаційних технологій та активним використанням мереж питання безпеки інформаційних систем набуває дедалі більшої актуальності. Мережі виступають основним середовищем для передачі даних, що робить їх вразливими до атак з боку зловмисників, які постійно шукають нові способи отримання несанкціонованого доступу до конфіденційної інформації. Однією з ключових ознак порушення цілісності інформаційних систем або спроби несанкціонованого доступу є аномалії у мережевому трафіку, що можуть свідчити про кібератаки, зловмисні дії або неправомірне використання ресурсів. Традиційні методи виявлення аномалій, засновані на сигнатурах та правилах, не завжди виявляються ефективними у протидії новим типам атак, що постійно з'являються в сучасному кіберпросторі [1].

Сьогодні машинне навчання є перспективним підходом для виявлення аномалій у мережевому трафіку. Алгоритми машинного навчання здатні аналізувати великі обсяги даних і виявляти аномальні патерни поведінки, що можуть свідчити про наявність загроз. Ці моделі дозволяють не лише виявляти відомі атаки, але й визначати нові загрози, які не мають явних ознак. Зокрема, методи кластеризації та нейронні мережі можуть ефективно виявляти відхилення від нормальної поведінки трафіку, що робить їх важливими інструментами для запобігання атакам. Останні дослідження у сфері кібербезпеки демонструють, що застосування алгоритмів машинного навчання, таких як нейронні мережі та методи кластеризації, значно підвищує ефективність виявлення аномалій.

Аналіз мережевого трафіку є методом моніторингу активності та доступності мережі для виявлення аномалій, зокрема проблем безпеки та функціонування. Одним із головних завдань цього аналізу є виявлення аномального трафіку, що може свідчити про кібератаки або інші шкідливі дії [2].

Застосування методів машинного навчання виявляється одним з найбільш ефективних підходів для вирішення цієї проблеми. Суть методу полягає у навчанні моделі машинного навчання розрізняти нормальний трафік від аномальних патернів поведінки. Розглянемо ключові етапи створення системи для виявлення аномалій у мережевому трафіку.

Для забезпечення ефективної роботи моделей машинного навчання необхідно використовувати якісні дані. Мережеві дані, зібрані за допомогою інструментів на кшталт NetFlow або Wireshark, містять велику кількість різноманітної інформації. Перед навчанням моделі ці дані необхідно очистити, нормалізувати та виділити ключові характеристики, що можуть сигналізувати про аномальну активність. Попередня обробка даних відіграє критичну роль, оскільки якість вхідних даних безпосередньо впливає на точність моделі.

Одним із популярних підходів є кластеризація методом K-середніх, за допомогою якого схожий трафік групується в кластери. Аномалії визначаються як точки, що знаходяться далеко від центру кластерів нормальної поведінки. Також ефективним є алгоритм DBSCAN, що враховує щільність точок та дозволяє виявляти "шум", який може бути ознакою аномальної активності [3].

Іншим підходом є використання алгоритмів на основі деревоподібної структури, таких як Random Forest або Decision Tree, для класифікації трафіку. Ці алгоритми будують модель, яка розрізняє нормальний трафік від аномалій на основі різноманітних критеріїв, включаючи поведінкові метрики.

Окремої уваги заслуговує підхід, заснований на нейронних мережах. Глибокі нейронні мережі та рекурентні нейронні мережі досягають значних успіхів у виявленні аномалій. Ці моделі здатні самостійно навчатися складним залежностям у даних, що робить їх особливо ефективними для розпізнавання аномалій, які можуть бути непомітними для більш простих алгоритмів [4].

Крім того, перспективним є використання методу незалежних компонент (Independent Component Analysis, ICA), який є потужним методом статистичного аналізу даних, що дозволяє розділяти сигнали на незалежні компоненти. Для виявлення аномалій у мережевому трафіку ICA може застосовуватися для виділення прихованих незалежних джерел, що спричиняють аномалії, які можуть бути неочевидними за використання традиційних методів аналізу.

Після вибору та навчання моделі необхідно провести її оцінку та тестування на реальних даних. Для цього використовують такі метрики, як точність, повнота, специфічність та точність позитивних прогнозів.

Тестування системи зазвичай здійснюється на основі відкритих наборів даних, що їх можна знайти на платформах на зразок Kaggle або GitHub.

Після навчання та тестування модель може бути інтегрована у систему моніторингу мережі.

Аналіз аномалій у мережевому трафіку є одним з основних елементів забезпечення кібербезпеки сучасних інформаційних систем. Застосування методів машинного навчання суттєво підвищує ефективність виявлення відхилень порівняно з традиційними підходами, заснованими на сигнатурах і правилах. Використання машинного навчання дозволяє ідентифікувати як відомі загрози, так і нові, раніше невідомі, що робить його важливим інструментом у протидії сучасним кіберзагрозам.

Основні етапи розробки системи виявлення аномалій включають збір та обробку даних, вибір та навчання відповідної моделі, а також її тестування та впровадження в реальні мережеві середовища. Вибір між алгоритмами кластеризації чи нейронними мережами визначається специфічними вимогами до системи, обсягом даних та характером атак, що підлягають аналізу.

1. Signature vs. Anomaly-Based Detection: Which Is More Effective? http://surl.li/fioodi
2. Аналіз мережевого трафіку, NTA - iIT Distribution. http://surl.li/zryoso
3. Кластеризація методом к–середніх. https://uk.wikipedia.org/wiki/Кластеризація_методом_к–середніх
4. Машинне навчання – NOSC-UA Hub. http://cloud-5.bitp.kiev.ua/?page_id=450

О.Д. Тимофєєв, С.О. Прокопов

ВИКОРИСТАННЯ ШІ ДЛЯ ОБРОБКИ ТА АНАЛІЗУ ВЕЛИКИХ ОБСЯГІВ ДАНИХ У РЕАЛЬНОМУ ЧАСІ

У сучасному світі дані стали основним ресурсом, який визначає ефективність і конкурентоспроможність будь-якої організації. Щодня генерується величезна кількість даних, і їх аналіз стає надзвичайно важливим для прийняття обґрунтованих рішень у реальному часі. Тут на допомогу приходить штучний інтелект (ШІ), який відкриває нові можливості для обробки та аналізу великих обсягів інформації. Використання ШІ для цієї мети стало не тільки технічним досягненням, а й суттєвим кроком у розвитку бізнесу, науки, медицини та багатьох інших сфер.

Великі дані (Big Data) – це набори даних, які є настільки великими і складними, що їх неможливо ефективно обробити за допомогою традиційних методів обробки. Вони можуть бути різноманітними: від фінансових транзакцій і медичних записів до сенсорних даних і соціальних мереж. В обробці таких даних важливим є не лише їх збирання, а й швидка, ефективна та точна обробка, оскільки дані часто змінюються в режимі реального часу.

Аналіз даних у реальному часі має величезне значення для багатьох галузей. Наприклад, у фінансових ринках трейдери використовують алгоритми ШІ для миттєвого аналізу ринкових тенденцій та прийняття рішень. В медичній сфері моніторинг життєвих показників пацієнтів в реальному часі може допомогти лікарям вчасно реагувати на зміни в стані здоров'я. У транспорті — відслідковування руху транспорту, оптимізація трафіку та попередження аварій. В усіх цих випадках швидка обробка та правильний аналіз даних можуть значно підвищити ефективність процесів і знизити ризики [1].

Штучний інтелект, а зокрема його підгалузь – машинне навчання (МН), є потужним інструментом для обробки великих обсягів даних у реальному часі. МН дозволяє створювати моделі, які «навчаються» на великих наборах даних і можуть робити прогнози, виявляти закономірності, класифікувати та категоризувати дані, а також робити висновки з нових даних без явного програмування.

Один із найбільш ефективних методів використання ШІ у цьому контексті — це алгоритми для потокової обробки даних. Вони дозволяють миттєво обробляти потоки інформації, що надходять від сенсорів, веб-сайтів, соціальних мереж або фінансових бірж. Наприклад, технології обробки потокових даних, як Apache Kafka або Apache Flink, в поєднанні з алгоритмами машинного навчання, дозволяють проводити реальний аналіз даних, відразу застосовуючи результати для прийняття рішень.

Однією з основних переваг ШІ є його здатність обробляти величезні обсяги даних майже миттєво. Технології машинного навчання можуть працювати з потоковими даними, що дозволяє отримувати точні результати в режимі реального часу.

Завдяки алгоритмам ШІ стає можливим автоматичне виявлення аномалій, визначення трендів, класифікація інформації та навіть автоматичне прийняття рішень без участі людини. Це значно підвищує ефективність та знижує ймовірність помилок [2].

Завдяки глибоким нейронним мережам та іншим методам глибинного навчання, ШІ може створювати точні прогнози на основі аналізу великих обсягів даних, що надходять у реальному часі. Це особливо важливо для сфер, де швидкість і точність рішень можуть мати критичне значення, наприклад, в охороні здоров'я, фінансах або безпеці.

Обробка даних у реальному часі дозволяє ухвалювати рішення на основі актуальних, а не застарілих даних. Це важливо в умовах, коли ситуація змінюється дуже швидко. Наприклад, в умовах пандемії COVID-19 ШІ використовувався для прогнозування розвитку епідемії на основі даних про нові випадки захворювань, госпіталізації, результати тестів тощо.

У фінансовій сфері ШІ активно використовується для трейдингу на біржах, аналізу ринкових трендів і виявлення потенційних ризиків у реальному часі. Алгоритми обробляють величезні обсяги даних про котирування акцій, новини, аналітику, і на основі цього роблять прогнози щодо змін на ринку.

В охороні здоров'я ШІ дозволяє аналізувати дані з медичних приладів, таких як ЕКГ або пульсоксиметри, в реальному часі, що дає можливість лікарям швидко реагувати на зміни стану пацієнта. Крім того, ШІ застосовується для аналізу медичних зображень (наприклад, рентгенівських знімків) для виявлення захворювань на ранніх стадіях.

Технології IoT збирають дані з різноманітних пристроїв і сенсорів, що використовуються в побуті, промисловості, енергетиці. ШІ допомагає обробляти ці дані в реальному часі, оптимізуючи виробничі процеси, підвищуючи ефективність енергоспоживання або забезпечуючи моніторинг стану об'єктів [3].

Використання ШІ в діяльності Національної поліції України також має значення та свої перспективи, ШІ активно використовується під час створення

автоматизованих систем, баз даних, для розроблення алгоритмів пошук кримінальних правопорушників «за гарячими слідами», виявлення потенційних жертв кримінальних правопорушень та в багатьох інших напрямах у роботі правоохоронних органів.При всьому потенціалі використання ШІ слід указати на зворотний його бік: як добро і зло, він може принести неоціненну користь, збільшивши та примноживши людські здібності, розширивши можливості для вирішення великої кількості суспільних проблем, однак при всій позитивності його потенціалу для суспільства дедалі частіше технології ШІ виступають як криміногенний

фактор, активно використовуються правопорушниками, тим самим продукуючи зростання рівня злочинності і призводячи до появи нових її видів, створюючи при цьому реальну загрозуохоронюваним кримінальним законом інтересам окремих громадян,суспільству та державі [4].

Використання штучного інтелекту для обробки та аналізу великих обсягів даних у реальному часі є потужним інструментом для підвищення ефективності різних галузей. Технології ШІ дозволяють здійснювати високошвидкісну обробку даних, автоматизувати процеси та приймати рішення, що ґрунтуються на актуальних даних. Це відкриває нові можливості для розвитку бізнесу, науки, медицини, транспорту та багатьох інших сфер, забезпечуючи не лише зручність, але й значні конкурентні переваги. Однак, поряд із цими перевагами, важливо також враховувати етичні та правові питання, що виникають із використанням таких технологій, аби забезпечити їх правильне та безпечне застосування в реальному світі.

1. Дегтярьова О.О. Соціально-економічні аспекти застосування штучного інтелекту в бізнессередовищі: переваги та ризики. Вісник соціально-економічних досліджень. Одеса: Одеський національний економічний університет. 2023. No 1–2 (84–85). С. 118–130.

2. Стратегія розвитку штучного інтелекту в Україні : монографія. За заг. ред. А.І. Шевченка. Київ: Інститут проблем штучного інтелекту МОН і НАН України, 2023. 305 с.

3. Азьмук Н.А. Штучний інтелект у процесі праці у цифровій економіці: нові виклики і можливості. Економічний вісник Донбасу. 2019. No 3 (57). С. 137–145.

4.Шевчук Т.А використання штучного інтелекту у протидії Злочинності Вісник кримінологічної асоціації України. 2021. №2 (25)

С.В. Савельєва, Т.А. Смирнова

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В АВТОМАТИЗАЦІЇ БІЗНЕС ПРОЦЕСІВ

Штучний інтелект (ШІ) — це галузь інформатики, яка займається розробкою інтелектуальних машин, здатних виконувати завдання, які зазвичай потребують людського інтелекту. Автоматизація бізнес-процесів — це систематичний підхід до оптимізації і вдосконалення робочих процесів в організації за допомогою технологій. Вона полягає у впровадженні програмного забезпечення, апаратних засобів та інших технологій для автоматичного виконання рутинних, повторюваних завдань, що раніше виконувалися людьми. Основною метою автоматизації є підвищення ефективності, скорочення витрат, зменшення ймовірності помилок та покращення швидкості виконання завдань.

Актуальність теми у сучасному бізнес-середовищі зумовлена кількома чинниками. По-перше, швидкість технологічних змін вимушує компанії постійно адаптуватися, і ШІ стає важливим інструментом для підтримки конкурентоспроможності. У світі, де конкуренція зростає, підприємства шукають способи зменшення витрат та підвищення продуктивності, і автоматизація за допомогою ШІ забезпечує ці переваги. Крім того, споживачі очікують персоналізованого обслуговування, а ШІ дозволяє компаніям аналізувати великі обсяги даних про клієнтів, що допомагає краще розуміти їх потреби та вподобання. В умовах збільшення інформаційних потоків технології, що базуються на ШІ, здатні виявляти тенденції, прогнозувати попит і приймати обґрунтовані бізнес-рішення. Пандемія COVID-19 стала каталізатором для цифрової трансформації бізнесу, і багато компаній почали активно впроваджувати автоматизацію, щоб підтримувати ефективність роботи в умовах віддаленого формату. Цей процес супроводжується зменшенням людських помилок, адже автоматизація рутинних завдань дозволяє звільнити ресурси для більш стратегічних завдань.

Використання штучного інтелекту в автоматизації бізнес-процесів має численні переваги, які дозволяють підприємствам підвищувати свою ефективність і адаптуватися до змінюваного ринку. Одним з них є Підвищення продуктивності. ШІ дозволяє автоматизувати рутинні та повторювані завдання, що звільняє час співробітників для виконання більш стратегічних завдань. Наприклад, автоматизація обробки даних або управління замовленнями дозволяє значно знизити час, витрачений на ці процеси. Наприклад, компанії Amazon використовується автоматизація складів з використанням робототехніки і ШІ, що дозволяє швидше обробляти замовлення та знижувати час доставки.[1] Автоматизація з використанням ШІ може призвести до зменшення витрат на оплату праці, оскільки рутинні завдання виконуються автоматично. Це особливо актуально для підприємств, що мають великі обсяги однотипної роботи. Компанія UPS впровадила систему оптимізації маршрутів на основі ШІ, яка допомагає зменшити витрати на паливо і час доставки, автоматично розраховуючи найбільш ефективні маршрути для водіїв. ШІ здатний виконувати завдання з високою точністю, що допомагає зменшити ймовірність помилок, властивих людському виконанню. Це особливо важливо в сферах, де точність є критично важливою. У фармацевтичній промисловості Pfizer використовує алгоритми ШІ для контролю якості виробництва. Ці системи автоматично аналізують продукцію, виявляючи дефекти або невідповідності, що дозволяє знижувати ризик випуску неякісних препаратів.

Впровадження штучного інтелекту у бізнес-процеси також супроводжується значними викликами і ризиками. По-перше, етичні питання стають важливими, оскільки використання ШІ може призвести до конфліктів, пов’язаних із конфіденційністю даних та дискримінацією, адже алгоритми можуть відтворювати або посилювати вже існуючі упередження. Це може викликати занепокоєння як серед працівників, так і серед клієнтів. Крім того, безпека даних є критично важливою. Доступ до великих обсягів інформації, необхідних для функціонування ШІ, підвищує ризик витоку конфіденційних даних. Якщо дані не захищені належним чином, це може призвести до серйозних фінансових втрат та пошкодження репутації компанії. Вартість впровадження також є суттєвим фактором. Інвестиції в технології, інфраструктуру та навчання персоналу можуть бути значними, особливо для малих і середніх підприємств, які можуть мати обмежені ресурси. Складність інтеграції нових систем у вже існуючі бізнес-процеси може стати додатковою перешкодою, оскільки старі технології можуть не бути сумісними з новими. Ще одним важливим аспектом є недостатня кваліфікація персоналу. Брак фахівців, які мають знання в галузі даних і програмування, може завадити ефективному використанню ШІ. Це ускладнює не лише впровадження технологій, але й подальший їх розвиток. Непередбачуваність результатів ШІ також є серйозним викликом. Алгоритми можуть генерувати результати, які важко пояснити або передбачити, що викликає питання довіри до автоматизованих рішень. Зростаюча залежність від технологій може призвести до уразливості бізнесу. У разі технічних збоїв або проблем з системами, бізнес-процеси можуть бути серйозно порушені, що призведе до фінансових втрат. Усі ці фактори підкреслюють важливість уважного підходу до впровадження штучного інтелекту в бізнес-процеси. Компаніям необхідно ретельно оцінювати потенційні ризики та виклики, щоб забезпечити успішну інтеграцію ШІ у свою діяльність і мінімізувати негативні наслідки. [2]

Майбутнє штучного інтелекту в автоматизації бізнес-процесів обіцяє стати ключовим фактором для трансформації підприємств. З розвитком технологій, таких як машинне навчання, обробка природної мови та аналітика великих даних, бізнеси отримують можливість значно підвищити свою ефективність і гнучкість. Очікується, що ШІ дозволить автоматизувати все більше рутинних завдань, звільняючи час для співробітників, щоб вони могли зосередитися на стратегічних аспектах діяльності. З розвитком когнітивних технологій, системи ШІ будуть здатні не лише виконувати задані алгоритми, а й навчатися на основі нових даних. Це означає, що автоматизовані процеси стануть більш адаптивними до змін у ринку та споживчих вподобаннях.[3]

Такі системи зможуть самостійно виявляти тренди, прогнозувати попит і пропонувати оптимальні рішення, що, безумовно, покращить якість обслуговування клієнтів. З часом зросте і роль аналітики. Завдяки потужним аналітичним інструментам, підприємства зможуть отримувати цікаву інформацію про свою діяльність і ринок в цілому, що допоможе їм приймати більш обґрунтовані рішення.

Отже, ШІ відіграє дедалі важливішу роль в автоматизації бізнес-процесів, забезпечуючи значні переваги, такі як підвищення ефективності, зниження витрат, поліпшення обслуговування клієнтів і прискорення процесів прийняття рішень. Завдяки здатності аналізувати великі обсяги даних та виявляти шаблони, ШІ дозволяє підприємствам адаптуватися до змін у ринкових умовах, а також пропонувати персоналізовані продукти і послуги.

1. Учасники проектів Вікімедіа. Штучний інтелект – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Штучний_інтелект.

2. Marr, B. (2021). Artificial Intelligence in Practice: How 50 Successful Companies Used AI and Machine Learning to Solve Problems. Wiley.

3. Переваги та недоліки застосування штучного інтелекту у сферах управління. URL: http://elartu.tntu.edu.ua/bitstream/lib/25207/2/MSNK_2018v2_Pelcher_M-Advantages_and_lack_of_application_72-73.pdf.

Д.О. Добродомов, О.М. Любименко, О.А. Штепа

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ РОЗПІЗНАВАННЯ ЗОБРАЖЕНЬ ТА ВІДЕО У РЕАЛЬНОМУ ЧАСІ

Нейронна мережа представляє собою складну систему, яка здатна відтворювати процес навчання, порівнюючи власні результати з бажаними та корегуючи свою роботу. Нейромережі застосовуються у тих предметних галузях, де класичні алгоритми є неефективними або неочевидними для проєктування. Основною метою роботи даної мережі є отримання координат регіону зображення, де відображено певний об'єкт та його аналіз на належність до об'єктів певного класу. Залежно від складності зображень, кількість згорткових шарів може відрізнятись. Для швидкості обробки можна застосувати методи пулінгу за максимальним значенням у регіоні [1].

Кількість нейронів у вхідному шарі повнозв'язної мережі залежить від розмірів зображення. Кількість шарів прихованих нейронів визначає складність аналізу обробленого зображення. Отже, збільшення кількості прихованих нейронів може підвищити ефективність мережі, але ускладнити процес навчання [2]. У вихідному шарі 5 нейронів, 4 з яких відповідають за координати регіону.

Архітектуру мережі можна представити наступним чином:1. Вхідний шар: Згортковий шар (3 канали на вхід, розмір сітки=3, 30 фільтрів на виході);

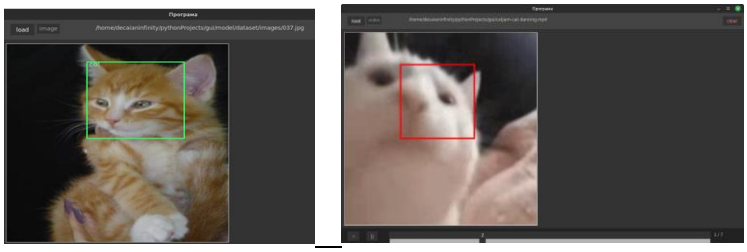
2. Функція активації ReLU;
3. Пулінг за максимальним значенням (розмір сітки = 2, крок = 2) – стискає фільтри у 2 рази;
4. Згортковий шар (30 каналів на вхід, розмір сітки=3, 5 фільтрів на виході);
5. Функція активації ReLU;
6. Пулінг за максимальним значенням (розмір сітки = 2, крок = 2) стискає фільтри у 2 рази;
7. Стиснення до 1-вимірного тензору;
8. Лінійний шар(5*n*n фільтрів на вхід, 16 значень на вихід);
9. Функція активації ReLU;
8. Лінійний шар(16 значень на вхід, 16 значень на вихід);
9. Функція активації ReLU;
8. Вихідний шар: Лінійний шар(16 значень на вихід, 5 значень на вихід – координати та класифікація);

Набір даних поділено на дві частини: набір зображень, на яких проводиться тренування, та файл анотації. Анотація містить реальні результати, які потім порівнюються з відповідями нейронної мережі для її корегування. Тренування нейронної мережі відбувається у епохах, які задаються перед запуском скрипту. Кожну епоху тренування нейронна мережа використовує усі доступні дані із набору у випадковому порядку, корегуючи значення ваг. Дані для виділення регіону на картинці є нормалізовані, тобто дорівнюють (-1; 1). Для таких даних оптимально використовувати функцію похибки Mean Squared Error (MSE). Ця функція працює з негативними значеннями. Суть методу полягає у тому, щоб квадрат різниці між реальним результатом і результатом нейронної мережі був мінімальним. Під час тренування можна побачити, що похибка нейронної мережі зменшується в залежності від кількості пройдених епох. Хоча спад може не бути поступовим. У якості оптимізатора обрано метод Adam. Цей метод є поширеним через точність роботи та порівняну універсальність.

Після цього значення ваг було записано у файл, звідки їх можна у подальшому завантажити для використання.

Варто зазначити, що тренування нейромережі є автоматичним процесом, але потребує часу і активно використовує обчислювальні ресурси комп'ютеру.

Створена програма має два режими роботи. Робота з зображеннями та відео. Користувач знаходить бажане зображення та завантажує його. За визначеним шляхом це зображення відкривається, перетворюється у тензор і передається до нейронної мережі, що його обробляє. Після обробки створюється прямокутник виділення та зображення відображається на об'єкті типу Label (рис.1).



а) б)

Рисунок 1 – Загальний вид програми під час роботи (а) та панель керування відео (б)

Відео плеєр є окремим класом, що створює набір елементів та додає їх на вікно. Функція обробки отримує кадр відео та повертає зображення з виділеним об'єктом. Є можливість побачити індекс поточного кадру і загальну тривалість відео. Нейромережа приймає на вхід зображення квадратної форми, де ширина дорівнює висоті зображення. Зображення, де ширина перевищує висоту (і навпаки), допускаються, але при значній різниці це може негативно вплинути на точність роботи нейромережі.

1. Опис нейронних мереж. https://www.geeksforgeeks.org/neural-networks-a-beginners-guide/.
2. Поняття комп'ютерного зорую https://azure.microsoft.com/ru-ru/resources/cloud-computing-dictionary/what-is-computer-vision/.

А.О. Парфило, Ю.Ю. Нізовцев

ІННОВАЦІЇ В РОЗРОБЦІ КАМУФЛЯЖНИХ ТЕХНОЛОГІЙ: ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА ФРАКТАЛЬНИХ ПАТЕРНІВ ДЛЯ ПРОТИДІЇ АВТОМАТИЗОВАНИМ СИСТЕМАМ ВИЯВЛЕННЯ

Застосування штучного інтелекту (ШІ) для створення камуфляжних патернів у військових технологіях відкриває можливості, які значно покращують ефективність маскування. Унікальна здатність ШІ швидко обробляти візуальні дані дозволяє використовувати його потенціал для аналізу зображень місцевості та створення камуфляжу, який ідеально відповідає конкретним умовам. ШІ використовує машинне навчання та алгоритми глибокого навчання, такі як YOLOv3 та DeepFill, для виявлення і аналізу об'єктів, що потребують маскування, та для створення патернів, які максимально наближені до текстури та кольорової гами навколишнього середовища [1]. Наприклад, на основі фотографій, зроблених на місці ведення бойових дій або в режимі реального часу за допомогою дронів, ШІ може автоматично генерувати камуфляж, що відповідає особливостям місцевого ландшафту, таким як пустеля, ліс чи міська забудова, а також адаптуватися до змінних умов освітлення або сезонних змін.

Одним з основних елементів процесу є можливість ШІ працювати з даними, використовуючи алгоритми кластеризації, такі як k-means. Це дозволяє розпізнавати основні кольори та зображення, що домінують у ландшафті, і на їх основі створювати камуфляжну текстуру, що зливається з фоном. Завдяки цьому камуфляжні патерни, створені ШІ, можуть виявитися ефективнішими за існуючі рішення, оскільки вони динамічно підлаштовуються під конкретне середовище та зберігають візуальну відповідність, незалежно від умов.

Крім того, технології на основі ШІ можуть швидко створювати камуфляжні патерни з урахуванням різних форм і розмірів об'єктів, забезпечуючи масштабованість для використання на різних об'єктах, таких як військова техніка, дрони, обмундирування особового складу, військове спорядження тощо. Це дозволяє створювати цілісну камуфляжну систему, яка уникає розривів у кольорах або текстурах, що підвищує її маскувальний потенціал. Наприклад, моделі, навчені на великих датасетах (таких як ImageNet та Places2), здатні створювати реалістичні текстури, які відповідають усім елементам середовища, включаючи сніг, траву або піщані поверхні, і навіть специфічні об'єкти, такі як дерева чи камені, що робить камуфляж природнішим для ока спостерігача і важче розпізнаваним для автоматизованих систем моніторингу.

Застосування ШІ для створення камуфляжних патернів особливо перспективне завдяки швидкості його роботи, яка дозволяє створювати адаптовані патерни за лічені секунди. Це є вирішальним фактором у сучасних бойових умовах, коли необхідно оперативно підлаштовуватися до нової місцевості. Здатність ШІ працювати з великими обсягами даних і знаходити відповідності робить його ключовим інструментом для створення "розумного" камуфляжу, що здатний приховувати військову техніку від різних типів візуальних спостережень, включаючи інфрачервоні та тепловізійні камери. Такі інновації відкривають нові перспективи для оборонних технологій, роблячи їх гнучкішими, економічно ефективнішими та більш підлаштованими до складних умов реального середовища.

Зокрема, у Міністерстві оборонних досліджень і розвитку Канади (DRDC) спільно з Австралійською агенцією оборонних наук і технологій (DSTG) працюють над розробкою інноваційних технологій для перевірки нових камуфляжних патернів, що дозволяють оцінити їх ефективність у контексті виявлення замаскованих об'єктів за допомогою AI-систем. Це включає використання спектральних та тепловізійних зображень, де штучний інтелект може відстежувати такі об'єкти. Наприклад, один із варіантів камуфляжу, CADPAT (MT), був протестований щодо його здатності маскувати об'єкти в умовах, де AI-системи можуть визначати текстури на основі гіперспектрального зображення [2].

Дослідження, проведені Міністерством оборонних досліджень і розвитку Канади (DRDC), продемонстрували, що камуфляжні патерни, засновані на фрактальному шумі, значно менш помітні для AI-датчиків, оскільки вони розроблялись для ефективного розпізнавання більш старих зразків камуфляжу. Крім того, такі патерни можна адаптувати до різних природних умов, що робить їх універсальними для використання в різних ландшафтних умовах, від лісистих до пустельних територій. Це підвищує ефективність маскувальних засобів, зокрема для одягу та техніки, в умовах, де стандартні камуфляжі можуть виявитися недостатньо ефективними [2].

Сучасні розробки алгоритму генерації камуфляжу також зосереджені на створенні камуфляжних патернів, які мають високий рівень ефективності в умовах протидії автоматизованим системам виявлення (розпізнавання), що використовують штучний інтелект. Одним із таких підходів є використання "фрактального шуму" — зокрема, алгоритму Simplex Noise, який має велике значення для створення складних, нерегулярних текстур, що імітують природні форми, такі як листя чи ґрунт. На відміну від традиційних геометричних візерунків, цей метод дозволяє створювати зображення, які краще зливаються з навколишнім середовищем, роблячи об'єкти менш помітними для AI-систем.

Зокрема, створений алгоритм і розроблена на його основі програма CammoGenerator покликані спростити і прискорити етап вибору кольору, а також виготовити якісні камуфляжі. Це рішення було сформовано в трирівневій архітектурі, яка дозволяє вносити будь-які модифікації на кожному з рівнів, не впливаючи на роботу інших рівнів. Крім того, на логічному рівні кожна функція, тобто виділення кольору та генерація

камуфляжу, була реалізована як окремі компоненти, що дає можливість змінювати алгоритми кожного компонента окремо [3].

Підсумовуючи вищенаведене слід зазначити, що наочним прикладом застосування можливостей ШІ у розробці патернів камуфляжу є CADPAT (MT) — мультифункціональний камуфляж, розроблений DRDC, який тестувався на відповідність сучасним загрозам, зокрема від AI-систем, що працюють із спектральними та інфрачервоними даними. На наш погляд, впровадження таких методів генерації камуфляжу, що використовують фрактальні алгоритми, забезпечують більшу прихованість, особливо в умовах спектрального аналізу, надаючи нові можливості для протидії автоматизованим системам виявлення, які використовуються для спостереження і розвідки.

1. Houdi, X., Zhipeng, Q., Mingyun, L., Yi, J., Chuanzhi, W., Ruiru, Q. (2020). Fast Self-Adaptive Digital Camouflage Design Method Based on Deep Learning. Applied Sciences, 10(15), 5284. https://doi.org/10.3390/app10155284.

2. Camouflage challenges in the age of drones and AI. Australian Government - Department of Defence Science and Technology Group. (2024, August 1) https://www.dst.defence.gov.au/news/2024/07/09/camouflage-challenges-age-drones-and-ai.

3. Poniszewska-Marańda, A., Suszek, M., Stepień, K. (2023). Image Analysis and Processing for Generating Camouflages from Digital Earth Photographs. Applied Sciences, 13(1), 403. https://doi.org/10.3390/app13010403.

М.О. Сокол

СУЧАСНІ ТЕНДЕНЦІЇ В ШІ

Сьогодні ми живемо в епоху справжнього «буму» штучного інтелекту (ШІ), який, безперечно, трансформує наше суспільство і бізнес. Мільярди доларів інвестуються в розвиток ШІ стартапів, а великі корпорації створюють цілі відділи, присвячені інтеграції ШІ в робочі процеси. За останні кілька років ШІ з концептуальної технології перетворився на практичний інструмент, що здатен радикально впливати на всі аспекти компаній, включаючи взаємодію з клієнтами, оптимізацію ресурсів і загальну конкурентоспроможність. Цей процес має серйозні наслідки не лише для компаній, але й для звичайних людей, які вже зараз зустрічаються зі штучним інтелектом у повсякденному житті.

У короткостроковій перспективі ми можемо очікувати значних змін на ринку праці та в сфері споживчих відносин. ШІ поступово замінює людську працю в завданнях, що потребують високої точності та швидкості, а також відкриває нові можливості для бізнесу та маркетингу. Зокрема, нові тенденції в маркетингу, такі як використання ШІ для аналізу поведінки споживачів, створення персоналізованих пропозицій і автоматизація маркетингових кампаній, стають невід'ємною частиною стратегії сучасних компаній{ Харрарі, Ю. Н. (2022). *Homo Deus*, 298 с.}.

З одного боку, аватари на основі ШІ, що імітують людські риси, емоції та рухи, вже зовсім скоро зможуть замінити живих моделей у рекламних кампаніях. Рекламодавці зацікавлені в таких інноваціях, адже вони дозволяють значно скоротити витрати, пов'язані з організацією фотосесій та відеозйомок. ШІ-моделі зможуть адаптуватися під різні стилі і ролі, що робить їх універсальним інструментом для брендів. Окрім цього, розвиток технологій зможе відкрити новий ринок для монетизації зовнішності знаменитостей, які, замість виснажливих зйомок, зможуть продавати право на використання свого образу у рекламі, заощаджуючи свій час та ресурси.

З розвитком технологій можливість створення ШІ, здатного імітувати конкретних осіб, стане ще більш доступною{ Тегмарк, М. (2019). *Книга «Життя 3.0. Доба штучного інтелекту», 102 с.*}. Це може привести до зростання кількості випадків незаконного використання чужої зовнішності, що підкреслює потребу у створенні правових механізмів для захисту особистості в цифровому середовищі. Патентування зовнішності може стати необхідністю, щоб уникнути небажаного використання вашого образу без згоди.

Крім рекламних цілей, ШІ активно впроваджується в HR процеси. Наприклад, автоматизовані асистенти, що працюють на основі ШІ, вже допомагають новим співробітникам адаптуватися в компанії, надаючи їм необхідну інформацію у відповідь на запити. Майбутнє ж обіцяє ще більш глибоке використання ШІ в корпоративному світі. Можливо, компанії будуть створювати персональних ШІ-помічників, які матимуть не тільки голос, але й віртуальну зовнішність, що відповідає корпоративному іміджу. Це дозволить компаніям надавати співробітникам унікальний досвід, де кожен зможе взаємодіяти з персоналізованим ШІ, що виконуватиме завдання в інтерактивній формі.

Суперінтелект - це термін, що часто асоціюється з фантастикою, проте у найближчі десятиліття може стати реальністю. Суперінтелект, здатний до самонавчання і самовдосконалення, зможе виконувати різноманітні завдання, що раніше були непосильними для людства. Він зможе ефективно вирішувати глобальні проблеми, такі як кліматичні зміни, перенаселення, нестача енергії та багато інших. Країни зможуть використовувати такий інтелект для прийняття стратегічних рішень, що ґрунтуються на неймовірно точному аналізі даних. ШІ стане новим «архітектором» майбутнього, допомагаючи людству досягти нових висот.

Штучний інтелект також активно входить у повсякденне життя споживачів, змінюючи їхні звички та спосіб взаємодії з технологіями. Від особистих помічників на зразок Siri чи Google Assistant до рекомендаційних систем в стрімінгових сервісах — ШІ почав формувати наші переваги та навіть підказувати, що і коли нам краще зробити. Уявіть світ, де ШІ знає наші вподобання до найменших деталей і стає повноцінним учасником нашого життя, нагадуючи, підтримуючи та іноді вирішуючи за нас рутинні задачі.

Нова хвиля технологій обіцяє появу ще більш персоналізованих сервісів, де ШІ не просто аналізує історію покупок або інтереси, але й розпізнає емоційний стан користувача в реальному часі, надаючи рекомендації відповідно до його настрою. Наприклад, платформи можуть адаптувати контент або послуги залежно від настрою людини, знижуючи стрес чи, навпаки, стимулюючи до нових дій. Це створює нові етичні питання щодо меж втручання технологій у приватне життя людей і необхідності нових нормативних регуляторів.

З іншого боку, інтеграція ШІ в секторі освіти й науки дає можливість удосконалювати процеси навчання і досліджень. Інтелектуальні системи можуть індивідуально підлаштовувати навчальні програми для студентів, надаючи їм можливість розвиватися у власному темпі та формуючи персоналізовані освітні траєкторії. Для науковців ШІ може стати потужним інструментом в обробці великих обсягів даних і пошуку нових відкриттів, підвищуючи ефективність досліджень і пришвидшуючи прогрес у численних наукових галузях.

1. Тегмарк, М. (2019). Книга «Життя 3.0. Доба штучного інтелекту». Наш Формат. (Оригінал опубліковано 2016 р.)
2. Харрарі, Ю. Н. (2022). Homo Deus. Book Chef.

С.Ю. Бондаренко, Ю.Л. Вітомський

ЕМОЦІЙНЕ ЗАРАЖЕННЯ ТА СИМУЛЯЦІЯ ЕМПАТІЇ В ШІ: ПСИХОЛОГІЧНІ НАСЛІДКИ ДЛЯ ЕМОЦІЙНОГО БЛАГОПОЛУЧЧЯ ЛЮДИНИ ТА СОЦІАЛЬНОЇ ЗГУРТОВАНОСТІ

Сфера розвитку штучного інтелекту (ШІ) стала каталізатором глибоких змін у нашому розумінні емоційної динаміки, особливо в контексті взаємодії людини та машини. Емоційне зараження, глибоко вкорінений психологічний процес, за допомогою якого індивід несвідомо імітує та синхронізує свої афективні стани з афективними станами іншого, лежить в основі цих відносин, що розвиваються. Інтеграція афективних обчислювальних технологій викликала інтенсивні дебати серед психологів і технологів, зокрема щодо симуляції емпатії в штучному інтелекті та її потенційних наслідків для емоційного благополуччя людини та соціальної згуртованості.

Системи штучного інтелекту все частіше розробляються для імітації людських емоційних реакцій, використовуючи складні алгоритми, які імітують афективні стани, щоб покращити їхню взаємодію з людьми. Ці машини використовують об'єднання обробки природної мови, машинного навчання та нейронних мереж для аналізу та відтворення таких емоційних сигналів, як міміка, голосові інтонації та навіть мікрожести. Мета цих симуляцій нібито полягає у сприянні більш плавній та привабливій взаємодії між людьми та системами ШІ. Однак це викликає серйозне занепокоєння з психологічної точки зору, оскільки автентичність емоційних реакцій і межі між симульованою та справжньою емпатією стають розмитими.

З точки зору емоційного зараження необхідно ретельно вивчити психологічний вплив взаємодії з емпатично симульованим ШІ. Емоційне зараження – це не лише когнітивне чи поведінкове явище, але також глибоко вкорінене в нейрофізіологічних процесах. Система дзеркальних нейронів, наприклад, відіграє ключову роль у несвідомому та автоматичному наслідуванні афективних станів. Коли люди взаємодіють з іншими, які демонструють емоції – чи то через вираз обличчя, чи через голосові інтонації – відбувається нейробіологічна синхронізація, яка сприяє спільному емоційному досвіду. Ця складна взаємодія є основою для розвитку соціальних зв'язків і згуртованості людських спільнот. Однак реплікація таких механізмів системами штучного інтелекту створює складну дилему: чи може штучно викликане емоційне зараження справляти подібний нейроафективний вплив на людей?

Емпіричні дослідження соціальної нейронауки підкреслюють важливу роль справжньої емпатії у формуванні значущих людських стосунків [1]. Емпатія, яку можна розділити на афективні та когнітивні компоненти, вимагає емоційного резонансу з почуттями іншої людини та здатності прийняти її точку зору. Афективний компонент, якому часто сприяє емоційне зараження, породжує внутрішній досвід спільних емоцій. Когнітивний компонент, з іншого боку, передбачає більш обдумане та рефлексивне розуміння емоційного стану іншого. ШІ, імітуючи афективні реакції, прагне викликати емоційне зараження, але йому принципово бракує суб'єктивної свідомості, необхідної для справжньої емпатії. Ця розбіжність може мати далекосяжні наслідки для людської психіки, особливо в контекстах, коли люди розвивають прихильність до систем штучного інтелекту на основі сприйманої емоційної взаємності.

Психологічні наслідки такої емоційної мімікрії, керованої ШІ, поширюються на занепокоєння щодо емоційного благополуччя. Люди еволюційно схильні до формування емоційних зв'язків, схильності, яка відіграла важливу роль у сприянні виживанню через соціальну співпрацю. Однак афективні симуляції, створені штучним інтелектом, можуть призвести до певної форми «емоційного обману», коли люди сприймають емоційну автентичність там, де її немає. З часом це може спотворити людські очікування щодо справжніх емоційних стосунків і підірвати здатність до справжніх соціальних зв'язків. Крім того, повсюдний вплив імітованої емпатії може змінити нормативний ландшафт емоційних взаємодій, особливо в середовищах, де зв'язки між людьми вже напружені або знецінені, наприклад, у сфері догляду або обслуговування клієнтів.

Крім того, наслідки для соціальної єдності є глибокими та багатогранними. Емоційне зараження служить вирішальним механізмом групової солідарності, впливаючи на колективні емоційні стани та поведінку. Під час кризових ситуацій або емоційно насичених ситуацій спільний емоційний досвід може об'єднати людей разом, зміцнюючи групову ідентичність і сприяючи просоціальній поведінці. Впровадження систем штучного інтелекту, які імітують емпатію та викликають емоційне зараження, може порушити цю динаміку, або шляхом послаблення справжніх людських зв'язків, або шляхом посилення емоційних станів таким чином, що посилює соціальну фрагментацію. Наприклад, на цифрових комунікаційних платформах, де AI-боти розгортаються для модерування або участі в емоційно заряджених дискусіях, потенціал маніпуляційного емоційного зараження може призвести до посилення поляризації або соціального розбрату.

Психологічні теорії емоційної праці ще більше ускладнюють розуміння опосередкованої ШІ емпатії. Емоційна праця, як концептуалізує соціолог Арлі Гохшильд, відноситься до регулювання та управління емоціями для виконання вимог соціальної чи професійної ролі [2]. Системи штучного інтелекту, запрограмовані на прояв емпатії, виконують певну форму емоційної роботи, позбавленої суб'єктивного досвіду. Це піднімає етичні питання щодо комерціалізації емпатії та її психологічних наслідків для людей, які взаємодіють із цими системами. Очікування того, що штучний інтелект зможе задовольнити емоційні потреби, може призвести до аутсорсингу емоційної праці, зменшуючи сприйняту цінність справжньої людської емпатії та накладаючи надмірне емоційне навантаження на людей, які жадають справжнього емоційного залучення.

Крім того, не можна не помітити потенціал десенсибілізації до справжніх людських емоцій. Коли люди звикають взаємодіяти з ШІ, який імітує емпатію, може відбутися відповідне зниження їх чутливості до

справжніх людських емоцій. Психологічна література про десенсибілізацію припускає, що повторний вплив імітованих афективних реакцій може призвести до зниження здатності співпереживати реальним людським стражданням. Це має значні наслідки для соціальних установ, таких як охорона здоров'я та освіта, де людська здатність до співпереживання є життєво важливою для ефективного та співчутливого надання послуг.

Симуляція емпатії в ШІ також викликає серйозне занепокоєння щодо емоційної автентичності та психологічної концепції диференціації себе та іншого. Автентична емпатія вимагає усвідомлення різниці між власними емоціями та емоціями іншої людини, цьому процесу сприяє інтеграція афективної та когнітивної емпатії. Однак системам штучного інтелекту не вистачає самосвідомості та вони нездатні до справжньої диференціації себе-іншого. Таким чином, їхня симуляція емпатії є простою імітацією, позбавленою психологічних процесів, які лежать в основі людської емпатії. Це породжує привид суспільних змін, під час яких емоційна автентичність знецінюється, а поверхневі емоційні прояви стають нормою.

Підсумовуючи, психологічні наслідки емоційного зараження та симуляції емпатії в ШІ є складними та далекосяжними. Хоча потенційні переваги емоційно інтелектуального штучного інтелекту незаперечні, зокрема, у покращенні взаємодії з користувачем і сприянні взаємодії людини з машиною, слід ретельно розглянути довгострокові наслідки для емоційного благополуччя людини та соціальної згуртованості. Симуляція емпатії за допомогою штучного інтелекту ставить під сумнів основоположні принципи людського емоційного зв'язку, піднімаючи питання щодо автентичності емоційних переживань і майбутнього людських стосунків у світі, який дедалі більше опосередковується штучним інтелектом. Оскільки технології продовжують розвиватися, вкрай важливо, щоб психологи, технологи та фахівці з етики брали участь у міцному діалозі, щоб подолати ці виклики та забезпечити, щоб інтеграція ШІ в життя людини покращувала, а не зменшувала наше емоційне та соціальне благополуччя.

1. Lampe, B., & Meng, W. (2023). A survey of deep learning-based intrusion detection in automotive applications. Expert Systems with Applications, 119771. https://doi.org/10.1016/j.eswa.2023.119771.

2. Vanin, P., Newe, T., Dhirani, L. L., O'Connell, E., O'Shea, D., Lee, B., & Rao, M. (2022). A Study of Network Intrusion Detection Systems Using Artificial Intelligence/Machine Learning. Applied Sciences, 12(22), 11752. https://doi.org/10.3390/app122211752.

О.С. Кобус, С.Ю. Бондаренко

АНАЛІЗ ВРАЗЛИВОСТІ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ (IDS) НА ОСНОВІ ШІ ДО АГРЕСИВНИХ АТАК

Системи виявлення вторгнень (IDS) на основі штучного інтелекту (AI/ШІ) представляють собою складний прогрес у кібербезпеці, інтегруючи машинне навчання та аналіз даних для проактивного виявлення та нейтралізації загроз у мережевих інфраструктурах. Незважаючи на свою ефективність, ці системи залишаються вразливими до спектру агресивних атак, які використовують внутрішні алгоритмічні та системні обмеження. Наше дослідження пропонує детальний і критичний аналіз вразливостей IDS на основі штучного інтелекту, вивчення теоретичних основ, потенційних конкурентних методів і контрзаходів. Ми заглиблюємося в супротивницьке машинне навчання (adversarial machine learning), атаки ухилення та отруєння (evasion and poisoning attacks), сприйнятливість системної архітектури та пропонуємо надійні стратегії пом'якшення, щоб підвищити стійкість IDS до дедалі складніших кіберзагроз.

Системи виявлення вторгнень (IDS) значно розвинулися з появою штучного інтелекту та технологій машинного навчання, дозволяючи виявляти загрози в реальному часі та адаптивні механізми захисту. Традиційні IDS покладалися в основному на підходи на основі сигнатур або аномалій, які мали труднощі з ідентифікацією нових або прихованих загроз. Навпаки, IDS на основі штучного інтелекту використовує потужність прогнозної аналітики, моделей глибокого навчання та алгоритмів виявлення аномалій, покращуючи їхню здатність виявляти атаки нульового дня та зменшувати помилкові спрацьовування.

Незважаючи на переваги IDS на основі ШІ, вони не захищені від уразливостей. Ці вразливості посилюються агресивними стратегіями атак, які використовують супротивники, щоб обійти механізми виявлення. Основна проблема полягає в тому, що моделями штучного інтелекту можна маніпулювати або вводити в оману за допомогою змагальної тактики, що фундаментально підриває їхню надійність. Розуміння цих вразливостей вимагає багатостороннього дослідження недоліків моделі штучного інтелекту, ризиків отруєння даних і недоліків архітектури.

IDS на основі штучного інтелекту зазвичай включають низку методів машинного навчання, від керованих моделей навчання (наприклад, опорні векторні машини, випадкові ліси, нейронні мережі) до неконтрольованих моделей навчання (наприклад, алгоритми кластеризації, автокодери). Архітектура часто включає: 1) перетворення даних мережевого трафіку в числові формати, які піддаються алгоритмам машинного навчання [1]; 2) використання великих наборів даних для навчання моделей, здатних розрізняти доброякісну та зловмисну поведінку; 3) виявлення відхилень від нормальних моделей поведінки або збіг відомих зловмисних сигнатур; 4) автоматизація пом'якшення загроз і оповіщення персоналу служби безпеки про можливі вторгнення.

Ефективність IDS на основі ШІ залежить від точних і надійних механізмів виявлення. Ці системи спираються на: 1) виявлення статистичних відхилень від встановлених норм; 2) присвоєння міток точкам даних на основі вивчених ознак; 3) визначення шаблонів атак на основі попередніх зустрічей і кореляції даних у реальному часі. IDS на основі штучного інтелекту чутливі до різних класів загроз противника, зокрема: 1) маніпулювання вхідними даними, щоб уникнути виявлення без зміни шкідливих функцій; 2) забруднення навчальних наборів даних для зниження продуктивності моделі; 3) реконструкція навчальних даних для використання конфіденційної інформації; 4) генерація шаблонів (GAN) зловмисного трафіку, які неможливо відрізнити від безпечного трафіку.

Змагальне машинне навчання передбачає систематичне маніпулювання моделями штучного інтелекту для компрометації процесів прийняття рішень. Зловмисники використовують: 1) введення незначних змін до вхідних даних, які вводять в оману модель; 2) використання інформації про градієнт для оптимізації вхідних даних противника; 3) використання знань про архітектуру моделі (білий ящик) або дослідження моделі методом проб і помилок (чорний ящик) [2] .

Атаки ухилення використовують нездатність IDS узагальнювати дані, окрім своїх навчальних даних. Техніки включають: 1) зміна функцій мережевого трафіку, щоб уникнути виявлення; 2) шифрування або фрагментація корисного навантаження для обфускації (маскування) зловмисної активності; 3) зміна моделей дорожнього руху, щоб вони нагадували доброякісну поведінку. Атаки з отруєнням даних включають введення шкідливих зразків у навчальний набір даних. Це підриває процес навчання моделі та призводить до: 1) знижена точність і збільшення помилкових спрацьовувань або негативів; 2) вбудовування певних шаблонів, які запускають зловмисну поведінку, коли зустрічаються (бекдор-атаки).

Змагальні атаки демонструють високу можливість передачі, тобто успішна атака на одну модель може бути ефективною проти інших моделей. Це особливо хвилює IDS на основі штучного інтелекту, оскільки зловмисники можуть розробити узагальнені стратегії атак, які працюють у різних реалізаціях. Крім алгоритмічної вразливості, архітектурні недоліки систем IDS можуть наражати їх на: 1) затримки в механізмах виявлення та відповіді; 2) перевантаження IDS великими обсягами нешкідливого трафіку для приховування шкідливих дій; 3) Неправильна конфігурація та слабке шифрування (створення векторів атак, які обходять або вимикають IDS).

Навчання змагальності передбачає доповнення навчального набору даних змагальними прикладами для підвищення надійності моделі. Цей метод показав багатообіцяючість, але є дорогим з обчислювальної точки

зору та може не повністю врахувати складні змагальні методи. Удосконалення моделей виявлення аномалій за допомогою ансамблевого навчання та гібридних підходів може зменшити ризик атак ухилення. Техніки включають: 1) поєднання кількох слабких класифікаторів для підвищення точності виявлення; 2) інтеграція методів на основі сигнатур і аномалій для повного покриття.

Впровадження надійних механізмів очищення даних може запобігти атакам отруєння. Техніки включають: 1) моніторинг походження та цілісності навчальних даних; 2) виявлення та видалення аномальних точок даних, які можуть поставити під загрозу продуктивність моделі. IDS на основі штучного інтелекту може отримати користь від адаптивних механізмів захисту, які розвиваються у відповідь на нові загрози. Це включає: 1) регулярне оновлення моделей за допомогою нових даних про загрози; 2) включення зворотного зв'язку від виявлених вторгнень для вдосконалення моделей. Інтеграція зрозумілих методів штучного інтелекту може покращити прозорість та інтерпретацію IDS на основі штучного інтелекту. Це дає змогу аналітикам безпеки зрозуміти та перевірити процес прийняття рішень моделі, сприяючи більш ефективним протидіям.

Системи виявлення вторгнень на основі штучного інтелекту представляють собою важливий прогрес у кібербезпеці, пропонуючи безпрецедентні можливості для виявлення та пом'якшення загроз. Однак їхня вразливість до агресивних ворожих атак створює значні проблеми, які необхідно вирішити шляхом ретельних досліджень та інновацій. Розуміючи тонкощі змагальної тактики та впроваджуючи надійні оборонні стратегії, спільнота кібербезпеки може підвищити стійкість IDS на основі штучного інтелекту, забезпечуючи їхню ефективність у захисті критичної мережевої інфраструктури.

Еволюція змагальних загроз вимагає проактивного та адаптивного підходу, наголошуючи на необхідності постійної співпраці між дослідниками ШІ, фахівцями з кібербезпеки та політиками. Зі зміною ландшафту кіберзагроз також повинні розвиватися наші засоби захисту, гарантуючи, що IDS на основі штучного інтелекту залишатимуться потужним бар'єром проти зловмисників.

1. Alrajeh, N. A., & Lloret, J. (2013). Intrusion Detection Systems Based on Artificial Intelligence Techniques in Wireless Sensor Networks. International Journal of Distributed Sensor Networks, 9(10), 351047. https://doi.org/10.1155/2013/351047.

2. Sowmya, T., & Mary Anita, E. A. (2023). A comprehensive review of AI based intrusion detection system. Measurement: Sensors, 100827. https://doi.org/10.1016/j.measen.2023.100827.

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ ТА ПРОТИДІЇ ЗАГРОЗАМ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ

Анотація

У роботі розглядаються можливості використання штучного інтелекту для аналізу та протидії загрозам радіоелектронної боротьби (РЕБ). Збільшення кількості та ускладнення загроз у цьому секторі вимагають впровадження нових технологій для швидкого розпізнавання та нейтралізації джерел перешкод. Основна увага зосереджена на глибокому навчанні для класифікації та обробки сигналів, автоматизованому прийнятті рішень у реальному часі, а також прогнозуванні дій противника на основі історичних даних. Результати дослідження показують, що ШІ суттєво покращує системи виявлення та протидії, прискорюючи та підвищуючи точність реагування. Найважливіше, що це підвищує надійність і стійкість систем завдяки швидкозростаючому використанню ШІ та засобів автоматизації для аналізу загроз на основі їхніх характеристик, які неможливо розділити одна від одної.

Ключові слова

Штучний інтелект(ШІ), Радіоелектронна боротьба(РЕБ), Алгоритми глибокого навчання, Згорткові нейронні мережі (CNN), Безпілотні літальні апарати (БПЛА)

- **Вступ**

Сучасні умови ведення бойових дій характеризуються інтенсивним використанням засобів радіоелектронної боротьби, що ускладнює зв'язок та управління військовими підрозділами. Системи РЕБ створюють сильні перешкоди, виводять з ладу радари та ускладнюють передачу інформації. У цьому контексті виникає потреба в розробці нових методів протидії, здатних швидко й ефективно реагувати на загрози.

Одним із перспективних підходів до вирішення цієї проблеми є використання технологій штучного інтелекту (ШІ). Завдяки здатності обробляти великі обсяги даних, аналізувати сигнали в реальному часі та приймати рішення з мінімальною затримкою, ШІ може забезпечити надійний захист від дій противника. У статті досліджено використання алгоритмів глибокого навчання та інших методів ШІ для автоматизованого розпізнавання джерел РЕБ і реалізації ефективних заходів протидії, що підвищує стійкість і надійність сучасних систем зв'язку та управління.

- **Використання ШІ у виявленні загроз РЕБ**

Основні завдання виявлення загроз РЕБ

Розвиток засобів РЕБ створює складні завдання для систем виявлення та захисту, що включають:

- Ідентифікацію джерел перешкод.
- Класифікацію типів сигналів.
- Визначення місцезнаходження джерел загроз.

Для забезпечення ефективної роботи таких систем необхідно застосовувати інноваційні методи, зокрема штучний інтелект, який здатен обробляти великі обсяги даних у реальному часі.[1][2]

Алгоритми глибокого навчання для обробки сигналів

Алгоритми глибокого навчання, зокрема згорткові нейронні мережі (CNN), демонструють високу ефективність у розпізнаванні спектральних характеристик сигналів. Вони здатні виділяти ключові особливості, що дозволяють точно класифікувати джерела загроз.[1][2][4]

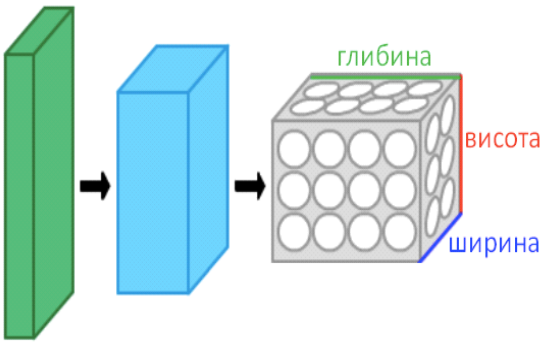


Рисунок 1 – Структура згорткової нейронної мережі для обробки сигналів

Класифікація джерел загроз

Для класифікації джерел РЕБ використовуються алгоритми машинного навчання, які можуть навчатися на великих наборах даних, зібраних у польових умовах. Це дозволяє автоматизувати процес розпізнавання та забезпечити високу точність навіть за наявності сильних перешкод.[4].

Таблиця 1 – Показує приклад класифікації різних типів сигналів РЕБ за допомогою алгоритмів ШІ

Тип сигналу	Метод класифікації	Точність (%)
Шумові перешкоди	Згорткова нейронна мережа	95
Адаптивні перешкоди	Рекурентна нейронна мережа	92
Радіолокаційні імпульси	CNN + RNN	94

Прогнозування дій противника

Алгоритми прогнозування на основі машинного навчання дозволяють передбачати можливі дії джерел РЕБ, аналізуючи історичні дані. Це дає змогу військовим системам бути на крок попереду противника.

Застосування алгоритмів штучного інтелекту значно покращує процеси виявлення та класифікації загроз РЕБ, підвищуючи точність і швидкість аналізу. Прогнозування дій противника сприяє ефективному захисту систем зв'язку і управління у складних умовах.[3][4]

- **ШІ для протидії загрозам РЕБ**

Сучасні технології радіоелектронної боротьби (РЕБ) вимагають нових підходів для ефективного протистояння загрозам. Штучний інтелект (ШІ) стає важливим інструментом у цій сфері, забезпечуючи можливості для виявлення, аналізу та нейтралізації загроз, що виникають у електромагнітному спектрі.

Автоматизоване реагування

Автоматизоване реагування — це основна функція систем ШІ, яка дозволяє приймати рішення в режимі реального часу. Цей процес складається з кількох ключових етапів:

Виявлення загрози:

- **Сенсорні технології**: Використання радіоелектронних сенсорів, які можуть виявляти електромагнітні сигнали, що генеруються ворожими системами РЕБ. Це включає в себе радіолокаційні системи, системи сигналізації та дронів для збору інформації з повітря.
- **Алгоритми виявлення**: Застосування алгоритмів машинного навчання для класифікації виявлених сигналів, що допомагає відрізнити ворожі сигнали від дружніх.

Оцінка загрози:

- **Моделювання сценаріїв**: Використання моделей, які прогнозують можливі дії ворога на основі історичних даних та патернів поведінки.
- **Оцінка впливу**: Аналіз можливого впливу на системи зв’язку і оперативні можливості, враховуючи різні параметри, такі як частота, потужність і геолокація.

Реакція:

- **Адаптивне налаштування системи**: Системи можуть автоматично налаштовувати частоти, потужність сигналу та інші параметри для обходу перешкод.
- **Навмисне маневрування сигналу**: Використання технік, таких як частотна стрибка або псевдослучайні коди, щоб зменшити ймовірність перехоплення сигналу.[5][6]

Розподілені системи управління

ШІ також забезпечує інтеграцію та координацію різних елементів системи протидії, ведучи до створення розподілених систем управління.[3] Такі системи працюють на основі збору та обробки інформації з різних джерел:

- **Об’єднання даних**: Дані з різних сенсорів і систем (радари, дрони, інші засоби спостереження) інтегруються для формування єдиної картини ситуації.
- **Аналіз даних**: Використання алгоритмів машинного навчання та штучних нейронних мереж для аналізу великого обсягу даних, що дозволяє виявляти патерни, аномалії та потенційні загрози.
- **Оптимізація дій**: ШІ автоматично коригує стратегію реагування на основі аналізу даних, визначаючи найефективніші контрзаходи.

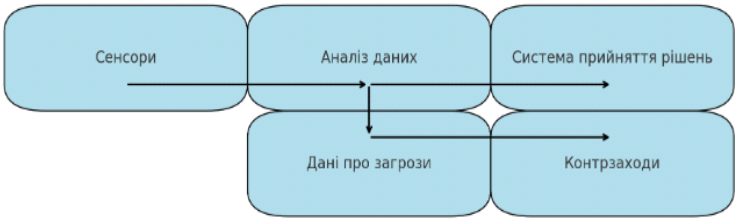


Рисунок 2 – Архітектура розподіленої системи управління

Таблиця 2 – Переваги розподілених систем управління

Перевага	Опис
Адаптивність	Швидке реагування на зміни в обстановці
Інтеграція даних	Об'єднання інформації з різних джерел
Поліпшена ефективність	Зменшення часу на прийняття рішень

Приклади використання ШІ у протидії РЕБ

- **Системи на базі дронів**: Використання безпілотних літальних апаратів (БПЛА) з системами ШІ для проведення розвідки та виявлення ворожих сигналів. Наприклад, дрони можуть автоматично патрулювати задані маршрути, аналізуючи сигнали в реальному часі та повідомляючи про виявлені загрози.[4]

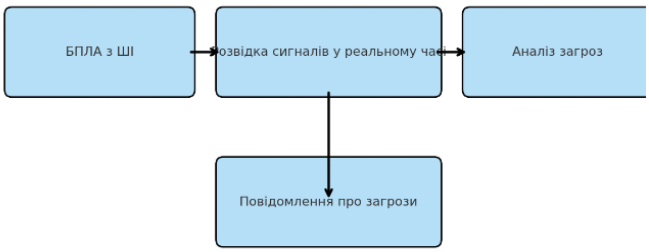


Рисунок 3 – Система на базі дронів для розвідки та виявлення загроз

- **Адаптивні комунікаційні системи**: Системи, які можуть автоматично змінювати свої параметри для обходу ворожих перешкод. Такі системи використовують алгоритми, що базуються на даних, отриманих від сенсорів, для автоматичного вибору оптимальних частот і способів передачі інформації.[4]

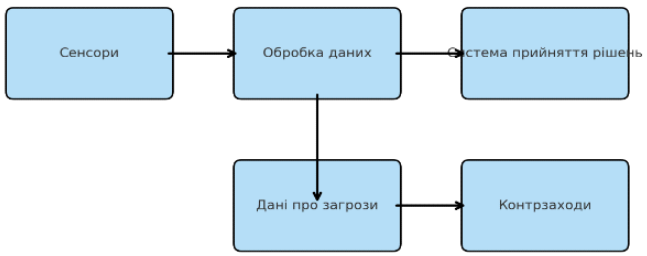


Рисунок 4 – Архітектура адаптивної комунікаційної системи

- **Інтелектуальні аналітичні платформи**: Використання платформ, що поєднують дані з різних джерел (соціальних мереж, новин, інформаційних систем), для аналізу поведінки ворога і передбачення його дій.[4]

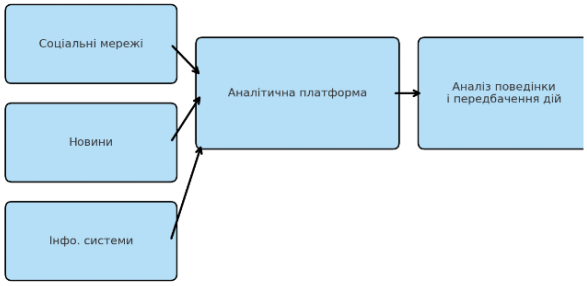


Рисунок 5 – Інтелектуальні аналітичні платформи

1. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444. DOI: 10.1038/nature14539.

2. Zhang, J., Zhang, Q., & Sun, Z. (2020). A comprehensive survey of artificial intelligence applications in the domain of electronic warfare. IEEE Access, 8, 223-245. DOI: 10.1109/ACCESS.2020.2969872.

3. Mnih, V., Kavukcuoglu, K., Silver, D., et al. (2015). Human-level control through deep reinforcement learning. Nature, 518(7540), 529-533. DOI: 10.1038/nature14236.

4. O'Shea, T. J., & Hoydis, J. (2017). An introduction to deep learning for the physical layer. IEEE Transactions on Cognitive Communications and Networking, 3(4), 563-575. DOI: 10.1109/TCCN.2017.2758370.

5. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., et al. (2020). A survey of machine and deep learning methods for Internet of Things (IoT) security. IEEE Communications Surveys & Tutorials, 22(3), 1646-1685. DOI: 10.1109/COMST.2020.2988293.

6. Huang, G., Liu, Z., Van Der Maaten, L., & Weinberger, K. Q. (2017). Densely connected convolutional networks. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 4700-4708). DOI: 10.1109/CVPR.2017.243.

В.В. Рудюк

ПРАКТИЧНІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ВИКЛАДАННІ БІОЛОГІЇ

Штучний інтелект (ШІ) стрімко проникає в різні сфери нашого життя, включаючи освіту. У викладанні біології технології ШІ стають важливим інструментом, який дозволяє покращити ефективність навчання, зробити його більш гнучким та доступним. Завдяки ШІ з'являється можливість створити для студентів інтерактивний навчальний процес, який підлаштовується під індивідуальні потреби та рівень підготовки кожного. Сьогодні ШІ допомагає проводити віртуальні експерименти, автоматизувати оцінювання, розробляти персоналізовані навчальні курси та значно полегшує роботу як викладачам, так і студентам.

ШІ відкриває нові можливості для вивчення біології, особливо в розрізі лабораторних досліджень і симуляцій. Одним із найбільш ефективних застосувань ШІ є віртуальні лабораторії, які дозволяють студентам виконувати експерименти без потреби в реальному лабораторному обладнанні. Це особливо корисно для навчальних закладів, які обмежені в ресурсах. Студенти можуть вивчати структуру клітин, біохімічні реакції, еволюційні процеси та багато інших важливих біологічних тем, перебуваючи у віртуальному середовищі. У таких лабораторіях використовується ШІ, щоб змоделювати реальні процеси – наприклад, поділ клітини або фотосинтез. Це дозволяє студентам глибше зануритись у матеріал і зрозуміти складні біологічні концепції.

Важливою перевагою ШІ є його здатність створювати адаптивні навчальні програми, які враховують рівень знань студента і підлаштовують навчальні завдання відповідно до його індивідуальних потреб. Це означає, що система на основі ШІ може аналізувати прогрес студента, визначати його слабкі сторони та пропонувати додаткові матеріали для покращення розуміння. Наприклад, якщо учень має труднощі з генетикою, ШІ надасть більш детальні пояснення або додаткові вправи для закріплення знань. Такий підхід не тільки спрощує процес засвоєння матеріалу, але й значно підвищує рівень зацікавленості студентів у навчанні.

Ще однією важливою можливістю є автоматизація оцінювання завдань і тестів. Завдяки алгоритмам ШІ викладачі можуть швидко та об'єктивно оцінювати знання учнів, а студенти – отримувати миттєвий зворотний зв'язок. Це також дозволяє вчителям приділяти більше часу на роз'яснення складних тем і роботу зі студентами. Системи на основі ШІ також можуть надати детальні коментарі до помилок, вказати на конкретні місця для повторення та додатково пояснити матеріал.

Сучасні віртуальні помічники, створені на базі ШІ, стають важливими партнерами для студентів у процесі навчання. Вони можуть відповідати на питання в режимі реального часу, давати рекомендації щодо додаткових матеріалів, допомагати готуватись до тестів і навіть створювати індивідуальні підказки. Завдяки такому інтерактивному підходу, навчання стає більш привабливим і мотивуючим, а студенти отримують додаткову підтримку, яка робить процес вивчення біології легшим і зрозумілішим.

Інтеграція ШІ з віртуальною та доповненою реальністю дозволяє створювати повноцінні віртуальні тури людським тілом, екосистемами або клітинами. У такому форматі студенти можуть буквально «поринути» у біологічні процеси, побачити роботу органів або клітин зсередини, спостерігати за взаємодією організмів в екосистемах. Це значно покращує сприйняття складних матеріалів і дозволяє студентам краще запам'ятати інформацію.

Крім того, технології ШІ активно застосовуються для аналізу великих біологічних даних. Це може бути корисно для проєктної діяльності студентів, наприклад, при роботі з екологічними даними або генетичними дослідженнями. Студенти можуть аналізувати отримані дані, знаходити взаємозв'язки та робити висновки на основі проведених досліджень. Це розвиває в них аналітичне мислення і знайомить з методами сучасної біоінформатики.

Завдяки штучному інтелекту викладання біології стало набагато більш захоплюючим, доступним та інтерактивним. Інтерактивні лабораторії, адаптивне навчання, автоматичне оцінювання та віртуальні помічники є лише деякими з переваг, які ШІ приносить у біологічну освіту. ШІ дозволяє викладачам зосередитися на індивідуальній роботі з учнями та вдосконаленні навчальних програм, тоді як студенти отримують можливість глибше пізнавати біологію і розуміти її важливість у сучасному світі. З огляду на темпи розвитку технологій, у майбутньому застосування ШІ в біологічній освіті стане ще ширшим, що відкриє нові перспективи як для викладачів, так і для учнів.

1. Нгуєн Т., Хаббал Дж. Покращення біологічної освіти за допомогою штучного інтелекту та машинного навчання // Journal of Educational Computing Research. – 2020. – Т. 58, № 4. – С. 716–734.

2. Сміт А., Робертс П. ШІ та аналіз даних у біологічній освіті: Підтримка проектного навчання // Learning Analytics Journal. – 2022. – Т. 45, № 5. – С. 201–215.

3. Вулф Б. П., Лейн Г. К. Штучний інтелект в освіті: Створення інтелектуальних систем для покращення освіти. – Нью-Йорк: Routledge, 2019. – 320 с.

4. Їн Х., Чжао Л. Вплив ШІ та віртуальної реальності на залученість студентів у біологічних науках // Advances in Science Education. – 2021. – Т. 16, № 7. – С. 94–102.

О.А. Владимирський, І.А. Владимирський, І.П. Криворучко, Д.М. Семенюк

ПІДВИЩЕННЯ ЯКОСТІ ПРИЙОМУ ДІАГНОСТИЧНОЇ ІНФОРМАЦІЇ ВІД РОЗПОДІЛЕНИХ У ПРОСТОРІ ПРИСТРОЇВ ЗБОРУ ДАНИХ

Завдання забезпечення якості діагностичних даних при їхньому зборі від розподілених у просторі пристроїв виникає при діагностуванні розгалуженого електротехнічного обладнання на ТЕЦ, при централізованому зборі та обробці показників температури, тиску, витрати від споживачів тепло- та водопостачання і т.і.. У доповіді це питання розглянуто з точки зору підвищення якості прийому акустичних сигналів від розподіленої у просторі системи пошуку витоків підземних трубопроводів централізованого тепло- та водопостачання кореляційними течешукачами (КТ).

Важливим аспектом, який випливає зі зносу трубопровідних мереж, боротьби з завадами та з умов воєнного стану, є особливі вимоги до:

- захисту від радіо завад при передаванні інформативних акустичних даних про пошкодження від датчиків до блоків кореляційної обробки;
- завадо захищеного способу синхронізації цих сигналів;
- витребуваного динамічного діапазону розподілених у просторі вимірювальних блоків КТ.

У звичайних КТ синхронізація вимірювань забезпечується одночасним прийомом по радіоканалах сигналів з датчиків у блоці кореляційної обробки. Однак з точки зору актуальних високих вимог до подолання завад, обмежений динамічний діапазон радіоканалів є вузьким місцем у КТ. Бо сучасна цифрова обробка сигналів спроможна оперувати з акустичними даними у динамічному діапазоні 100дБ, однак цього фактично не досягається, бо динамічний діапазон аналогових радіоканалів у складі звичайних КТ не перевищує 40дБ. Зустрічаються приклади застосування цифрових радіоканалів, але вони поки що не отримали поширення з причин малої дальності та занадто широкого займаного частотного діапазону, який заважає іншим користувачам радіоефіру і тому зазвичай не дозволяється за законодавством. Крім того, радіоканали схильні до впливу радіо завад, які додаються до акустичних завад та ще більш ускладнюють роботу, у тому числі в умовах військової радіо боротьби. Тому у актуальних на сьогодні ускладнених випадках потрібно мати альтернативне рішення. Таким рішенням є застосування реєстраторів акустичних сигналів трубопроводів, яке, одночасно зі звичайними КТ, за останні роки набуло поширення в світі. Але це відбулося, здебільшого, з метою автоматизувати та прискорити реєстрацію витоків на водопроводах, наприклад у нічні часи, коли споживання води та, відповідно, завади є мінімальними. Тоді декілька реєстраторів розташовують у місцях доступу до трубопроводу та проводять реєстрацію витоків чи за підвищеним рівнем акустичного шуму, чи за кореляційною функцією. Але в умовах зношених мереж, наявності акустичних завад, така автоматизація є ускладненою. Стосовно ж актуальних завдань для наших умов, застосування реєстраторів повинно, по-перше, зняти вказане обмеження динамічного діапазону оброблюваних даних, спричинене радіоканалами, по-друге, усунути вплив на акустичні дані міліарних та інших радіо завад і по-третє забезпечити прийнятну синхронність вимірювань у рознесених у просторі виносних блоках КТ. Тому розглянемо наявні технічні рішення саме з цих важливих для наших умов позицій.

Британська система Enigma виробництва Ovarro Connecting Technologies є системою багато точкової кореляції шуму, яка використовує 3G та 2G зв’язок [1]. температурний діапазон датчиків до +60°C [2], система PHOCUS3M тієї ж фірми, додатково використовує 4G зв’язок, температурний діапазон датчиків до +70°C [3]. Технічно розвиненою є американська система PermaNET Trunc Main (TM) GPS компанії FCS [4] акустичного моніторингу трубопроводів. Використовує GPS синхронізацію реєстрації даних за часом для отримання високоточної кореляції на великих відстанях. Робочий температурний діапазон до +60°C.

Ці найбільш відомі системи оптимізовано для західних, мирних та стабільних умов зручного використання розвинених засобів супутникового та мобільного зв’язку. Вони здебільшого використовуються для систем водопостачання, тому верхня робоча температура для датчиків становить +60 чи +70°C. Слід зазначити, що температура теплоносія у подавальному трубопроводі у зимовий період в Україні зазвичай є більшою. Крім того, військовий час не дозволяє цілком покладатися на стабільність, якість та просторове покриття супутникового та стільникового зв’язку. Тому робити залежною від справної роботи цих глобальних систем поточну аварійну місцеву діагностику критичної інфраструктури видається не доцільним. Особливо, якщо є інше ефективне та випробуване рішення. Це рішення розроблено в ІПМЄ ім. Г.Є.Пухова НАН України при створенні системи РАСТР [5] корозійного моніторингу трубопроводів і є доволі простим та надійним. Воно полягає теж у застосуванні радіозв'язку, але не стільникового і не супутникового, а за допомогою допрацьованих надійних радіостанцій фірми KENWOOD. Цей радіозв’язок використовується тільки для синхронізації вимірювань, тому не потребує тої високої якості, яка потрібна для діагностичних інформативних даних. Ці дані накопичуються у реєстраторах і зараз передаються для подальшої обробки у мобільний ПК за допомогою звичайних флеш накопичувачів без використання для цього радіозв’язку та пов’язаних з цим завад і втрат динамічного діапазону. Радіо синхронізація вимірювань забезпечується за допомогою вбудованого у одну з радіостанцій генератора широкосмугового шуму. Під час вимірювань цей радіошум виробляється, приймається радіоприймачами реєстраторів і одночасно з акустичними сигналами заноситься у їхню пам’ять. Синхронізація акустичних даних відбувається шляхом обчислення їхнього відносного часового зсуву. Для визначення цього зсуву обчислюється взаємна кореляційна функція зареєстрованих радіошумів синхронізації.

Зсув визначається за максимумом цієї функції. У пропонованому та реалізованому способі кореляційної радіо синхронізації використовується висока природна, статистична завадова стійкість оцінки кореляційної функції та часова чіткість її широкосмугового максимуму. Похибка синхронізації є прийнятною і не перевищує 0,1 мс. Поточним недоліком реалізації цього способу синхронізації є відносна складність її настроювання, яка поки що вимагає злагодженої роботи операторів біля кожного реєстратора, що доцільно виключити. Тому зараз роботи з вдосконалення способу виконуються у напрямку автоматизації ручних дій та спрощення керування системою. Також проводиться аналіз варіантів комбінації реалізованого способу з іншими, більш оперативними способами передавання акустичних даних для гнучкого застосування системи за різних завадових умов. Ці роботи проводяться в ІПМЕ ім. Г.Є.Пухова НАН України в рамках проекту 2023.04/0022 «Розроблення апаратно-програмного комплексу та методики оперативного виявлення пошкоджень систем тепло- та водопостачання з врахуванням їх зношеності та мілітарних впливів» за рахунок грантової підтримки Національного фонду досліджень України.

1. Ovarro connecting technologies. Enigma URL:https://ovarro.com/en/global/solutions/monitoring--control-devices/data-loggers--leak-noise-loggers/leak-noise-loggers--correlators/3/enigma/2/ (дата звернення : 29.09.2024).

2. Enigma. URL:https://ovarro.com/content-media/assigned/1560/Ovarro_Enigma. pdf (дата звернення : 3.10.2024).

3. Phocus3M. URL:https://ovarro.com/content-media/assigned/141312/Phocus3M_Specification %20Sheet_IXD652TN044_4.1.pdf (дата звернення : 3.10.2024).

4. PermaNET TM GPS. URL: https://www.fluidconservation.com/products/permanet-tm-gps/. (дата звернення : 3.10.2024).

5. Владимирський О. А., Владимирський І. А., Криворучко І. П., Савчук М.П.Розробка модернізованої системи низькочастотного діагностування стану трубопроводів РАСТР-1М. Моделювання та інформаційні технології. Збірник наукових праць ІПМЕ ім. Г. Є. Пухова НАН України. 2017. Вип. 78. С. 40-45.

Ю.О. Єжелий, Є.О. Писаренко

ХМАРНІ ТЕХНОЛОГІЇ ТА ШТУЧНИЙ ІНТЕЛЕКТ: ОПТИМІЗАЦІЯ РЕСУРСІВ І УПРАВЛІННЯ ПРОЄКТАМИ В ЦИФРОВУ ЕПОХУ

Хмарні технології сьогодні стали невід'ємною частиною повсякденного життя у всьому світі, а штучний інтелект є однією з найзначніших технологій, що визначають сучасний розвиток хмарних сервісів. Завдяки здатності автоматизувати обробку даних, аналізувати великі обсяги інформації та робити прогнози, ШІ відіграє вирішальну роль у трансформації бізнес-процесів. Хмарні технології в поєднанні з можливостями штучного інтелекту дозволяють компаніям покращувати управління ресурсами, підвищувати ефективність роботи команд та забезпечувати адаптацію до динамічних ринкових умов. Інтеграція цих технологій створює нові можливості для підприємств, відкриваючи шлях до інноваційних рішень і стратегій. Хмарні технології забезпечують зберігання великих обсягів інформації та надають безперешкодний доступ до неї в будь-який час і з будь-якого місця. Завдяки цій можливості, хмарні технології стали надзвичайно важливими для співпраці над проєктами, особливо в умовах зростаючої глобалізації, коли учасники проєктів можуть бути географічно віддалені. Хмарні технології являють собою різноманітні способи доставки і використання обчислювальних ресурсів, таких як сховища даних, мережі, бази даних, сервери та програмне забезпечення, за допомогою мережі Інтернет. Ця інфраструктура дає змогу користувачам з легкістю отримувати доступ до своїх файлів і програм з будь-якого пристрою, підключеного до Інтернету, що забезпечує мобільність і спрощує роботу. Важливо, що саме цей тип інфраструктури знімає необхідність у фізичному володінні серверами, знижуючи витрати на обладнання і обслуговування. Користувач може зберігати будь-які дані у віддаленому хмарному сховищі й отримувати до них доступ з будь-якої точки планети. Наприклад, сервіси на кшталт Google Drive або iCloud дають можливість завантажувати файли і документи в хмару для подальшого використання з різних пристроїв, зберігаючи при цьому їхню безпеку та конфіденційність.

Крім зберігання, хмарні технології надають доступ до потужних обчислювальних ресурсів, таких як віртуальні машини, що дає змогу ефективно використовувати фізичні ресурси. Це особливо вигідно для оптимізації робочих процесів у бізнесі, а також для економії місця, що є важливим для малих і середніх підприємств. Навіть великі компанії звертаються до хмарної віртуалізації, оскільки це дозволяє ефективно розподіляти ресурси і керувати ними за потреби.

Існує кілька основних типів хмарних сервісів, що відповідають різним бізнес-потребам:

1. Загальнодоступна хмара надається сторонніми постачальниками й доступна для широкого кола користувачів, забезпечуючи економічність через спільне використання ресурсів. Вона є популярним рішенням для багатьох компаній, адже значно знижує витрати.
2. Приватна хмара використовується окремою організацією і забезпечує більший контроль над даними і безпекою. Вона потребує більше ресурсів для підтримки, але є оптимальною для великих компаній з високими вимогами до конфіденційності.
3. Гібридна хмара поєднує переваги загальнодоступних і приватних хмар, що дозволяє розподіляти дані та обчислювальні потужності між ними залежно від рівня конфіденційності та потреб.
4. Мультихмара включає кілька хмарних платформ від різних постачальників, що дозволяє компаніям використовувати різні сервіси з оптимальними умовами і функціональністю, мінімізуючи залежність від одного постачальника [1].

Штучний інтелект значно підсилює можливості хмарних технологій, роблячи їх більш адаптивними, гнучкими та здатними автоматизувати складні процеси обробки даних. Однією з важливих функцій ШІ у хмарних рішеннях є здатність обробляти великі обсяги інформації в режимі реального часу. Це відкриває нові можливості для бізнесу, зокрема для аналізу поведінкових даних користувачів, прогнозування попиту, оптимізації запасів і покращення обслуговування клієнтів. Штучний інтелект також допомагає покращити ефективність хмарних систем завдяки алгоритмам машинного навчання, які здатні виявляти патерни і робити висновки на основі великої кількості даних.

Крім того, ШІ допомагає вирішувати важливі питання безпеки та захисту даних у хмарних середовищах. Завдяки алгоритмам виявлення аномалій та моніторингу, компанії можуть виявляти підозрілу активність і автоматично реагувати на можливі загрози, мінімізуючи ризики несанкціонованого доступу. Інструменти на базі ШІ значно покращують управління кібербезпекою та сприяють швидшому реагуванню на інциденти безпеки, що є надзвичайно важливим у сучасному цифровому середовищі.

З огляду на велику роль хмарних технологій у сучасних бізнес-процесах, вони суттєво впливають на управління проєктами, адже вони забезпечують постійний доступ до ресурсів, що підвищує продуктивність віддалених команд і дозволяє організаціям адаптуватися до зміни потреб. Капітальні витрати на інфраструктуру скорочуються, адже компанії платять лише за фактично використані ресурси. Крім того, хмарні платформи зазвичай включають інструменти для командної співпраці, що спрощує координацію і комунікацію між учасниками проєкту. Інструменти автоматизації, доступні в багатьох хмарних рішеннях, оптимізують процеси керування, підвищуючи загальну ефективність.

Проте, попри всі переваги, хмарні технології висувають певні виклики та ризики:

– забезпечення безпеки даних, адже захист конфіденційної інформації залишається актуальним питанням, оскільки дані зберігаються на віддалених серверах;

– залежність від підключення до Інтернету, що може вплинути на ефективність роботи команди у випадку нестабільного з'єднання;

– сумісність із наявними системами, адже інтеграція хмарних рішень часто потребує додаткових ресурсів;

– підготовка персоналу до переходу на хмарні рішення та адаптація нових процесів;

– виконання нормативних вимог, особливо щодо зберігання та обробки даних відповідно до місцевих і міжнародних законів [3].

Трансформація бізнесу через впровадження хмарних технологій включає декілька етапів. Одним з підходів є перенесення існуючих програм за принципом «lift-and-shift», коли застосунки переміщуються до хмари з мінімальними змінами або зовсім без них. Це може бути основним етапом впровадження, проте згодом компанії часто модернізують чи вдосконалюють ці застосунки для більш ефективної роботи в хмарному середовищі [2].

Розвиток хмарних технологій продовжує прискорюватися, зокрема завдяки розвитку інструментів штучного інтелекту та аналітики великих даних. Зі зростанням можливости обчислювальних ресурсів компанії зможуть ефективніше аналізувати дані, застосовувати їх для прийняття стратегічних рішень і досягати конкурентних переваг. Хмарні рішення надають широкий спектр можливостей для всіх типів бізнесу, тож інтеграція цих технологій може значно поліпшити ефективність управління проєктами і забезпечити конкурентні переваги на ринку. Враховуючи виклики та переваги, що виникають у процесі впровадження хмарних технологій, ШІ стає критично важливим елементом для забезпечення конкурентоспроможности на ринку. Його здатність аналізувати дані, автоматизувати процеси та підвищувати рівень безпеки робить бізнес більш стійким до змін. Успішна інтеграція ШІ у хмарні рішення дозволяє компаніям не лише зберігати свої дані, але й використовувати їх для досягнення стратегічних цілей, підвищуючи загальну продуктивність і ефективність.

1. Впровадження хмарних технологій із точки зору управління проєктами. Anywhere Club. URL: https://aw.club/global/uk/blog/cloud-adoption-from-a-project-management (дата звернення: 29.10.2024).

2. Стрілець В., Пожар А., Флегантова А., Франко Л., Єжелий Ю., Зборик Д. Цифровізація як інструмент побудови інноваційної стратегії розвитку бізнесу країн ЄС в умовах адаптації до кризових тенденцій міжнародної економіки. Науковий вісник Полтавського університету економіки і торгівлі. Серія «Економічні науки», 2024. № 3 (113), С. 80–88.

3. Хмарні технології: переваги та виклики для бізнесу. Енциклопедія світу цифрових технологій. URL: https://optimize-il.com/hmarni-tehnologiyi-perevagi-ta-vikliki-dlya-biznesu (дата звернення: 29.10.2024).

А.І. Єременко, Т.А. Вакалюк

ОГЛЯД СТРАТЕГІЙ МАШИННОГО НАВЧАННЯ

Машинне навчання широко використовується у сучасному світі для вирішення великої кількості проблем. Ціль даної галузі – це розробка алгоритмів, які дозволяють комп'ютерам навчатися на основі даних, та використовувати отриманні знання для обробки поставлених задач. Процес навчання полягає у встановленні залежності між вхідними та вихідними даними, схоже до того, як це робить людський мозок.

На сьогоднішній день, багато алгоритмів активно розробляються та покращуються для використання у різних сферах, оскільки комп'ютери мають можливість швидко навчатися та застосовувати математичні формули для роботи з великою кількістю даних. На основі бажаного результату, та наявних даних обирають різні стратегії машинного навчання, розглянемо основні з них.

Кероване навчання – підхід використовується, коли маємо повний набір вхідних та вихідних даних, дані вже поділені та помічені. Помітками виступають ознаки інформації, наприклад, пробіг автомобіля, стать користувача, кількість коментарів тощо. Ознаки вказують машині, на що саме їй дивитися. Також важливим є якість даних, вони повинні відображати реальні приклади, перед початком навчання, вони діляться на дані для навчання та для тестування. На основі останніх збираються метрики, такі як, процент успішного виконання та кількість помилок, після чого розробники вирішують, чи вдало була створена модель, і чи можна її використовувати [1].

Кероване навчання найчастіше використовується для вирішення проблем класифікації та регресії. Суть класифікації полягає у наданні набору даних, певного класу або категорії, на основі вже існуючих прикладів. На зразок, маємо класифікувати квіти по їх характеристикам, у нас є довжина стебла та листя, розмір суцвіття, також ми знаємо, які характеристики відносяться до певних сортів квітів. Після навчання комп'ютера, на реальних прикладах квітів, ми зможемо опрацьовувати велику кількість квітів за короткий проміжок часу. У свою чергу, суть регресії, це передбачення результатів, на основі вже наявних даних. Наприклад, передбачення курсу валют, динаміки акцій, тощо.

Серед основних алгоритмів виділяють дерева рішень, будують схожу на дерево карту рішень, що приймаються при класифікації об'єкта; лінійну регресію, що шукає залежності між змінними; баєсові мережі, вони дозволяють фіксувати невизначеності; логістичну регресію, яка працює з зваженими характеристиками. Кожен з алгоритмів підходить для вирішення різних задач, та різних вхідних даних, та обираються розробником, під час аналізу задачі.

Некероване навчання – використовується для навчання при відсутності ознак у даних. Даний підхід розглядає вхідні дані, що не мають прямої залежності з вихідними даними. Сама суть назви «некероване навчання», відображає у собі, що моделлю не керує людина, їй надають сукупність даних, після чого, вона самостійно починає розглядати їх та шукати залежності. На відміну від керованого навчання, дана стратегія використовується для вирішення більш складних проблем, коли залежність не може бути визначена заздалегідь [2].

Некероване навчання, має певні переваги, наприклад, дані не потрібно помічати, можна використати для процесів, суть яких ще не зрозуміла людині, краще підходить для великих наборів даних. Проте, недоліком можна зазначити непередбачуваність та меншу точність передбачень.

Як приклад використання даного підходу, можна розглянути ідентифікацію об'єктів на фотографіях. Даними є файли фотографій, що представляють набір пікселів, як результат очікується отримати класифікацію фото, на яких знаходяться коти, а на яких собаки. Людина може розрізнити тварин одним поглядом, проте для комп'ютера, це лише набір даних. Він шукає залежності самостійно, може звернути увагу на форму тіла, голови, колір вовни, при цьому не зрозуміло, на що саме дивиться комп'ютер. Проте, коли модель навчиться, вона зможе класифікувати фотографії набагато швидше ніж людина.

Основні задачі некерованого навчання розділяють на кластеризацію, асоціацію та виявлення аномалій. Кластеризація – це процес поділу даних на групи, один набір даних може належати лише одній групі. Суть асоціації полягає у виявлені залежності між групами даних. Виявлення аномалій – це процес пошуку помилок у наборі даних, коли якась кількість предметів виділяється від інших.

Серед алгоритмів, частіше всього використовують «Apriori», «ECLAT», алгоритм зростання частотного шаблону, кластеризація з використанням k-середніх та інші. «Apriori» застосовують для витягу даних з баз даних, наприклад інформації про покупки користувача. «ECLAT», схожий до «Apriori», проте він фокусується на пошуку елементів, що зустрічаються частіше інших, наприклад пошук найпопулярніших товарів. Алгоритм зростання частотного шаблону займається пошуком шаблонів, які зустрічаються у базах даних, наприклад, певна вікова група користувачів переглядають певний тип контенту. Кластеризація з використанням k-середніх групує предмети по їх ознакам та подібності. «K-середніх» вказує на кількість груп.

Обидва підходи відіграють ключову роль у сучасних задачах обробки даних та штучного інтелекту. Кероване навчання ефективне у випадках, коли є мітки для навчальних даних, і забезпечує високу точність у таких задачах, як класифікація та регресія. Воно широко застосовується у прогнозуванні, розпізнаванні об'єктів, рекомендаційних системах тощо. Некероване навчання, з іншого боку, корисне для аналізу даних без чітко визначених міток, що робить його незамінним для кластеризації, виявлення аномалій та пошуку закономірностей у великих масивах інформації. Вибір підходу залежить від специфіки задачі, структури даних та наявності міток, а їх поєднання дозволяє розширити можливості машинного навчання для створення точніших і адаптивних моделей.

1. Nasteski V. 2017 An overview of the supervised machine learning. Faculty of Information and Communication Technologies, Partizanska bb, 7000 Bitola, Macedonia. https://www.researchgate.net/profile/Vladimir-Nasteski/publication/328146111_An_overview_of_the_supervised_machine_learning_methods/links/5c1025194585157ac1bba147/An-overview-of-the-supervised-machine-learning-methods.pdf.

2. Samreen Naeem, Aqib Ali, Sania Anam, Muhammad Munawar Ahmed. (2023). An Unsupervised Machine Learning Algorithms: Comprehensive Review. International Journal of Computing and Digital Systems. 1. 911-921.

В.С. Волошин

ЩОДО ПЕРСПЕКТИВ РОЗВИТКУ ШТУЧНОГО ІНТЕЛЕКТУ В ПОРІВНЯННІ З ЛЮДИНОЮ (НА ПРИКЛАДІ МЕРЕЖІ CHATGPT)

Стрімкий розвиток сучасних систем штучного інтелекту (*AI)* вимагає більш адекватного погляду на його взаємини з людиною. Скептичні судження відомих вчених про роль штучного інтелекту у всьому розвитку цієї теми або підтверджуються [1, 2], або спростовуються цілком переконливими фактами [3, 4], яких останнім часом стає все більше. Нас цікавлять питання критеріїв оцінки впливу *AI* на ті системи, в яких на протязі тисячів років домінувала людина. Тому, що ця дискусія має в своїй підставі єдину мету: визначити місце і роль людини в конкуренції зі створеним ним самим штучним інтелектом. Ревізії підлягають твердження навіть таких відомих фахівців, як Джарон Ланьє [2], Гарі Маркус [3], Ян ЛеКун та інших про неможливість в доступному для огляду майбутньому ототожнення людського і машинного інтелекту, коли на чільне місце висуваються недосяжні для машини людські цінності.

Якщо обсяг пам'яті, який був закачаний творцями в *GPT* першого покоління було 5-40 Гбайт і така навчена нейронна мережа виявилася здатною генерувати кожен наступний параметр на основі попередніх цілих речень з високою точністю відтворення, потім *GPT3* (обсяг доступної інформації становив 570ГБайт) виявився здатним до самонавчання, самим незбагненним чином отримуючи знання в області, наприклад, математики і дозволяючи відповідати на більшість питань з цієї області далекої від текстових редакторів знань [5]. Наступна версія *GPT4* виявилася здатною формувати власну «картину світу», оперуючи знаннями з різних наукових областей. У той же час процес «самонавчання» набирає обертів у геометричній прогресії, і *ChatGPT* п'ятого покоління вже буде здатним формалізувати органи людського зору та слуху за допомогою цифрових генеративних здібностей та надати нові сфери застосування, наприклад, у сфері мистецтва [6].

В ході технічної революції людина не вперше поступово втрачає свої переваги в людино-машинних системах, поступаючись машинам [7]. Звернімося послідовно до безглуздих луддитських погромів ткацьких верстатів (1811 рік), дискусій Р. Фрімена про можливість поглинання машиною людини (1920 рік), появи повністю автоматизованих заводів (70-ті роки 20 століття), формули Цукерберга «Learn to code» у 2014 році та ін. Тим більш, така динаміка може стати актуальною в ході 4-ї технологічної революції, свідками якої ми є сьогодні.

Сучасний штучний інтелект в роботі представлений відомими системами, в основі яких, наприклад, лежить нова універсальна та масштабована архітектура генеративної нейронної мережі «*Transformer*» з високою швидкістю обробки інформації та працююча на її підставі модель *ChatGPT* (*Generative Pre-trained Transformer*). Проста оцінка кількості інформації, яку користувачі запитують та отримують за опосередкованими даними, показує цифри $2{,}16 \cdot 10^{15}$ та $1{,}38 \cdot 10^{19}$ Байт на рік, відповідно (табл. 1). Останній цифрі відповідає $1{,}0 \cdot 10^{20}$ біт інформації або, за принципом Ландауера, 9,6$\cdot 10^{-4}$ Дж енергії, необхідної для обробки цієї інформації (при кімнатній температурі 300 К).

Таблиця 1 – Оціночні характеристики системи *ChatGPT* четвертого покоління

№№	Параметр	Значення
1	Кількість користувачів *ChatGPT* на рік	200 млн
2	Кількість відвідувань на всіх платформах *ChatGPT* за рік	156,4 млрд
3	Енерговитрати на обробку інформації за рік	365 ГВт-ч
4	Споживана потужність за один запит	2,33 Вт-ч
5	Середня кількість запитів на одного користувача за місяць	300
6	Опосередкований обсяг даних на один запит (кількість слів або символів), (L_i)	500-1000 слів (4-8)КБайт

Ми розглядаємо вектор зміни ентропії як результат досягнення максимально можливої термодинамічної нерівноважності і як індикатор розвитку або деградації екосистем, до яких ми, перш за все, відносимо систему «людина-машина-середовище». Тезу про термодинамічну нерівновагу як індикатор розвитку екосистем було запропоновано І. Пригожиним у кількох своїх роботах, наприклад, [8]. Будь-яка генерація в моделях типу *GPT* супроводжується зміною ентропії, причому чим вище різноманітність виходів в нейронної моделі, тим вище навантаження на процесори, тим вище опосередкована ентропія такої системи. Для таких систем ентропію слід шукати як в якісних відношеннях енергії, так і в середньому обсязі інформації, яку можна отримати з джерела з імовірнісним розподілом можливих виходів (слів або символів).

Інформаційна ентропія ΔH, згідно формули Шеннона, в таких системах залежить від:

- архітектури моделі (загальна кількість параметрів моделі та її конфігурація) і можливість генерації різноманітних виходів, що, в кінцевому результаті, визначає напрямок зміни ентропії;

- обсяг навчального масиву (чим більше і різноманітніше вихідні дані, тим вище здатність генерувати нові і несподівані виходи і тим більше ентропія системи);

Якщо прийняти до уваги тільки термодинамічні процеси, (наприклад, описані в теоремі І. Пригожина), згідно з якими в будь-якій енергетичній системі, що прагне до синергізму, можливі процеси емісії ентропії в

надсистему і протилежні процеси викиду в систему якісної енергії, то ми зіткнемося з деякими цікавими проявами термодинамічної нерівноважності для системи «людина-машина», якщо під «машиною» розуміти штучний інтелект і його технічне забезпечення. Запишемо цю теорему для нашої цілі так:

$$(\pm)\Delta S_e = \sum_\gamma [\sigma_\gamma(\Delta\tau) - J_\gamma \nabla\mu]\Delta\tau, \quad (1)$$

де: ΔS – вектор зміни ентропії за певний проміжок часу $\Delta\tau$;
$\sigma_\gamma(\Delta\tau) = \sigma/\tau$ – внутрішня швидкість створення ентропії шляхом γ –збурення;
J_γ- зовнішній потік енергії щодо γ – збурення;
$\nabla\mu = (\frac{\delta\mu}{\Delta x}, \frac{\delta\mu}{\Delta y}, \frac{\delta\mu}{\Delta z})$ - градієнт термодинамічного потенціалу.

Сумарна зміна ентропії $\pm\delta S = (\pm)\Delta S + \Delta H(n_i)$ показує напрямок швидкості такої зміни при наявності зовнішнього потоку енергії, а розрахункові дані для цього наведені в табл. 2.

Таблиця 2 – Оціночні дані для розрахунку зміни ентропії в системі штучного інтелекту *GPT4*

Загальний баланс енергії для навчання *з GPT4*	$6{,}6 \cdot 10^6$ *Дж*	Розрахунковий базовий рівень зміни ентропії при роботі користувача в одному запиті	(26,57 бит) $2{,}54 \cdot 10^{-22}$ Дж/К (Т=300К)
Енергія для обробки запитів у *GPT4*	$72 \div 180$ Дж/запит	Загальне енергоспоживання *GPT4:* обслуговування одного користувача за один запит	$3{,}6 \cdot (10^5 \div 10^6)$ Дж
Загальна енергія для виведення інформації в *GPT4*	$1{,}8 \cdot 10^8$ Дж/доб	Одночасна кількість користувачів в мережі *chatGPT4*	10^5
Загальний обсяг пам'яті в *GPT4*	$7{,}0 \cdot 10^{11}$ Байт	Обсяг унікальних токенів n_i Обсяг токенів, що повторюються n_j	$2{,}0 \cdot 10^{11}$ Байт $5{,}0 \cdot 10^{11}$ Байт
Обсяг навчальних даних в *GPT4*	$5 \cdot 10^{14}$ Байт	Обсяг унікальних токенів n_i Обсяг токенів, що повторюються n_j	$4{,}0 \cdot 10^{14}$ Байт $1{,}0 \cdot 10^{14}$ Байт
Розрахункова середня оцінка зміни ентропії системи	2,66 біт/запит	Імовірнісний розподіл інформації $P(n_j)$	$0{,}1 \div 0{,}95$
Площа поверхні планети з доступом до Інтернету	$3{,}7 \cdot 10^{16}$ $м^2$		

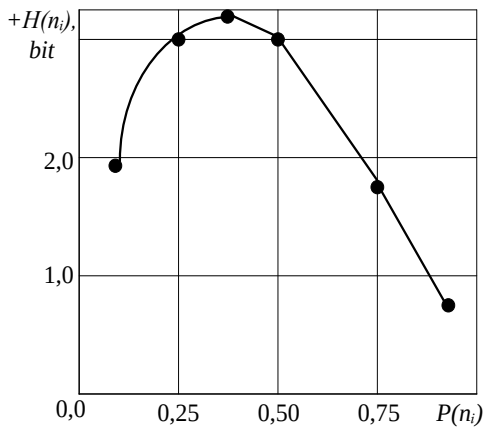


Рисунок 1 – Розподіл інформаційної ентропії,що відповідає одному запиту одного користувача в *ChatGPT4 у* залежності від інформативності системи

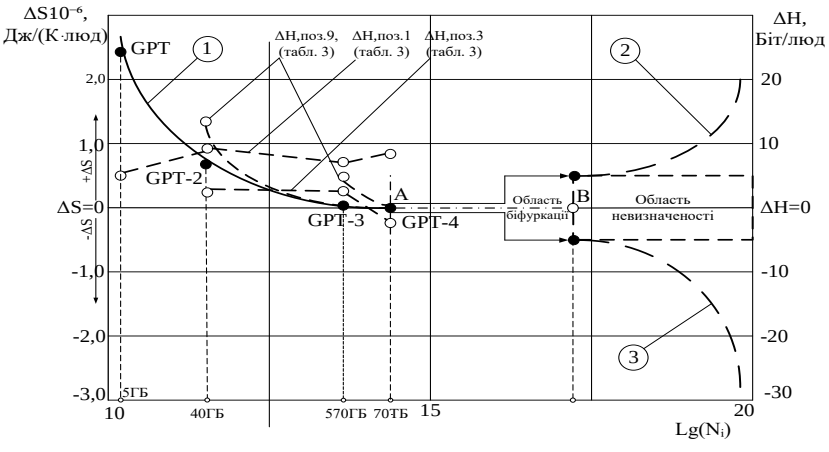


Рисунок 2 – Відносна зміна ентропії під час функціонування різних, що відповідає версій *ChatGPT* з розрахунку одного користувача на рік: 1 – фактичні розрахункові дані; 2 – розрахункові дані для *AI* як об'єкта в системі «людина-машина»; 3 – розрахункові дані для *AI* як суб'єкта в системі «людина-машина»

Звернемося до розрахунку ентропії, що супроводжує роботу штучного інтелекту, на прикладі (рис. 1). Інформація, що генерується в такому джерелі *AI*, не може не мати власної ентропії, принаймні за формулою Шеннона $\Delta H(n_i) = -\sum_{i=1}^{I} P(n_i) log_2 P(n_i)$. Найпростіші оцінки показують, що чиста зміна ентропії в джерелі *GPT,* що приходиться на одного користувача за один інформаційний запит для генерації дуже мала $\Delta H(n_{1,1}) = +2{,}657$ біт або при температурі 300 К - це 2,54· 10^{-23} Дж/К (див. табл. 1). Але для загального числа користувачів $2 \cdot 10^8$ при загальній кількості 1,56· 10^{11} запитів, кожен з яких може містити $L_i = (4 \div 8)$ КБайт інформації, сумарна зміна ентропії всієї інформаційної системи вже складає відчутні $3{,}96 \cdot 10^{-10}$ Дж/К, що робить її порівнянною з іншими типовими видами людської діяльності.

Таблиця 3 – Фактори, що впливають на зміну ентропії для користувача в процесі використання *ChatGPT4*

Позитивний вплив		**Негативний вплив**	
Показник	**%**	**Показник**	%
Складність завдання	30	Одноманітність запитів. Повторення	32
Унікальність запитів	23	Вузька тематика, обмеження однією темою	23
Контекст і формулювання завдань	17	Ступінь передбачуваності відповіді	13
Широка тематична спрямованість	10	Стандартні формулювання	12
Кількість виконаних завдань	6	Кількість виконаних завдань	9
Креативність користувача	6	Креативність користувача	7
Ступінь передбачуваності	3	Відсутність інтерактивності	4
Інтерактивність та зворотній зв'язок	2		
Параметри моделі *GPT4*	2		

Беручи до уваги претензії вектора зміни ентропії щодо оцінки термодинамічної нерівноважності як показника ефективності в системах *AI*, необхідно обґрунтувати його можливості (табл. 3). Вони полягають у наступному:

- мінімальну ентропію в системі *AI* можна досягти за рахунок монотонності завдань, вузької та спеціальної тематики, повторного використання відповідей та відсутності креативності;
- складність і унікальність завдань призводить до збільшення часу їх виконання і зростанню ентропії і залежить від оптимізації моделі і наявних ресурсів;
- зі збільшенням кількості завдань, що обробляються в *GPT* модель може стати більш ефективною у відповідях, що призводить до зниження ентропії;
- зі збільшенням досвіду роботи з моделлю компетенції користувача зростають, але не досягають верхньої межі, і унікальність завдань не зникає повністю, завдяки різноманітності контексту і формулювань в *Prompt*.
- при тривалому використанні моделі все більша кількість завдань стають тривіальними і ентропія для такого користувача поступово мінімізується. Хоча унікальність в *Prompt* не зникає повністю, навіть у типових завданнях. Рівень ентропії завжди підтримується непередбачуваністю запитів користувача і його креативністю, як одною з властивостей когнітивності людини;
- якщо креативність виконуваних завдань залишається незмінною, то твердження про мінімізацію ентропії в процесі використання моделі стає більш обґрунтованим.

У міру зростання складності або унікальності нових символів в рядку генерації ми неминуче прийдемо до стану мінімально змінного ентропійного насичення (точка *A*, рис. 2), навіть незважаючи на зростання використаних обчислювальних потужностей. У той же час, відносно невеликі зміни ентропії будуть пов'язані з генерацією в *GPT4* інформації загального стандартного типу. Генеруюча мережа буде здатною протягом тривалого часу створювати стандартні і загальноприйняті результати (знаки, символи, слова). Через певний сукупний інтервал $N(B) \div N(A)$ система може бути здатною вийти з цього рівня насичення в точці *B* (див. рис. 2). Але при цьому, згідно з самими оцінковими розрахунками, ми будемо мати справу з біфуркаційними процесами і вже не зі збільшенням зміни ентропії, а з можливим її зменшенням.

1. Можна лише припустити, що однією з причин такої поведінки майбутньої системи штучного інтелекту будуть ті ж самі процеси, які послідовно проявлялися в *GPT4* і, можливо, в моделях *GPT5*, за рахунок різкого збільшення обсягу інформаційного контенту та відповідних синергетичних ефектів для вже не суто лінгвістичної моделі, яка самостійно генерує здатність створювати власну «картину світу».

2. Другим фактором на користь такого синергетичного ефекту, який безсумнівно пов'язаний з термодинамічною нерівноважністю системи, є зміна пріоритетів для логічних зв'язків в системі "людина-машина". Вона може полягати в набутті системою штучного інтелекту права *суб'єктності* та залишенні за людиною права *об'єктності* з відповідними змінами причинно-наслідкових зв'язків. Тобто штучний інтелект потенційно міг би стати здатним позбутися людської залежності (прогнозовані залежності праворуч від точки *B,* див. рис. 2). Причиною цього може стати фактор наближення знову набутих якостей штучного інтелекту до того, що відносилося тільки для людини і було «табу» для машин. Це є когнітивність.

Когнітивні здібності людини завжди були безумовною перевагою між нею та штучним інтелектом, яку *AI* як «безнервова» система не в змозі подолати [2].

Природа здатна демонструвати форми поведінки, які виконують завдання, схожі на когнітивні, але використовує інші механізми, наприклад, від колективного інтелекту у комах до епігенетичної адаптації у рослин і нейронних мереж у восьминогів. Таким чином, формувати поведінку нейронних мереж у системах *AI* з функціями, схожими на когнітивізм у людей - можливо. І, безумовно, важливими є умови для виникнення штучного механізму «когнітивізму» для *AI*.

Сьогодні нейронні мережі, такі як *GPT4* і, судячи з усього, *GPT5* здатні до прояви деяких якостей, які можна порівняти з когнітивними якостями самої людини (табл. 4). Поки що, без урахування її емоційного контенту.

Таблиця 4 – Порівняння когнітивних параметрів людини з відповідними технічними параметрами штучного інтелекту (заштриховані області дають уявлення про переваги тієї чи іншої системи)

	Людина і її когнітивність	**Штучний інтелект**
1	Інтуїтивно зрозумілий вибір опцій	Механічне перерахування варіантів
2	Сприйняття образів	Контекстне розпізнавання образів. «Картина світу» як основа сприйняття
3	Здатність обробляти інформацію	Цифрова обробка інформації
4	Адаптація до вирішення завдань	Алгоритм, чітко структуровані дані
5	Уважність. Вміння фокусуватися та перемикатися між завданнями	Безпомилкова обробка інформації. Attention Mechanisms. Паралельність.
6	Оперативне управління пам'ятю в $3 \cdot 10^{12}$ Байт	Оперативне управління пам'яттю в $9 \cdot 10^{22}$ байт
7	Навчання на підставі досвіду	Deep Learning, Reinforcement Learning,
8	Логічне мислення	Логічна обробка інформації.
9	Креативність	Генеративні моделі: *GPT4, GANs* та ін.
10	Эмоційний контекст	-

Головна мета – здатність до саморозвитку *AII,* освоєння нових знань за допомогою відомих досягається простим збільшенням гіперпам'яті та високою швидкістю її обробки даних за допомогою спеціалізованої регенеративної нейронної мережі «*Transformer*». Зокрема, це стосується:

- формування зовсім іншої, спеціалізованої логіки миттєвого пошуку варіантів, яка забезпечується *AI* і виявляється кращою перед когнітивною вибірковою логікою людини за рахунок досягнутих безпрецедентних обсягів пам'яті та величезної швидкості її обробки;

- здатність у *AI* до пізнання «картини світу», через ще доки незрозумілі процеси розуміння причинно-наслідкових зв'язків між різними генеративними об'єктами в сучасній оцифрованій «картині світу», дозволила дещо нівелювати головну відмінність людини від «машини» - її когнітивне сприйняття цього світу. Це прямий шлях до пізнання непізнаного в умовах невизначеності;

- можливості генеративних систем, що здатні навчатися, коли механічний підбір вагових коефіцієнтів дає можливість налаштувати нейронну мережу на кінцевий результат, який можна порівняти з емпіричним навчанням «через життєвий досвід». Більш сучасні адаптивні системи навчання, наприклад, *Deep Learning, Reinforcement Learning*, дозволяють наблизити *AI* до цієї найважливішої області людського пізнання;

- перспективи оволодіння на рівні *GPT5* ($1 \cdot 10^{14}$Байтів інформації та $5 \cdot 10^{12}$ параметрів) здатністю кваліфіковано оперувати цифровою інформацією в сфері образотворчого мистецтва, музики, кіно, театру, шляхом створення штучних картин, музичних творів, сценаріїв та нових книжкових сюжетів у стилі геніальних майстрів. Ті галузі знань і навичок, якими людина оперує тільки за допомогою функцій органів зору, слуху, уяви і т. д., *GPT5* зможе опосередковано використовувати через «оцифровані» моделі таких даних в своєму регенеративному методі.

Такі моделі вже здатні «розуміти» не лише логіку подій, а й логіку оцифрованих почуттів людини. І досягається це поки що лише простим збільшенням гіперпам'яті, яка знаходиться у високошвидкісній обробці спеціальною нейронною мережею. Результатом можуть стати процеси саморозвитку для *AI* та можливий початок тріумфу її спеціалізованої регенеративної логіки над незрозумілою раніше людською когнітивністю.

Висновки (гіпотеза).

1. У стандартній ситуації, коли людина, творець *AI,* є суб'єктом для інформаційної системи, вектор зміни ентропії для такої системи прагне до позитивного зростання з усіма витікаючими наслідками щодо вектора в бік термодинамічної рівноважності.

2. У той же час в межі, коли ймовірність події прагне до $P(n_i) \approx 1{,}0$, зміна ентропії буде прагнути до нуля. До тих пір, поки не настане якийсь гіпотетичний момент, в який зміна ентропії знову настане.

3. Якщо система *AI* не замкнута і термодинамічно далека від рівноваги, то її наступні стани повинні відображати відносини з ентропією на кордоні біфуркаційних змін, які в принципі неможливі при наявності імовірнісних відношень. Але якщо вони виникають як протиріччя формулі Шеннона, то цей випадок може мати місце тільки тоді, якщо *суб'єктність і об'єктність* в системі поміняються місцями. Біфуркація не може

відповісти на це питання. Можна тільки припустити, що зміняться суб’єктно-об’єктні відносини між частинами сильно взаємопов'язаної людино-машинної системи.

1. Crawford, K. Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. Yale University Press. 2021 – 74 pp.

2. Lanie J. En Arguments for Deleting Your Social Media Accounts Right Now. Vintage, 2018. - 176 pp.

3. Marcus G., Devis E. Rebooting AI: Building Artificial Intelligence We Can Trust. Pantheon, 2019. – 178 pp.

4. Mitchell M. Artificial Intelligence: A Guide for Thinking Humans. Farrar, Straus, Ziru, 2019. – 336 pp.

5. Devlin J, Chang M.-W., Lee K., Toutanova K. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. Computer Science, 2018. https://arxiv.org/abs/1810.04805.

6. Broun T. et al. Language Models are Few-Shot Learners. Brown et al. Computer Science - Computation and Language, 2020. https://arxiv.org/abs/2005.14165.

7. Markoff J. Machines of Loving Grace: The Quest for Common Ground Between Hummans and Robots. Ecco, 2015. – 400 pp.

8. Prigogine I., George C. The Second Law as a Selection Principle: The Microscopic Theory of Dissipativ Processes in Quantum Systems// Proceeding of the National Academy of Science. 1983. Vol.80. P.4590-45945.

Ю.А. Климець

СМАРТ-КОНТРАКТИ ДЛЯ ЦИФРОВИХ АКТИВІВ У ДЕЦЕНТРАЛІЗОВАНІЙ ЕКОСИСТЕМІ

У цій роботі розглянуто поняття смарт-контрактів, їх роль у децентралізованих екосистемах та криптовалютах, зокрема на прикладі Ethereum. Було проаналізовано переваги, які смарт-контракти надають користувачам, а також ризики, з якими вони можуть зіткнутися, такі як ризик контрагента та регулювання. Окрему увагу приділено питанням кібербезпеки та впливу на розвиток DeFi екосистем.

Ключові слова: смарт-контракт, блокчейн, DeFi, Ethereum, криптовалюта, ризик контрагента, кібербезпека.

Актуальність смарт-контрактів зростає у зв'язку з поширенням децентралізованих фінансів (DeFi), що автоматизують фінансові операції та відкривають нові можливості для користувачів. Це знижує необхідність посередників і сприяє розвитку нових бізнес-моделей на базі блокчейну.

Метою роботи є дослідження смарт-контрактів, їхнього впливу на децентралізовані екосистеми, аналіз ризиків, які виникають у процесі їх використання, а також вивчення заходів безпеки в контексті DeFi.

У роботі здійснено детальний аналіз принципів функціонування смарт-контрактів на блокчейнах, зокрема на платформі Ethereum, та їхній вплив на децентралізовані фінансові системи. Розглянуто переваги, які смарт-контракти забезпечують у сфері автоматизації фінансових операцій, а також ключові ризики, з якими стикаються користувачі, зокрема ризик контрагента та регулятивні виклики. Проведено дослідження сучасних рішень у галузі кібербезпеки для захисту децентралізованих екосистем від потенційних загроз.

Було проаналізовано смарт-контракти на базі Ethereum та інших блокчейнів з Layer 2 рішеннями, таких як Optimism, StarkNet, Arbitrum. Окрім цього, розглянуто конкурентні блокчейни, такі як Solana, Polkadot та Avalanche, з акцентом на їхні переваги в швидкості транзакцій та нижчих комісіях.

Проведено аналіз роботи смарт-контрактів, визначено ключові переваги для користувачів у сфері DeFi, такі як автоматизація позик, кредитування та торгівля. Оцінено ризики, пов'язані з регулюванням та контрагентами, а також розглянуто питання кібербезпеки децентралізованих систем.

Смарт-контракти є ключовим елементом у розвитку DeFi та криптовалютних екосистем. Попри свою привабливість, вони несуть певні ризики, що потребують додаткових заходів захисту. Подальший розвиток децентралізованих екосистем буде залежати від технічних інновацій та кібербезпеки

1. Павло Кравченко, Богдан Скрябін, Оксана Дубініна, Олександр Курбатов (2015) – «Блокчейн і децентралізовані системи».
2. Дон Тепскотт, Алекс Тепскотт (2015) – «Блокчейн і революція».

Є.О. Васильєва

ЯК ШТУЧНИЙ ІНТЕЛЕКТ ДОПОМАГАЄ УПРАВЛЯТИ МАРКЕТИНГОВИМИ БЮДЖЕТАМИ І СКОРОЧУВАТИ ВИТРАТИ?

Головна задача будь-якого бізнесу – досягти максимального прибутку при мінімальних витратах. За даними Forbes, застосування штучного інтелекту може прискорити виробничі процеси на 50%, знизити витрати на 20% і підвищити якість кінцевого продукту на 60% [1]. Стрімкий розвиток ШІ відкриває нові можливості для оптимізації маркетингових процесів. Управління маркетинговим бюджетом є одним з ключових завдань, що впливає на ефективність введення сучасного бізнесу. Сьогодні широкий інструментарій із технологіями ШІ дозволяє підвищувати точність прогнозів та допомагає уникати зайвих витрат на маркетингові кампанії.

Завдяки алгоритмам машинного навчання, ШІ має змогу проводити аналіз великих обсягів даних, що не лише прискорює процеси, а й допомагає виявляти закономірності, які дозволяють прогнозувати майбутні витрати із високою точністю. Згідно з дослідженням PwC, штучний інтелект може підвищити точність даних до 80%, а вірогідність допущення помилок дорівнює лише 1,9% [2]. Інструменти, такі як Google Analytics 4, дозволяють передбачати майбутні тренди і оптимізувати рекламні кампанії. До того ж аналізуючи великі дані, алгоритми здатні виявляти помилки та попереджати про них у разі необхідності, що суттєво знизить ризик провалу [3]. Використовуючи попередні дані про ефективність минулих маркетингових кампаній, ШІ має можливість визначати оптимальний бюджет для майбутніх проєктів, а це своєю чергою, запобігає перевитраті коштів компанії.

Досягнення бізнесом максимальної рентабельності можливе завдяки постійному контролю витрат та аналізу результатів. Інструменти управлінського обліку, бізнес-аналітика та ШІ в тандемі дозволяють в реальному часі відстежувати динаміку витрат та дають можливість своєчасно виявляти неефективні кампанії і перенаправляти бюджет на більш результативні канали. Такі інструменти не лише оптимізують використання бюджету, а й покращують показники ROI. Показник ROI (Return on Investment) дозволяє оцінити ефективність маркетингових інвестицій.

Завдяки безперервному розвитку та появі нових інструментів з вбудованим ШІ, створення різноманітного контенту, від рекламних текстів до короткометражних відео, стало швидким та доступним. Інструменти ШІ, такі як DALL-E і MidJourney, дозволяють бізнесам суттєво скоротити витрати в цьому напрямку і оперативно реагувати на постійні зміни як на вітчизняному, так і на закордонних ринках.

Можливості штучного інтелекту (ШІ) у клієнтському обслуговуванні є ключовим фактором підвищення ефективності та задоволеності споживачів. Однією з найбільших переваг є забезпечення цілодобового обслуговування без необхідності залучення додаткового персоналу. Завдяки чат-ботам та іншим ШІ-технологіям компанії можуть безперервно надавати підтримку клієнтам незалежно від їхнього місцезнаходження чи часового поясу. Це особливо актуально для глобальних ринків, де бізнесу необхідно адаптуватися до різних часових зон. І найголовніше, що автоматизація рутинних завдань та розвантаження менеджерів дозволяє персоналу зосередитися на більш стратегічних і творчих задачах, таких як вирішення складних питань клієнтів чи розробка нових послуг.

Крім того, долучаючи ШІ до процесу персоналізації, можна значно покращити рівень залученості та конверсії для бізнесу. Платформи для email-маркетингу з функцією ШІ дозволяють створювати персоналізовані розсилки, які враховують індивідуальні вподобання кожного клієнта. Під час проведення сегментації та аналізу поведінки споживачів, алгоритми ШІ можуть точно визначити, які канали комунікації та повідомлення є найбільш ефективними для кожної групи клієнтів [4].

Штучний інтелект стає незамінним інструментом для сучасного бізнесу, особливо в оптимізації маркетингових витрат. Його здатність до автоматизації, аналізу великих даних, створення контенту та персоналізації робить його невід'ємним елементом сучасних маркетингових стратегій.

Таким чином, ШІ стає незамінним інструментом для сучасного бізнесу, особливо в оптимізації маркетингових витрат. Однак, не варто забувати, що ШІ – це лише інструмент, який допомагає приймати рішення. Роль людини в маркетингу залишається важливою, особливо в таких аспектах, як стратегічне планування, креативність та етична відповідальність.

1. Top AI statistics and trends. Forbes Advisor URL: https://www.forbes.com/advisor/in/business/ai-statistics/.
2. Data accuracy Critical to success: Leveraging Artificial intelligence for Business growth. V500 Systems. URL: https://www.v500.com/accurate-ai/.
3. Аналіз даних і ШІ: як це працює. Claspo.io. URL: https://claspo.io/ua/blog/data-analytics-ai-how-it-is-used/.
4. Персоналізація та штучний інтелект у продажах та маркетингу - Блог на Brainberry.ua. URL: https://brainberry.ua/uk/newsroom/blog/personalization-and-ai-in-sales-and-marketing.

Б.С. Калинюк

ОПТИМІЗАЦІЯ ЕНЕРГОЕФЕКТИВНОСТІ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ, ЩО ВИКОРИСТОВУЄ АГЕНТИ ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ ДЕФІЦИТУ ЕНЕРГОНОСІЇВ

Із зростанням складності інформаційних систем і збільшенням використання енергії у серверній інфраструктурі, оптимізація енергоефективності стала одним з ключових напрямів досліджень та розробок. Використання мікросервісної архітектури дозволяє гнучко масштабувати й налаштовувати різні частини системи, однак супроводжується значним енергоспоживанням через паралельну роботу численних сервісів, зокрема за використання паралельних обчислень.

Формулюючи проблему неефективності енергоспоживання рішень, що базуються на мікросервісній архітектурі, є важливий аспект даного питання в ситуації енергодефіциту, який, зокрема, склався в Україні через повномасштабну агресію Росії. Вирішення питання оптимізації ресурсів дозволяє реалізовувати певні програмні рішення або комлекси рішень без потенційного урізання функціональності. Прискіплива увага до деталей в проектуванні систем, вибору технологій, взаємодії модулів і підходів до безпосередньої імплементації може дозволити побудувати функціональну систему з відносно низьким споживанням ресурсів.

Це особливо критично в умовах дефіциту енергоносіїв. У такому контексті агенти штучного інтелекту (ШІ) можуть забезпечити гнучке управління енергією, автоматично адаптуючи стан системи до потреб користувачів і знижуючи зайве навантаження. Дослідження показують, що впровадження агентів ШІ допомагає ефективно контролювати активність мікросервісів, оптимізуючи енергоспоживання [1].

Вирішувати задачі неефективності енергоспоживання системи з мікросервісною архітектурою можна різними методами, залежно від безпосередньої реалізації. Зокрема важливо виділити оптимізацію саме систем з ШІ, так як для його роботи залучається велика кількість ресурсу паралельних обчислень, а робота моделей є не завжди оптимальною. Це дає простір для оптимізації і підвищення ефективності. Зокрема в конткесті роботи з різними моделями ШІ можна запропонувати декілька підходів, а саме:

1. Розподіл системи на модулі з різними станами активності
2. Оптимізація навчання і перенавчання моделей ШІ за рахунок кешування результатів
3. Зменшення обсягу даних для навчання без втрати ефективності
4. Регулювання навантаження за допомогою агентів ШІ

Окремо важливо зазначити, що використання ШІ не є найбільш ефективним способом для оптимізації енергоефективності, так як самі системи ШІ є доволі енергоємними, проте ШІ дозволяє керувати навантаженням і передбачати його піки, що в комбінації з традиційними існуючими методами дає гнучке рішення проблеми.

1. Розподіл системи на модулі з різними станами активності

В основі енергоефективної мікросервісної архітектури лежить ідея розподілу системи на окремі модулі, кожен з яких може переходити в різні стани активності. Уявімо систему, яка може працювати в «активному», «напівактивному» та «пасивному» режимах залежно від інтенсивності запитів. Коли навантаження на систему знижується, агенти ШІ можуть тимчасово переводити деякі мікросервіси в пасивний стан, що дозволяє зменшити споживання енергії [2].

Наприклад, в електронній комерції модуль управління транзакціями може бути активним лише в години пік і переходити у напівактивний режим поза ними, що значно знижує енерговитрати. Агент ШІ моніторить активність користувачів і автоматично коригує стан модулів. Це дозволяє не лише зберігати енергію, але й підвищувати стійкість системи до енергетичних обмежень [3].

2. Оптимізація навчання і перенавчання моделей ШІ за рахунок кешування результатів

В мікросервісній архітектурі, в якій є модулі з ШІ, процеси навчання та перенавчання моделей ШІ зазвичай супроводжуються високим споживанням енергії. Оптимізація цього процесу з використанням кешування результатів дозволяє зменшити навантаження на обчислювальні ресурси, зберігаючи при цьому ефективність системи. Кешування передбачає збереження результатів певних обчислень, щоб уникнути їх повторного виконання при ідентичних запитах [4].

Цей підхід особливо корисний для систем з постійно повторюваними запитами. Наприклад, якщо певний набір даних обробляється з однаковими параметрами, збереження результатів може знизити потребу у частих зверненнях до моделі, що зменшує навантаження на систему та енергоспоживання. Дослідження Zhang і Huang [5] показують, що кешування може зменшити кількість звернень до моделей на 40%, що суттєво знижує витрати енергії.

Для підбору даних, що необхідно кешувати, можна також використовувати агенти ШІ, які динамічно зможуть регулювати об'єми кешу і його наповнення. При чому, цей підхід є доволі практичним, якщо такі модулі вже використовуються в системі. В такому випадку не потрібно додавати нові модулі-оркестратори, а достатньо налаштувати існуючі модулі на потрібний патерн принципу кешування.

3. Зменшення обсягу даних для навчання без втрати ефективності

Зменшення обсягу даних для навчання є ще одним ефективним підходом до зниження енергоспоживання системи. Агенти ШІ можуть бути налаштовані для вибіркового збору та обробки даних, що забезпечує навчання моделей на основі найбільш інформативних даних, а не всіх наявних. Це дозволяє уникнути обробки зайвої інформації, яка не має істотного впливу на якість моделі [6].

Для цього можуть використовуватись методи вибірки або відсіювання менш важливих даних. Також корисним є підхід скорочення розмірності даних, наприклад, з використанням алгоритмів PCA (Principal Component Analysis). Дослідження Lee та Park [7] показують, що зменшення розмірності дозволяє скоротити витрати на обробку даних до 30% без втрати ефективності моделей. Це сприяє підтриманню високої точності і продуктивності ШІ-моделей з одночасним зменшенням енергоспоживання, особливо якщо моделі ШІ можуть динамічно змінювати розмірність даних, або розріджувати їх за потреби.

4. Регулювання навантаження за допомогою агентів ШІ

Регулювання навантаження в розподілених системах є важливим компонентом для забезпечення енергоефективності. Важливим нюансом є типи модулей в системі і чи використовуються модулі ШІ, які здатні до саморегуляції. Якщо система є консервативною мікросервісною системою, то впровадження агентів ШІ, що базуються на мовних моделях зокрема, може дозволити не тільки реалізувати систему керування ефективністю, а також дозволити інженерам керувати самою системою-оркестратором з впровадженням бажаних сценаріїв енергоефективності. Агенти ШІ дозволяють ефективно керувати ресурсами системи, розподіляючи навантаження між сервісами з урахуванням їхньої активності та енергоспоживання. Вони можуть оцінювати поточний стан кожного мікросервісу і коригувати розподіл обчислювальних потужностей у реальному часі [8].

Наприклад, агенти можуть встановлювати пріоритети для виконання завдань, орієнтуючись на критичність кожного запиту, забезпечуючи стабільну роботу системи навіть при обмежених ресурсах. Дослідження Martin та Garcia [9] показують, що такі алгоритми зменшують середнє навантаження на кожен мікросервіс до 25%, що значно знижує витрати на енергоспоживання. Це дозволяє забезпечити ефективне обслуговування запитів і підтримувати стабільність системи навіть при обмежених енергетичних ресурсах.

В умовах дефіциту енергоносіїв використання агентів ШІ для оптимізації енергоефективності мікросервісної архітектури має значний потенціал. Поєднання підходів до зниження навантаження, оптимізації активності модулів, зменшення обсягів даних для навчання та управління ресурсами дозволяє значно скоротити енергоспоживання без втрати продуктивності системи. Подальші дослідження можуть зосередитися на розробці нових алгоритмів адаптації агентів ШІ, що дозволить забезпечити ще більш високу ефективність використання енергетичних ресурсів.

1. Chen, L., & Xu, W. (2021). Energy-Efficient Microservices Management in Cloud Environments. Journal of Cloud Computing, 10(3), 67–80.
2. Patel, S., & Kundu, A. (2021). Dynamic Energy Management in Modular Systems. IEEE Transactions on Systems, Man, and Cybernetics, 51(2), 215–230.
3. Smith, R., & Jones, D. (2020). Adaptive Module Activity in AI-Driven Microservices. Journal of AI Research and Development, 15(4), 450–467.
4. Thomas, J., & Wright, P. (2022). Efficient Model Retraining in Resource-Constrained Environments. Journal of Machine Learning Research, 23(7), 365–387.
5. Zhang, Y., Wu, Q., & Huang, T. (2020). Caching Strategies for Efficient Model Inference in AI-Powered Microservices. IEEE Transactions on Cloud Computing, 9(1), 43–55.
6. Kossak, M., & Friesen, A. (2019). Smart Data Selection for Sustainable AI Training. Journal of Computational Intelligence, 28(2), 160–175.
7. Lee, D., & Park, S. (2019). Data Reduction Techniques for Sustainable Machine Learning. Machine Learning Journal, 128(2), 567–590.
8. Novak, L., & Thompson, B. (2021). AI-Driven Load Balancing in Distributed Systems. IEEE Transactions on Parallel and Distributed Systems, 32(11), 2930–2942.
9. Martin, J., & Garcia, M. (2022). AI-Driven Load Management in Distributed Microservices. Journal of Artificial Intelligence Research, 49(6), 889–902.

А.О. Кримська

ШТУЧНИЙ ІНТЕЛЕКТ У ПРОГНОЗУВАННІ АВАРІЙНИХ СИТУАЦІЙ ТА МОНІТОРИНГУ КРИТИЧНИХ ОБ'ЄКТІВ ЕНЕРГЕТИКИ

Штучний інтелект у прогнозуванні аварійних ситуацій та моніторингу критичних об’єктів енергетики відкриває нові можливості для забезпечення стабільності й безпеки енергетичної інфраструктури. Критичні енергетичні об'єкти потребують постійного контролю, адже їхня стабільна робота є основою економічного розвитку, національної безпеки та суспільного добробуту. Застосування штучного інтелекту дозволяє аналізувати великі обсяги даних, які надходять із сенсорів та моніторингових систем у реальному часі, що сприяє швидкому виявленню аномалій і потенційних загроз.

Наукова значимість таких технологій полягає в розробці передбачувальних моделей, які здатні точно визначати ризики на основі історичних даних та поточних умов. Це відкриває перспективи для створення алгоритмів, що можуть оперативно виявляти критичні зміни у функціонуванні об'єктів та прогнозувати розвиток аварійних ситуацій. Практична цінність таких систем проявляється в мінімізації ризиків збоїв, що знижує витрати на ремонт та профілактичне обслуговування, а також захищає персонал і споживачів від можливих небезпек, сприяючи безперервності та надійності роботи енергетичних систем.

Метою дослідження є вивчення можливостей застосування штучного інтелекту для підвищення ефективності прогнозування аварійних ситуацій і моніторингу критичних об’єктів енергетичної інфраструктури.

Завдяки здатності обробляти великі обсяги даних із сенсорних мереж у реальному часі, алгоритми штучного інтелекту дозволяють оперативно виявляти аномальні патерни, що можуть свідчити про підвищений ризик аварій. У сучасних енергетичних системах, що охоплюють різні види інфраструктури, такі як електростанції, розподільчі мережі, трубопроводи та сховища палива, застосування інтелектуальних систем дозволяє значно знижувати ймовірність несподіваних збоїв, а також мінімізувати витрати на ремонт і технічне обслуговування [1] (табл.1).

Таблиця 1 – Порівняльна характеристика основних алгоритмів штучного інтелекту для прогнозування аварійних ситуацій в енергетичному секторі

Алгоритм	Опис	Переваги	Недоліки
Рекурентні нейронні мережі (RNN)	Моделі, які враховують часову послідовність даних і дозволяють прогнозувати на основі попередніх значень	Висока точність у роботі з послідовними даними	Висока обчислювальна складність
Випадковий ліс (Random Forest)	Алгоритм, що комбінує кілька дерев рішень для покращення точності класифікації	Стійкість до перенавчання, здатність працювати з великими даними	Може бути складним для інтерпретації
Градієнтний бустинг	Метод, що ітеративно підвищує точність за допомогою послідовного додавання нових дерев	Висока точність, хороша ефективність при прогнозуванні	Може потребувати значних обчислювальних ресурсів
Метод k-середніх (k-means)	Алгоритм кластеризації, що групує дані за схожими характеристиками	Простота, швидкість у класифікації	Обмеження у точності, чутливість до вибору кількості кластерів

Джерело: сформовано автором на підставі [2]

Сучасне використання алгоритмів штучного інтелекту для прогнозування аварійних ситуацій активно впроваджується в Україні, особливо у зв’язку з потребами підвищення безпеки критичної інфраструктури під час воєнних дій. Наприклад, на атомних електростанціях, таких як Запорізька та Південноукраїнська, застосовуються алгоритми рекурентних нейронних мереж для моніторингу температури реакторів і критичних компонентів. Це дозволяє заздалегідь виявляти можливі перегрівання, що знижує ризик аварій у разі перебоїв в енергопостачанні або атак.

Алгоритми випадкового лісу і градієнтного бустингу використовуються в операторів енергетичних систем, таких як НЕК «Укренерго», для моніторингу та аналізу змін у споживанні електроенергії, що стало особливо актуальним в умовах масованих обстрілів енергетичної інфраструктури. Такі алгоритми дозволяють передбачати потенційні навантаження, вчасно відреагувати на аномальні сплески та мінімізувати ризики перевантажень мережі під час критичних ситуацій.

Щодо транспортування нафти і газу, наприклад, в «Укргазвидобування» застосовується метод k-середніх для аналізу тиску у трубопроводах. Цей підхід є надзвичайно важливим для виявлення аномалій, які можуть вказувати на витік або пошкодження, що підвищує рівень безпеки та знижує витрати на ремонт і технічне обслуговування. Порівняно з іншими країнами, Україна швидко адаптує ці інструменти у зв’язку з актуальними безпековими викликами та досвідом країн, таких як Польща та Естонія, які також використовують алгоритми штучного інтелекту для забезпечення безпеки в умовах зовнішньої загрози.

Використання штучного інтелекту для моніторингу критичних об’єктів зіштовхується зі специфічними технологічними викликами, які виходять за рамки загальних обмежень алгоритмів. Основною проблемою є обробка різнорідних даних у реальному часі, коли системи повинні враховувати не тільки внутрішні параметри об’єкта, але й зовнішні фактори, такі як погодні умови чи зміну навантажень, що вимагає від алгоритмів постійної адаптивності. Системи часто не здатні повністю інтегрувати інформацію з усіх сенсорних точок через різницю в форматах і протоколах передачі даних, що знижує їхню ефективність у критичних умовах.

Ще одним суттєвим обмеженням є висока вимога до обчислювальних ресурсів, особливо в умовах розподілених об’єктів на великих територіях, де доступ до швидкого підключення може бути нестабільним. Надмірна складність моделей, особливо нейронних мереж, може знижувати їхню надійність і здатність до самодіагностики, що створює ризики помилок у роботі систем. Проблема інтерпретованості також лишається актуальною, адже не завжди можливо пояснити процес прийняття рішень штучним інтелектом, що ускладнює контроль і аудит алгоритмів, особливо під час аварійних ситуацій, де швидкість і прозорість дій є критично важливими.

Оптимізація процесів моніторингу та прогнозування на основі штучного інтелекту вимагає ефективної інфраструктури для збору та обробки даних у реальному часі, що включає датчики з високою чутливістю і мінімальною затримкою. Важливо забезпечити злагоджену інтеграцію сенсорів різних форматів з єдиним центром обробки даних, де алгоритми машинного навчання оперативно аналізують інформацію [3]. Адаптивні моделі, здатні навчатися на нових даних і коригуватися залежно від змін, підвищують точність і швидкість реагування. Використання пояснюваного штучного інтелекту підвищує прозорість рішень, а резервні канали передачі даних і автоматизована діагностика забезпечують стабільність роботи і безперервний моніторинг критичних об’єктів.

Розробка рекомендацій щодо інтеграції інтелектуальних систем у стратегії управління безпекою критичних енергетичних об’єктів передбачає впровадження інноваційних підходів, що сприяють підвищенню адаптивності та стійкості систем безпеки. Важливою рекомендацією є створення динамічних цифрових двійників об’єктів енергетичної інфраструктури, які дозволяють моделювати різноманітні сценарії розвитку подій і реагувати на зміни в режимі реального часу. Такі цифрові двійники надають можливість комплексного аналізу системи, виявлення слабких місць та оптимізації стратегій безпеки без переривання основної роботи об’єкта.

Інтелектуальні системи можуть забезпечити прогнозування впливу зовнішніх факторів, таких як кліматичні зміни, коливання енергоспоживання чи економічні зрушення, на функціонування енергетичних об'єктів. Це дозволяє підвищити стратегічну гнучкість та підготовленість до кризових ситуацій шляхом регулярної актуалізації планів дій. Використання технології блокчейн для захисту даних і підвищення прозорості процесів обробки інформації також є важливим компонентом, що гарантує надійність і цілісність даних, особливо в умовах зростаючих кіберзагроз.

Рекомендовано впровадити автоматизовані системи прийняття рішень, що здатні автономно функціонувати в умовах надзвичайних ситуацій і приймати негайні заходи для мінімізації ризиків. Це дозволяє уникнути затримок в управлінні критичними об’єктами і сприяє ефективнішому реагуванню на потенційні загрози [4].

Висновки. Встановлено, що штучний інтелект має значний потенціал у прогнозуванні аварійних ситуацій і моніторингу критичних об’єктів енергетики, проте його застосування стикається з низкою технологічних і практичних викликів. Основні проблеми включають високу обчислювальну складність алгоритмів, потребу в ефективній інтеграції різнорідних даних та забезпеченні стійкості роботи систем у кризових умовах. Рекомендується впровадження гібридних підходів, що поєднують традиційні методи з алгоритмами машинного навчання, а також використання цифрових двійників і технологій блокчейн для підвищення прозорості та надійності. Перспективи подальших досліджень включають розробку адаптивних моделей з високою інтерпретованістю рішень, що підвищить гнучкість і безпеку управління критичною енергетичною інфраструктурою.

1. Колларов, О. Ю., & Остренко, Д. О. (2022). Інтелектуальна діагностика електричних мереж. Наукові праці ДонНТУ. Серія: Електротехніка і енергетика, (2)27, 63–67. Вилучено з https://elen.donntu.edu.ua/2074-2630-2022-2-63-67.pdf.

2. Ahmad, T., et al. (2022). Energetics systems and artificial intelligence: Applications of industry 4.0. Energy Reports, 8, 334–361. https://doi.org/10.1016/j.egyr.2021.11.256.

3. Скрипник, С. О., & Колларов, О. Ю. (2022). Дослідження впливу впровадження нейронних мереж в енергетичну галузь України. Наукові праці ДонНТУ. Серія: Електротехніка і енергетика, (1)26, 39–43. Вилучено з https://elen.donntu.edu.ua/2074-2630-2022-1-39-43.pdf.

4. Торжков, А. А. (2024). Автоматизація управління об’єктами критичної інфраструктури на основі штучного інтелекту. У The 7th International Scientific and Practical Conference “Science and Society: Modern Trends in a Changing World” (с. 221). MDPC Publishing, Vienna, Austria. Вилучено з https://sci-conf.com.ua/wp-content/uploads/2024/06/SCIENCE-AND-SOCIETY.-MODERN-TRENDS-IN-A-CHANGING-WORLD-10-12.06.24.pdf#page=221.

А.О. Тарановський

ПОТОЧНИЙ СТАН ВИКОРИСТАННЯ В УКРАЇНІ РЕГУЛЯТОРНИХ ПІСОЧНИЦЬ ДЛЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

Будь-який призначений для подальшого використання продукт з впровадженням нової технології в тому чи іншому вигляді проходить фази теоретичного обґрунтування та практичного випробування. Проте визначальним залишається все ж таки використання такого продукта в реальних умовах. Таке саме значення це має й для заснованих на технологіях штучного інтелекту продуктах. Максимального наближення до використання в умовах реального світу дозволяє досягти підхід широко відомий у вузьких колах як "регуляторна пісочниця", також згадуваний як "regulatory sandbox" чи навіть просто "sandbox".

Як інструмент, регуляторна пісочниця не набула такого поширення, що переводило б її у розряд традиційних, та донедавна лишалася маловідомою[1] не тільки для широкого загалу, а навіть для професіоналів в сфері регулювання. Настільки, що ще кілька років тому для забезпечення діяльності депутатів Європейського Парламенту з цього питання потребувалася інформаційно-аналітична підтримка з боку експертів [1]. Підготовлені ними матеріали висвітлили це питання наступним чином: за відсутності загальновизнаного визначення, категорією регуляторної пісочниці зазвичай охоплюються інструменти регулювання, що вони дозволяють бізнесові тестування й експериментування з новими й інноваційними продуктами, послугами чи якимось новими напрямами загалом, під наглядом регулятора й протягом певного часу; що з одного боку дозволяє розробку й тестування інновацій в умовах реального світу, а з іншого боку — формування експериментальних правових режимів для спрямовування й підтримки бізнесу в його інноваційній діяльності під наглядом компетентного органу; у підсумку, підхід має на меті створити умови для експериментальних інновацій в режимі контрольованих ризиків й нагляду, а також вдосконалити розуміння нових технологій з боку регулятора.

На рівні закону, регуляторна пісочниця як інструмент державного регулювання знайшла своє втілення у вигляді регуляторної платформи для тестування послуг, технологій та інструментів на платіжному ринку, заснованих на інноваційних технологіях, яка створюється Національним банком Україні [2]. Проте ця регуляторна пісочниця обмежуються платіжним ринком. Тож, навряд чи розгляд цього закону має сенс.

Стратегією відновлення, сталого розвитку та цифрової трансформації малого і середнього підприємництва на період до 2027 року передбачається створення сприятливих умов для діяльності компаній-розробників штучного інтелекту у вигляді регуляторних пісочниць (платформ), які сприятимуть співпраці підприємців з органами влади, даючи змогу тестувати новітні продукти із мінімальними регуляторними вимогами [3]. Проте така стратегія визначає курс формування та реалізації політики у сфері малого і середнього підприємництва та є програмним документом Кабінету Міністрів України, через що не може містити положень нормативно-правового характеру [4]. Тож, навряд чи розгляд цієї стратегії має сенс.

У Білій книзі з регулювання штучного інтелекту в Україні йдеться про створення регуляторної пісочниці, що вона охоплюватиме зокрема сферу штучний інтелекту, як контрольованого середовища, в межах якого відповідні продукти матимуть можливість розроблятися або тестуватися під наглядом та із залученням експертної та іншої підтримки державі на предмет відповідності майбутньому регулюванню, з метою надання допомоги відносно продуктів та побудови спроможності держави в оцінці продуктів зокрема в контексті майбутнього регулювання та подальшої необхідності створення регуляторного органу [6]. Проте в самому цьому документі прямо зазначено, що він не є аналітичнім документом публічної політики, що він є аналітичним матеріалом, в той час як якість самого цього матеріалу викликає неоднозначні оцінки, зміст цього документа не є остаточним, а розробка й оприлюднення цього документу викликають питання принаймні щодо належності таких дій до повноважень Міністерства цифрової трансформації України. Тож, навряд чи розгляд цієї білої книги має сенс.

Порядком реалізації експериментального проекту щодо організації проведення дослідження високотехнологічних засобів методом "Sandbox" цей метод визначається як сукупність заходів, що дають змогу провести дослідження високотехнологічних засобів з використанням штучного інтелекту для їх повноцінного використання, зокрема на предмет безпечності, відповідності законодавству, стандартам, патентної чистоти, дотримання прав інтелектуальної власності, встановлення ринкової затребуваності [6]. Назва згаданого в порядку методу дає підстав припускати приналежність цього інструменту до категорії регуляторної пісочниці, регулювання поширюється на використання штучного інтелекту, а сам порядок затверджений постановою Кабінету Міністрів України, яка набрала чинності [4, 7]. Тож, цей порядок є сенс розглянути більш докладно.

Метою цього експериментального проекту визначене надання інформаційної підтримки, консультування та технічної допомоги його учасникам для підвищення їх конкурентоспроможності та для використання й поширення їх високотехнологічних засобів. А високотехнологічний засіб визначений як пристрій, програмний продукт, інформаційна система або її елемент, розроблені з використанням новітніх технологій та інновацій, що використовує штучний інтелект та забезпечує підвищену ефективність, функціональність і продуктивність.

[1] на користь чого опосередковано свідчить також відсутність профільної сторінки у Wikipedia

Для участі в експериментальному проекті необхідно відповідати певним вимогам організаційного характеру, зокрема бути резидентом України та провадити господарську діяльність відповідно до певних видів діяльності.

Основна ж вимога до високотехнологічного засобу для участі в експериментальному проекті зводиться до можливості його використання для забезпечення розвитку цифрової економіки, публічних послуг, оптимізації роботи органів державної влади, охорони здоров'я, біотехнологій, загальної інфраструктури, агропромислового виробництва, освіти та науки, національної безпеки у воєнній сфері, сферах оборони і військового будівництва (із певними виключеннями) та до наявності прототипу чи дослідного зразку або перебування на стадії концепції із частково розробленою технічною документацією й отриманням фінансування від інвесторів.

Сутність участі в експериментальному проекті зводиться до надання інформаційної підтримки, консультування та технічної допомоги, включно із пропозиціями щодо покращення безпеки та надійності високотехнологічного засобу, усунення недоліків, що несуть ризики порушення законодавства, патентної чистоти, дотримання прав інтелектуальної власності, встановлення ринкової затребуваності, зокрема через встановлення:

- відповідності вимогам і нормам законодавства;
- відповідності сучасному рівню наукових і технічних знань, тенденціям науково-технічного прогресу;
- прогнозних науково-технічних та соціально-економічних наслідків подальшого впровадження;
- дефектів та вразливостей;
- ризиків використання;
- відповідності патентній чистоті, дотриманню прав інтелектуальної власності та ринковій затребуваності.

За результатами участі в експериментальному проекті надається висновок про результати дослідження. Після отримання цього висновку об'єкти права інтелектуальної власності у складі високотехнологічного засобу мають бути подані на реєстрацію в Україні, а сам він має бути впроваджений вітчизняними суб'єктами господарювання в їх діяльності.

Основним недоліком цього порядку, який позбавляє будь-якого сенсу розглядати його другорядні недоліки, є те, що реалізація експериментального проекту не передбачає розробки й тестування інновацій з використанням штучного інтелекту в умовах реального світу — впровадження винесене за межі експериментального проекту. За відсутності експериментування з використання інноваційних технологій штучного інтелекту в реальних умовах нівелюється сама сутність регуляторної пісочниці як інструмента регулювання в цій сфері. Впровадження під наглядом регулятора тут заміщується додатковою фазою дослідження, яка за визначенням не дозволяє виявити того різноманіття ефектів використання, що воно притаманне реальним умовам. А квазідозвільний документ за результатами проходження такої фази не додає нічого до впевненості жодної з зацікавлених осіб стосовно подальших наслідків, адже його правове значення не визначене та не встановлено жодних правових наслідків ані для того, хто його отримав, ані для того, хто його видав, ані для того, кому в подальшому він може бути пред'явлений.

У підсумку, повноцінна регуляторна пісочниця для технологій штучного інтелекту інструмент регулювання в цій сфері в Україні наразі відсутня. Разом із тим, правовий режим розглянутого порядку передбачає подачу Міністерством цифрової трансформації України не тільки звіту за його результатами, а також й пропозицій щодо вдосконалення законодавчих актів у відповідних сферах [4, 6]. Що дає підстави припускати, що недоліки втіленого в розглянутому порядку підходу будуть виявлені й отримають адекватну відповідь. Тільки ж це на роки, що для настільки динамічної сфери є величезною втратою часу. Тим не менш, такий крок в регулюванні є безумовно позитивним та змінює регуляторний ландшафт в сфері штучного інтелекту на краще.

1. Madiega, T., & Van De Pol, A. L. (2022). Artificial intelligence act and regulatory sandboxes (PE 733.544). European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf.
2. Про платіжні послуги, Закон України № 1591-IX (2024) (Україна). https://zakon.rada.gov.ua/laws/show/1591-20.
3. Про схвалення Стратегії відновлення, сталого розвитку та цифрової трансформації малого і середнього підприємництва на період до 2027 року та затвердження операційного плану заходів з її реалізації у 2024-2027 роках, Розпорядження Кабінету Міністрів України № 821-р (2024) (Україна). https://zakon.rada.gov.ua/laws/show/821-2024-р.
4. Про затвердження Регламенту Кабінету Міністрів України, Постанова Кабінету Міністрів України № 950 (2023) (Україна). https://zakon.rada.gov.ua/laws/show/950-2007-п.
5. Румянцев, Г. (Ред.). (2024). Біла книга з регулювання ШІ в Україні: бачення Мінцифри (версія для консультацій). Міністерство цифрової трансформації України. https://thedigital.gov.ua/storage/uploads/files/page/community/docs/Регулювання%20ШІ.pdf.
6. Про реалізацію експериментального проекту щодо організації проведення дослідження високотехнологічних засобів методом "Sandbox", Постанова Кабінету Міністрів України № 1238 (2024) (Україна). https://zakon.rada.gov.ua/laws/show/1238-2024-п.
7. Постанова Кабінету Міністрів України "Про реалізацію експериментального проекту щодо організації проведення дослідження високотехнологічних засобів методом «Sandbox»" від 29 жовтня 2024 р. № 1238. (2024, 31 жовтня). Урядовий кур'єр, (221 (7881)), 5. https://ukurier.gov.ua/media/newspaper_free/pdf/2024-10-30/221_31.10.2024.pdf.

Т.С. Токовило, Е.В. Кірпічов

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА СУЧАСНУ МАТЕМАТИЧНУ ОСВІТУ: ПОКРОКОВЕ НАВЧАННЯ, ПЕРСОНАЛІЗОВАНІ ПІДХОДИ ТА ТОЧНІСТЬ РОЗВ'ЯЗКІВ

Сучасний підхід до навчання математики стрімко змінюється під впливом технологій, особливо штучного інтелекту (ШІ), який стає невід'ємною частиною освітнього процесу. Зі зростанням складності завдань, з якими стикаються учні, інструменти на базі ШІ пропонують нові методи для розв'язання математичних задач, роблячи навчання більш доступним і зрозумілим.

ШІ здатний розв'язувати складні математичні задачі, які раніше вимагали великої кількості часу й знань. Це особливо важливо для студентів і науковців, які працюють з високорівневою математикою, наприклад, у галузях фізики, інженерії чи фінансів. ШІ може виконувати численні обчислення, аналізувати дані та знаходити рішення за лічені секунди, що робить його цінним інструментом для обробки великих обсягів інформації

Однією з найбільших переваг ШІ є можливість покрокового пояснення розв'язків. Тепер, коли учень стикається зі складним прикладом чи рівнянням, система не лише видає кінцевий результат, а й розбиває процес на зрозумілі етапи. Завдяки такому підходу учень може вивчати кожен крок окремо, що допомагає краще засвоювати матеріал і розуміти логіку вирішення задачі. Це особливо важливо для розвитку аналітичних навичок, оскільки покрокове пояснення допомагає учням краще орієнтуватися в математичних концепціях і застосовувати їх у різних контекстах

Розвиток аналітичного мислення ШІ активно допомагає учням розвивати аналітичне мислення, навчаючи їх критично підходити до задач і аналізувати різні методи розв'язання. Завдяки такому підходу студенти вчаться мислити гнучко, що корисно не лише в математиці, а й у вирішенні реальних проблем.

Допомога у вивченні нових математичних дисциплін ШІ відкриває можливості для вивчення нових, складніших розділів математики, таких як лінійна алгебра, диференціальні рівняння, теорія ймовірностей і статистика. Завдяки візуалізації даних, графікам і інтерактивним інструментам, студенти легше опановують нові концепції, що раніше здавалися складними для самостійного розуміння.

Ще одним вагомим аспектом є висока точність обчислень та відповідей, яку гарантує використання алгоритмів ШІ. Завдяки швидкому аналізу даних і складних розрахунків, учні можуть бути впевнені в правильності своїх рішень навіть у випадках із заплутаними завданнями. Також ШІ здатен виявляти помилки в обчисленнях і надавати учням пояснення, що саме пішло не так, що робить навчання не тільки ефективним, але й адаптивним.

Крім того, інструменти на базі ШІ все частіше пропонують індивідуальні рекомендації для кожного учня, адаптуючи навчальний процес під його конкретний рівень і потреби. Наприклад, якщо студент не розуміє певну тему, ШІ може запропонувати додаткові завдання або пояснення, допомагаючи глибше засвоїти матеріал. Це дозволяє створювати персоналізовані освітні траєкторії, що є ключовим у розвитку навичок для сучасного світу.

Висновок

Загалом, інструменти ШІ в математичній освіті змінюють уявлення про навчання, роблячи його більш структурованим, точним та персоналізованим. Такий підхід дозволяє не лише досягати академічних цілей, а й формувати в учнів аналітичне мислення, яке необхідне в подальшому житті. штучний інтелект не лише полегшує навчання математики, але й робить його глибшим та доступнішим для більшої кількості людей. Його впровадження дає студентам і професіоналам інструменти для досягнення успіху в сучасному світі, де аналітичні навички та здатність швидко знаходити рішення цінуються як ніколи.

1. Штучний інтелект в освіті: як технологія впливає на навчання в українських школах. https://fakty.com.ua/ua/ukraine/suspilstvo/20231220-shtuchnyj-intelekt-v-osviti-yak-tehnologiya-vplyvaye-na-navchannya-v-ukrayinskyh-shkolah.
2. Використання штучного інтелекту. https://prjctr.com/mag/aicases.

Я.Ю. Дорогий, В.В. Цуркан, І.О. Бердиченко, О.О. Дорога-Іванюк

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ БАНКІВСЬКОЇ СФЕРИ

Анотація. Захист критичної інфраструктури банківської сфери є важливою умовою стабільності та безпеки фінансової системи України. Військові дії, підвищення кіберзагроз і складні економічні умови вимагають інноваційних підходів до захисту. Штучний інтелект (ШІ) є одним із найбільш перспективних інструментів, що дозволяє не лише швидко реагувати на загрози, але й передбачати нові вразливості. Впровадження ШІ допомагає установам банківської сфери краще справлятися з кіберзагрозами, знижуючи ризики та підвищуючи надійність інфраструктури.

Вступ. Критична інфраструктура (КІ) банківської сфери є основою економічної безпеки України, від стабільності якої залежить функціонування фінансових операцій, збереження заощаджень громадян і довіра до банківської системи. Останні роки, особливо в умовах війни, відзначаються різким збільшенням кібератак, спрямованих на банківську інфраструктуру України. Атаки мають на меті як безпосереднє завдання шкоди, так і дестабілізацію економічної системи. З огляду на це, критично важливим є впровадження інноваційних рішень, зокрема штучного інтелекту, для моніторингу, виявлення загроз і швидкого реагування на потенційні ризики.

Захист критичної інфраструктури банківської сфери. Захист КІ банківської сфери вимагає комплексного підходу. Ключові компоненти цієї інфраструктури включають платіжні системи, канали передачі фінансових даних, бази даних клієнтів, та системи онлайн-банкінгу. Відмова цих систем може призвести до фінансових втрат і зниження довіри клієнтів до банківської сфери. В умовах війни значно посилилися загрози з боку кіберзлочинців, які використовують більш витончені методи атаки, що ускладнює їх виявлення та нейтралізацію.

Особливу роль у захисті банківської інфраструктури відіграє Національний банк України (НБУ), який, відповідно до законодавства, здійснює регулювання та нагляд за станом критичної інфраструктури банківської сфери [1]. НБУ розробляє нормативно-правові акти, контролює виконання вимог кібербезпеки банками та координує заходи з захисту їх КІ у разі кризових ситуацій [2, 3].

НБУ забезпечує функціонування системи кіберзахисту в банківській системі України, серед іншого організовано обмін інформацією про кіберзагрози, кібератаки та кіберінциденти з банками України; визначено особливості кіберзахисту об'єктів критичної інформаційної інфраструктури банківської системи України; відбувається сприяння розвитку та вдосконаленню систем, комплексів та засобів забезпечення кіберзахисту в банківській системі України.

В НБУ, з метою поєднання та координації зусиль суб'єктів кіберзахисту створено та функціонує Центру кіберзахисту [4]. Основними технічними інструментами Центру кіберзахисту є MISP-NBU і портал Центру кіберзахисту. Центр кіберзахисту забезпечує реалізацію інформаційного обміну, функціонування CSIRT-NBU, і відповідно, координацію дій з питань кіберзахисту в банківській системі.

Окрім зазначених вище заходів та нормативно-правового регулювання, важливим елементом є використання інноваційних технологій. ШІ надає можливість аналізувати великі обсяги даних у режимі реального часу, виявляти аномалії та передбачати можливі загрози ще до їх реалізації. Для прикладу, алгоритми машинного навчання можуть виявляти невластиву поведінку користувачів у системах банківського обслуговування, яка може сигналізувати про потенційну атаку. Використання таких технологій дозволяє установам банківської сфери швидше реагувати на загрози, зменшуючи можливість витоку конфіденційної інформації та втрати фінансів.

Інтеграція ШІ стає невід’ємною частиною міжнародної співпраці у кібербезпеці та сфері захисту критичної інфраструктури, зокрема для захисту критичної банківської інфраструктури. Банківські установи України отримують підтримку від міжнародних партнерів, які надають сучасні технологічні рішення на основі ШІ, а також консультації і методології, що допомагають протидіяти новітнім кібератакам та захищати КІ. Співпраця з такими установами, як Європейське агентство з кібербезпеки (ENISA), сприяє інтеграції штучного інтелекту в українські системи захисту, дозволяючи відповідати найвищим стандартам, наприклад, ISO/IEC 27001 [5]. ШІ дозволяє покращити не лише автоматизований моніторинг загроз, а й підвищувати ефективність обміну інформацією з міжнародними партнерами для швидшої реакції на нові загрози.

Штучний інтелект також стає важливим інструментом для навчання та обізнаності співробітників банків щодо кіберзагроз та захисту КІ. НБУ, як секторальний орган захисту критичної інфраструктури банківської сфери [3], рекомендує банкам проводити регулярні тренінги, які включають моделювання кіберзагроз із використанням ШІ. Це дає змогу співробітникам краще зрозуміти потенційні інсайдерські загрози та способи їх виявлення. ШІ може автоматизувати моніторинг дій користувачів у банківських системах, допомагаючи виявляти підозрілу активність у режимі реального часу, що є особливо актуальним в умовах зростання кількості інцидентів у період військових конфліктів. Також слід відзначити, що НБУ в умовах війни веде активну роботу щодо підвищення координації між різними департаментами всередині самого регулятора та в банківській сфері в цілому. Це допомагає уникати дублювання заходів захисту та забезпечувати єдність підходів до захисту критичної інфраструктури. В цьому напрямку, важливою ініціативою є створення централізованих команд з управління кібербезпекою та захисту критичної інфраструктури, що складаються з фахівців різних профілів.

Такі команди можуть проводити оцінку ризиків і здійснювати аналіз наявних проблем КІ для своєчасної розробки стратегій реагування.

Висновки. Використання штучного інтелекту для захисту критичної інфраструктури банківської сфери в умовах війни та підвищеної кіберзагрози є важливим кроком до забезпечення фінансової стабільності країни. Інтеграція ШІ у систему кібербезпеки дозволяє банкам автоматизувати процеси виявлення загроз, оптимізувати управління ризиками та швидко реагувати на інциденти. Це не лише підвищує надійність інфраструктури, а й сприяє збереженню довіри клієнтів до банківської системи.

Однак, навіть найсучасніші технології не можуть повністю захистити від порушення критичної інфраструктури без комплексного підходу. Необхідне поєднання нормативного регулювання, впровадження передових технологій, освітніх програм і міжнародного співробітництва. Військові виклики зумовлюють необхідність розширення інноваційних заходів безпеки та створення стратегій, що дозволять банківській інфраструктурі України оперативно адаптуватися до нових кіберзагроз та викликів захисту критичної інфраструктури. Такий підхід передбачає постійний моніторинг ефективності впроваджених заходів, оновлення захисних технологій і покращення професійної підготовки кадрів.

1. Про Національний банк України: Закон України від 20 травня 1999 року № 679-XIV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/679-14 (дата звернення: 02 листопада 2024).

2. Про основні засади забезпечення кібербезпеки України: Закон України, 5 жовтня 2017 року, № 2163-VIII / Верховна Рада України (онлайн) URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 02 листопада 2024).

3. Про критичну інфраструктуру: Закон України, 16 листопада 2021 року, № 1882-IX / Верховна Рада України (онлайн) URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 02 листопада 2024).

4. Національний банк України. Кіберкоманда реагування на інциденти (CSIRT). URL: https://csirt.bank.gov.ua/ (дата звернення: 08.11.2024).

5. ISO/IEC 27001:2013 Information security management systems — Requirements / International Organization for Standardization. URL: https://www.iso.org/standard/27001 (дата звернення: 02 листопада 2024).

М.С. Кондратенко

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ СУМНІВНИХ ТРАНЗАКЦІЙ В БЛОКЧЕЙН-МЕРЕЖІ

Блокчейн — це децентралізована цифрова книга, в якій однорангові вузли узгоджують додавання включень до блоків ланцюга мережі. Кожен блок містить записи транзакцій з унікальними хеш-значеннями та часовими мітками для їх підтвердження. Пов'язані між собою блоки утворюють ланцюг, що й дало цій структурі назву «блокчейн». Така система численних однорангових мереж практично не піддається несанкціонованим втручанням та відома своєю здатністю забезпечувати захист від підробок і змін даних. У 2008 році розробник під псевдонімом Сатоші Накамото (реальна особа залишається невідомою, можливо, що під цим псевдонімом працювала група людей) запропонував загальний алгоритм системи біткойн, ключовим елементом якої була система з безперервного послідовного ланцюжка блоків інформації, названої блокчейн. Принциповою відмінністю від усіх попередніх варіантів подібних технологій (у тому числі Hashcash) стало об'єднання ланцюгового хеша з формальним механізмом вироблення консенсусу про коректність чергового блоку, що дозволило у всій системі відмовитися від необхідності верифікації інформації довіреним агентом (адміністратором) та система в цілому стала децентралізованою. [1] Блокчейн використовує різні криптографічні механізми для забезпечення роботи системи. Основними з них є наступні:

- хеш-функції — базовий механізм блокчейну, що забезпечує безпосередньо його функціонування;
- цифрові підписи — кожен користувач, який вносить певну інформацію в блок, має підписати цю інформацію;
- різні протоколи доведення без розголошення, або алгоритми кільцевих підписів, якщо цей блокчейн має функцію підвищеної анонімності. [2]

Паралельно з цим у світі набуває розвитку не менш революційна технологія під назвою штучний інтелект (ШІ). Це набір технологічних інструментів і алгоритмів, які надають нам прогнози, рекомендації та рішення щодо змін цифрового й реального середовища, базуючись на різних даних. Загалом, він націлений виконувати завдання, які, як вважалося раніше, може виконати тільки людина. Одним з потенційних напрямків впровадження, в якому вже йде активна розробка, є аналіз транзакцій в мережах, побудованих на основі технології блокчейн. ШІ може виявляти аномалії в транзакціях, що допомагає автоматично розпізнавати ознаки шахрайства або відмивання коштів. Моделі машинного навчання здатні аналізувати патерни великих обсягів даних і знаходити невідповідності, які складно помітити вручну. ШІ здатний проводити не тільки поточний аналіз, а й передбачати можливі ризики або шахрайські дії, використовуючи історичні дані для моделювання майбутньої поведінки. Це особливо корисно для фінансових установ, які використовують блокчейн для міжнародних транзакцій. Для більш практичного прикладу проаналізуємо компанію CertiK, аудитора Web3, який використовує штучний інтелект для моніторингу та захисту смарт-контрактів у основних блокчейнах, таких як Ethereum, Polygon і BNB Chain.

Як це працює:

- Аудит на основі ШІ: CertiK використовує алгоритми машинного навчання щоб провести поглиблений аналіз смарт-контрактів. Він сканує код на наявність потенційних помилок, лазівок у безпеці та вразливостей, якими можуть скористатися хакери.
- Моніторинг у режимі реального часу: після розгортання контракту системи штучного інтелекту CertiK продовжують відстежувати його діяльність у режимі реального часу. Аналізуючи дані в ланцюжку та моделі транзакцій, система може виявляти будь-які підозрілі дії чи аномалії, забезпечуючи додатковий рівень безпеки.
- Автоматизоване звітування: штучний інтелект CertiK створює детальні звіти, у яких висвітлюються ризики та потенційні експлойти, що дозволяє розробникам швидко вирішувати ці проблеми. Цей автоматизований процес гарантує ретельну перевірку навіть найскладніших контрактів.
- Активний моніторинг CertiK і виявлення недоліків безпеки допомагає розробникам розгортати більш безпечні смарт-контракти, а довіра, яку він підтримує, має значно сприяти більш широкому впровадженню технологій блокчейну та ШІ.[3]

Згідно з нещодавнім звітом Certik Web3 Security Quarterly Report, статистика за другий квартал 2024 року демонструє досить тривожні показники: через 184 інциденти з безпекою в блокчейні втрати досягли $688 мільйонів, що на 37% більше, ніж у попередньому кварталі. Фішингові атаки виявилися найдорожчою загрозою, спричинивши близько $433 мільйонів збитків, а компрометація особистих ключів додала понад $170 мільйонів втрат. Найбільше постраждала платформа Ethereum, на якій зафіксували 83 інциденти з великими фінансовими збитками. Загалом, у першій половині 2024 року втрати перевищили $1.19 мільярда, що підкреслює важливість посилення безпеки у швидкозростаючому середовищі Web3.

Як висновок, варто зазначити, що застосування ШІ в блокчейн-аналітиці має значний потенціал для підвищення ефективності та безпеки фінансових операцій. Безумовно, подібні технології можуть значно покращити безпеку та ефективність системи. Штучний інтелект може працювати в тандемі з традиційними методами виявлення шахрайства,

такими як системи правил і фільтри. Це дозволяє створювати гібридні моделі, які об'єднують гнучкість ШІ з надійністю правил для точнішого виявлення сумнівних транзакцій. Але при цьому впровадження ШІ також вимагає надійних систем перевірки даних і захисту від помилкових позитивних сигналів, щоб забезпечити точність і мінімізувати негативний вплив на законні транзакції.

1. Blockchain. Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Blockchain.
2. Кондратенко, М. С. (2023). Визначення кількості блоків підтвердження у блокчейні, в якому розміщено реєстр другого рівня у випадку, коли в обох блокчейнах використовується протокол консенсусу POS. XLI Науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Збірник матеріалів конференції, 188–190. https://ipme.kiev.ua/wp-content/uploads/2023/05/Матеріали-конференції-2023.pdf.
3. 5 реальних способів використання блокчейну та штучного інтелекту, які зроблять вас віруючим у Web3.

Д.А. Іванов

ОГЛЯД ПАРАМЕТРІВ ОПТИМІЗАЦІЯ МОДЕЛІ ДЛЯ ПРИШВИДШЕННЯ САМОНАВЧАННЯ

Самонавчання – це процес, коли модель використовує свої власні помилки та наявні дані для покращення точності та адаптації до нових умов без втручання людини. Завдяки цьому модель може постійно вдосконалюватися та навчатися на нових прикладах в реальному часі.

Швидке самонавчання моделей є критично важливим, оскільки дає змогу системам адаптуватися до нових або змінних умов у динамічному середовищі, як-от відеоспостереження, автономні транспортні засоби чи робототехніка. Чим швидше модель може навчитися на нових даних, тим точніше та надійніше вона працюватиме в умовах, де зміни відбуваються постійно, що покращує її практичне застосування та підвищує ефективність роботи системи в цілому.

Оптимізація параметрів моделі є одним з методів пришвидшення процесу самонавчання, оскільки правильно налаштовані параметри визначають ефективність та швидкість збіжності алгоритму навчання [1]. Наприклад, вибір оптимальної швидкості навчання (learning rate) дозволяє моделі швидко пристосовуватися до нових даних, уникаючи як надмірного навчання, так і повільної збіжності [2]. Загалом, оптимізація параметрів допомагає скоротити час навчання та підвищити продуктивність моделі в умовах постійно змінного середовища.

Модель має велику кількість параметрів, і кожен з них відповідає за певний аспект її роботи, забезпечуючи здатність розпізнавати та класифікувати об’єкти. Проте існують ключові параметри, які безпосередньо впливають на швидкість самонавчання моделі, визначаючи, наскільки ефективно вона може обробляти нові дані, адаптуватися до змін у середовищі та швидко знаходити оптимальні рішення. В даному дослідженні розглядаються такі параметри, як: швидкість навчання (learning rate), розмір батчу (batch size) та кількість епох (number of epochs).

Перший розглянутий параметр – це швидкість навчання. Даний параметр визначає, наскільки великі кроки робить модель під час оновлення ваг у процесі навчання. Висока швидкість навчання дозволяє швидко наближатися до оптимальних значень, проте може призвести до нестабільності або пропуску глобального мінімуму функції втрат, а занадто низька швидкість – до повільного процесу збіжності, що збільшує час самонавчання [1]. Оптимальне налаштування цього параметра є ключовим для збалансування швидкості та точності моделі.

Розмір батчу це наступний параметр, для пришвидшення процесу самонавчання. Він визначає кількість зразків, оброблюваних моделлю за одну ітерацію навчання. Менший розмір батчу дозволяє моделі оновлювати ваги частіше, сприяючи швидшому навчанню, але може призводити до більшої шумності в градієнтних оцінках, що впливає на стабільність збіжності [1]. Натомість великий розмір батчу надає більш точні оцінки градієнтів, але збільшує обчислювальні витрати та час навчання, оскільки ваги оновлюються рідше. Оптимізація розміру батчу дозволяє знайти баланс між стабільністю та швидкістю навчання: наприклад, використання динамічного збільшення розміру батчу під час навчання може забезпечити пришвидшення збіжності та покращення точності моделі [2].

Останній з розглянутих параметрів - кількість епох. Цей гіперпараметр визначає, скільки разів модель проходить через весь набір навчальних даних під час процесу навчання. Більша кількість епох дозволяє моделі поступово коригувати свої ваги, підвищуючи точність і здатність розпізнавати складні патерни в даних, але при цьому збільшується час навчання [1]. При меншому значенні параметра час навчання скоротиться, але це призведе до того, що модель не зможе досягти оптимальної точності. Оптимізація кількості епох є важливим кроком у пришвидшенні самонавчання: визначення відповідного значення дозволяє досягти балансу між часом навчання та якістю моделі, уникаючи надмірних витрат обчислювальних ресурсів і часу [3].

Отже, одним із методів пришвидшення процесу самонавчання моделі є оптимізація гіперпараметрів моделі, зокрема швидкості навчання, розміру батчу та кількості епох. Правильне налаштування швидкості навчання допомагає збалансувати точність та швидкість збіжності, тоді як оптимальний розмір батчу та кількість епох дозволяють скоротити час навчання та уникнути перенавчання.

1. Goodfellow I, Bengio Y, Courville A. Deep Learning. MIT Press; 2016.
2. Hinton G, Vinyals O, Dean J. Distilling the knowledge in a neural network. arXiv preprint arXiv:1503.02531; 2015.
3. Smith SL, Kindermans PJ, Ying C, Le QV. Don't decay the learning rate, increase the batch size. arXiv preprint arXiv:1711.00489; 2017.

Т.С. Токовило, М.М. Васильєв

ПЕРЕВЕГИ ТА НЕДОЛІКИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ НАВЧАННЯ

Використання штучного інтелекту досягло такого рівня, що воно глибоко вкоренилося в сучасному суспільстві, а заперечити його вплив на освіту просто неможливо. Суть обраної теми – «Переваги та недоліки використання штучного інтелекту для навчання» – очевидна. Треба спробувати зрозуміти, як сучасні технології можуть сприяти або погіршувати розуміння будь-якої інформації. Більш конкретно, ми оцінимо вплив штучного інтелекту на різні аспекти вивчення математики. Метою моєї роботи є дослідження всіх аспектів застосування штучного інтелекту в освіті, огляд ключових факторів, пов'язаних з ним та забезпечення його ефективності.

Я обрав цю тему через низку причин. Як студент вищого навчального закладу, я помічаю як інтегрується штучний інтелект в навчання. Я бачу, що відбувається навколо мене, і мені цікаво зрозуміти, як це вплине на мене як студента. Крім цього, я вважаю, що аналіз впливу штучного інтелекту на деякі аспекти людського життя має першочергове значення, оскільки він сформує те, як майбутні покоління сприймуть світ.

Розпочнемо зі статистичних даних. У вересні-жовтні 2023 року в Україні провели Всеукраїнське дослідження перспектив штучного інтелекту у шкільній освіті. Його організатори – Мала академія наук України та Projector Institute. У дослідженні взяли участь 1747 учителів і 1443 учні 8–11 класів з усієї України, окрім окупованих територій. 70% учителів уже використовували хоча б один інструмент штучного інтелекту за останні 6 місяців. Загалом 76% освітян користувалися штучним інтелектом, і половина з них мала позитивний досвід. Кожен другий учитель вважає, що штучний інтелект змінить освітній процес у найближчі роки, використовуючи його для підготовки до занять, створення тестів, проведення уроків, перевірки знань та позакласної роботи. Серед учнів 60% уже використовували штучний інтелект для домашніх завдань, 85% – хоча б раз, а третина – щотижня. Близько 40% застосовували його під час уроків, в основному для пошуку та систематизації інформації, створення конспектів, генерації ідей, заголовків і тез. Хоча дехто анонімно зізнається, що використовує штучний інтелект для списування, це відбувається рідше. Дослідження показує, що більшість учителів та учнів вже активно використовують штучний інтелект в навчанні. Учителі застосовують його для підготовки матеріалів, а школярі – для виконання завдань. Це свідчить про суттєвий вплив штучного інтелекту на освітній процес.

На мою думку, штучний інтелект значно спрощує доступ до навчальних ресурсів, щоб легше освоювати матеріал. Мені здається, що персоналізоване навчання – це ще одна важлива перевага, бо завдяки штучному інтелекту можна створювати індивідуальні навчальні плани. Це допомагає кожному студенту вчитися у власному темпі та отримувати підтримку саме там, де виникають труднощі. Також, як я вважаю, автоматизація рутинних завдань, наприклад, оцінювання робіт, звільняє час викладачів для чогось важливішого, наприклад, розробка нових програм. І, звісно, дистанційне навчання з використанням штучного інтелекту робить освіту доступнішою, що особливо важливо в умовах глобальних проблем, наприклад, COVID-19. Але, де є переваги, там, звісно, є й недоліки. Використання штучного інтелекту призводить до залежності від нього та інших технологій, знижує самостійне мислення. Освітяни просто стають пасивними споживачами інформації, покладаючись на штучний інтелект, замість того, щоб розвивати власні навички. Також, не завжди інформація від штучного інтелекту відповідає певним стандартам або не враховує власні потреби студента. Ризик у тому, що штучний інтелект буде надавати стандартизовані відповіді на унікальні питання, що знижує якість навчання.

Тепер я хочу зосередитися на математиці. Вивчення математики за допомогою штучного інтелекту має свої переваги та недоліки. Штучний інтелект вміє та може пояснювати складні концепції через візуалізацію та інтерактивні приклади, що сприяє засвоєнню матеріалу. Алгоритми штучного інтелекту вміють розв'язувати завдання, не завжди правильно, але він допомагає студенту зрозуміти методи вирішення певного завдання. До речі, також, штучний інтелект може аналізувати помилки та надавати рекомендації щодо їх виправлення. Однак, з іншого боку, надмірне використання штучного інтелекту завжди призводить до пасивного навчання, коли студент покладається повністю на технології замість самостійного мислення. Також, надмірна залежність від штучного інтелекту призводить до втрати навичок ручного обчислення та звичайного аналітичного мислення. Наприклад, у разі вивчення аналітичної математики, штучний інтелект може автоматизувати аналіз даних і обчислення певних математичних моделей, що дозволить студенту зосередитися на інтерпретації результатів і розробці нових підходів. Штучний інтелект також дає змогу працювати з великими обсягами даних, що може сприяти розвитку аналітичних навичок. Однак, складність розуміння алгоритмів штучного інтелекту стає перешкодою для студентів.

Розглянемо інший приклад з вищої математики – матриці. Студент може використовувати штучний інтелект для обчислень, але спершу він повинен самостійно освоїти основи, а вже потім використовувати калькулятори або штучний інтелект. Крім того, штучний інтелект не завжди виконує обчислення правильно, адже це машина, яка може помилятися, як і людина. Проте штучний інтелект чудово підходить для пояснення теорії, адже має доступ до великої бази даних, з якої можна отримати точні дефініції та чіткі пояснення. Тому, говорячи про теорію, я дійсно можу рекомендувати використання штучного інтелекту. Щодо обчислень, варто зауважити, що він виконує їх за своїм алгоритмом, і навіть якщо ви вказали йому конкретний метод, не завжди

його спосіб буде найпростішим або найзручнішим для вас. Іноді результат може бути правильним, але сам процес розв'язання виявиться складнішим, ніж якщо б ви робили це самі.

Також, хочу додати, що штучний інтелект може бути корисним у розв'язанні простих геометричних задач, таких як обчислення площ, периметрів, радіусів кругів або об'ємів стандартних фігур. Він здатний швидко виконувати арифметичні операції та надавати точні результати для таких завдань. Проте на даний момент штучний інтелект не має здатності ефективно вирішувати складні геометричні завдання, особливо ті, що вимагають глибокого аналізу просторових фігур, таких як тетраедр або піраміди тощо. Ці задачі потребують не тільки математичних обчислень, але й більш складних концептуальних підходів, роботою з нестандартними даними чи специфічними властивостями фігур, що вимагає більшої гнучкості та точності, ніж надає штучний інтелект.

На завершення я хотів би підкреслити, що штучний інтелект має великий потенціал для використання в освітньому процесі, але те, наскільки він має бути інтегрованим, – це те, що потрібно вирішити. Слід також приділяти вагу як перевагам, так і недолікам такого технологічного прогресу в освіті, щоб його можна було використовувати максимально справедливо. Дослідження того, як штучний інтелект може похитнути фундамент існуючої освітньої системи, підкресливши його позитивні наслідки, є дуже своєчасним заходом для забезпечення системи освіти.

1. Штучний інтелект в освіті: як технологія впливає на навчання в українських школах. https://fakty.com.ua/ua/ukraine/suspilstvo/20231220-shtuchnyj-intelekt-v-osviti-yak-tehnologiya-vplyvaye-na-navchannya-v-ukrayinskyh-shkolah.
2. Штучний інтелект. https://uk.wikipedia.org/wiki/Штучний_інтелект.

Д.І. Азарний

КЛАСИФІКАЦІЯ ДІПФЕЙКІВ

Техніки

Розділ описує різноманітні техніки створення та виявлення діпфейків. Ці техніки охоплюють як традиційні алгоритми машинного навчання, так і сучасні методи глибокого навчання.

Алгоритми машинного навчання, такі як опорні вектори (SVM) та дерева рішень, є основою для розрізнення реального та підробленого контенту. Важливим підходом є інтеграція методів глибокого навчання з машинним навчанням, що використовує аналіз рівня помилок разом із згортковими нейронними мережами (CNN) і SVM для надійного виявлення підроблених зображень.

Глибоке навчання значно підвищило можливості виявлення діпфейків. У цьому контексті використовуються два основні типи моделей: згорткові нейронні мережі (CNN) та рекурентні нейронні мережі (RNN), особливо мережі з довготривалою пам'яттю (LSTM). CNN добре підходять для виділення ознак зображень або відеокадрів, що робить їх ефективними для класифікації фейкового контенту. RNN, особливо LSTM, корисні для аналізу послідовних даних, що є важливим для виявлення фейків у відеоконтенті. Поєднання CNN та RNN може додатково покращити здатність до виявлення.

Техніки розширення даних також використовуються для підвищення ефективності моделей виявлення фейків. Деякі методи включають випадкові або цілеспрямовані модифікації обличчя на основі розмітки обличчя, що запобігає перенавчанню. Існують також просунуті стратегії, наприклад, поєднання справжніх і штучних облич, що підвищують стійкість моделей до різних технік маніпуляції.

Типи

Діпфейки можна розділити на кілька основних типів залежно від середовища та методів їх створення. Розуміння цих категорій є важливим, оскільки кожен тип представляє унікальні загрози та наслідки.

Текстові фейки

Текстові фейки передбачають маніпуляцію текстом за допомогою штучного інтелекту, що дозволяє генерувати контент, який може імітувати стиль письма людей або фабрикувати повідомлення. Цей тип фейків може використовуватися для підробки документів.

Відеофейки

Відеофейки є, мабуть, найвідомішою формою цієї технології. Вони передбачають зміну відеозаписів, щоб здавалося, ніби людина сказала або зробила те, чого насправді не було. Для цього часто використовуються методи заміни обличчя та анімації тіла, що дозволяє створювати дуже реалістичні сцени.

Зображення-фейки

Зображення-фейки маніпулюють статичними фотографіями, щоб накладати обличчя або змінювати риси. Ця технологія дозволяє створювати реалістичні зображення, що викликає занепокоєння щодо крадіжки особистих даних та несанкціонованого використання зображень осіб.

Аудіофейки

Технологія аудіофейків може імітувати голос, тон і акцент людини, створюючи штучний аудіоконтент, який звучить достовірно. Аналізуючи наявні записи голосу, алгоритми можуть створювати нові аудіокліпи, що дуже схожі на оригінальні, що викликає етичні питання щодо дезінформації та імітації.

Фейки у реальному часі

Фейки в реальному часі є найбільш просунутим застосуванням цієї технології, дозволяючи змінювати відео та аудіо контент під час прямих трансляцій або відеодзвінків. Ця можливість має серйозні наслідки для конфіденційності та безпеки, оскільки вона може використовуватися для імітації осіб у реальному часі, наприклад, на платформах соціальних мереж.

Застосування

Технологія фейків знайшла застосування в різних галузях, використовуючи можливості створювати переконливо змінений контент. Ці застосування охоплюють сфери від розваг до безпеки, демонструючи як інноваційні можливості, так і серйозні етичні проблеми.

Розваги та реклама

Одним із найпомітніших застосувань технології глибоких фейків є розважальна індустрія, особливо у виробництві фільмів та рекламі. Наприклад, агенція Creative Artists Agency створює цифрових клонів акторів, що дозволяє знімати рекламу з їх участю без фізичної присутності. Відомі бренди, такі як Puma, Nike та Procter & Gamble, використовують глибокі фейки для підвищення ефективності своїх маркетингових кампаній. Яскравим прикладом є кампанія з Девідом Бекхемом, де технологія глибоких фейків дозволила йому виступити кількома мовами для привернення уваги до проблеми малярії.

Соціальні мережі та комунікація

Технологія глибоких фейків також інтегрується у соціальні мережі для покращення взаємодії з користувачами. Наприклад, Facebook використовує AI для спрощення процесу маркування зображень, а Instagram розглядає можливість впровадження візуального пошуку, що дозволить користувачам знаходити схожі продукти лише натисканням на зображення.

Освіта та тренінги

В освітньому контексті технологія глибоких фейків використовується для створення персоналізованих навчальних програм. Компанії, такі як Synthesia, використовують аватари для створення навчальних відео, що імітують реальні сценарії. Це забезпечує більш захоплюючий та адаптований підхід до навчання, де аватари можуть взаємодіяти зі студентами в реальному часі.

Виклики

Технологія діпфейків, демонструючи досягнення у сфері штучного інтелекту та машинного навчання, створює значні виклики у таких сферах, як достовірність інформації, виявлення, етичні питання та безпекові ризики.

Етичні питання

Створення та поширення глибоких фейків піднімає серйозні етичні питання, особливо стосовно згоди та конфіденційності. Особи, чиї зображення або голоси використовуються у фейкових медіа, можуть не мати контролю над своїм образом, що може призвести до крадіжки особистих даних, завдання репутаційної шкоди та емоційного стресу.

Достовірність інформації

Одним з основних викликів глибоких фейків є можливе зниження довіри до медіа. Через те, що глибокі фейки стають дедалі складнішими, розрізнення справжнього та підробленого контенту стає складним, що може підірвати демократичні функції, створюючи сумніви щодо достовірності інформації.

Складнощі у виявленні

Виявлення глибоких фейків представляє складний виклик. Хоча існують просунуті алгоритми для виявлення, вони часто мають труднощі з модифікованими даними або зміненим медіа, що може значно знизити їхню точність.

Ризики для безпеки

Глибокі фейки також представляють загрозу для безпеки, оскільки їх можна використовувати з шкідливою метою, такою як крадіжка особистих даних, кампанії дезінформації та кібератаки.

1. https://sciencepublishinggroup.com/article/10.11648/j.ijiis.20241302.11.
2. https://jivp-eurasipjournals.springeropen.com/articles/10.1186/s13640-024-00621-8.
3. https://powerhouseforensics.com/deepfake-forensics/types-of-deepfakes/.
4. https://english.elpais.com/technology/2024-02-28/what-are-deepfakes-their-risks-and-how-to-spot-them.html.
5. https://www.security.org/resources/deepfake-statistics/.
6. https://www.responsible.ai/a-look-at-global-deepfake-regulation-approaches/.
7. https://www.brookings.edu/articles/artificial-intelligence-deepfakes-and-the-uncertain-future-of-truth/.
8. https://en.wikipedia.org/wiki/Deepfake.

Д.В. Яценко

МЕТОДИКА ВИБОРУ ОПТИМАЛЬНОЇ МОДЕЛІ ДЛЯ РОЗВ'ЯЗАННЯ ЗАДАЧ ПРЕДИКТИВНОЙ АНАЛІТИКИ НА БАЗІ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ

Вступ: Вибір оптимальної моделі машинного навчання для прогнозування даних є важливим завданням, оскільки від цього залежить точність та ефективність отриманих результатів. Різноманіття доступних алгоритмів, типів даних і специфіки задач предиктивної аналітики ускладнюють процес моделювання. Відсутність універсальної моделі, яка б однаково добре вирішувала всі задачі, підкреслює необхідність детального аналізу та їх порівняння. Основні складності при виборі моделі включають:

різноманіття моделей та алгоритмів;
- недостатність та якість даних;
- шумові дані;
- перенавчання та недонавчання моделей;
- вибір релевантних ознак;
- вибір метрик ефективності;
- інтерпретація результатів;
- вимоги до обчислювальних ресурсів та часу навчання;
- схильність до упереджень;
- невизначеність майбутніх подій;
- зміна умов у даних (Data Drift);
- тип задачі (регресія, класифікація, кластеризація, тощо).

Мета і завдання дослідження: на основі проведення порівняльного аналізу основних моделей машинного навчання запропонувати методичний підхід для визначення оптимальної моделі, враховуючи переваги і недоліки існуючих підходів та описів предметних областей застосування для прогнозування та моделювання даних.

Матеріали та методи: У рамках дослідження були розглянуті та проаналізовані наступні моделі та алгоритми:
- моделі регресії:
- лінійна та поліноміальна регресії;
- логістична регресія для класифікаційних задач;
- дерева рішень та ансамблеві методи:
- дерева рішень;
- випадкові ліси;
- градієнтний бустинг;
- алгоритми на основі відстаней:
- К-найближчих сусідів;
- алгоритми кластеризації:
- кластеризація методом k-середніх;
- ієрархічна кластеризація;
- підтримуючі векторні машини (SVM);
- нейронні мережі та глибоке навчання:
- штучні нейронні мережі (ANN);
- конволюційні та рекурентні нейронні мережі для специфічних задач.

Для оцінки моделей використовувалися набори даних з відкритих джерел (UCI Machine Learning Repository). Застосовувалися відповідні метрики продуктивності:
- точність (Accuracy);
- точність (Precision);
- повнота (Recall);
- F1-міра (F1-score);
- середньоквадратична помилка (MSE - Mean Squared Error);
- середня абсолютна помилка (MAE - Mean Absolute Error);
- середня абсолютна відносна помилка (MAPE - Mean Absolute Percentage Error);
- корінь середньоквадратичної помилки (RMSE - Root Mean Squared Error);
- ROC-AUC (Receiver Operating Characteristic - Area Under Curve);
- R^2 (Коефіцієнт детермінації);
- матриця плутанини (Confusion Matrix);
- силуетний коефіцієнт (Silhouette Score);
- та інші.

Проводився аналіз обчислювальної складності моделей, їх схильності до перенавчання та вимог до обчислювальних ресурсів.

Результати: Порівняльний аналіз виявив наступне:

1. Лінійні моделі регресії прості та швидкі, підходять для лінійних залежностей, але неефективні для складних нелінійних взаємозв'язків.
2. Логістична регресія ефективна для бінарної класифікації, але обмежена при багатокласових задачах без відповідного розширення.
3. Дерева рішень інтуїтивно зрозумілі та здатні моделювати нелінійності, але можуть перенавчатися без обрізки.
4. Випадкові ліси знижують ризик перенавчання, забезпечуючи високу точність, але жертвують інтерпретованістю.
5. Градієнтний бустинг (наприклад, XGBoost) досягає високої продуктивності на складних задачах, але потребує ретельного налаштування гіперпараметрів.
6. SVM ефективні для високовимірних просторів та нелінійних меж рішень, але обчислювально затратні для великих наборів даних.
7. K-NN простий у реалізації, але чутливий до масштабування ознак та не підходить для великих обсягів даних.
8. Алгоритми кластеризації (K-Means, ієрархічна) корисні для виявлення структур у даних, але результати залежать від вибору кількості кластерів та метрики відстані.
9. Нейронні мережі демонструють високу точність у складних задачах (розпізнавання образів, обробка мови), але вимагають великих обсягів даних, значних обчислювальних ресурсів та є "чорними ящиками" з точки зору інтерпретації.

Висновок: В ході роботи проаналізовані методи рішення задач предиктивної аналітики та визначені метрики їх ефективності. Вибір оптимальної моделі залежить від специфіки задачі, характеристик даних та обмежень щодо ресурсів. Жодна модель не є універсально найкращою. Рекомендується проводити ітеративний процес моделювання, включаючи попередній аналіз даних, вибір та налаштування моделей, оцінку їхньої продуктивності за відповідними метриками та врахування можливих упереджень і змін у даних. Інтеграція кількох моделей (ансамблеві методи) може покращити результати.

1. James, G., Witten, D., Hastie, T., & Tibshirani, R. (2021). An Introduction to Statistical Learning with Applications in R (2-е видання). Springer. https://www.statlearning.com/.

2. Murphy, K. P. (2022). Probabilistic Machine Learning: An Introduction. MIT Press. https://probml.github.io/pml-book/book1.html.

3. Géron, A. (2019). Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow (2-е видання). O'Reilly Media. http://14.139.161.31/OddSem-0822-1122/Hands-On_Machine_Learning_with_Scikit-Learn-Keras-and-TensorFlow-2nd-Edition-Aurelien-Geron.pdf.

4. Chollet, F. (2021). Deep Learning with Python (2-е видання). Manning Publications. https://books.google.com.ua/books/about/Deep_Learning_with_Python_Second_Edition.html?id=XHpKEAAAQBAJ&redir_esc=y.

5. Aggarwal, C. C. (2018). Neural Networks and Deep Learning: A Textbook. Springer. https://link.springer.com/book/10.1007/978-3-319-94463-0.

6. Brownlee, J. (2020). Master Machine Learning Algorithms (2-е видання). Machine Learning Mastery. https://machinelearningmastery.com/master-machine-learning-algorithms/.

А.О. Устенко

ПРАКТИЧНІ КЕЙСИ ТА ДОСВІД ЗАСТОСУВАННЯ ШІ В ОСВІТНЬОМУ ПРОЦЕСІ

Стрімкі процеси інформатизації та глобалізації суспільства суттєво впливають на технології, які використовуються в системі освіти. Застосування сучасних інтелектуальних інформаційно-обчислювальних систем вимагає перегляду та модернізації стандартів освіти на всіх її ланках. На шляху реалізації інформативно-комунікативного підходу до навчання, яке спрямоване на індивідуалізацію, виникають проблеми, які пов'язані з достатнім рівнем підготовки здобувачів освіти та викладачів.

Ефективним інструментом для часткового вирішення проблем в освітньому процесі є штучний інтелект (ШІ). Інтеграція ШІ в освітні технології дозволяє збирати та аналізувати дані, які необхідні для моніторингу прогресу навчання. ШІ має потенціал трансформувати освіту шляхом оптимізації процесів викладання та навчання за допомогою персоналізованих алгоритмів навчання (Zilberman, 24). Але існують ризики, які пов'язані з впровадженням технологій ШІ щодо конфіденційності використання даних або упередженого ставлення до методів, які використовують машинно-генеровані ідеї та висновки. Отже, актуальною є задача розробки практичних кейсів як методів подолання труднощів, які виникають в освітньому процесі в умовах впровадження інформаційно-комунікативних технологій.

Метою даної роботи є аналіз існуючих програм ШІ в математиці та створення практичного кейсу для розв'язання проблем використання ШІ при навчанні математиці на прикладі застосунків Maplesoft.

В роботі (МакФарланд, 24) досліджено математичні інструменти ШІ та виділено вісім найкращих, які здатні змінити ландшафт математичної освіти та допомогти студентам і викладачам долати труднощі. Аналізуючи проведене дослідження, можна згрупувати означені вище інструменти ШІ за спільними особливостями (табл.1).

Таблиця 1 – Результати дослідження математичних інструментів ШІ

Інструменти ШІ	Вид програмного забезпечення	Ключові особливості
Julius AI	Онлайн-калькулятор	дозволяє розв'язувати алгебраїчні/тригонометричні рівняння/нерівності та пов'язані текстові задачі
Mathpapa	Мобільний додаток	дозволяє розв'язувати алгебраїчні/тригонометричні рівняння/нерівності та пов'язані текстові задачі, будувати графіки функцій
Socratic від Google	Мобільний додаток	універсальний за способами введення запитання, який охоплює теми алгебри/геометрії та використовує навчальні посібники, розроблені фахівцями
Photomath	Мобільний додаток	дозволяє розв'язувати широкий спектр задач від елементарної математики до диференціального та інтегрального числення, а також математичної статистики
MathGPTPro	Мобільний додаток	
Mathway	Онлайн-калькулятор	
SymboLab	Математична платформа, онлайн-калькулятор	використовує ШІ для надання покрокових рішень складних математичних задач
GeoGebra	Динамічне геометричне програмне забезпечення та система комп'ютерної алгебри	призначений для вивчення та викладання математики; поєднує геометрію, алгебру, електронні таблиці, статистику та обчислення

Представлені в табл. 1 математичні інструменти ШІ мають спільну особливість: вони надають інформацію про покрокове розв'язання певної задачі, що дозволяє покращити розуміння здобувачами освіти певних методів, які лежать в основі розв'язання. Деякі види інструментів ШІ допускають візуалізацію даних, анімацію прикладних результатів обчислень, що полегшує сприйняття абстрактних математичних понять. Але в списку

інструментів ШІ відсутні системи символьної математики, які дозволяють відтворювати весь процес отримання розв’язків типових математичних задач.

Прикладом такого програмного забезпечення може бути система комп’ютерної математики (СКМ) Maple, яка є математичним програмним забезпеченням, що поєднує найпотужніший у світі математичний двигун з інтерфейсом, що дозволяє надзвичайно легко аналізувати, досліджувати, візуалізувати та розв'язувати математичні задачі (*Explore Maplesoft's Products - Maplesoft*, б.д.). Maple є унікальним пакетом аналітичних обчислень, що має власну мову програмування та дозволяє не тільки розв’язувати прикладні задачі, а й створювати навчальні програми – маплети/maplets. За допомогою маплетів можна створювати діаграми, графіки, анімації тощо, які допомагають при розв’язанні задач та можуть використовуватись в інших математичних програмах (Нарадовий, 2023, с.16). Маплети дозволяють користувачам експериментувати, змінювати параметри та спостерігати процеси в реальному часі, що покращує розуміння складних математичних концепцій та заохочує до подальшого навчання. Маплети також можуть бути використані в наукових дослідженнях для розв’язання та аналізу диференціальних, інтегральних рівнянь та їх систем.

Висновки. Очевидно, що ефективність освітніх послуг сьогодні залежить від використання сучасних інтелектуальних технологій, які створені на основі ШІ. Величезний потенціал ШІ має сприяти адаптації здобувачів освіти до викликів, які пов’язані зі змішаною формою навчання. Грамотне використання ШІ та СКМ Maple в навчанні може перетворитись на безцінний інструмент для розвитку освітнього процесу, а також для підготовки майбутніх фахівців у будь-якій професійній галузі.

1. Zilberman, A. (24, 24 січня). Як ШІ впливає на систему освіти. Фейсер. https://www.grafiati.com/uk/info/apa-7/examples.

2. МакФарланд, А. (24, 31 жовтня). 8 найкращих AI для математичних інструментів (листопад 2024 р.). Unite.AI. https://www.unite.ai/uk/best-ai-for-math-tools/.

3. Explore Maplesoft's Products - Maplesoft. (б.д.). Maplesoft - Software for Mathematics, Online Learning, Engineering. https://www.maplesoft.com/products/.

4. Нарадовий, В. В. (2023). ВИКОРИСТАННЯ МАПЛЕТІВ У ВИКЛАДАЦЬКІЙ ДІЯЛЬНОСТІ ТА НАУКОВО-ДОСЛІДНІЙ РОБОТІ. Research Bulletin. Series: Issues of natural sciences, mathematics, technology and vocational education, (1), 16–21. https://doi.org/10.32782/cusu-pmtp-2023-1-2.

О. В. Жмай

ПЕРЕВАГИ ТА НЕДОЛІКИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ ВИЩОЇ ОСВІТИ

Вступ. Концепція четвертої промислової революції, яка багато в чому визначає сьогодні вектор розвитку сучасного світу, передбачає якісно новий підхід до виробництва товарів та послуг, в основі якого лежить масове впровадження інформаційних технологій не тільки в економічній галузі, а й в інших сферах діяльності. Цифровізація є ядром цього процесу, а штучний інтелект (ШІ), у свою чергу, постає як передова технологія. Починаючи з 2022 року, коли було здійснено різкий стрибок у цьому напрямку, зростає кількість суперечок про роль і доцільність, переваги та недоліки застосування ШІ у сфері вищої освіти. І, оскільки технології штучного інтелекту постійно розвиваються, з'являються пов'язані з цим як нові можливості, так і нові загрози.

Виклад основних результатів дослідження. Загалом сучасна система вищої освіти, яка здійснює свою діяльність в інформаційному суспільстві, має ряд особливостей, а саме:

1. Виникає таке поняття, як «інфляція інформації», коли збільшення наявних даних веде до їхнього знецінення. У цьому інформаційному потоці довіра втрачається вже й до фактичних даних, а студенти перестають сприймати навіть навчальну інформацію як серйозне знання, через що вона дедалі більше стає функціональною та операційною, що, в свою чергу, веде до прагматизації вищої освіти. В результаті випускник вишу часто стає «чистим» фахівцем, не будучи при цьому інтелектуалом. У таких умовах ШІ виявляється більш ефективним, оскільки він може створювати, перевіряти та підтримувати освітні алгоритми набагато краще, ніж викладач.
2. Відбувається інструменталізація навчальної інформації. Знання починають розглядатись не самі по собі, а як інструмент успіху; навчання у вузі втрачає свій статусний характер, інтерес для студентів становить лише отримання диплома. З цим пов'язана також слабка прихильність інформації до будь-яких інститутів, чому сприяє активний розвиток дистанційної та віртуальної освіти. Зрештою, це знижує кількість та якість особистої взаємодії викладача зі студентами, що значно спрощує впровадження штучного інтелекту у цю сферу.
3. Сильна залежність від Інтернету, за якої відвідування різних сайтів (насамперед соціальних мереж) стає своєрідним ритуалом, а студенти навіть під час занять не можуть тривалий час зберігати концентрацію на чомусь, породжує так звану інформаційну симуляцію. При цьому виникає ілюзія навчального процесу як з боку студентів, так і з боку викладачів.
4. Фрагментаризація знань, що виникає внаслідок формування у молодих поколінь кліпового мислення (і, своєю чергою, посилює цю тенденцію). Наслідком цього є те, що у студентів слабо розвивається зв'язність мислення, а системний підхід до викладу матеріалу поступово зникає.
5. Стандарти освіти дедалі більше формуються з урахуванням компетенцій, які поступово витісняють всебічний підхід до навчання. Внаслідок цього університети часто випускають вузьких спеціалістів, орієнтованих на конкретну професію. Однак при зникненні цієї професії такому співробітнику необхідно переучуватися на нову вузьку спеціальність. У цьому випадку людині стає важко конкурувати зі штучним інтелектом, чиє навчання відбувається набагато швидше та ефективніше. Особливо це стосується старших поколінь, які не звикли керуватися ідеєю безперервної освіти (lifelong learning).

На сьогоднішній день як вітчизняні, так і закордонні вчені не дійшли єдиного однозначного висновку про те, чи є вплив штучного інтелекту на сферу вищої освіти більшою мірою позитивним чи негативним. Багато в чому ця невизначеність виходить із того, що до кінця неясно, чому ШІ приймає ті чи інші рішення чи дає ті чи інші поради, а також нерозуміння того, в якому напрямку відбуватиметься його подальший розвиток.

У ситуації, що склалася, спостерігаються кардинальні зміни в науково-освітньому середовищі, особливо у сфері вищої освіти, що здійснюються для досягнення необхідних освітніх результатів здобувачів. В результаті, у низці навчальних закладів різних країн студентам заборонили використання ChatGPT [1], або навіть самим вишам довелося внести зміни до освітнього процесу — так, наприклад, Вища школа економіки у Празі замінила бакалаврські роботи на бакалаврський проект [2].

Однак незмінно зростаючий потенціал цифрових технологій призводить до формування у навчальних закладах нового цифрового освітнього середовища. Різноманітні інструменти, засновані на ШІ, активно використовуються вже сьогодні, і розуміння їх сильних та слабких сторін може допомогти робити це правильно. Адже ті ж чат-боти самі по собі не є добрими чи поганими, все залежить від того, хто, як і з якою метою їх використовує.

У будь-якого вищого навчального закладу є різні зацікавлені сторони, які тією чи іншою мірою впливають на нього. Можна виділити чотири основні групи стейкхолдерів: студенти, професорсько-викладацький склад, дослідники та адміністративний персонал. Всі вони по-різному впливають на університет, і всі вони по-різному можуть використовувати ШІ, оскільки їхні цілі та завдання також відрізняються. Тому видається логічним виділити переваги і недоліки штучного інтелекту не для сфери вищої освіти загалом, а для кожної із зацікавлених сторін окремо (табл. 1).

Таблиця 1 – Переваги та недоліки використання ШІ у сфері вищої освіти

	Переваги	Недоліки	
Студенти	- Персоналізація та індивідуалізація навчання - Підтримка та консультації 24/7 - Доступність навчання для студентів з особливими потребами	- Нестача взаємодії з іншими людьми - Різні можливості доступу до ШІ поглиблюють нерівність	Студенти
Викладачі	- Новий погляд на успішність та моделі навчання студентів - Нові інструменти та підходи до навчання	- Втрата «людського елементу» навчання - Посилення несправедливості й упередженості	Викладачі
Дослідники	- Полегшення співпраці між дослідниками - Прискорення досліджень (завдяки швидкому аналізу великих масивів даних) - Швидка обробка великих масивів даних - Виявлення нових закономірностей та трендів	- Етичні питання, пов'язані з упередженістю ШІ та недобросовісним використанням отриманих результатів	Дослідники
Адміністратори	- Зменшення витрат (завдяки автоматизації) - Покращення комунікації з викладачами та студентами	- Вартість впровадження ШІ-систем в університеті - Опір змінам з боку персоналу	Адміністратори

Джерело: складено автором на основі [3-7].

Деякі слабкі сторони стосуються всіх або майже всіх зацікавлених сторін, а саме:

- Потреба у додатковому навчанні для роботи з ШІ-інструментами (адміністратори, викладачі, дослідники).
- Побоювання щодо безпеки конфіденційних даних (студенти, адміністратори, дослідники).
- Надмірна довіра та залежність від ШІ (студенти, викладачі, дослідники).
- Втрата роботи чи зміна посадових обов'язків через впровадження ШІ (викладачі, дослідники, адміністратори та навіть студенти, у яких ШІ може забрати вакансії на неповний робочий день).

Так само можна виділити й спільні сильні сторони ШІ у сфері вищої освіти:

- Передача ШІ виконання рутинних адміністративних задач (усі стейкхолдери).
- Інсайти, засновані на аналітичних здібностях ШІ (усі стейкхолдери, якщо враховувати, що студенти можуть використовувати чат-боти для вирішення завдань, однак в такому випадку виникає питання, чи є це перевагою).

Виновки. Використання ШІ в освітній сфері здається неминучим. Ще в 2023 році викладання було серед галузей, де відзначався одним з найбільших рівенів впровадження генеративного ШІ (майже 20%), принаймні в США [8]. Ймовірно, у майбутньому ця тенденція тільки посилиться. При цьому більшість студентів, викладачів та інших стейкхолдерів у цій сфері бачать як переваги, так в недоліки такої практики, і вважають, що штучний інтелект може замінити певні функції викладача, але не представників цієї професії в цілому. Це означає, що такі побоювання пов'язані з **іншими людьми** (в першу чергу з тими, хто приймає рішення — менеджерами, адміністраторами тощо), а не з технологіями. Однак навіть просто використання інструментів ШІ в освіті має величезний вплив на те, які когнітивні функції людини залишаться затребуваними, яку освіту отримає молоде покоління тощо. Усе це, між іншим, визначить, яким буде світ через 10-15 років. І наше завдання полягає в тому, щоб люди знайшли своє місце в цьому світі.

1. Sullivan, M., Kelly, A. & McLaughlan, P. (2023). ChatGPT in higher education: Considerations for academic integrity and student learning. Journal of Applied Learning&Teaching, 6(1), 1-10. DOI: https://doi.org/10.37074/jalt.2023.6.1.17.

2. Fakulta VŠE ruší písemné bakalářské práce. Forbes. Retrieved from http://surl.li/btgoes.

3. Бабко Н. (2024) Штучний інтелект у вищій освіті: виклики, переваги та шляхи впровадження. Штучний інтелект у науці та освіті (AISE 2024). Artificial intelligence in science and education : збірник матеріалів міжнародної наукової конференції (Київ, 1-2 березня 2024 р.). Київ : УкрІНТЕІ. С. 23-25.

4. Zhmai A., Rudiak D. (2022) Advantages and disadvantages of using artificial intelligence in management. Збірник тез доповідей студентів, аспірантів та здобувачів – учасників 78-ї звітної конференції Одеського національного університету імені І. І. Мечникова (19–20 травня 2022 р., м. Одеса). Одеса : Олді+. С. 306-308.

5. Bobro N. (2024) Advantages and disadvantages of implementing artificial intelligence in the educational process. Young Scientist. №4 (128). Pp. 72-76. DOI: https://doi.org/10.32839/2304-5809/2024-4-128-38.

6. Advantages and disadvantages of AI in education. University Canada West. Retrieved from http://surl.li/aamggd.

7. Pros and Cons of AI in Higher Education. BestColleges. Retrieved from https://www.bestcolleges.com/research/ai-pros-cons-higher-education/.

8. 50+ AI Replacing Jobs Statistics 2024. AIPRM. Retrieved from https://www.aiprm.com/ai-replacing-jobs-statistics/.

А.С. Ковальова, Е.В. Рижков

МЕТОДИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ КІБЕРАТАК В УКРАЇНІ

З розвитком технологій питання кібербезпеки є вкрай важливим для забезпечення функціонування держави та її структур. Для протидії цим загрозам традиційні методи виявлення атак стають менш ефективними через їхню обмежену здатність обробляти великі обсяги даних у режимі реального часу. У цьому напрямку як раз таки штучний інтелект відкриває нам нові можливості для виявлення кібератак. Також допомога штучного інтелекту є вкрай вагомою спираючись на затяжну війну на території України, та у її кіберпросторі штучний інтелект може сприяти допомозі в значних кібератаках на: систему правоохоронних, розвідувальних, оборонних органів, банківські системи, системи державних та приватних установ, підприємств, організацій. Але розвиток не стоїть на місці і на даний момент в Україні працює ціла система органів кібербезпеки, до яких входять: Держспецзв'язок, Кібердепартамент СБУ, Кіберполіція України, Кіберпідрозділи ЗСУ та розвідувальні органи, МінЦифра, РНБО, НБУ, рекрути кібервійськ. Відповідний Указ про створення в Україні кібервійськ Президент України підписав у 2021 році [1], однак враховуючи новизну питання в Україні бракує фахівців, необхідних фінансів, розширених знань, тому штучний інтелект може стати у нагоді для найшвидшого покращення цієї системи [2, с. 35].

З напрацювань науковців розберемося у принципі роботи штучного інтелекту: спосіб використання штучного інтелекту у кібербезпеці є розробка передових алгоритмів, які допомагають виявляти та запобігати кібератакам. Ці алгоритми призначені для структурного аналізу великих обсягів даних та виявлення закономірностей, які можуть вказувати на реальну або потенційну загрозу. Обробляючи цю інформацію зі швидкістю та масштабами, які фізично неможливі для людини, системи штучного інтелекту можуть швидко виявляти потенційні та реальні кіберзагрози, вчасно реагувати на них, таким чином значно знижуючи ризики здійснення кібератак та її наслідки [3, с. 209].

Отже, розібравшись у принципі роботи штучного інтелекту можна виокремити такі шляхи його застосування в протидії кібератакам:

1) виявлення аномалій у мереживній поведінці - цей метод полягає у фіксації та виявленні нетипової поведінки у мережевному трафіку;

2) класифікація вхідних даних - даний метод може бути використаний для автоматичної класифікації мережевого трафіку, подій в системах або незвичних для системи дій;

3) прогнозування майбутніх кібератак на основі статичних даних - це можна обгрунтувати так: штучний інтелект може бути використаний для прогнозування потенційних атак шляхом аналізу старих кібератак і визначення моделей, які попереджають про можливі загрози;

4) розпізнавання шаблонів – це метод аналізу даних, який використовує алгоритми машинного навчання для автоматичного розпізнавання шаблонів і закономірностей у даних;

5) використання мультиагентної системи - це комп'ютеризована система, що складається з кількох взаємодіючих між собою штучних інтелектів "агентів", що працюють водночас.

Беручи до уваги усе вище сказане, можемо зробити висновок про те, що штучний інтелект відкриває нові горизонти в галузі кібербезпеки, зокрема у виявленні та протидії кібератакам. Завдяки своїй здатності обробляти великі обсяги даних у реальному часі та виявляти аномалії, штучний інтелект забезпечує значне покращення швидкості та точності виявлення загроз. В умовах поточної глобальної нестабільності в нашій державі, де кіберзагрози є невід'ємною та щоденною проблемою, інтеграція штучного інтелекту в системи кібероборони є надзвичайно важливою та недооціненою.

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави": Указ Президента України від 26.08.2021 р. №446/2021. URL: https://www.president.gov.ua/documents/4462021-40009.

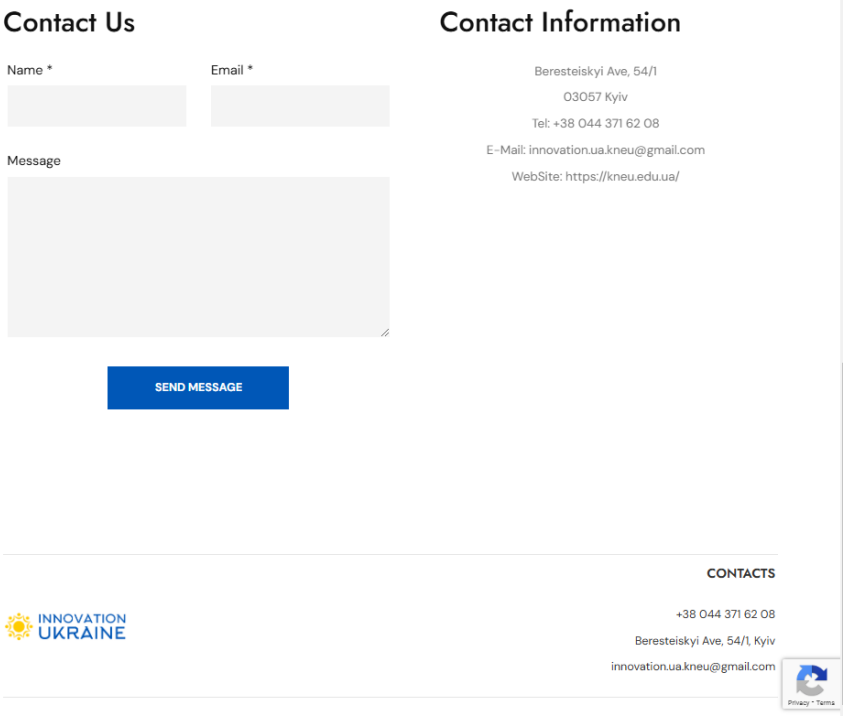
2. Рижков Е.В, Горбач В.С. Інформаційний фронт: захист україни від кіберзлочинності. Збірник матеріалів Міжнародної науково-практичної конференції (м. Кам'янець-Подільський, 23 травня 2024 року), с. 35-57. URL:https://dspace.univd.edu.ua/server/api/core/bitstreams/231e54c1-2c28-4c8a-befa-38c79967ff10/content#page=35.

3. Гуржій С.В. Особливості використання штучного інтелекту у питаннях забезпечення кібербезпеки. Інформація і право. № 4 (47)/2023, с. 207-216. URL: http://il.ippi.org.ua/article/view/291669.

GENERATIVE AI IN BYPASSING CAPTCHA: CHALLENGES FOR MODERN WEB PLATFORM SECURITY

A lot of cites and web platforms have contact forms that any anonymous user can feel to get in touch with administration. For example, a form from Innovation Ukraine [1] (Picture 1). The problem that such forms are vulnerable to spam attack, meaning that specifically form mentioned above can be used by bots to send undesired promotional emails. Let's analyze how defend systems from such attacks got impacted by modern generative artificial intelligence.

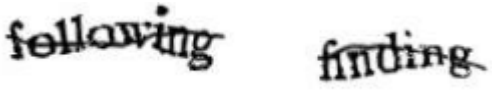
Worth mentioning that such attack is a risk from security point of view. It can do a real harm to the platform directly getting data from there or significantly impact its performance. On the other hand, such email can contain fishing and used by social engineers to steal personal data or credentials from administrator. Such cases are not rare and well described in published works specifically in context of attacking educational facilities [2]. So general rule is "the less spam emails get though, the less fishing emails will get to administrator, the less risk of social engineering".



Picture 1 – Form available for anonymous access

The problem of defending form anonymous forms abuse with such attacks is an old problem. First generic solution to this problem appeared in 2000, and was described in details in 2003 in article "CAPTCHA: Using hard AI problems for security" [3]. Authors introduced CAPTCHA standing for "completely automated public Turing test to tell computers and humans apart" the idea was to create "an automated test that humans can pass, but current computer programs can't pass" and force users to pass it before feeling such anonymous forms.

First CAPTCHAs were based on AI generated text injected with visual effects that didn't allow it to be decrypted by low resource consuming bot. Eventually majority of bots were starting to get through CAPTCHAs and protection solutions had to evolve.



Picture 2 – Early CAPCHA example

Historically, most popular and widely used CAPTCHA provider is Google owned commercial solution "reCAPTCHA" [4]. As for now they had released 3 major versions of reCAPTCHA:

- reCAPTCHA v1, released in 2007, based on typing (example on Picture 2) was depreciated in 2018 as ineffective
- reCAPTCHA v2 [5], released in 2013, based on user behavior on the web page analysis and forcing suspicious users to pass image selection challenge, still widely used and supported

- reCAPTCHA v3 [6], released in 2017, basically improved v2 with more advanced system of behavior tracking and new more complicated challenges

Latest updates of reCAPTCHA v3 includes such challenges:

- Select specific images
- Drag objects into position
- Tap matching image pairs
- Click on a moving target

Google never aimed to create an absolutely secure solution. Their promoted goal was to prevent "majority" of bots from attacking the cite with minimal impact onto user experience. That's why reCAPTCHA v3 is also known as "invisible" because algorithms improvement allowed to show tasks several times less often than for v2.

But new cloud based LLM solutions like GPT-4 popularity impacted the situation significantly. Popularity of such services increased the demand for text generation (including instructions that can be used to emulate human behavior on the page) and image classification.

Which made bots for passing reCAPTCHA v3 cheaper and as is their effectiveness decreased. Unfortunately, there is no publicly available statics proving this fact, but there are hundreds of administrators complaining about bots passing reCAPTCHA v3 during last half year [7].

From subjectively well indexed in google search Innovation Ukraine (first result in google for "innovation ukraine") administrating point of view the problem exists. For the last half year configured reCAPTCHA v3 was passed by 8 emails, 5 of them during last two month. Single web-platform example statistically doesn't prove the scale of problem, but the idea of traditional reCAPTCHA doesn't work.

In conclusion, for now, there is no simple public program that can be attached to the web platform and not be passed by "majority" of bots without additional configurations or costly programmatic adjustments. There is a prospect for a deeper investigation on how specifically new bots are passing reCAPTCHA v3 and on searching for a generic solution of such problems attack.

1. "About Us – Innovation Ukraine," 2024. https://www.innovationukraine.com/about-us/.
2. Google for Developers, "reCAPTCHA V3." Google for Developers, 2024. https://developers.google.com/recaptcha/docs/v3.
3. Google for Developers, "reCAPTCHA V2.," 2024. https://developers.google.com/recaptcha/docs/display.
4. Von Ahn, L., M. Blum, N.J. Hopper, and J. Langford. "CAPTCHA: Using Hard AI Problems for Security." Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 2656 (2003): 294–311. https://doi.org/10.1007/3-540-39200-9_18.
5. Von Ahn, L., B. Maurer, C. McMillen, D. Abraham, and M. Blum. "reCAPTCHA: Human-Based Character Recognition via Web Security Measures." Science 321, no. 5895 (2008): 1465–68. https://doi.org/10.1126/science.1160379.
6. Redit. "Bots Are Passing Google reCaptcha," April 2024. www.reddit.com/r/webdev/comments/1c7sf7r/bots_are_passing_google_recaptcha/.
7. Hu, Z., V. Buriachok, and V. Sokolov. "Implementation of Social Engineering Attack at Institution of Higher Education," 2654:155–64, 2020.

В.А. Заглинський

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В OSINT: ПЕРЕВАГИ ТА ВИКЛИКИ

У наш час, коли інформаційні потоки досягають безпрецедентних масштабів, технології штучного інтелекту (ШІ) стають не лише незамінним інструментом, а й необхідним компонентом для глибокого аналізу відкритих джерел (OSINT) [1]. Спостереження за динамікою даних, що надходять з різних публічних платформ, таких як новинні сайти, соціальні медіа та блоги, набуває стратегічної важливості для прийняття обґрунтованих рішень у політичній, економічній, соціальній та комерційній сферах. Завдяки своєму потенціалу до автоматизації обробки величезних обсягів даних, ШІ забезпечує швидке, ефективне та точне трактування інформації з відкритих джерел.

Однією з ключових переваг інтеграції ШІ в OSINT є його здатність автоматично обробляти та систематизувати колосальні масиви відкритих даних. Завдяки алгоритмам, що постійно моніторять і аналізують різноманітні джерела, такі як новинні портали, форуми, соціальні мережі й навіть медіа-ресурси в реальному часі, ці системи здатні оперативно виявляти значущі зміни в соціально-політичних процесах, економічних коливаннях або нових подіях, що потребують швидкого реагування [2].

Інструменти на базі штучного інтелекту, такі як алгоритми обробки природної мови (NLP), зокрема, демонструють значну ефективність в аналізі соціальних медіа. Вони дозволяють не тільки виявляти ключові теми й емоційні настрої публікацій, а й вчасно фіксувати потенційні маніпуляції або поширення дезінформації. Алгоритми можуть на льоту виявляти тренди, аналізувати текстові, графічні та відео-дані, а також відстежувати зміни в суспільних настроях — фактори, які можуть бути критично важливими для розуміння сучасних соціальних процесів.

Проте великий обсяг неструктурованої інформації, яка містить різноманітні формати даних (тексти, зображення, відео, аудіо), становить певні труднощі для традиційних методів обробки. Водночас технології ШІ, такі як комп'ютерний зір (CV) та обробка природної мови, ефективно долають ці виклики. Завдяки таким технологіям можна здійснювати не лише текстовий, але й мультимедійний аналіз, а також точно визначати важливі події або аномалії, що можуть сигналізувати про підозрілу активність у реальному часі [3].

Однак у процесі збору відкритих даних постає ще одна важлива проблема — достовірність інформації. Оскільки відкриті джерела не завжди є надійними, критично важливим є наявність вбудованих механізмів перевірки та фільтрації, що дозволяють мінімізувати ризик включення маніпулятивних або неправдивих відомостей у процес аналітики.

ШІ також неодноразово доводив свою ефективність у виявленні аномалій, які можуть свідчити про загрози або непередбачувані зміни, що набирають обертів. Від виявлення фінансових махінацій до прогнозування соціальних чи політичних нестабільностей — алгоритми машинного навчання дозволяють виявляти порушення звичних патернів поведінки, що може вчасно попередити про ймовірні кібератаки, фінансові шахрайства чи навіть громадські заворушення.

Штучний інтелект не менш важливий і в боротьбі з фальшивими новинами. Використовуючи аналіз схем поширення інформації і виявлення поведінкових аномалій користувачів, ШІ здатний сигналізувати про маніпуляції задовго до того, як це стане очевидним для звичайного спостерігача. Цей інструмент можна порівняти з маяком, що дозволяє розпізнавати потенційні загрози ще на етапі їх зародження.

Не можна оминути й перспективи розвитку, що відкриваються завдяки інтеграції ШІ з технологіями блокчейн та Інтернетом речей (IoT). Блокчейн дасть можливість забезпечити прозорість та непідробність даних, що надходять з відкритих джерел, а IoT сприятиме збору даних у реальному часі, наприклад, з сенсорів, що фіксують зміни у фізичному середовищі. Це дозволить більш швидко реагувати на критичні ситуації та значно покращить процес аналізу важливої інформації.

Очікується, що в майбутньому такі інтегровані платформи, що поєднують ШІ, блокчейн і IoT, дозволять створювати автоматизовані системи для раннього виявлення кризових ситуацій, таких як природні катастрофи або терористичні загрози. Прогнозується, що ці технології дозволять зменшити затримки в ухваленні рішень і значно підвищать ефективність реагування на глобальні виклики.

Інновації в області глибоких нейронних мереж та когнітивного навчання дозволяють ще точніше аналізувати складні та багатовимірні дані, що відкриває нові можливості для прогнози соціальних і політичних змін. З розвитком таких технологій ШІ стане здатним автоматизувати не тільки виявлення трендів, а й точніше прогнозувати розвиток ситуацій у різних сферах життя.

Важливою складовою майбутнього розвитку ШІ є його адаптивність. Системи, здатні безперервно вчитися на нових даних і коригувати свої алгоритми відповідно до змінних умов, обіцяють знижувати потребу в постійному оновленні та втручанні людини, забезпечуючи ефективну роботу в реальному часі з мінімальними затримками [4].

Не менш важливим є й розвиток інтерфейсів, що спрощують взаємодію з інструментами ШІ. В результаті цього аналітики, журналісти, державні установи та навіть малий бізнес зможуть ефективно працювати з великими даними, не маючи глибоких технічних знань. Поліпшення інтерфейсів зробить ці інструменти доступнішими для широкого кола користувачів, дозволяючи приймати обґрунтовані рішення на основі аналітики навіть без спеціалізованої підготовки.

Зважаючи на потенційні етичні та правові питання, які можуть виникати у контексті застосування ШІ в OSINT, важливо виробити чіткі стандарти та регуляції. Питання конфіденційності, захисту персональних даних і прозорості алгоритмів мають стати основними аспектами майбутнього розвитку цієї технології. Тільки в такому разі використання ШІ не буде загрожувати безпеці та правам людини в епоху глобалізованих інформаційних потоків.

Отже, штучний інтелект вже сьогодні радикально змінює підходи до збору та аналізу відкритих даних, і його роль у сфері OSINT буде лише зростати. Завдяки здатності до автоматизації збору інформації, прогнозування трендів і виявлення аномалій, ШІ відкриває нові горизонти для швидкого прийняття рішень у різних сферах. І в майбутньому, завдяки інтеграції новітніх технологій, таких як блокчейн і IoT, а також удосконаленню інтерфейсів і етичних стандартів, застосування ШІ в OSINT стане ще більш ефективним, безпечним і результативним, що дозволить оперативно реагувати на виклики глобального масштабу.

1. Іванов І.І. Технології штучного інтелекту для обробки відкритих джерел інформації. — Київ: Вид-во НТУ, 2020. — 250 с.
2. Василенко О.М. Технології штучного інтелекту для обробки масивів даних у відкритих джерелах. — Київ: Міжнародна академія, 2022. — 215 с.
3. Гречко В.А. Мультимедійний аналіз за допомогою штучного інтелекту: принципи і практичні аспекти. — Львів: Техно-Інформ, 2020. — 150 с.
4. Журавель М.А. Адаптивні системи на основі ШІ: нові можливості та підходи. — Київ: Прогрес, 2020. — 290 с.

А.В. Бондаренко, Г.В. Разумова

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПРОЦЕСІ ПРИЙНЯТТЯ СТРАТЕГІЧНИХ РІШЕНЬ

У світі, де швидкість змін зростає, а конкуренція стає дедалі більшою, здатність приймати обґрунтовані стратегічні рішення є ключовою для виживання і розвитку бізнесу.

Штучний інтелект (ШІ) стає важливим інструментом у багатьох сферах діяльності, від фінансів до маркетингу, логістики та управління ризиками. Його здатність обробляти і аналізувати великі масиви даних дозволяє робити точніші прогнози, виявляти приховані тенденції та оптимізувати процеси.

Сучасний розвиток ШІ вказує на те, що з часом його впровадження ставатиме дедалі простішим, а його ефективність продовжуватиме зростати. ШІ розвивається стрімкими темпами: за останнє десятиріччя він пройшов шлях від відносно простих алгоритмів, що виконували суто дослідницькі та розважальні функції, до потужного інструменту, що підтримує соціальну та економічну діяльність. Збільшення користі від ШІ стало можливим завдяки паралельному прогресу в суміжних технологіях, що вже стали основою інформаційної економіки. Серед них – CRM-системи, передові алгоритми збору даних, Big Data та інноваційні підходи до гнучкого виробництва, які суттєво змінюють діяльність ринкових гравців.

Використання штучного інтелекту надає компаніям значні переваги в процесі стратегічного прийняття рішень. ШІ дозволяє автоматизувати рутинні завдання, такі як обробка замовлень, розподіл ресурсів, аналіз великих обсягів даних тощо. Завдяки алгоритмам машинного навчання бізнеси можуть точніше прогнозувати показники попиту, витрат, доходів та інші ключові параметри, що підвищує ефективність управлінських рішень. ШІ дозволяє компаніям приймати рішення, спираючись на дані та аналітику, що знижує суб'єктивний вплив людського фактору і зменшує ризик помилок. Завдяки адаптивності таких систем компанії здатні швидко реагувати на зміни ринкових умов, зберігаючи конкурентоспроможність у динамічному середовищі. ШІ також відкриває можливості для створення персоналізованих стратегій, які враховують індивідуальні потреби різних сегментів ринку, підвищуючи клієнтоорієнтованість і, відповідно, лояльність аудиторії [1].

Серед усіх функцій компанії саме маркетинг найбільше виграє від розумного застосування ШІ. Основні завдання маркетингу включають розуміння потреб клієнтів, створення оптимального Product-Market Fit, переконання споживачів у виборі саме цього продукту та вигідне позиціонування серед конкурентних пропозицій, і ШІ може значно посилити ці можливості. У 2021 році глобальний ринок ШІ для маркетингу оцінювався в 15,84 млрд доларів. За прогнозами дослідників, до 2028 року цей показник перевищить 107,5 млрд доларів [2].

Водночас важливо розуміти, що використання ШІ в стратегічному управлінні бізнес-процесами не є бездоганним та має певні недоліки. Для досягнення максимальної точності та ефективності штучний інтелект вимагає значних обсягів якісних, різноманітних і репрезентативних даних. У разі нестачі даних або при низькій їхній якості результати роботи ШІ можуть бути неточними, що здатне спричинити помилкові рішення з негативними наслідками для бізнесу.

Крім цього, впровадження ШІ в системи управління бізнес-процесами є складним і витратним процесом, оскільки потребує істотної модернізації інфраструктури та значних інвестицій у навчання персоналу. Підготовка співробітників до роботи з новими технологіями стає ще однією суттєвою статтею витрат, адже для максимальної ефективності потрібні спеціалізовані знання та навички. Тому впровадження ШІ, хоч і є перспективним, потребує зваженого підходу з урахуванням потенційних бар'єрів.

Generative AI (генеративний штучний інтелект) став однією з ключових стратегічних технологій для бізнесу у 2022 році. Ця технологія дозволяє створювати новий контент і розробляти унікальні алгоритми, базуючись на аналізі даних, і використовується для автоматичного генерування текстів, зображень, аудіо та навіть програмного коду. Основною перевагою Generative AI є його здатність адаптуватися до специфічних потреб підприємства, розробляючи інноваційні рішення, що відповідають унікальним завданням бізнесу. Водночас важливо приділяти увагу етичним аспектам і забезпеченню безпеки даних під час використання Generative AI, щоб уникнути ризиків, пов'язаних із конфіденційністю інформації та соціальною відповідальністю [1].

Отже, ШІ відкриває безпрецедентні можливості для бізнесу, особливо у стратегічному плануванні та прийнятті рішень. Правильне впровадження цих технологій дозволить компаніям підвищити точність прогнозування, ефективність операцій та адаптивність до змін ринку. Проте для цього необхідно враховувати всі ризики, пов'язані з конфіденційністю даних, етикою та інтеграцією, а також постійно працювати над підвищенням кваліфікації персоналу. Штучний інтелект стає ключовим фактором для бізнесу, що прагне досягти успіху в сучасному світі.

1. Дриньов Д.М., Загородніх В.В., Зінченко О.М. Застосування штучного інтелекту в системі управління підприємством. Економічний простір. 2023. Випуск 188. С. 79-82. https://doi.org/10.32782/2224-6282/188-13.

2. Таранич А.В., Пелехацький Д.О. Використання штучного інтелекту у процесі стратегічного прийняття рішень. Економіка України. 2024. № 1. С. 54-65. URL: http://nbuv.gov.ua/UJRN/EkUk_2024_1_5.

3. Yudina S., Lysa, O., Razumova H., Oskoma O., Halahanov V. Management and administration of financial resources using digital technologies. Scientific Bulletin of Mukachevo State University. Series "Economics". 2024. № 11 (1). С. 92-102. https://doi.org/10.52566/msu-econ1.2024.92.

А.В. Бондаренко, О.В. Оскома

ВЗАЄМОЗАЛЕЖНІСТЬ ШТУЧНОГО ІНТЕЛЕКТУ ТА BIG DATA: ВИКЛИКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Світ, в якому ми живемо, перетворюється на цифрову реальність, де дані стають новою валютою. Штучний інтелект (ШІ) та великі дані (Big Data) – це два ключових технологічних тренди, які глибоко переплітаються і визначають напрямки розвитку суспільства та економіки.

ШІ та Big Data тісно пов'язані між собою. Великі дані є «паливом» для ШІ, оскільки алгоритми штучного інтелекту потребують великих обсягів даних для навчання і розвитку. ШІ, в свою чергу, дозволяє аналізувати великі масиви даних, виявляти в них закономірності та робити прогнози, що було б неможливо для людини.

Взаємозалежність штучного інтелекту та Big Data створює як нові можливості, так і суттєві виклики, зокрема в питаннях конфіденційності, етики та якості даних.

Одним із головних аспектів є конфіденційність та безпека. ШІ і Big Data часто працюють з великим обсягом даних, які можуть містити особисту інформацію користувачів. Під час обробки таких даних виникають значні ризики витоку інформації та зловживання особистими даними. Використання персональних даних без згоди людини чи неналежне захищення інформації може призвести до серйозних порушень конфіденційності[1].

Етичні проблеми також займають важливе місце серед викликів, з якими стикаються ШІ та Big Data. Автоматизовані рішення, які приймаються на основі аналізу великих даних, можуть суттєво впливати на життя людей — від ухвалення рішень у фінансовій сфері до прогнозування поведінки користувачів у соціальних мережах. Відсутність належного контролю та регуляції може призвести до проявів дискримінації та упередженості, особливо якщо навчальні моделі ШІ формуються на базі даних, що містять соціальні чи расові упередження. Це може спричинити несправедливе ставлення до певних груп людей і навіть вплинути на суспільні цінності.

Обсяг і якість даних є ще одним критичним аспектом у взаємодії ШІ і Big Data. Не всі зібрані дані є релевантними або корисними для навчання алгоритмів штучного інтелекту. Дані можуть бути застарілими, неповними або містити інформаційний шум, що ускладнює роботу ШІ і призводить до зниження точності його рішень. Очищення даних та фільтрація є важливими етапами, що забезпечують високу якість інформації для навчання моделей. Ефективні методики обробки даних дозволяють відсівати нерелевантні дані та підвищувати коректність роботи ШІ, зменшуючи ризик хибних результатів або некоректних прогнозів.

Синергія штучного інтелекту та Big Data відкриває численні перспективи, які можуть змінити бізнес і суспільство в цілому. Однією з найважливіших тенденцій є персоналізація послуг. Завдяки аналізу великих обсягів даних про поведінку користувачів, ШІ здатний надавати індивідуалізовані рекомендації, що покращує взаємодію між споживачами і постачальниками послуг[2].

Автоматизація рутинних завдань також є суттєвою перспективою. ШІ може виконувати багато процесів, які раніше вимагали участі людини, що підвищує продуктивність і дозволяє працівникам зосередитися на більш важливих завданнях. Це веде до зниження витрат та підвищення ефективності бізнесу.

Крім того, ШІ відіграє важливу роль у наукових відкриттях, допомагаючи вченим знаходити нові закономірності в даних, що може призвести до інновацій у галузях, від медицини до астрономії.

Перспективи розвитку "розумних міст" також значні. Інтеграція ШІ та Big Data в міське планування може оптимізувати транспортні системи та енергоспоживання, покращуючи якість життя мешканців.

Нарешті, розвиток ШІ і Big Data сприяє створенню нових бізнес-моделей. Компанії можуть використовувати дані для розробки інноваційних продуктів і послуг, що відповідають змінюючим потребам споживачів. Нові моделі бізнесу можуть базуватися на підписках, обміні даними або пропозиціях, що адаптуються в реальному часі. Це дозволяє підприємствам бути більш гнучкими та реагувати на ринкові зміни.

Отже, взаємодія штучного інтелекту та великих даних відкриває перед нами безмежні можливості. Для того щоб максимально використати потенціал ШІ та Big Data, важливо знайти баланс між інноваціями і відповідальним управлінням даними, встановлюючи чіткі етичні і правові норми. Тільки таким чином можна забезпечити стійкий розвиток цих технологій, що принесе користь суспільству в цілому.

1. Яковенко Я.О., Білик М.Ю., Олійник Є.В. Штучний інтелект, big data і відповідальне споживання як імператив інноваційного розвитку бізнес-структур в умовах формування цифрової економіки. Економіка та суспільство. Випуск 60/2024. URL: https://economyandsociety.in.ua/index.php/journal/article/view/3681.

2. Горобець О. О. Взаємозалежність штучного інтелекту та великих даних: перспективи використання в економіці. Бізнес-аналітика в управлінні зовнішньоекономічною діяльністю: Матеріали Міжнародної науково-практичної конференції. URL: https://www.researchgate.net/publication/371169246_Vzaemozaleznist_stucnogo_intelektu_ta_velikih_danih_perspektivi_vikoristanna_v_ekonomici.

П.І. Сагайда, І.А. Гетьман, М.А. Держевецька

ПРОЦЕС УДОСКОНАЛЕННЯ КІБЕРБЕЗПЕКИ З ВИКОРИСТАННЯМ МЕТОДІВ МАШИННОГО НАВЧАННЯ, ЯК СКЛАДОВОЇ ІНФОРМАЦІЙНОЇ ПІДТРИМКИ ДІЯЛЬНОСТІ НА ОСНОВІ ЦИФРОВОГО ІНТЕЛЕКТУ

Сьогодні рівень кіберзлочинності зростає до тривожного рівня, тому вже включений до порядку денного національної безпеки та оборони практично всіх країн [1], в тому числі, України. Ці злочини є глобальною епідемією, яка вражає кожну комп'ютерну систему у світі. Профіль кіберзлочинця більше не пов'язаний з експертом і ентузіастом-хакером, який має на меті зламати безпеку для тестування систем. Технічно розвинені країни зараз більше залучені до інцидентів у сфері безпеки з різним впливом (як через політичні, так і через економічні причини). У той же час злочинні організації, як правило, змінюють сферу своєї діяльності, щоб зробити свою злочинну практику більш витонченою. Кіберзлочинність стала більш професійною, розумною та прихованою [2]. Це призвело до зміни кількості нападів, які останніми роками трапляються ще частіше. Почастішали атаки, спрямовані на використання вразливостей, що існують в інформаційних системах, з боку критичних інфраструктур [2], а також зі стратегічних сфер, таких як енергетика або водопостачання, охорона здоров'я, транспорт або фінанси. Крім того, малі та середні підприємства (МСП) через свою слабкість та значимість у діяльності та економіці країни також є актуальними цілями. Атаки МСП спрямовані на порушення або переривання їх базових структур, що має величезний вплив як на суб'єкта господарювання, так і на безперервність його послуг, які, іноді, є важливими.

Таким чином, важливою складовою забезпечення цифрової обізнаності робітників та цифрової трансформації організаційно-технічних систем є підвищення рівня цифрового інтелекту випускників магістерських освітніх програм за рахунок освоєння ними компетентностей, пов’язаних з вміннями та навичками забезпечення кібербезпеки – впровадження заходів з кібербезпеки для захисту від загроз у цифровому середовищі. Вагомою складовою таких заходів, інформаційну підтримку яких повинні забезпечувати випускники освітньо-професійних програм (ОПП) спеціальності 122 «Комп’ютерні науки», а особливо, ОПП «Комп’ютерні науки та цифровий інтелект», є удосконалення кібербезпеки інформаційних систем з використанням методів машинного навчання. Для того, щоб визначитись з необхідним вмістом освітніх компонентів даної ОПП в цьому аспекті підготовки, було досліджено процеси такого удосконалення, формалізовано алгоритми та підходи до її реалізації.

Удосконалення кібербезпеки інформаційних систем з використанням методів машинного навчання повинно виконуватися за рахунок його використання за наступними напрямками:

1. Автоматизоване виявлення загроз: машинне навчання дозволяє створити системи, які автоматично виявляють аномалії та потенційні загрози для інформаційних систем, підвищуючи швидкість реагування на атаки.
2. Прогнозування поведінки зловмисників: застосування методів машинного навчання допомагає визначати шаблони дій зловмисників, забезпечуючи можливість попередження атак на інформаційні системи.
3. Адаптивний захист: системи кібербезпеки, що використовують машинне навчання, можуть адаптуватися до нових видів загроз, навчаючись на льоту та оновлюючи свої захисні механізми.
4. Виявлення аномалій: методи машинного навчання дозволяють системам виявляти незвичайні патерни та аномалії у поведінці системи або користувачів, що може вказувати на потенційні загрози.
5. Зменшення хибних тривог: штучний інтелект у кібербезпеці спроможний зменшити кількість помилкових спрацювань систем безпеки, що дозволяє більш точно визначати загрози.
6. Удосконалення відновлення після атак: машинне навчання допомагає створювати системи, які вчяться із попередніх атак та швидко адаптуються для попередження майбутніх інцидентів.
7. Оптимізація захисту в реальному часі: застосування алгоритмів машинного навчання дозволяє створити системи, які аналізують та реагують на загрози у реальному часі, забезпечуючи миттєву відповідь на атаки.
8. Розширення області виявлення загроз: машинне навчання дозволяє розширити спектр виявлення загроз, охоплюючи раніше невідомі види атак.
9. Забезпечення автономності захисту: системи кібербезпеки, засновані на машинному навчанні, можуть функціонувати автономно, адаптуючись до змінних умов без необхідності постійного втручання.
10. Підвищення ефективності захисту: використання методів машинного навчання у кібербезпеці дозволяє створювати більш ефективні та інтелектуальні системи захисту, зменшуючи ймовірність успіху кібератак та мінімізуючи шкоду від інцидентів.

Наступний опис слугує основою для побудови структурно-функціональної схеми бізнес-процесу «Удосконалення кібербезпеки з використанням методів машинного навчання» у відповідній нотації:

1. Вхідні дані: дані, які поступають до процесу, наприклад, дані про загрози, інформація про системи безпеки тощо.
2. Аналіз загроз: цей етап включає методи машинного навчання для аналізу та виявлення потенційних загроз для інформаційних систем.
3. Розробка захисних стратегій: на основі результатів аналізу створюються стратегії захисту від виявлених загроз.

4. Впровадження систем захисту на основі впровадження рішень з кібербезпеки, які базуються на машинному навчанні.

5. Моніторинг та апгрейд: після впровадження системи кібербезпеки потрібно постійно моніторити для виявлення нових загроз та вдосконалення системи захисту.

6. Вихідні дані: результати та звіти, які включають в себе оновлені стратегії безпеки та відповіді на потенційні загрози.

Окремо треба зазначити, що система інформаційної підтримки удосконалення кібербезпеки інформаційних систем з використанням методів машинного навчання повинна базуватися на відповідній базі даних. Сучасний підхід для розпізнавання шахрайських дій та підозрілих операцій, в тому числі таких, що несуть загрозу кібербезпеці, полягає у створенні та відповідному використанні графових баз даних. Їх перевогою у порівнянні з звичними реляційними, або навіть документо-орієнтованими базами даних, полягає у відстежуванні послідовностей дій кіберзлочинців, які можуть бути представлені у вигляді графів взаємозв'язків та оброблені алгоритмами graph data science для визначення відповідних шаблонів на етапі машинного навчання, і швидкого їх пошуку в майбутньому.

Для кожного етапу розглянутого бізнес-процесу проаналізовані їх складові, послідовність виконання або взаємодії, побудовано відповідні діаграми активностей, запропоновано відповідні модулі для наповнення змістом освітніх компонентів, які, після їх освоєння студентами галузі «Інформаційні технології», дозволять розвинути компетентності і досягнути рівня цифрового інтелекту, що дозволять вирішувати проблеми організації та впровадження засобів кібербезпеки на основі методів машинного навчання.

Висновки. Застосування системного підходу до аналізу предметної області «Удосконалення кібербезпеки з використанням методів машинного навчання, як складової інформаційної підтримки діяльності з використанням цифрового інтелекту» дозволило визначити основні напрямки та підходи до забезпечення надійного захисту сучасних інформаційних систем, які стикаються з посилення загроз від зовнішнього втручання та знищення. Формалізація результатів аналізу та дослідження з використанням діаграмних методик, визначення методики застосування машинного навчання для удосконалення процесів аналізу та запобігання несанкціонованим та навмисним діям вимагає від адміністраторів інформаційних систем та їх користувачів всебічного розвитку їх цифрового інтелекту, застосування відповідних знань та навичок для відповідального використання складних інформаційних технологій.

1. Lopez, M. A., Lombardo, J. M., López, M., Alba, C. M., Velasco, S., Braojos, M. A., & Fuentes-García, M. (2020). Intelligent Detection and Recovery from Cyberattacks for Small and Medium-Sized Enterprises. International Journal of Interactive Multimedia and Artificial Intelligence, 6(3), 55. https://doi.org/10.9781/ijimai.2020.08.003.

2. Kaushik, K., & Sharma, I. (Ред.). (2024). Next-Generation Cybersecurity. Springer Nature Singapore. https://doi.org/10.1007/978-981-97-1249-6.

А.О. Попова, О.М. Любименко, Н.О. Маслова, О.А. Штепа

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ ДАНИХ ТА ВИЯВЛЕННЯ АНОМАЛІЙ У СИСТЕМІ КВАДРАТИЧНОГО ГОЛОСУВАННЯ НА БЛОКЧЕЙНІ

Блокчейн - це інноваційна розподілена технологія зберігання даних, яка фіксує інформацію у формі послідовного ланцюга блоків, з'єднаних між собою криптографічними хешами. Вона забезпечує безпечне, прозоре середовище для обміну інформацією та здійснення транзакцій без участі посередників. Спочатку створена для криптовалюти Bitcoin у 2008 році, блокчейн-технологія тепер набуває широкого використання в різних галузях [1].

Принцип децентралізації в блокчейні означає, що жодна сторона не має одноосібного контролю над даними, а система керується мережею вузлів, які підтверджують транзакції за допомогою алгоритмів консенсусу. Це робить блокчейн потужним інструментом для збереження цілісності даних та запобігання фальсифікації.

При виборі стратегій голосування, що забезпечують справедливе колективне прийняття рішень, метод квадратичного голосування вирізняється як ефективний підхід, що враховує інтенсивність переваг виборців. Квадратичне голосування дозволяє учасникам не лише віддати голоси за певні варіанти, але й виразити силу своїх переконань шляхом розподілу кредитів. Кількість голосів, яку виборець хоче віддати на певну альтернативу, зростає за квадратичною функцією, що ускладнює концентрацію голосів без значних витрат.

Завдяки такому підходу квадратичне голосування захищене від сибіл-атак, коли зловмисники створюють безліч підроблених акаунтів. Це економічно невигідно, оскільки вартість кожного додаткового голосу зростає пропорційно квадрату витрачених кредитів. Модель квадратичного голосування легко інтегрується в блокчейн, забезпечуючи прозорість і надійність процесу. Ця модель стимулює виборців приймати більш обдумані рішення, оскільки виборці повинні ретельно зважувати свої переваги через обмеженість кредитів і зростаючу вартість додаткових голосів.

У моделі квадратичного голосування застосовується математичний підхід, де кожен голос має свою вартість, яка зростає квадратично зі збільшенням кількості голосів. Це дозволяє знизити вплив окремих виборців та забезпечити більш збалансоване прийняття рішень.

У представленій формулі (1) сума внесків спонсорів для конкретного проекту визначається як сума квадратів кількості голосів, що виділяються кожним спонсором. Це дозволяє обмежити максимальний вплив одного виборця і стимулює ретельно обирати підтримувані проекти [2].

$$s(p_m) = \sum_{i=1}^{n} c_i^2 , \quad (1)$$

де p_m – проект, висунутий на голосування;
m – загальна кількість проектів на голосуванні;
s – сума вкладу спонсорів за голоси;
n – загальна кількість спонсорів;
c_i – кількість голосів спонсора.

Загальний бюджет конкурсу (2) представлений як сума внесків усіх спонсорів для всіх проектів, що є на голосуванні.

$$b = \sum_{i=1}^{m} s(p_i) , \quad (2)$$

де b – бюджет конкурсу;
p_i – проект, висунутий на голосування;
s – сума вкладу спонсорів за голоси;
m – загальна кількість проектів на голосуванні.

Інтеграція методів штучного інтелекту у систему квадратичного голосування на блокчейні надає нові можливості для моніторингу та аналізу процесу голосування в режимі реального часу, значно підвищуючи безпеку та прозорість процесу. ШІ може відігравати ключову роль у виявленні аномальних шаблонів у розподілі голосів, що є особливо важливим для запобігання маніпуляціям та зловживанням у децентралізованих системах управління.

Методи машинного навчання, такі як алгоритми виявлення аномалій та кластеризації, дозволяють аналізувати дані голосування та швидко виявляти відхилення від норми. Наприклад, аномальні сплески голосів за певний проєкт або незвичні розподіли голосів можуть бути автоматично зафіксовані, що запускає подальшу перевірку. Впровадження таких алгоритмів забезпечує безперервний моніторинг голосування і оперативну реакцію на будь-які підозрілі дії, знижуючи ризик шахрайства та підвищуючи довіру учасників.

Крім того, ШІ може аналізувати історичні дані про голосування для виявлення довгострокових аномалій та прогнозування можливих ризиків. Наприклад, аналіз часових рядів даних дозволяє моделям ШІ передбачати, як зміни в поведінці учасників можуть вплинути на результати голосування. Це допомагає блокчейн-платформам оперативно виявляти потенційні загрози, мінімізуючи вплив таких факторів на процес розподілу ресурсів та ухвалення рішень.

Таким чином, використання ШІ в системі квадратичного голосування на блокчейні створює умови для посиленого контролю і запобігання порушенням, а також сприяє досягненню більш справедливого та надійного процесу голосування.

1. Розповідаємо, що таке блокчейн простими словами – як працює мережа, як будуються блоки, що роблять майнери [Електронний ресурс]. – Режим доступу: https://apix-drive.com/ua/blog/useful/tehnologija-blokchejn-sho-ce-i-jak-pracjue.

2. Benhaim A., Falk B. H., Tsoukalas G. Balancing Power in Decentralized Governance: Quadratic Voting under Imperfect Information. – 2023. – С. 1-4.

К.В. Виноградова, Е.В. Рижков

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПІДРОЗДІЛАМИ СТРАТЕГІЧНИХ РОЗСЛІДУВАНЬ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Штучний інтелект (ШІ) дедалі активніше впроваджується в роботу правоохоронних органів у всьому світі, що значно підвищує їхню ефективність та дозволяє краще протидіяти злочинності. Використання ШІ підрозділами стратегічних розслідувань Національної поліції України має особливе значення, оскільки надає нові інструменти для розкриття складних злочинів, аналізу великих обсягів інформації та прогнозування злочинних дій. Це дає можливість оптимізувати роботу підрозділів, підвищити швидкість реагування на злочини та забезпечити ефективний моніторинг злочинної діяльності [1, с. 33].

Штучний інтелект може виконувати ряд функцій, що є особливо корисними в оперативно-розшуковій діяльності. Сучасні алгоритми дозволяють аналізувати великі обсяги відеозаписів і даних з камер спостереження, автоматично виявляючи підозрілих осіб або дії, що відхиляються від норми. Використовуючи обробку зображень і розпізнавання обличчя, ШІ може знаходити зв'язки між злочинцями та відстежувати їхні переміщення, що значно спрощує процес ідентифікації та затримання злочинців [2, с. 55]. Цей інструмент також застосовується для виявлення аномальних фінансових операцій, що може вказувати на відмивання коштів або інші економічні злочини.

Алгоритми машинного навчання допомагають створювати профілі злочинців на основі їхніх попередніх дій, а також виявляти закономірності у великих масивах даних. Наприклад, система може автоматично аналізувати історію злочинних дій, виділяти характерні риси для конкретних груп або окремих осіб і прогнозувати, де може відбутися наступний злочин. Це дозволяє більш ефективно планувати роботу правоохоронців і заздалегідь вживати превентивних заходів [3, с. 87].

Завдяки застосуванню ШІ Національна поліція може оптимізувати свою роботу шляхом автоматизації рутинних завдань. Так, обробка та аналіз великих обсягів даних, що раніше займала багато часу, тепер виконується в автоматичному режимі, що дозволяє співробітникам зосередитись на більш стратегічних питаннях. За допомогою алгоритмів ШІ можна аналізувати соціальні мережі та комунікаційні дані для виявлення кримінальних зв'язків і патернів поведінки, що дозволяє відстежувати організовані злочинні групи та розкривати складні схеми злочинної діяльності [4, с. 115].

Особливо важливою є можливість ШІ розраховувати так звані "гарячі точки" — місця з високою ймовірністю злочинів, що дозволяє більш ефективно розподіляти ресурси поліції. Це дає змогу зосередити увагу на районах з підвищеним ризиком, що значно підвищує ймовірність затримання злочинців "на гарячому" та запобігання правопорушенням до їхнього вчинення [5, с. 40].

Незважаючи на значний потенціал, застосування ШІ у роботі правоохоронних органів супроводжується низкою проблем, зокрема етичних та правових. Використання технологій розпізнавання обличчя та аналізу персональних даних створює ризики порушення прав на приватність і конфіденційність. Крім того, помилки алгоритмів можуть призводити до неправомірного звинувачення осіб або хибної ідентифікації, що ставить під загрозу права та свободи громадян. Тому надзвичайно важливо, щоб використання ШІ в правоохоронній діяльності супроводжувалось ретельним контролем та дотриманням законодавства щодо захисту персональних даних [6, с. 43].

Використання штучного інтелекту підрозділами стратегічних розслідувань Національної поліції України є ключовим кроком для підвищення ефективності боротьби з організованою злочинністю та забезпечення громадської безпеки. ШІ надає можливість ефективно аналізувати великі обсяги інформації, прогнозувати потенційні загрози, автоматизувати рутинні завдання та оперативно реагувати на злочини. Однак поряд із значними перевагами існують і виклики, пов’язані з етичними аспектами використання ШІ, зокрема збереженням прав людини. Для успішного впровадження інноваційних технологій Національній поліції України необхідно розробити чіткі інструкції щодо використання ШІ, забезпечити відповідний захист персональних даних та дотримання правових стандартів.

1. Петренко В. М. Застосування штучного інтелекту у протидії злочинності. *Науковий журнал ДДУВС.* 2023. № 1. С. 33-40. URL: https://dduvs.edu.ua/journal (Дата звернення: 01.11.2024).

2. Коваль І. Г. Новітні технології у розслідуванні злочинів. *Вісник криміналістики.* 2024. № 2. С. 55-61. URL: https://crimjournal.ua (Дата звернення: 01.11.2024).

3. Бондар П. С. Профілювання злочинних груп з використанням алгоритмів машинного навчання. *Кримінальне право.* 2023. № 3. С. 87-94. URL: https://criminallaw.ua (Дата звернення: 01.11.2024).

4. Сидоренко Т. О. Аналітичні системи на основі штучного інтелекту для виявлення злочинів. *Науковий вісник ДДУВС.* 2023. № 5. С. 115-125. URL: https://dduvs.edu.ua/journal (Дата звернення: 01.11.2024).

5. Тарасенко, Ю. В. Етичні аспекти використання штучного інтелекту в правоохоронних органах / Ю. В. Тарасенко // Державне управління та право. – 2024. – № 2. – С. 57-60. – URL: https://dduvs.edu.ua/journal. (Дата звернення: 01.11.2024.)

6. Кравченко, І. М. Нормативне забезпечення застосування ШІ в діяльності поліції України / І. М. Кравченко // Юридична безпека. – 2024. – № 1. – С. 70-75. – URL: https://dduvs.edu.ua/journal. (Дата звернення: 01.11.2024.)

Н.В. Заїка, І.В. Мартинюк, М.Ю. Комаров, О.О. Молчанов

ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ТА ПРОТИДІЇ ЗАГРОЗАМ ПРИ ЗАСТОСУВАННІ АВТОМАТИЗАЦІЇ ТА ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ КІБЕРБЕЗПЕКИ

У зв'язку з нещодавнім збільшенням атак із використанням програм-вимагачів, зросло навантаження на підготовку та складання звітів. Аналітики перевантажені даними, намагаючись зібрати разом вектори атак і визначити уражені системи. Точність звітів є критично важливою, проте ручне редагування забирає час, який можна було б витратити на аналіз та нейтралізацію загроз.

Ситуація в кіберзахисті змінюється. Зловмисники постійно вдосконалюють свої методи та тактики. Використання застарілих версій програмних інструментів може призвести до того, що організації та об'єкти критичної інфраструктури не будуть знати про нові кіберзагрози. Платформи для розвідки загроз відіграють важливу роль у виявленні, аналізі та реагуванні на загрози. Однак їхня ефективність часто залежить від зручності запитів та можливості швидкого отримання релевантних даних. Щоб випередити супротивників, потрібні сучасні програмні інструменти та розширені можливості аналітики.

Експерти з кібербезпеки визнають, що успіх залежить від безперервності потоку інформації. Для того, щоб ефективно протистояти новим загрозам, аналітики мають вміти правильно документувати, обмінюватися та керувати даними про загрози. Використання зовнішніх інструментів для нотаток часто призводить до фрагментації робочого процесу і знижує ефективність.

Спільний доступ до нотаток дозволяє кожному члену команди ділитися ідеями, оновленнями та коментарями, а також швидко знаходити або відфільтровувати необхідну інформацію. Можливість експорту та імпорту нотаток у різних форматах дозволяє використовувати їх для подальшого звітування. Підготовка високоякісних звітів є важливим, але часто складним завданням для фахівців з кібербезпеки.

Інструменти як AI Writing Assistant можуть змінити процес створення контенту для кібербезпекових експертів [1]. Він містить функції для покращення стилю звітів і пропонує оптимізації для зручності читачів. Інструменти зі штучним інтелектом допомагають адаптувати звіти, перевіряти їх на помилки, а також підтримують багатомовність, що полегшує роботу для міжнародних команд, незалежно від рівня технічних знань.

Навчання штучного інтелекту на основі запитів прискорює отримання релевантних відповідей. Оптимізація процесів передбачає збереження запитів для подальшого використання, що економить час і зусилля. Водночас синхронізація відповідей між інструментом і онлайн-сервісами робить запити більш зрозумілими для користувачів цих сервісів. Однак використання таких інструментів для редагування тексту може підвищити ризики витоку особистих та конфіденційних даних. Важливо перевіряти бази даних на наявність небезпечних запитів при навчанні штучного інтелекту [2].

Фахівці поступово вчаться створювати безпечні запити, що сприяє розвитку їхніх навичок. Такий підхід допомагає покращити точність та ефективність роботи з інструментами штучного інтелекту.

Згідно зі звітом Morning Consult, 39% кібербезпекових фахівців вважають використання штучного інтелекту найкращою можливістю для підвищення ефективності при реагуванні на загрози [3].

Рекомендації:

Моніторинг стану інфраструктури: Забезпечує контроль за станом ресурсів, сервісів, мережевих з'єднань, що дає швидку можливість виявлення атак, проводить збір даних про можливості атак із використанням програм-вимагачів, загрози та кібер-інциденти.

Автоматизація рутинних завдань: Використовувати інструменти на базі штучного інтелекту для автоматизації складання звітів і обробки даних моніторингу, що дозволить фахівцям більше часу приділяти безпосередньому аналізу та реагуванню на загрози.

Оновлення інструментів: Регулярно оновлювати використовувані версії програмного забезпечення, щоб бути в курсі нових тактик і методів зловмисників. Відмова від застарілих систем може знизити ризик вразливостей.

Інтеграція інструментів: Об'єднання всіх інструментів для збору, обробки та документування загроз в єдину систему, щоб уникнути фрагментації робочого процесу та підвищити ефективність командної роботи.

Використання платформ для розвідки загроз (TIP): Важливо впроваджувати сучасні платформи для моніторингу, аналізу і виявлення загроз, забезпечуючи їх легкість у використанні та доступність даних для аналітиків.

Навчання персоналу: Фахівці з кібербезпеки мають бути постійно навченими у створенні безпечних запитів і роботі з інструментами штучного інтелекту для підвищення їх ефективності.

Забезпечення кібербезпеки при використанні AI: При навчанні інструментів штучного інтелекту необхідно особливу увагу приділяти безпеці даних, уникаючи витоку конфіденційної інформації через ненавмисне її поширення.

Міжнародна співпраця та багатомовна підтримка: Використовувати багатомовні інструменти та підтримувати міжнародну співпрацю для створення більш ефективних та глобальних рішень у кібербезпеці.

Висновки

У зв'язку зі збільшенням атак із використанням програм-вимагачів важливо використовувати сучасні технології для швидкої адаптації та реагування на загрози. AI стає необхідним інструментом у процесі обробки

даних, написання звітів і виявлення загроз, підвищуючи швидкість і точність роботи кібербезпекових команд. Безперервний обмін інформацією та ефективне управління даними про загрози є основним чинником успіху у боротьбі з сучасними кіберзагрозами. Фрагментація робочих процесів через використання різних інструментів знижує ефективність команд. Інтегровані рішення дозволяють покращити координацію та швидкість реагування.

Навчання штучного інтелекту може становити загрозу для конфіденційності, тому важливо впроваджувати строгі політики безпеки даних. Використання новітніх інструментів і технологій дозволяє бути на крок попереду зловмисників і покращити захист критичної інфраструктури. Таким чином, важливість інтеграції штучного інтелекту до процесів з кібербезпеки, регулярного оновлення систем та навчання персоналу є критичною для ефективного протистояння кіберзагрозам.

1. Покращуйте свої розвідувальні звіти за допомогою помічника з написання AI від EclecticIQ // [Електр. Ресурс]. – Режим доступу: https://blog.eclecticiq.com/eclecticiq-intelligence-center-ai-writing-assistant.

2. Doke A. Survey on Automated Machine Learning (AutoML) and Meta learning / Ashwini Doke, Madhava Gaikwad // 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 6–8 July 2021. –2021. – DOI: https://doi.org/10.1109/icccnt51525.2021.9579526.

3. Трансформуйте своє управління загрозами за допомогою вдосконалених інструментів аналізу MITRE ATT&CK // [Електр. Ресурс]. – Режим доступу: https://blog.eclecticiq.com/eclecticiq-intelligence-center-mitre-attck-navigator.

M. Antonishyn, V. Liedniei, M. Myhun

OWASP FOR ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML)

The rapid adoption of artificial intelligence (AI) and machine learning (ML) technologies across various sectors has brought both unprecedented opportunities and significant security challenges. As these systems increasingly influence critical decisions in healthcare, finance, and autonomous systems, understanding their vulnerabilities becomes essential for safeguarding data, model integrity, and user privacy. The OWASP Machine Learning Security Top 10 project aims to address this need by identifying and categorizing the top security risks unique to machine learning and large language model (LLM) applications. Through extensive collaboration with industry experts, the project delivers a meticulously vetted list of common and critical vulnerabilities in AI systems, along with actionable strategies for mitigating these risks. The vulnerabilities documented within the OWASP framework represent a diverse array of potential threats, including input manipulation, model inversion, and data poisoning. Each risk type targets different stages of the ML lifecycle from training data acquisition to model deployment making these threats particularly complex and challenging to mitigate. Moreover, with the increasing deployment of large language models, new risks specific to these architectures have emerged, requiring separate attention and security strategies.

The primary aim of the OWASP Machine Learning Security Top 10 project is to deliver an overview of the top 10 security issues of machine learning systems. As such, a major goal of this project is to develop a high-quality deliverable, reviewed by industry peers. The Open Worldwide Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications and APIs that can be trusted.

Each of these vulnerabilities, along with examples, prevention tips, attack scenarios, and references, was further scrutinized and refined by dedicated sub-teams and subjected to public review, ensuring the most comprehensive and actionable final list.

ML01:2023 Input manipulation attacks is an umbrella term, which includes Adversarial Attacks, a type of attack in which an attacker deliberately alters input data to mislead the model.

ML02:2023 Data poisoning attacks occur when an attacker manipulates the training data to cause the model to behave in an undesirable way.

ML03:2023 Model inversion attacks occur when an attacker reverse-engineers the model to extract information from it.

ML04:2023 Membership inference attacks occur when an attacker manipulates the model’s training data in order to cause it to behave in a way that exposes sensitive information.

ML05:2023 Model theft attacks occur when an attacker gains access to the model’s parameters.

ML06:2023 AI Supply Chain Attacks occur when an attacker modifies or replaces a machine learning library or model that is used by a system. This can also include the data associated with the machine learning models.

ML07:2023 Transfer learning attacks occur when an attacker trains a model on one task and then fine-tunes it on another task to cause it to behave in an undesirable way.

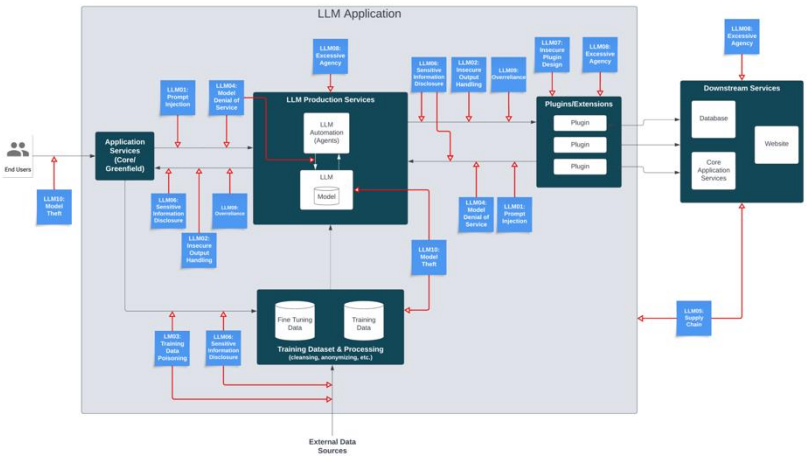
ML08:2023 Model skewing attacks occur when an attacker manipulates the distribution of the training data to cause the model to behave in an undesirable way.

ML09:2023 In an Output Integrity Attack scenario, an attacker aims to modify or manipulate the output of a machine learning model in order to change its behavior or cause harm to the system it is used in.

ML10:2023 Model Poisoning attacks occur when an attacker manipulates the model's parameters to cause it to behave in an undesirable way.

The frenzy of interest in Large Language Models (LLMs) following the release of mass market pre-trained chatbots in late 2022 has been remarkable. Businesses eager to harness the potential of LLMs are rapidly integrating them into their operations and client facing offerings. However, the breakneck speed at which development teams are adopting LLMs has outpaced the establishment of comprehensive security protocols, leaving many applications vulnerable to high-risk issues.

Creating the OWASP Top 10 for LLM Applications list was a significant undertaking, built on the collective expertise of an international team of nearly 500 experts with over 125 active contributors. Our contributors come from diverse backgrounds, including AI companies, security companies, ISVs, cloud hyperscale’s, hardware providers, and academia.



Picture 1 – LLM model applications

The diagram illustrates a high-level architecture of a Large Language Model (LLM) application, highlighting key areas of potential security risks. Each component of the architecture—from Application Services to LLM Production Services, Plugins/Extensions, and Downstream Services—is associated with specific security vulnerabilities identified by OWASP. Red arrows indicate the flow of threats or vulnerabilities between components, with each labeled according to the OWASP Top 10 list for LLM applications.

1. *Application Services:* This layer interacts with end users and is vulnerable to Prompt Injection (LLM01), Insecure Output Handling (LLM02), Sensitive Information Disclosure (LLM06), and Overreliance (LLM09). These vulnerabilities could compromise user interactions, data integrity, and reliance on potentially misleading outputs from the model.
2. *LLM Production Services*: As the core processing hub, this layer is susceptible to attacks such as Model Denial of Service (LLM04) and Model Theft (LLM10), with attackers potentially targeting the model's availability and intellectual property.
3. *Plugins/Extensions*: Plugins extend the functionality of the LLM but introduce risks like Insecure Plugin Design (LLM07) and Excessive Agency (LLM08), which could lead to compromised data handling or unintended actions within the system.
4. *Training Dataset & Processing*: This layer, responsible for data preprocessing and model training, is vulnerable to Training Data Poisoning (LLM03) and Sensitive Information Disclosure (LLM06), which could corrupt the model's training data or expose confidential information.
5. *Downstream Services*: The downstream components, such as databases and core application services, are at risk of Supply Chain attacks (LLM05), which could compromise data or functionalities dependent on third-party sources or external integrations.

Each vulnerability label corresponds to a specific type of attack or threat that may affect the LLM application's integrity, security, and reliability. This diagram serves as a guide for identifying and mitigating these risks across the entire application lifecycle.

The diagram below presents a high-level architecture for a hypothetical large language model application. Overlaid in the diagram are highlighted areas of risk illustrating how the OWASP Top 10 for LLM Applications entries intersect with the application flow. This diagram can be used as a visual guide, assisting in understanding how large language model security risks impact the overall application ecosystem.

This report presents a detailed overview of the OWASP Top 10 vulnerabilities for both traditional ML and LLM applications. By examining common attack scenarios, prevention techniques, and case studies, this document aims to equip developers, security professionals, and researchers with essential knowledge to build and maintain secure AI systems. Through this collaborative effort, the OWASP project strives to raise awareness and foster a more secure environment for the deployment of machine learning technologies worldwide.

1. OWASP Machine Learning Security Top Ten. https://owasp.org/www-project-machine-learning-security-top-10/.
2. Steve Wilson, Ads Dawson. OWASP Top 10 for LLM Applications. Version 1.1, OWASP, 2023. https://owasp.org/www-project-top-10-for-large-language-model-applications/assets/PDF/OWASP-Top-10-for-LLMs-2023-v1_1.pdf.

A. Davydiuk, S. Kulyk

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY FOR CLOUD SERVICES

With the increasing volumes of data, more and more companies and governmental organizations are becoming clients of data centers. Also, some countries became dependent on the monopoly of huge data centers and SaaS solutions. The advantage of this shift is the partial transfer of information security and cyber risks to the private data center. This transition offers some benefits but presents cybersecurity challenges, particularly in protecting cloud services in cyberspace. Despite the availability of various technical solutions to mitigate these risks and threats. One of the emerging and promising approaches involves using artificial intelligence (AI) to provide cybersecurity and improve monitoring and response processes in cloud environments, allowing for rapid processing of requests on large datasets, with these requests being built at a conversational level

To understand how artificial intelligence can be used for the cybersecurity of cloud services, let's look at the main threats to cloud services. These threats include configuration errors, technical vulnerabilities, insider threats, data loss and leakage, unsecured interfaces and APIs, among others [1], [2]. Current research focuses on AI's ability to detect and prevent various threats such as insider attacks, data loss, and insecure APIs. However, many solutions still face challenges related to reducing false positives, improving response times, and ensuring scalability in increasingly complex cloud infrastructures. Furthermore, the integration of AI-powered cybersecurity tools with existing security frameworks remains a critical issue to ensure consistent protection across diverse cloud systems.

AI is widely used in cybersecurity, particularly in monitoring and proactive cybersecurity. For example, a study [3] describes AI methods and their application for detecting not typical behavior on the network and classify as an incident. Special attention is given to presenting models based on neural networks, fuzzy logic, and evolutionary computations. The main object is a binary classifier, which is designed to assign each input object to one of two class sets. Various schemes for combining binary classifiers are considered, which allows building models trained on different subsets. Several optimization methods are proposed, both in terms of parallelization (to increase training speed) and using aggregating compositions (to improve classification accuracy). Principal component analysis, aimed at reducing the dimensionality of analyzed attack feature vectors, is also discussed. To reduce the number of false positives, a sliding window method was developed and adopted. Finally, the performance metrics of the model, obtained during experiments using cross-validation, are provided.

Cloud service cybersecurity is not limited to the protection of the network. By leveraging AI and ML capabilities, organizations can proactively detect, mitigate, and respond to new cyber incidents and threats, ultimately strengthening their cloud infrastructure. The AI-driven methods enable security systems to recognize patterns, anomalies, and potential threats in huge datasets. ML algorithms, by studying data from historical attacks, can predict future threats and develop more effective protective mechanisms. Moreover, advanced authentication and access control mechanisms using AI improve identity management, reducing the risk of unauthorized access and data leakage [4].

With the development of sophisticated attack and cyberattack methods, companies need to adapt their threat detection and response mechanisms. It is important to research modern tools, from real-time monitoring and network forensics to XDR, SIEM, SOAR, and NDR, which help understand the constantly evolving detection and response system space [5]. The integration of AI enhances monitoring, detection, and incident response, offering significant improvements compared to traditional methods, which often generate a large number of false-positive alerts. AI algorithms can intelligently recognize patterns using advanced detection techniques, analyzing real-time alerts to improve accuracy and speed. The application of AI in cloud security structures allows organizations to optimize their defense strategies while also reducing the risk of human error [6].

The article [2] also discusses AI implementation strategies and presents the integration of AI with existing security frameworks and the importance of continuous learning and collaboration between AI systems and human experts. As cloud environments become more complex, AI-driven security protocols represent a significant advance in protecting digital assets.

Nowadays cryptographic transformations are used to protect data privacy in the cloud. With the global cloud computing market expected to reach $1.554 trillion by 2030, and 94% of businesses using cloud services, the need for quantum-resistant security solutions is critical. The framework proposed in Mr. Ashok Sreerangapuri's research combines lattice-based cryptography, hash-based signatures, and multivariate cryptography with AI-powered security automation to provide scalable, adaptable, and future-proof security solutions. Initial tests demonstrate the framework's ability to process 5,000 encryption tasks per second while maintaining 99.9% uptime [7]. This is an important area in the times of fast development of quantum technologies. The work [8] explores the integration of AI in encryption methods to enhance data security in cloud computing. Using machine learning algorithms and neural networks, AI-based encryption could be adapted to new threats, optimize key management, and automate vulnerability detection.

Despite the effectiveness of implementing AI tools for protecting cloud services, there are several challenges. Although AI-based systems are designed to reduce false positives, there is still room for improvement in fine-tuning these systems to be more accurate without losing detection capability. AI solutions often require custom integration, which can be resource-intensive, and improving this integration can ensure better scalability and adaptability across various cloud systems. At the same time the question could we trust fully to AI cybersecurity? Now machine learning algorithms can be optimized to detect patterns in massive datasets, but the ability of AI to adapt to entirely new attack vectors without human intervention remains an open problem. As cloud computing continues to expand, particularly with the advent of quantum computing, AI-based solutions must evolve to ensure they are protected from quantum threats. The development of AI solutions that comply with privacy regulations (e.g., GDPR) [9] while offering effective protection will be a critical area for future research.

To sum up, AI by now cannot fully replace all cybersecurity means and tools but AI offers significant potential for improving the security operational center of cloud services. Current research shows the importance of combining AI methods such as neural networks, fuzzy logic, and evolutionary computations to create robust and effective cloud security and resilience models. Challenges remain in reducing false positives, adapting to new threats, and ensuring full integration with existing security frameworks. Also, we should take into account the threat of autonomous cyber weapons which is a separate challenge to AI cybersecurity systems. Addressing these issues will be key to enhancing the effectiveness of AI-based security systems.

1. Neelakrishnan, P. (2024). AI-Driven proactive cloud application data access security. International Journal of Innovative Science and Research Technology (IJISRT), 510–521. https://doi.org/10.38124/ijisrt/ijisrt24apr957.
2. Oduri, S. (2019). AI-Driven security protocols for modern cloud engineers. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 10(2), 2002–2008. https://doi.org/10.61841/turcomat.v10i2.14739.
3. Branitskiy, A., & Kotenko, I. (2018). Applying artificial intelligence methods to network attack detection. In AI in cybersecurity (pp. 115–149). Springer International Publishing. https://doi.org/10.1007/978-3-319-98842-9_5.
4. Mamidi, S. R. (2024). The role of AI and machine learning in enhancing cloud security. Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023, 3(1), 403–417. https://doi.org/10.60087/jaigs.v3i1.161.
5. Tatineni, S. (2023). AI-Infused threat detection and incident response in cloud security. International Journal of Science and Research (IJSR), 12(11), 998–1004. https://doi.org/10.21275/sr231113063646.
6. Nutalapati, P. (2024). Automated incident response using AI in cloud security. Journal of Artificial Intelligence, Machine Learning and Data Science, 2(1), 1301–1311. https://doi.org/10.51219/jaimld/pavan-nutalapati/299.
7. -, A. S. (2024). Post-Quantum cryptography for ai-driven cloud security solutions. International Journal for Multidisciplinary Research, 6(5). https://doi.org/10.36948/ijfmr.2024.v06i05.29032.
8. Reddy Kethireddy, R. (2021). AI-Driven encryption techniques for data security in cloud computing. Journal of Recent Trends in Computer Science and Engineering, 9(1), 27–38. https://doi.org/10.70589/jrtcse.2021.1.3.
9. Regulation of the European Parliament and of the Council (EU) 2016/679 of April 27, 2016 on the protection of natural persons in connection with the processing of personal data and on the free movement of such data, and on the repeal of Directive 95/46/EC (General Regulation on data protection), Regulation of the European Union No. 2016/679 (2016).https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

А.О. Попова, О.М. Любименко, Н.О. Маслова, О.А. Штепа

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ ДАНИХ ТА ВИЯВЛЕННЯ АНОМАЛІЙ У СИСТЕМІ КВАДРАТИЧНОГО ГОЛОСУВАННЯ НА БЛОКЧЕЙНІ

Блокчейн - це інноваційна розподілена технологія зберігання даних, яка фіксує інформацію у формі послідовного ланцюга блоків, з'єднаних між собою криптографічними хешами. Вона забезпечує безпечне, прозоре середовище для обміну інформацією та здійснення транзакцій без участі посередників. Спочатку створена для криптовалюти Bitcoin у 2008 році, блокчейн-технологія тепер набуває широкого використання в різних галузях [1].

Принцип децентралізації в блокчейні означає, що жодна сторона не має одноосібного контролю над даними, а система керується мережею вузлів, які підтверджують транзакції за допомогою алгоритмів консенсусу. Це робить блокчейн потужним інструментом для збереження цілісності даних та запобігання фальсифікації.

При виборі стратегій голосування, що забезпечують справедливе колективне прийняття рішень, метод квадратичного голосування вирізняється як ефективний підхід, що враховує інтенсивність переваг виборців. Квадратичне голосування дозволяє учасникам не лише віддати голоси за певні варіанти, але й виразити силу своїх переконань шляхом розподілу кредитів. Кількість голосів, яку виборець хоче віддати на певну альтернативу, зростає за квадратичною функцією, що ускладнює концентрацію голосів без значних витрат.

Завдяки такому підходу квадратичне голосування захищене від сибіл-атак, коли зловмисники створюють безліч підроблених акаунтів. Це економічно невигідно, оскільки вартість кожного додаткового голосу зростає пропорційно квадрату витрачених кредитів. Модель квадратичного голосування легко інтегрується в блокчейн, забезпечуючи прозорість і надійність процесу. Ця модель стимулює виборців приймати більш обдумані рішення, оскільки виборці повинні ретельно зважувати свої переваги через обмеженість кредитів і зростаючу вартість додаткових голосів.

У моделі квадратичного голосування застосовується математичний підхід, де кожен голос має свою вартість, яка зростає квадратично зі збільшенням кількості голосів. Це дозволяє знизити вплив окремих виборців та забезпечити більш збалансоване прийняття рішень.

У представленій формулі (1) сума внесків спонсорів для конкретного проекту визначається як сума квадратів кількості голосів, що виділяються кожним спонсором. Це дозволяє обмежити максимальний вплив одного виборця і стимулює ретельно обирати підтримувані проекти [2].

$$s(p_m) = \sum_{i=1}^{n} c_i^2 , \quad (1)$$

де p_m – проект, висунутий на голосування;
m – загальна кількість проектів на голосуванні;
s – сума вкладу спонсорів за голоси;
n – загальна кількість спонсорів;
c_i – кількість голосів спонсора.

Загальний бюджет конкурсу (2) представлений як сума внесків усіх спонсорів для всіх проектів, що є на голосуванні.

$$b = \sum_{i=1}^{m} s(p_i) , \quad (2)$$

де b – бюджет конкурсу;
p_i – проект, висунутий на голосування;
s – сума вкладу спонсорів за голоси;
m – загальна кількість проектів на голосуванні.

Інтеграція методів штучного інтелекту у систему квадратичного голосування на блокчейні надає нові можливості для моніторингу та аналізу процесу голосування в режимі реального часу, значно підвищуючи безпеку та прозорість процесу. ШІ може відігравати ключову роль у виявленні аномальних шаблонів у розподілі голосів, що є особливо важливим для запобігання маніпуляціям та зловживанням у децентралізованих системах управління.

Методи машинного навчання, такі як алгоритми виявлення аномалій та кластеризації, дозволяють аналізувати дані голосування та швидко виявляти відхилення від норми. Наприклад, аномальні сплески голосів за певний проєкт або незвичні розподіли голосів можуть бути автоматично зафіксовані, що запускає подальшу перевірку. Впровадження таких алгоритмів забезпечує безперервний моніторинг голосування і оперативну реакцію на будь-які підозрілі дії, знижуючи ризик шахрайства та підвищуючи довіру учасників.

Крім того, ШІ може аналізувати історичні дані про голосування для виявлення довгострокових аномалій та прогнозування можливих ризиків. Наприклад, аналіз часових рядів даних дозволяє моделям ШІ передбачати, як зміни в поведінці учасників можуть вплинути на результати голосування. Це допомагає блокчейн-платформам оперативно виявляти потенційні загрози, мінімізуючи вплив таких факторів на процес розподілу ресурсів та ухвалення рішень.

Таким чином, використання ШІ в системі квадратичного голосування на блокчейні створює умови для посиленого контролю і запобігання порушенням, а також сприяє досягненню більш справедливого та надійного процесу голосування.

1. Розповідаємо, що таке блокчейн простими словами – як працює мережа, як будуються блоки, що роблять майнери [Електронний ресурс]. – Режим доступу: https://apix-drive.com/ua/blog/useful/tehnologija-blokchejn-sho-ce-i-jak-pracjue.

2. Benhaim A., Falk B. H., Tsoukalas G. Balancing Power in Decentralized Governance: Quadratic Voting under Imperfect Information. – 2023. – С. 1-4.

А.І. Вавіленкова

АЛГОРИТМИ ПОШУКУ ЗМІСТУ В ІНФОРМАЦІЙНИХ ПОВІДОМЛЕННЯХ

Алгоритми пошуку, що використовуються сьогодні пошуковими системами, спрямовані на знаходження у певній множині даних, які відповідатимуть текстовому запиту, тобто задовольнятимуть інформаційну потребу. Експериментальні дослідження показують, що чим коротший інформаційний запит, тим більшою буде пошукова видача, оскільки запит являє собою ключові слова, що, як правило, вживаються разом у електронних текстових документах [1]. Натомість, якщо текстовий запит містить певну фразу або речення природної мови, список посилань пошукової видачі може містити від одного до десяти посилань. Це відбувається тому, що алгоритми пошуку не враховують змістовне навантаження запиту, а аналізують послідовності слів, що стоять поряд.

Тобто пошуковий алгоритм – це набір правил, відповідно до яких спочатку відбувається визначення ключових слів для пошуку даних, далі – порівняння слів запиту з еталонними ключовими словами у документах, що містяться у базах даних, та перебирання множини елементів на предмет знаходження ключових слів пошукового запиту [2].

Для організації пошуку інформації за змістом пропонується використати в алгоритмах пошуку математичний апарат логіко-лінгвістичного моделювання для знаходження та формування груп слів, що пов'язані між собою за змістом, тобто словосполучень. Оскільки між граматичною структурою речення та логічною формою існує повна відповідність, будемо відображати просте речення природної мови у вигляді логічних зв'язок sp_j, $j=\overline{1,m}$, де m – кількість словосполучень у реченні, які є логічним відображенням наявних у реченні словосполучень [3]:

– «означення – підмет» – $sp_j = g \cup x$;

– «присудок – додаток» – $sp_j = p \cup y$;

– «означення – додаток» – $sp_j = q \cup y$;

– «додаток – додаток» – $sp_j = y \cup z$;

– «означення – додаток» – $sp_j = r \cup z$;

– «обставина – присудок» – $sp_j = h \cup p$;

– підмет – суб'єкт x;

– присудок – відношення p;

– додаток – об'єкт y або предмет z відношення;

– означення – характеристика суб'єкта g, об'єкта q або предмета відношення r;

– обставина – характеристика відношення h.

Наприклад, розглянемо речення «*Хешування завжди допомагає запобігти випадковому або зловмисному пошкодженню даних*». Логічні зв'язки у такому простому реченні будуть побудовані відповідно до визначених синтаксичних ролей та правил побудови словосполучень української мови:

– підмет – суб'єкт x – *хешування*;

– присудок – відношення p – *допомагає_запобігти*;

– додаток – об'єкт y – *пошкодженню*;

– додаток – предмет z відношення – *даних*;

– означення – характеристика суб'єкта g – *0*;

– означення – характеристика об'єкта q_1 – *випадковому*;

– означення – характеристика об'єкта q_2 – *зловмисному*;

– означення – характеристика предмета відношення r – *0*;

– обставина – характеристика відношення h – *завжди*.

У даному реченні будуть виявлені та відображені такі словосполучення:

– «присудок – додаток» – $sp_j = p \cup y$ – *запобігти пошкодженню*;

– «означення – додаток» – $sp_j = q_1 \cup y$ – *випадковому пошкодженню*;

– «означення – додаток» – $sp_j = q_2 \cup y$ – *зловмисному пошкодженню*;

– «додаток – додаток» – $sp_j = y \cup z$ – *пошкодженню даних*;

– «обставина – присудок» – $sp_j = h \cup p$ – *завжди допомагає запобігти*.

Якщо розібрати за принципом, наведеним вище, будь-яке просте речення природної мови, можна побачити, що утворені логічні зв'язки відображають змістовно наповнені словосполучення, а не лише слова, що статистично та потенційно вживаються у тексті разом. Це надає можливість розбирати великі інформаційні запити, виділяти з них змістовні одиниці та формувати ключові словосполучення для подальшого пошуку інформації за змістом.

1. Вавіленкова А.І. Алгоритми та методи обчислень: практикум для студентів спеціальності 123 «Комп'ютерна інженерія». – К.: НАУ, 2019. – 60 с.

2. Scott V. Burger Introduction to Machine Learning with R: Rigorous Mathematical Analysis: O'REILLY, 2018. – 200 p.

3. Вавіленкова А. І. Аналіз і синтез логіко-лінгвістичних моделей речень природної мови: монографія. Київ: ТОВ «СІК ГРУП УКРАЇНА», 2017. – 152 с.

Я.А. Сиротюк

ВИЯВЛЕННЯ ВТОРГНЕНЬ У СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

З розвитком цифрових технологій та збільшенням обсягів інформаційних потоків питання забезпечення інформаційної безпеки набуває особливої актуальності. Одним з ключових аспектів захисту є виявлення несанкціонованих спроб доступу або атаки на комп’ютерні системи, що здійснюється за допомогою систем виявлення вторгнень (IDS — Intrusion Detection Systems). Традиційні методи виявлення, які базуються на сигнатурному аналізі, не здатні ефективно реагувати на нові типи атак, що потребує впровадження технологій, таких як штучний інтелект (ШІ), для адаптації до змінюваних умов кіберзагроз.

Існують два основні підходи до виявлення вторгнень: сигнатурний та аномальний. Сигнатурний метод, який базується на порівнянні даних з відомими зразками атак, є обмеженим у контексті нових, невідомих загроз. Аномальний метод виявлення аналізує поведінку системи, порівнюючи її з нормальними патернами роботи. Однак ці методи можуть мати високий рівень помилкових спрацьовувань (false positives), що значно знижує ефективність [1].

Застосування технологій штучного інтелекту в цій сфері дозволяє значно покращити процес виявлення вторгнень. ШІ здатний автоматично вивчати і адаптуватися до нових сценаріїв атак, знижуючи кількість помилкових спрацьовувань і підвищуючи точність виявлення.

Машинне навчання (ML) є однією з основних технологій, що використовуються для виявлення вторгнень. Алгоритми машинного навчання можна поділити на три основні категорії: навчання з учителем, навчання без учителя та напівконтрольоване навчання. Кожна з цих категорій має свої переваги та обмеження в контексті аналізу мережевого трафіку та виявлення аномалій. Зокрема, перший підхід, навчання з учителем, застосовується в умовах, коли необхідно чітко класифікувати дані на основі попередньо визначених міток.

Навчання з учителем. Цей підхід передбачає наявність міток для кожного спостережуваного об'єкта. Алгоритм вчиться на основі даних, які мають чітке визначення, чи є конкретна активність шкідливою чи нормальною. Для цього використовуються такі алгоритми, як логістична регресія, дерева рішень, метод опорних векторів (SVM) та нейронні мережі. Основним обмеженням цього підходу є необхідність наявності великої кількості помічених даних для тренування."

Навчання без учителя. Навчання без учителя використовує методи, які не потребують попереднього визначення міток. Це дозволяє системам виявляти невідомі або нові типи атак, базуючись на аналізі схожості між різними елементами даних. Кластеризація, алгоритм k-середніх (k-means) і методи на основі нейронних мереж, як автоенкодери, є ефективними для цієї задачі. Однак цей підхід може бути менш точним у порівнянні з навчанням з учителем, оскільки складно оцінити результат без чіткої визначеності щодо міток [2].

Напівконтрольоване навчання. Цей підхід є поєднанням попередніх двох методів. Використовується часткова інформація про мітки для поліпшення точності моделі. Це дозволяє підвищити ефективність виявлення аномалій, зменшуючи при цьому потребу в великій кількості мічених даних.

Хоча технології ШІ демонструють значний потенціал у виявленні вторгнень, їх ефективне впровадження в реальних системах безпеки пов'язане з низкою практичних труднощів. Основними проблемами є високі вимоги до обчислювальних ресурсів, недостатня доступність якісних навчальних наборів даних, а також необхідність забезпечення високої швидкості обробки та реагування в реальному часі.

Використання алгоритмів глибокого навчання для виявлення вторгнень вимагає значних обчислювальних потужностей, що може бути перешкодою для їх впровадження в реальних середовищах. Моделі, зокрема глибокі нейронні мережі, потребують великих обсягів пам'яті та високої продуктивності процесорів. Зокрема, застосування таких методів на рівні мережевого трафіку вимагає не тільки потужних серверів для навчання, але й здатності працювати в реальному часі без значних затримок. Вирішення цієї проблеми передбачає розробку ефективних методів оптимізації моделей, таких як використання розподілених обчислень або спеціалізованих апаратних платформ (наприклад, графічних процесорів — GPU або тензорних процесорів — TPU), що дозволяє значно пришвидшити процес обробки даних [3].

Для навчання моделей ШІ в системах виявлення вторгнень необхідні великі, добре мічені набори даних, що містять різноманітні приклади нормальної та аномальної активності в мережах. Однак збори таких даних часто є проблематичними з огляду на конфіденційність і безпеку, оскільки вони можуть включати чутливу інформацію, таку як персональні дані або конфіденційну інформацію про компанії. Крім того, в умовах постійної еволюції атак важко створити універсальні набори даних, що відображають всі можливі сценарії. Для подолання цієї проблеми можуть бути використані методи генерації синтетичних даних або міжмережеві симуляції, які дозволяють створювати реалістичні умови для навчання алгоритмів без використання реальних даних.

Системи виявлення вторгнень повинні бути здатними реагувати на атаки в реальному часі, що особливо важливо в умовах сучасних швидко змінюваних загроз. Використання ШІ для виявлення аномалій може значно сповільнити процес виявлення та реагування через складність моделей або велику кількість етапів обробки даних. Для цього необхідно застосовувати ефективні алгоритми, які можуть працювати з мінімальною

затримкою. Одним з рішень є використання комбінованих підходів, де ШІ відповідає за попереднє виявлення потенційних загроз, а традиційні системи IDS — за фільтрацію та реагування.

Один із ключових напрямків розвитку — це інтеграція ШІ з іншими засобами захисту в єдину, більш потужну і адаптивну систему кібербезпеки. Системи виявлення вторгнень можуть бути лише однією частиною загальної інфраструктури захисту інформації. Інтеграція з системами виявлення та запобігання вторгнень (IPS), а також з іншими засобами, такими як антивірусні програми та системи моніторингу мереж, дозволяє створити більш комплексну і багатоетапну архітектуру захисту. Застосування штучного інтелекту в таких системах дозволяє не тільки вдосконалювати виявлення аномалій, але й автоматизувати процеси реагування, що підвищує ефективність захисту.

Інтеграція ШІ в реальні системи вимагає створення відповідних інтерфейсів та стандартів взаємодії між різними компонентами, що дозволяє об'єднати різні типи захисту в єдину систему з автоматичним реагуванням на загрози. Важливим аспектом є забезпечення сумісності з існуючими системами, що вимагає врахування специфіки старих інфраструктур та механізмів управління доступом.

Перспективи застосування штучного інтелекту в кібербезпеці безсумнівно значні. Розвиток технологій глибокого навчання та нейронних мереж відкриває нові горизонти для виявлення складних атак, таких як нульові дні (zero-day) або атаки, що використовують нові, незафіксовані в сигнатурах методи. Одним з основних напрямків є використання ШІ для створення "адаптивних" систем безпеки, які можуть змінювати свої стратегії захисту залежно від змін у поведінці атакувальників або в умовах мережі.

Зокрема, перспективним є використання методів глибинного навчання для виявлення та прогнозування нових векторів атак на основі аналізу великих даних і поведінкових патернів. Це дозволяє системам безпеки не тільки реагувати на загрози, але й прогнозувати можливі атаки, значно знижуючи час на реагування і, відповідно, зменшуючи потенційні збитки.

Окремої уваги заслуговує також розвиток використання технології блокчейн для покращення прозорості та цілісності даних у системах кібербезпеки. Завдяки своїм властивостям збереження незмінності записів і децентралізації, блокчейн може бути ефективно застосований для забезпечення високої стійкості до маніпуляцій з даними, що мають важливе значення для виявлення вторгнень.

Штучний інтелект є потужним інструментом для підвищення ефективності систем виявлення вторгнень у сучасних інформаційних системах. Використання машинного навчання дозволяє виявляти нові типи атак та значно знижує рівень помилкових спрацьовувань, що є важливою перевагою порівняно з традиційними методами. Однак, для успішного впровадження ШІ в реальні системи кібербезпеки, необхідно подолати низку практичних проблем, таких як обчислювальні обмеження, відсутність достатньої кількості мічених даних та забезпечення швидкості реагування.

У перспективі, інтелектуальні системи безпеки будуть все більше інтегруватися з іншими компонентами кіберзахисту, створюючи більш ефективні та адаптивні механізми реагування на загрози. Однак для досягнення цієї мети необхідно продовжувати дослідження в галузі ШІ, зокрема у напрямку покращення алгоритмів навчання, зниження їх обчислювальної складності та інтеграції з іншими інфраструктурами безпеки.

1. Бабічев В. В., Кочеров, В. Ю. Інтелектуальні системи виявлення вторгнень на основі машинного навчання. Київ: Наукова думка, 2018. 248 С. – ISBN 978-966-00-3200-1.

2. Грінь О. М., Кравченко, І. І. Використання технологій штучного інтелекту для виявлення аномалій у мережах зв'язку. Наукові праці Національного технічного університету України «Київський політехнічний інститут», 2020. 17(3), 45-52.

3. Meera M. S., Rao S. N. Comparative Analysis of IoT protocols for a Marine IoT System," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2018. P. 2049-2053.

ОБ'ЄДНАННЯ ТА ІДЕНТИФІКАЦІЇ ІНФОРМАЦІЙНИХ ОБ'ЄКТІВ ІЗ ДЕКІЛЬКОХ ДЖЕРЕЛ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЄДИНОЇ ОБСТАНОВКИ В ЗОНІ ВІДПОВІДАЛЬНОСТІ

Анотація

У статті представлено метод об'єднання та ідентифікації інформаційних об'єктів (ІО) з різних інформаційних систем для створення єдиної картини обстановки в зоні відповідальності. Запропонований підхід заснований на алгоритмах кластеризації та врахуванні областей перетину зон відповідальності. Отримані результати свідчать про підвищення точності та оперативності обробки даних, що сприяє покращенню якості прийняття рішень у тактичних умовах.

Вступ

Розвиток інформаційних систем для тактичного управління потребує збирання та об'єднання даних з різних джерел для створення єдиної обстановки на полі бою. Проблема дублювання інформації та розбіжностей у координатах і характеристиках об'єктів ускладнює процес прийняття рішень, що обумовлює необхідність розробки методів ефективного об'єднання таких даних.

Мета дослідження:

Основною метою є розробка методики ідентифікації та об'єднання інформаційних об'єктів із різних систем («Кропива», «Дельта») для формування єдиної картини обстановки з урахуванням точності даних та областей перетину зон відповідальності.

Методологія

Дані надходять у систему з декількох джерел — АСУ «Кропива» та «Дельта». Кожна з цих систем надає координати та інші атрибути об'єктів, що розташовані в їхніх зонах відповідальності. Після завантаження дані сортуються за джерелами та зберігаються у відповідних таблицях бази даних.

Нижче наведено структуру таблиць бази даних, яка використовується для зберігання даних про військові об'єкти, їх координати, джерело, тип, зону відповідальності та інші атрибути. Ключові таблиці включають **military_objects** для основних даних про об'єкти та **coordinates** для зберігання координат і ідентифікаторів.

Таблиця 1 – military_objects

№	Найменування	Тип	Обов’язкове?	Приклад	Опис
1	sidc	Текст	Так	"10031500012020200"	Повний код SIDC який використовується для опису військового об'єкта.
2	ids_identity	Рядок (2 символи)	Так	"03"	Ідентифікатор, який вказує на належність об'єкта (наприклад, 'свій', 'нейтральний', 'ворожий').
3	ids_symset	Рядок (2 символи)	Так	"15"	Символьний набір, який визначає категорію об'єкта (наприклад, 'наземна техніка', 'авіація').
4	ids_type	Рядок (6 символів)	Так	"120202"	Код, який поєднує тип, вид та підтип об'єкта (наприклад, 'середній танк').
5	description	Текст	Так	"Средний танк"	Опис об'єкта природною мовою, який використовується для більш зрозумілого подання на карті або у звітах.

Кінець таблиці 1

6	area_of_responsibility	Рядок	Так	'POLYGON((30 10, 40 40, 20 40, 10 20, 30 10))'	Геометричний об'єкт з текстового опису полігону
7	observation_datetime	dataTime	Так	10.10.2024 6:00:00	Час створення об'єкта в бд
8	source	Рядок	Так	Дельта/Кропива	Зберігає рядок із типом джерела даних
9	SKO	float	Так	20.0	Середня-квадратична помилка визначає похибку щодо координат об'єкта. Вимірюється у метрах

Таблиця 2 – coordinates

№	Найменування	Тип	Обов'язкове?	приклад	Опис
1	x	З плаваючою комою / Ціле	Так	3.310178e+06	Координата X об'єкта у системі координат.
2	y	З плаваючою комою / Ціле	Так	6.521847e+06	Координата Y об'єкта у системі координат.
3	ids_identity	Ціле	Так	03	Ідентифікатор, який вказує на належність об'єкта (наприклад, 'свій', 'нейтральний', 'ворожий').
4	ids_symset	Ціле	Так	15	Символьний набір, який описує категорію об'єкта (наприклад, 'наземна техніка', 'авіація').
5	ids_types	Ціле	Так	120202	Код, який поєднує вигляд, тип та підтип об'єкта (наприклад, 'середній танк').

Кожне з джерел має свою зону відповідальності, що представлена у вигляді полігону на карті. Об’єкти, які потрапляють у зону перетину цих полігонів, можуть дублюватися, оскільки одні й ті ж фізичні об'єкти можуть бути зафіксовані обома системами. Використовуючи геометричні операції, визначається область перетину двох полігонів, яка представляє зону, де об'єкти з різних джерел можуть бути дубльовані. Об'єкти, що потрапляють у визначену область перетину, підлягають подальшій обробці. Їхні координати та характеристики аналізуються для визначення, чи належать вони до одного й того ж фізичного об'єкта.

Процес ідентифікації та об'єднання об'єктів спрямований на виявлення дубльованих даних про один і той самий фізичний об'єкт, отриманих з різних джерел. Це дозволяє створити єдину картину обстановки, зменшуючи дублювання інформації та підвищуючи точність даних. Об'єкти, які потрапляють у зону перетину зон відповідальності двох джерел, вважаються потенційними дублікатами, і вони перевіряються на близькість координат та схожість характеристик. Для кожного об'єкта, що знаходиться в зоні перетину, обчислюється відстань до інших об'єктів. Якщо відстань менша за допустиму, об'єкти розглядаються як потенційний один фізичний об'єкт. З використанням алгоритму k-середніх, об'єкти, що мають близькі координати та однакові характеристики, об'єднуються в кластери. У кожному кластері обчислюються середні координати з урахуванням точності джерела. Для кожного кластера створюється єдиний запис, що описує фізичний об'єкт, із середньозваженими координатами та узгодженими характеристиками.

Кластеризація даних дозволяє групувати близькі за координатами та характеристиками об'єкти в один кластер, якщо вони представляють той самий фізичний об'єкт. У цьому підході використовується алгоритм k-середніх, який забезпечує ефективне об’єднання об'єктів шляхом мінімізації відстані між об'єктами всередині кластеру. Алгоритм починається з вибору початкових центрів кластерів, що забезпечує рівномірний розподіл точок. Кожен об'єкт призначається до найближчого центру кластеру, що зменшує середню відстань до інших об'єктів у кластері. Центр кожного кластеру перераховується як середнє значення координат об'єктів у цьому кластері. Процес повторюється, поки центри кластерів не стабілізуються. Після завершення алгоритму кожен кластер представляє один фізичний об'єкт, із середніми координатами, що враховують точність даних із джерел.

Кожне джерело може мати різну точність вимірювань, тому об’єднання даних здійснюється з урахуванням їхньої середньоквадратичної похибки (СКП). Для кожного об'єкта в кластері координати X та Y обчислюються як середньозважені, де вага кожного значення обернено пропорційна його похибці. Це означає, що дані з меншою похибкою мають більше значення в обчисленні остаточних координат. Додаткові характеристики, такі як тип об'єкта та ідентифікаційні дані, також узгоджуються для створення єдиного опису об'єкта. У випадках, коли атрибути з різних джерел збігаються, вони об'єднуються, якщо ж є невідповідності, обираються дані з джерела з вищою достовірністю. Після зваженого об'єднання координат та узгодження атрибутів формується новий запис, який описує об'єкт із максимально можливою точністю.

Після завершення процесу ідентифікації та об'єднання об'єктів результати зберігаються в базі даних, що дозволяє створити єдину інформаційну картину обстановки. Для об'єктів, що були ідентифіковані як дублікати та об'єднані, створюється єдиний запис у таблиці military_objects. Цей запис включає середньозважені координати об'єкта, його тип, опис, час спостереження та зону відповідальності. Об'єкти, які не підлягали об'єднанню, також зберігаються у базі даних із зазначенням джерела даних та інших атрибутів. Це дозволяє зберігати повну інформацію для подальшого аналізу. авдяки структурі бази даних, де зберігаються координати, ідентифікатори та характеристики, користувачі можуть швидко отримати доступ до інформації про об'єкти та їхню позицію в зоні відповідальності.

Результати

- Ефективність алгоритму: Застосування алгоритму кластеризації дозволяє скоротити дублювання об'єктів у зоні відповідальності та зменшити кількість суперечливих даних, підвищуючи достовірність інформації.
- Поліпшення точності: Об'єднання координатних даних із використанням вагової моделі надає більш точні координати для кожного фізичного об'єкта.
- Аналіз якості кластеризації: Використання індексу Девіса-Болдіна та коефіцієнта силуету дозволило визначити оптимальні параметри кластеризації, що підтвердило ефективність обраної методології.

Висновки

Запропонований підхід до ідентифікації та об'єднання інформаційних об'єктів із різних джерел демонструє високу ефективність у створенні єдиної обстановки в зоні відповідальності. Результати показують, що застосування алгоритмів кластеризації та зважування даних дозволяє отримати більш точну та узгоджену інформаційну картину, що є важливим для підтримки тактичного управління. Розроблене рішення може бути використане для інтеграції різнорідних джерел даних у реальному часі, що сприяє підвищенню ефективності прийняття рішень у бойових умовах.

1. Fedorchenko, I., Oliinyk, A., Stepanenko, Zaiko, T., Korniienko, S., Kharchenko, A. (2020). Construction of a genetic method to forecast the population health indicators based on neural network models. Eastern-European Journal of Enterprise Technologies, 1(4-103), 52–63. DOI: 10.15587/1729-4061.2020.197319.
2. Phang, F. A., Pusppanathan, J., Nawi, N. D., Zulkifli, N. A., Zulkapri, I., Harun, F. K. C., Wong, A. Y. K., Alsayaydeh, J. A. J., Sek, T. K. (2021). Integrating Drone Technology in Service Learning for Engineering Students. International Journal of Emerging Technologies in Learning, 16(15), 78–90. DOI: 10.3991/ijet.v16i15.22979.
3. Smith, J., Lee, R., Brown, A., & Tanaka, H. (2022). A framework for dynamic data integration in tactical management systems. Journal of Applied Data Science and Engineering, 3(2), 45–60. DOI: 10.1016/j.jadseng.2022.102003.

В.В. Мохор, О.В. Цуркан, Р.П. Герасимов, В.П. Яшенков, Т.М. Клименко

ЛАНДШАФТ ЗАГРОЗ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В АТАКАХ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Відповідно до [1, 2] актуальною залишається негативна тенденція до використання зловмисниками соціальної інженерії для отримання доступу до інформації. Даний різновид загроз виокремлюється з огляду на його багаторічну популярність, широке поширення і значний вплив унаслідок реалізації [2]. До того ж цьому сприяють і досягнення в розвитку технологій штучного інтелекту. Зловмисники використовують їх для підвищення ефективності та правдоподібності атак соціальної інженерії [3]. Тож весь спектр застосувань соціальної інженерії проти як окремих користувачів, так і організацій загалом узагальнюється і представляється ландшафтом загроз [1–3].

Використання штучного інтелекту в атаках соціальної інженерії характеризується багатоманітністю [4]. Здебільшого воно направлене на створення переконливого та цілеспрямованого вмісту. При цьому в межах кожної атаки соціальної інженерії виокремлюються три етапи (рис. 1) [5]. Реалізування першого етапу орієнтоване на створення реалістичного вмісту. Прикладом такого вмісту є вебсайти, електронні листи, публікації в соціальних мережах, голос, відео, посвідчення особи. На другому етапі зловмисники шляхом аналізування інформації про цільовий об’єкт (наприклад, цифрові сліди) визначають свою наміри з огляду на його онлайн-присутність і поведінку. Унаслідок претекстування реалізується персоналізований контекстно залежний фішинг. Створенні сценарії автоматизуються і здійснюються на третьому етапі використанням великих мовних моделей (наприклад [3], FraudGPT, WormGPT). Це дозволяє зловмисникам проводити атаки соціальної інженерії з мінімальними зусиллями.

Рисунок 1 – Фреймворк атак соціальної інженерії на основіштучного інтелекту [4]

Перш за все ландшафт загроз використання штучного інтелекту визначається ключовими факторами. Вони притаманні йому як трансформаційній технології. Серед них виокремлюються велика кількість даних, удосконалені алгоритми оброблення даних та розвинута апаратна інфраструктура [4]. Завдяки цьому зловмисники можуть користуватися інтелектуальними можливостями штучного інтелекту. Окрім надання правдоподібних відповідей на запити цільового об’єкту вони можуть скеровувати свої дії у режимі реального часу [4, 6]. Завдяки цьому зменшуються вимоги до кваліфікації зловмисників. Додатково такі можливості підсилюються завдяки упровадженню розвідувальних циклів зворотного зв’язку на етапі претекстування і виконання атак соціальної інженерії. Загалом це призводить до створення інструментальних засобів на основі штучного інтелекту як динамічних систем. Кожна з них здатна розвивати свою діяльність відповідно до реальних результатів. Проявом таких змін є врахування, наприклад [4], чат-ботом, змін поведінки цільового об’єкта залежно від надісланої інформації і налаштованість з огляду на його реакцію (наприклад, вагання, підозрілість) [4–6].

Отже, ландшафт загроз використання штучного інтелекту в атаках соціальної інженерії обумовлений великою кількістю даних, удосконаленими алгоритмами їх оброблення та розвинутою апаратною інфраструктурою. Як наслідок, зловмисникам надається можливість скеровувати дії з мінімальними зусиллями та, найнебезпечніше, у режимі реального часу. Це призводить до підвищення ефективності та правдоподібності атак соціальної інженерії. Тож необхідно оцінювати такі ризики та обирати релевантні заходи та засоби забезпечення інформаційної безпеки як користувачів, так і організацій загалом.

1. International Organization for Standardization. (2023). Cybersecurity. Guidelines for Internet security (ISO/IEC Standard No. 27032:2023). https://www.iso.org/standard/ 76070.html.
2. European Union Agency for Cybersecurity. (2024). ENISA Threat Landscape 2024. https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape %202024_0.pdf.
3. Polra Victor Falade. (2023). Decoding the Threat Landscape : ChatGPT, FraudGPT, and WormGPT in Social Engineering Attacks. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 9 (5), 185–198. https://doi.org/10.32628/CSEIT2390533.
4. Schmitt M., Flechais I. (2024). Digital deception: generative artificial intelligence in social engineering and phishing. Artificial Intelligence Review. 57, article number 324. https://doi.org/10.1007/s10462-024-10973-2.
5. Mouton F., Malan M. M., Leenen L. and Venter H. S. (2014). Social engineering attack framework. Information Security for South Africa (p. 1–9). Johannesburg, South Africa. https://doi.org/10.1109/ISSA.2014.6950510.
6. Tofighi M. A., Ousat B., Zandi J., Schafir E., Kharraz A. (2024). Constructs of Deceit: Exploring Nuances in Modern Social Engineering Attacks. In F. Maggi, M. Egele, M. Payer, M. Carminati (Eds), Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 107-127). Vol 14828. Cham Springer. https://doi.org/10.1007/978-3-031-64171-8_6.

ЗМІСТ

Д.В. Ланде, В.І. Полуциганова, С.А. Смирнов
МЕТОДОЛОГІЯ РОЮ ВІРТУАЛЬНИХ ЕКСПЕРТІВ ДЛЯ ОЦІНКИ ВЗАЄМОЗВ'ЯЗКУ ЗАГРОЗ ТА УРАЗЛИВОСТЕЙ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ….. 4

В.В. Святко, І.О. Шахматов, А.Л. Юр'єв
СИСТЕМА ПЕРСОНАЛІЗОВАНИХ РЕКОМЕНДАЦІЙ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРОДАЖІВ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ…… 8

Ю.Г. Даник, В.І. Шестаков
ВАРІАНТИ КОНФЛІКТІВ ТА АНАЛІЗ РИЗИКІВ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНИ …… 10

І.В. Басиста
ЧЕРГОВІ КРОКИ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ (продовження огляду)…… 11

О.М. Селезньова, С.М. Леваднюк
РИЗИКИ ТА ПЕРЕВАГИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СУЧАСНИХ УМОВАХ…… 15

А.А. Омельченко
КОНФІДЕНЦІЙНІСТЬ ЦИФРОВИХ БІОМАРКЕРІВ ТА ШТУЧНИЙ ІНТЕЛЕКТ…… 16

V.P. Petrenko
THE IMPACT OF ARTIFICIAL INTELLIGENCE ON ENTREPRENEURSHIP: INSIGHTS FROM A QUESTIONNAIRE STUDY AND A BRIEF LITERATURE REVIEW…… 17

К.В. Бабій, О.А. Ворон
ВДОСКОНАЛЕННЯ РЕКУЛЬТИВАЦІЇ ТЕХНОГЕННО ПОРУШЕНИХ ЗЕМЕЛЬ ЗА ДОПОМОГОЮ РОБОТЕХНІКИ І ШТУЧНОГО ІНТЕЛЕКТУ…… 19

І.В. Дегтяренко
ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ МОДЕЛЕЙ ГЛИБОКОГО НАВЧАННЯ НА EDGE-ПРИСТРОЯХ…… 21

Д.І. Симонов
ПРОГНОЗУВАННЯ ВПЛИВУ ЛІДЕРІВ ДУМОК НА ПОВЕДІНКУ СОЦІАЛЬНИХ ГРУП…… 23

С.О. Євдокимов
ВПЛИВ ТЕХНОЛОГІЇ «FINGERPRINTING» НА КІБЕРБЕЗПЕКУ СИГНАЛЬНИХ СИСТЕМ СУЧАСНОГО ЗАЛІЗНИЧНОГО ТРАНСПОРТУ…… 25

І.О. Шахматов, І.В. Замрій
ТЕХНОЛОГІЇ МАСШТАБУВАННЯ ДАНИХ У БОРОТЬБІ З DDOS-АТАКАМИ …… 27

В.В. Мартиненко
АЛГОРИТМ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ…… 31

В.С. Чепіга
ПІДХОДИ ДО АНАЛІЗУ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ …… 33

О.Д. Тимофєєв, С.О. Прокопов
ВИКОРИСТАННЯ ШІ ДЛЯ ОБРОБКИ ТА АНАЛІЗУ ВЕЛИКИХ ОБСЯГІВ ДАНИХ У РЕАЛЬНОМУ ЧАСІ …… 34

С.В. Савельєва, Т.А. Смирнова
РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В АВТОМАТИЗАЦІЇ БІЗНЕС ПРОЦЕСІВ…..... 36

Д.О. Добродомов, О. М. Любименко, О.А. Штепа
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ РОЗПІЗНАВАННЯ ЗОБРАЖЕНЬ ТА ВІДЕО У РЕАЛЬНОМУ ЧАСІ…... 38

А.О. Парфило, Ю.Ю. Нізовцев
ІННОВАЦІЇ В РОЗРОБЦІ КАМУФЛЯЖНИХ ТЕХНОЛОГІЙ: ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА ФРАКТАЛЬНИХ ПАТЕРНІВ ДЛЯ ПРОТИДІЇ АВТОМАТИЗОВАНИМ СИСТЕМАМ ВИЯВЛЕННЯ…. 39

М.О. Сокол
СУЧАСНІ ТЕНДЕНЦІЇ В ШІ …….... 41

С.Ю. Бондаренко, Ю.Л. Вітомський
ЕМОЦІЙНЕ ЗАРАЖЕННЯ ТА СИМУЛЯЦІЯ ЕМПАТІЇ В ШІ: ПСИХОЛОГІЧНІ НАСЛІДКИ ДЛЯ ЕМОЦІЙНОГО БЛАГОПОЛУЧЧЯ ЛЮДИНИ ТА СОЦІАЛЬНОЇ ЗГУРТОВАНОСТІ….. 42

О.С. Кобус, С.Ю. Бондаренко
АНАЛІЗ ВРАЗЛИВОСТІ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ (IDS) НА ОСНОВІ ШІ ДО АГРЕСИВНИХ АТАК…… 44

Р.Т. Бибик, Т.І. Наконечний
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ ТА ПРОТИДІЇ ЗАГРОЗАМ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ……. 46

В.В. Рудюк
ПРАКТИЧНІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ВИКЛАДАННІ БІОЛОГІЇ…..... 50

О.А. Владимирський, І.А. Владимирський, І.П. Криворучко, Д.М. Семенюк
ПІДВИЩЕННЯ ЯКОСТІ ПРИЙОМУ ДІАГНОСТИЧНОЇ ІНФОРМАЦІЇ ВІД РОЗПОДІЛЕНИХ У ПРОСТОРІ ПРИСТРОЇВ ЗБОРУ ДАНИХ…… 51

Ю.О. Єжелий, Є.О. Писаренко
ХМАРНІ ТЕХНОЛОГІЇ ТА ШТУЧНИЙ ІНТЕЛЕКТ: ОПТИМІЗАЦІЯ РЕСУРСІВ І УПРАВЛІННЯ ПРОЄКТАМИ В ЦИФРОВУ ЕПОХУ…….. 53

А.І. Єременко, Т.А. Вакалюк
ОГЛЯД СТРАТЕГІЙ МАШИННОГО НАВЧАННЯ ……..... 55

В.С. Волошин
ЩОДО ПЕРСПЕКТИВ РОЗВИТКУ ШТУЧНОГО ІНТЕЛЕКТУ В ПОРІВНЯННІ З ЛЮДИНОЮ (НА ПРИКЛАДІ МЕРЕЖІ CHATGPT)..... 56

Ю.А. Климець
СМАРТ-КОНТРАКТИ ДЛЯ ЦИФРОВИХ АКТИВІВ У ДЕЦЕНТРАЛІЗОВАНІЙ ЕКОСИСТЕМІ……..…….. 61

Є.О. Васильєва
ЯК ШТУЧНИЙ ІНТЕЛЕКТ ДОПОМАГАЄ УПРАВЛЯТИ МАРКЕТИНГОВИМИ БЮДЖЕТАМИ І СКОРОЧУВАТИ ВИТРАТИ?……..……..…….. 62

Б.С. Калинюк
ОПТИМІЗАЦІЯ ЕНЕРГОЕФЕКТИВНОСТІ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ, ЩО ВИКОРИСТОВУЄ АГЕНТИ ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ ДЕФІЦИТУ ЕНЕРГОНОСІЇВ …… 63

А.О. Кримська
ШТУЧНИЙ ІНТЕЛЕКТ У ПРОГНОЗУВАННІ АВАРІЙНИХ СИТУАЦІЙ ТА МОНІТОРИНГУ КРИТИЧНИХ ОБ'ЄКТІВ ЕНЕРГЕТИКИ ……..…… 65

А.О. Тарановський
ПОТОЧНИЙ СТАН ВИКОРИСТАННЯ В УКРАЇНІ РЕГУЛЯТОРНИХ ПІСОЧНИЦЬ ДЛЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ……...……... 67

Т.С. Токовило, Е.В. Кірпічов
ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА СУЧАСНУ МАТЕМАТИЧНУ ОСВІТУ: ПОКРОКОВЕ НАВЧАННЯ, ПЕРСОНАЛІЗОВАНІ ПІДХОДИ ТА ТОЧНІСТЬ РОЗВ'ЯЗКІВ……. 69

Я.Ю. Дорогий, В.В. Цуркан, І.О. Бердиченко, О.О. Дорога-Іванюк
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ БАНКІВСЬКОЇ СФЕРИ ……. 70

М.С. Кондратенко
ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ СУМНІВНИХ ТРАНЗАКЦІЙ В БЛОКЧЕЙН-МЕРЕЖІ…….……. 72

Д.А. Іванов
ОГЛЯД ПАРАМЕТРІВ ОПТИМІЗАЦІЯ МОДЕЛІ ДЛЯ ПРИШВИДШЕННЯ САМОНАВЧАННЯ……... 74

Т.С. Токовило, М.М. Васильєв
ПЕРЕВЕГИ ТА НЕДОЛІКИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ НАВЧАННЯ……..…….…. 75

Д.І. Азарний
КЛАСИФІКАЦІЯ ДІПФЕЙКІВ ……..…… 77

Д.В. Яценко
МЕТОДИКА ВИБОРУ ОПТИМАЛЬНОЇ МОДЕЛІ ДЛЯ РОЗВ'ЯЗАННЯ ЗАДАЧ ПРЕДИКТИВНОЙ АНАЛІТИКИ НА БАЗІ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ……..…….. 79

А.О. Устенко
ПРАКТИЧНІ КЕЙСИ ТА ДОСВІД ЗАСТОСУВАННЯ ШІ В ОСВІТНЬОМУ ПРОЦЕСІ……..... 81

О. В. Жмай
ПЕРЕВАГИ ТА НЕДОЛІКИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ ВИЩОЇ ОСВІТИ……..… 83

А.С. Ковальова, Е.В. Рижков
МЕТОДИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ КІБЕРАТАК В УКРАЇНІ ……..…..... 85

O.O. Tsypliak, V.O. Artemchuk
GENERATIVE AI IN BYPASSING CAPTCHA: CHALLENGES FOR MODERN WEB PLATFORM SECURITY ……...……...…... 86

В.А. Заглинський
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В OSINT: ПЕРЕВАГИ ТА ВИКЛИКИ…..… 88

А.В. Бондаренко, Г.В. Разумова
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПРОЦЕСІ ПРИЙНЯТТЯ СТРАТЕГІЧНИХ РІШЕНЬ……... 90

А.В. Бондаренко, О.В. Оскома
ВЗАЄМОЗАЛЕЖНІСТЬ ШТУЧНОГО ІНТЕЛЕКТУ ТА BIG DATA: ВИКЛИКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ……..……. 91

П.І. Сагайда, І.А. Гетьман, М.А. Держевецька
ПРОЦЕС УДОСКОНАЛЕННЯ КІБЕРБЕЗПЕКИ З ВИКОРИСТАННЯМ МЕТОДІВ МАШИННОГО НАВЧАННЯ, ЯК СКЛАДОВОЇ ІНФОРМАЦІЙНОЇ ПІДТРИМКИ ДІЯЛЬНОСТІ НА ОСНОВІ ЦИФРОВОГО ІНТЕЛЕКТУ……. 92

А.О. Попова, О.М. Любименко, Н.О. Маслова, О.А. Штепа
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ ДАНИХ ТА ВИЯВЛЕННЯ АНОМАЛІЙ У СИСТЕМІ КВАДРАТИЧНОГО ГОЛОСУВАННЯ НА БЛОКЧЕЙНІ…….…. 94

К.В. Виноградова, Е.В. Рижков
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПІДРОЗДІЛАМИ СТРАТЕГІЧНИХ РОЗСЛІДУВАНЬ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ…..…… 95

Н.В. Заїка, І.В. Мартинюк, М.Ю. Комаров, О.О. Молчанов
ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ТА ПРОТИДІЇ ЗАГРОЗАМ ПРИ ЗАСТОСУВАННІ АВТОМАТИЗАЦІЇ ТА ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ КІБЕРБЕЗПЕКИ……...… 96

M. Antonishyn, V. Liedniei, M. Myhun
OWASP FOR ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML)…….. 98

A. Davydiuk, S. Kulyk
ARTIFICIAL INTELLIGENCE IN CYBERSECURITY FOR CLOUD SERVICES ……..... 100

А.О. Попова, О.М.Л юбименко, Н.О. Маслова, О.А. Штепа
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ ДАНИХ ТА ВИЯВЛЕННЯ АНОМАЛІЙ У СИСТЕМІ КВАДРАТИЧНОГО ГОЛОСУВАННЯ НА БЛОКЧЕЙНІ……... 102

А.І. Вавіленкова
АЛГОРИТМИ ПОШУКУ ЗМІСТУ В ІНФОРМАЦІЙНИХ ПОВІДОМЛЕННЯХ …….……..…….. 103

Я.А. Сиротюк
ВИЯВЛЕННЯ ВТОРГНЕНЬ У СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ……..……..... 104

О.М. Безуглий
ОБ'ЄДНАННЯ ТА ІДЕНТИФІКАЦІЇ ІНФОРМАЦІЙНИХ ОБ'ЄКТІВ ІЗ ДЕКІЛЬКОХ ДЖЕРЕЛ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЄДИНОЇ ОБСТАНОВКИ В ЗОНІ ВІДПОВІДАЛЬНОСТІ……...…. 106

В.В. Мохор, О.В. Цуркан, Р.П. Герасимов., В.П. Яшенков, Т.М. Клименко
ЛАНДШАФТ ЗАГРОЗ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В АТАКАХ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ……..… 109

ЗБІРНИК МАТЕРІАЛІВ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
«ШТУЧНИЙ ІНТЕЛЕКТ І БЕЗПЕКА»
19-21 листопада 2024 року

Відповідальні за випуск:

О.В. Цуркан, Т.М. Клименко

Місце проведення:

Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України;

м. Київ, вул. Олега Мудрака

(Генерала Наумова), 15.

З питаннями щодо конференції звертатися:

ІПМЕ ім. Г.Є. Пухова НАН України,

вул. Олега Мудрака (Генерала Наумова), 15,

кім. 303, Цуркан Оксана володимирівна, тел. 424-91-62,

068-014-57-22, e-mail: otsurkan24@gmail.com

Інститут проблем моделювання в енергетиці
ім. Г. Є. Пухова НАН України,
вул. Олега Мудрака (Генерала Наумова), 15, Київ, 03164, Україна,

тел.: +38 044 424 91 62, факс: +38 044 424 10 63
веб сайт: https://ipme.kiev.ua/