

УДК 004.8

В.В. БЕГУН\*, С.В. БЕГУН\*\*, А.В. ТУРОК\*

## СПОДІВАННЯ НА ШІ ДЛЯ УКРАЇНИ, АБО ЩО НЕ ТАК ІЗ ВПРОВАДЖЕННЯМ ШІ В УКРАЇНІ

\*Інститут проблем математичних машин і систем НАН України, м. Київ, Україна

\*\*Державна установа «Інститут громадського здоров'я ім. О.М. Марзєєва Національної академії медичних наук України», м. Київ, Україна

**Анотація.** У статті представлено аналіз процесів розвитку технологій штучного інтелекту (ШІ) у світі й в Україні та його зв'язок з безпекою на основі ризик-орієнтованого підходу. Розглядаються новітні досягнення, коротко зміст технології, стан впровадження стандартизації та нормування процесів розвитку технології, можливі ризики життєдіяльності людини та їх особливості у нашій державі. Участь у процесі наукових установ України, зокрема НАН України, державне регулювання, державно-приватне партнерство, діяльність приватних фірм та можливості застосування технології ШІ у сфері безпеки. Стаття є оглядовою, тому містить багато цитованого матеріалу. Наводяться дані про поширення технології в Україні у різних сферах життєдіяльності, короткі дані про основні державні організації та підприємства, які займаються впровадженням ШІ, дані про деякі приватні підприємства та державно-приватне партнерство у цьому напрямі. Разом з тим автори звертають увагу на те, що переважна більшість робіт із цієї тематики належить до приватного бізнесу, який у своїй більшості заснований іноземними компаніями, а також на значне відставання офіційної науки, НАН України тощо. Фокусується увага на тому, що неналежна увага (у порівнянні з передовими країнами) приділяється питанням безпеки як безпосередньо технології ШІ, так і новим процесам діяльності за участю ШІ. Детально аналізується небезпека деяких приватних підприємств щодо використання ШІ у псевдонауковій сфері, так званої допомоги у створенні наукових статей та підвищенні наукового статусу вчених, освіті тощо. Автори бачать у цьому явище не тільки таке, що порушує етику наукової доброчесності, але й катастрофічний ризик для держави у цілому. Аналізується стан впровадження стандартів та законів, наводяться напрями розробки програмного забезпечення у сфері безпеки з використанням ШІ та хмарних технологій тощо. Пропонується прискорити впровадження технології та міжнародних нормативних документів на державному рівні з координацією НАН України.

**Ключові слова:** штучний інтелект (ШІ), безпека, аналіз розвитку ШІ, ІТ, ризик, освіта з безпеки.

**Abstract.** The article analyzes the processes of development of artificial intelligence (AI) technologies in the world and in Ukraine and its connection with security based on a risk-oriented approach. The latest achievements, a brief description of the technology, the state of implementation of standardization and regulation of the technology development processes, possible risks to human life and their specifics in our country are considered. Participation of Ukrainian scientific institutions, in particular the National Academy of Sciences of Ukraine, state regulation, public-private partnership, activities of private firms, and the possibilities of applying AI technology in the security sector are also discussed. The article is a review, so it contains a lot of cited material. It provides data on the spread of the technology in Ukraine in various spheres of life, brief information on the main state organizations and enterprises involved in the implementation of AI, and data on some private enterprises and public-private partnerships in this area. At the same time, the authors draw attention to the fact that the vast majority of works on this topic belong to private business, which is mostly founded by foreign companies, and that official science, the National Academy of Sciences, etc. are lagging behind. The article focuses on the fact that inadequate attention (compared to advanced countries) is paid to the security issues of both AI technology itself and new processes of activity involving AI. The authors analyze in detail the danger of some private enterprises using AI in the pseudo-scientific sphere — the so-called assistance in creating scientific articles and raising the

*scientific status of scientists, education, etc. The authors see this phenomenon not only as violating the ethics of scientific integrity, but also as a catastrophic risk for the state as a whole. The article analyzes the state of implementation of standards and laws, provides directions for the development of security software using AI and cloud technologies, etc. It is proposed to accelerate the introduction of technology and international regulations at the state level with the coordination of the National Academy of Sciences.*  
**Keywords:** artificial intelligence (AI), security, analysis of AI development, IT, risk, security education.

DOI: 10.34121/1028-9763-2025-1-12-31

## 1. Вступ

Розвиток технологій штучного інтелекту (ШІ) відбувається, на нашу думку, за експоненціальним законом за багатьма критеріями, як-от інтерес суспільства: кількість публікацій, кількість працівників у цій сфері, кількість споживачів, ефективність застосування в різних сферах технологій, фінансування у розвинутих країнах, що також підтверджується щорічними дослідженнями Стенфордського університету [1]. Кожна людина, яка має доступ до інтернету, незалежно від статусу стикається з цим явищем щоденно. На державному рівні причетні країни виділяють цю технологію у вищий пріоритет навіть за розміром фінансових витрат [1–3].

Застосування ШІ у сфері безпеки, також як й безпека саме технології, безумовно, має бути на часі, оскільки безпека є фундаментальною потребою життєдіяльності людини. На основі ШІ маємо створювати нові моделі запобігання небезпек. Фундаментальна наукова ідея викладена в багатьох авторських, і не тільки, публікаціях [4–8] про необхідність наукової підтримки державних служб України з напрямку безпеки (ДСНС, ДНАОП, екологія, радіаційна безпека), військової безпеки тощо. На жаль, безпека та військова безпека мають найнижчий рівень розвитку інформаційних технологій (ІТ), і не тільки впровадження ШІ, що не відповідає загальному вектору розвитку України та міжнародним стандартам (ISO 31010 тощо) і за що українське суспільство платить дуже велику ціну.

Так, навіть у звіті й планах Міністра цифрової трансформації М. Федорова ці напрями відсутні (Хто і як займався цифровізацією на державному рівні) [@zedigital](https://t.me/zedigital) [9]. Розробка програмного забезпечення (ПЗ) з безпеки не стає нашою пріоритетною метою, приватні підприємства під керівництвом (патронатом) міністра М. Федорова досягли значних успіхів майже в усіх сферах життєдіяльності, але кластер із безпеки, який існує в Інституті кібернетики, не має наповнення [10], що свідчить про слабкий зв'язок державних і приватних підприємств одного напрямку, тобто відсутність координації у сфері безпеки.

Основні положення безпеки на виробництві з розвитком ІТ змінюються відповідно до змін у світовій практиці дуже швидко, а разом і техногенна безпека та безпека довкілля. Нові технологічні процеси, нові засоби захисту надають значно кращі можливості, але при цьому можуть бути й значно більш тяжкі наслідки, особливо у разі помилок прийняття рішень на високому рівні. Внаслідок впровадження ШІ у виробничі процеси за останні роки світ праці пережив такі трансформації, що навіть обрати професію на все життя тепер виглядає як рідкісна розкіш, що додатково ускладнює ситуацію. Згідно з дослідженням McKinsey «Майбутнє роботи після COVID-19», кожному 16-му працівнику до 2030 року доведеться кардинально змінити професійний шлях [11].

За даними дослідження Всесвітнього економічного форуму (WEF) у 2021 році, до кінця 2025 року більше, ніж 85 мільйонів робочих місць можуть зникнути через автоматизацію. Завдяки штучному інтелекту, роботам і алгоритмам багато завдань можуть виконуватися набагато швидше та ефективніше. У зв'язку з цим змінюються вимоги до освіти та навчання, про що також буде мова. Сучасний ринок праці змінюється настільки швидко, що наша система освіти просто не встигає адаптуватися до нових вимог.

Слід зазначити, що нещодавно змінився стандарт вищої освіти відповідно прийнятому у державі напрямку європейської інтеграції [12]. В освіті у галузі ІТ з'явилися зміни

— з'явилася нова класифікація галузі знань «F Інформаційні технології, F3 Комп'ютерні науки» та код і найменування відповідної деталізованої галузі відповідно до Міжнародної стандартної класифікації освіти ISCED-F 2013 «0613 Software and applications development and analysis» — «Розробка та аналіз програмного забезпечення та додатків» замість попередніх класифікацій «Прикладна математика», «Інженерія програмного забезпечення», «Комп'ютерні науки». На наш погляд, порівняно зі старим кодом 122 «Комп'ютерні науки» формальні вимоги зменшені, перехід на нові стандарти дозволить українським ІТ спеціалістам легше інтегруватися у міжнародний ринок праці, але потрібна значна робота у напрямі адаптації навчальних матеріалів та перекваліфікації викладачів.

Отож бачимо, що ІІІ вже став важливою частиною нашого життя і його вплив з кожним днем стає все сильнішим. Ось декілька цифр і прогнозів, які підтверджують це [11]:

- «понад 1,8 тис. компаній у світі просто зараз працюють у галузі розробки штучного інтелекту;
- \$407 млрд — такий обсяг ринку ІІІ у 2027 році прогнозують фахівці;
- 314 млн людей у світі користуються ІІІ у 2024 році;
- 35 % світових компаній уже активно використовують ІІІ у своїй роботі;
- 41 % користувачів вважають, що ІІІ так чи інакше покращить їхнє життя».

Це зараз ми посягаємо друге місце в Європі у рейтингу відкритих даних Open Data Maturity та увійшли в топ-10 країн світу в рейтингу технологічних компетенцій Coursera. А ще 15 років тому картина була протилежною.

*Актуальність.* Автоматизація, штучний інтелект, глобалізація — ці сили невпинно перекроюють ринок праці. В концепції [14] сформульовано необхідність впровадження ІІІ в державі: «Використання технологій штучного інтелекту в пріоритетних галузях економіки пов'язане з необхідністю зміни виробничих процесів, насамперед процесу ухвалення рішень на різних рівнях державного управління». Отже, аналіз процесів впровадження ІІІ, у тому числі у галузі безпеки, є актуальним.

*Мета статті.* Огляд та аналіз розвитку технологій ІІІ в Україні й світі з постановкою задач нових досліджень у галузі в цілому в Україні та в Інституті проблем математичних машин і систем НАН України.

## 2. Основна частина

### 2.1. Аналіз сучасного стану розвитку

У статті використовується термінологія згідно з основним стандартом [15] та словником термінів у сфері штучного інтелекту, розробленого Міністерством цифрової трансформації України [15]. Ось основні терміни:

- Штучний інтелект. ІІІ (artificial intelligence, AI): <Системна> здатність спроектованої системи набувати, обробляти та застосовувати знання і навички.
- Нейронна мережа (neural network): Мережа примітивних обробних елементів, з'єднаних зваженими зв'язками з регульованими вагами, у якій кожен елемент видає значення, застосовуючи нелінійну функцію до своїх вхідних значень, і передає його іншим елементам або представляє його як вихідне значення.
- Вхідні дані (input data): Дані, для яких модель машинного навчання, що розгортається, обчислює прогнозований результат або висновок.

#### 2.1.1. Огляд публікацій

Згідно з результатами моніторингу публікацій у світі [1] у період 2010–2024 рр. загальна кількість публікацій за темою ІІІ збільшилася понад у 2,5 разів, а найбільше зростання

понад у 7 разів спостерігається у напрямі машинного навчання. Йдеться про понад 240 тисяч публікацій на рік у 2022-му році з тенденцією до зростання [1].

З українських виділяється робота Петька С.М., яка, за словами автора, присвячена «... дослідженню особливостей правового регулювання технологій штучного інтелекту в країнах цифрових лідерів...». Згідно з даною роботою відзначено динамічний розвиток технологій ШІ та їх вплив на людство, вказано на нові завдання для урядів країн щодо створення та прийняття нормативно-правових актів [2]. У цій роботі також добре описано історію розвитку технологій ШІ, детально наведено класифікацію процесів ШІ (рис. 1), стан нормативного й законодавчого регулювання та фінансування на той час (2023 р.).

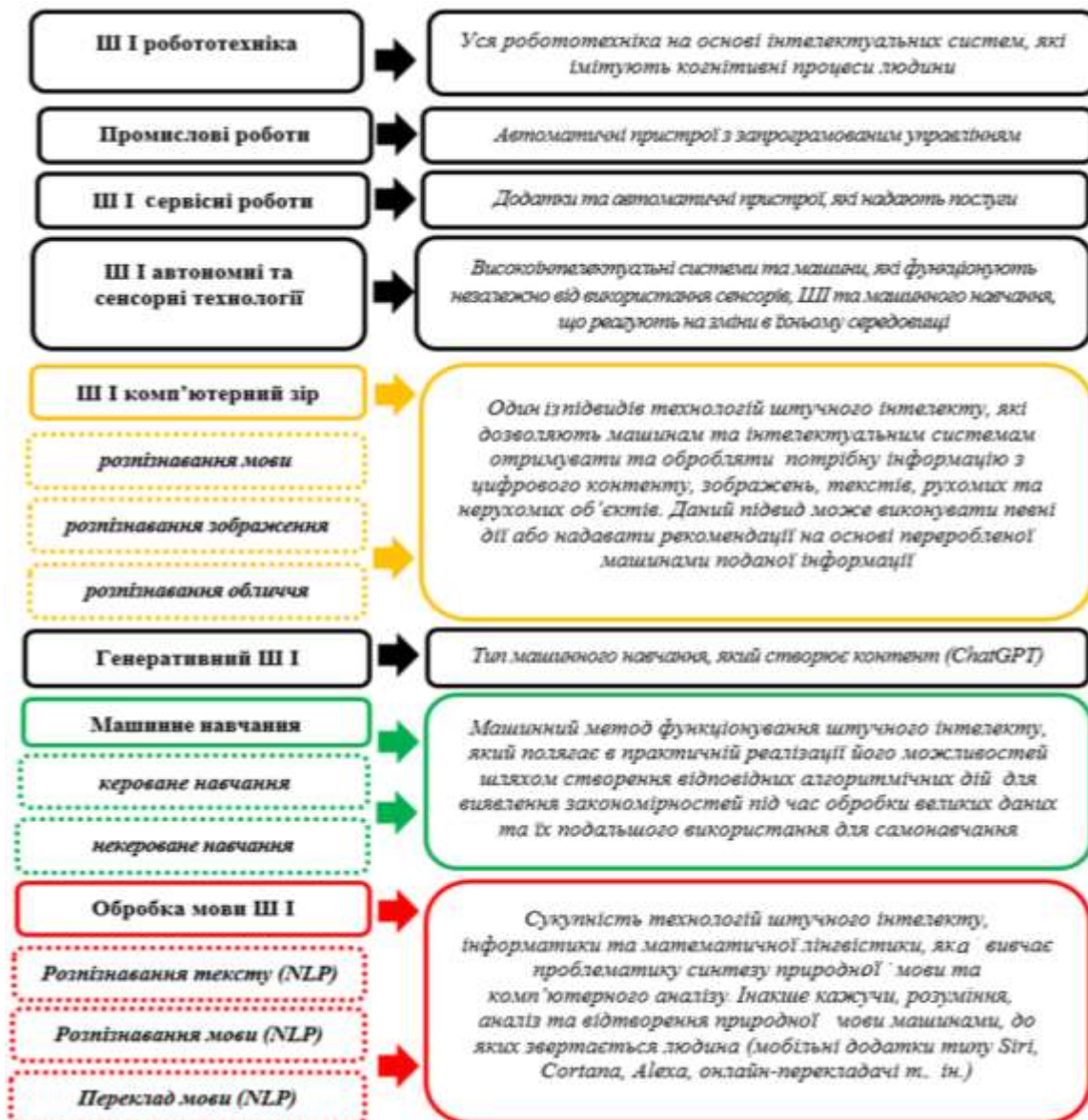


Рисунок 1 — Основні технології ШІ та його підвиди. Джерело [2]

У роботах Яценка В.О. у загальних рисах описано математичну частину технології та її прикладне застосування у військовій сфері тощо [17, 18]. Щодо математичної частини технології ШІ можна стверджувати, що мають місце всі математичні теорії з виходом у підсумку на теорію булевих функцій, оскільки як результат оптимізації потрібно здійснювати складний (до сотень параметрів) вибір.



У Китаї, що є одним із лідерів застосування ШІ у техніці, для популяризації та прискорення сприйняття у суспільстві ШІ створюються багато відеофільмів із демонстрацією успішного впровадження та переваг технологій ШІ (рис. 2). Як бачимо на цьому прикладі, ідеально використовуються всі технології ШІ: обробка мови (розпізнавання мови, переклад мови), таксі безпілотне рухається за вказівками на адресу пасажирів, машинне навчання (кероване навчання), комп'ютерний зір (розпізнавання зображень) із вибором оптимальних маршрутів, робототехніка (промислові роботи). Всі механізми складної машини управляються автоматично згідно з поставленим пасажиром завданням з урахуванням усіх зовнішніх факторів та обставин.



Рисунок 2 — Повітряне таксі зі штучним інтелектом на 2 пасажирів, скриншот відео [15]

Стосовно публікацій для ознайомлення з загальною технологією в цілому серед безлічі джерел є пропозиція від самого Біла Гейтса [20]: «...книга, яку я рекомендую більше, ніж будь-яку іншу книгу про штучний інтелект, — главам держав, бізнес-лідерам і всім, хто запитусь, тому що вона пропонує щось рідкісне: ясне уявлення як про неймовірні можливості, так і реальні ризики, які на нас чекають», — написав Гейтс. Звертаємо увагу на коло осіб, яким один із засновників ІТ пропонує ознайомлення з новою технологією — це починається з «глав держав», що вже свідчить про роль нової технології у суспільстві. Йдеться про книгу «Наступна хвиля: технології, влада і найбільша дилема XXI століття», яка була опублікована у 2023 році. Її автором є один із піонерів штучного інтелекту Мустафа Сулейман, співзасновник лабораторії DeepMind, яку у 2014 році продав компанії Google, а нині обіймає посаду генерального директора Microsoft AI. У своїй книзі Сулейман прогнозує, що швидкий розвиток штучного інтелекту повністю змінить роботу в більшості галузей. Він посилається на дослідження 2023 року від консалтингової компанії McKinsey, яке стверджує, що до 2030 року автоматизовано буде близько половини всіх робочих процесів. Коротко зміст книги викладено в [21], із передмови: «Найближчим часом на нас чекає бурхливий розвиток штучного інтелекту, біотехнологій, квантових обчислень, альтернативної енергетики та робототехніки. Вони принесуть величезні прибутки своїм розробникам і поліпшать життя мільярдів людей. Але разом із цим на нас чекають глобальні ризики. Ми стоїмо перед вибором між майбутнім, сповненим можливостей, і майбутнім, сповненим небезпек. Настає епоха передових технологій, і ми маємо бути го-

тові до неї». Отож, як бачимо, потрібно пам'ятати не тільки про користь ШІ, а й про глобальні ризики, на що вказує як автор книги Мустафа Сулейман, так і Біл Гейтс — фундатори технології.

Прикладом обговорення проблем впровадження ШІ українською мовою є інтернет-видання «Штучний інтелект і безпека» [22], яке нещодавно випустила компанія «Сідкон», де також обговорюються питання безпеки без глибокого розгляду моделей та методів ШІ. Також на сайтах компаній, що працюють у галузі ШІ в Україні, теж є багато інформації про досягнення у даній галузі.

### 2.1.2. Головні світові досягнення

Почнемо з того, що «...ШІ — це технологія, яка здатна творити добро. Наприклад, AlphaFold від DeepMind, за оцінками, заощадив 400 мільйонів років часу дослідників на вивчення білкових структур завдяки використанню обчислювальних потужностей штучного інтелекту. Можливості відкриваються в усіх сферах — у персоналізації освіти і навчанні, у значно кращій діагностиці здоров'я, у вивченні закономірностей у величезних масивах даних, що дає змогу проводити всі види досліджень більш вичерпно і швидше» [1].

Головні досягнення технології у 2024 році наведені в оглядовій статті [4].

2024 рік став важливим етапом для розвитку ChatGPT. З кожним днем функціонал платформи змінювався, роблячи її ще більш інтегрованою в щоденні завдання та комунікацію. Завдяки спільним силам розробників, тепер користувачі можуть спілкуватися зі штучним інтелектом не лише текстово, а й через аудіо та відео. Платформа здатна підтримувати розмову на будь-яку тему, використовуючи більш детальну й актуальну інформацію завдяки інтегрованому пошуку в інтернеті.

Одним із найяскравіших винаходів у сфері ШІ став реліз генератора відео Sora від OpenAI. Sora надає можливість створювати відео з текстових описів, перетворювати фотографії у відео, а також використовувати функцію «Re-mix» для модифікації вже створених відео. Є також функція «розкадровки», що дозволяє створювати сцени чи послідовності відео з низки підказок.

Gemini 2.0 від Google зміг побороти конкуренцію, створивши для своїх користувачів розвиненого інтелектуального помічника, який зараз набагато швидше та точніше здатний обробляти запити користувачів, володіючи понад 100 мовами. Цей помічник задовольняє потреби як приватних осіб, так і корпоративних користувачів. Маючи підвищену продуктивність та енергоефективність, помічник здатний, окрім здійснення мультимодальних можливостей генерування тексту, звуку та зображень, розпізнавати об'єкти та швидко знаходити їх, виконувати дії від імені користувача.

Чудовим застосунком у 2024 році стала онлайн-платформа електронного продажу SmartTender, за допомогою якої електронний помічник юриста швидко обробляє тисячі відкритих тендерів, виділяючи основні вимоги в тендері та параметри, а також повідомляючи компанію виробника про відповідність вимог тендера. ШІ виділяє найбільш перспективні тендери, враховуючи ринкову ситуацію, аналізуючи ціни конкурентів за лічені хвилини.

Так звані «літаючі таксі», призначені для перевезення пасажирів на короткі відстані в межах міст, планує подарувати людству компанія Joby Aviation у наступному році. Це перші у своєму класі воднево-електричні літаки, які будуть долати дистанції у 842 км.

Щодо поширення технології у світі варто звернутися знову до доктора Петька: «...у 2022 році найбільша вага серед регіонів світу в призмі сегментації глобального ринку технологій ШІ припадає на Північноамериканський регіон із показником 36,84 %. Далі йде Європейський регіон — 25,97%; Азійсько-Тихоокеанський регіон — 23,93%; Латинська Америка, Близький Схід та Африка (LAMEA) займають останнє місце з показником 14,26 %» [2]. Нині основними виробниками технологій ШІ є Microsoft, IBM, Alphabet,

Apple, Oracle, Open AI [1], за прогнозами провідних експертів найближчим часом Азійсько-Тихоокеанський регіон буде попереду, враховуючи зростаюче застосування ШІ в індустріальному напрямі [2]. Разом із тим новий президент США Трамп анонсував створення ШІ-компанії з інвестиціями у 500 мільярдів доларів [3]. Він «... вважає, що цей проєкт створить близько 100 тисяч нових робочих місць для американців. Великі дата-центри для ШІ будуть розміщуватися у кластерах на території США, для яких зараз шукають відповідне місце. Трамп обіцяє «допомагати шляхом підписання надзвичайних декларацій»» [3]. Надзвичайні заходи будуть потрібні у зв'язку з потребами значної енергетичної потужності для роботи великих потужностей комп'ютерів. Мова йде про Гігавати потужності.

Як один із найкращих прикладів подальшого розвитку технології компанії Google та OpenAI повідомили про розробку чипу квантового комп'ютера [1]: «квантовий чип Willow компанії Google, як повідомляється, виконав еталонне обчислення — завдання, розв'язання якого займає у найшвидших сучасних суперкомп'ютерів десять септильйонів років (це десять із 24 нулями), менш ніж за п'ять хвилин. А нова модель оЗ компанії OpenAI стала великим технічним проривом, наближаючи ШІ до того моменту, коли він зможе перевершити людину у виконанні будь-яких когнітивних завдань. Цей епохальний рубіж називають «універсальним штучним інтелектом» (AGI)».

#### *Використання ШІ в ЗСУ у рамках міжнародного співробітництва*

У 2024 році українська армія активно впровадила передові технології на основі штучного інтелекту (ШІ), що суттєво підвищують її обороноздатність та ефективність на полі бою. Так, розвідувальні безпілотики Vector, які активно використовуються в Україні, отримали новітнє оновлення з використанням штучного інтелекту. На безпілотниках встановили інноваційний сенсор AI Receptor, який базується на чипі Jetson Orin Nvidia, та оснащений кількома датчиками. Це оновлення дозволяє дронам виконувати оптичну навігацію навіть у складних умовах — вночі або при поганій видимості. Крім того, система забезпечує автоматичне виявлення й ідентифікацію об'єктів, що значно підвищує ефективність розвідки.

Однією з ключових розробок стала платформа Avengers, створена Центром інновацій Міністерства оборони України. Ця система автоматично аналізує відео з дронів та стаціонарних камер, щотижня виявляючи до 1 тисячі одиниць ворожої техніки. Завдяки цьому оператори можуть швидше приймати рішення, зменшуючи ризик помилок через втому.

Українські інженери активно працюють над вдосконаленням безпілотних літальних апаратів (БПЛА), оснащуючи їх технологіями ШІ. Це дозволяє дронам самостійно обходити системи радіоелектронної боротьби (РЕБ) противника та виконувати завдання навіть при втраті зв'язку з оператором. Такі інновації підвищують автономність та ефективність БПЛА на полі бою.

Крім того, Україна активно співпрацює з міжнародними технологічними компаніями для інтеграції рішень на основі ШІ в оборонну сферу. Зокрема, компанія Helsing пропонує посилити програмні рішення для протидії швидкому розвитку РЕБ ворога, що допоможе безпілотним апаратам вражати цілі навіть при втраті зв'язку.

У 2024 році також проводяться випробування систем управління вогнем із застосуванням ШІ, зокрема, для самохідних артилерійських установок Caesar. Інтеграція ШІ дозволяє скоротити витрати боєприпасів на 30 %, підвищуючи точність та ефективність артилерійських ударів.

Водночас українські розробники працюють над оснащенням FPV-дронів технологіями машинного зору, що дозволяє дронам самостійно розпізнавати та слідувати за цілями без постійного контролю оператора. Це підвищує ефективність ударних дронів та зменшує залежність від людського фактора.

### 2.1.3. Позитивні кроки розвитку ІІІ в Україні

Відомості щодо цього викладені в офіційному виданні «Біла книга з регулювання ІІІ в Україні: бачення Мінцифри» [23] та статті Viktoriia Pushkina «Огляд українського GovTech: хто розробляє проєкти для державного сектору, у чому полягають виклики і які перспективи» [24].

Наведемо цитату з передмови [23] міністра цифрової трансформації М. Федорова: «Від початку створення Мінцифри і до сьогодні наша ціль залишається незмінною — побудувати найзручнішу цифрову державу у світі. Ми віримо, що майбутнє України — у розвитку цифрової економіки та інновацій. Штучний інтелект — важлива частина цього шляху. Сьогодні ІІІ в Україні вже використовують у різних напрямках: від військових технологій до GovTech. Бачимо важливий сенс у розвитку технологій ІІІ також у сферах освіти, охорони здоров'я, економіки, урбаністичного планування та багатьох інших. Це дасть змогу нашій державі не просто адаптуватися до світових тенденцій, а й стати лідером у цій галузі».

Головна думка, на наш погляд, яка проходить наскрізною лінією у нашій статті, — це те, що підприємства України все більше впроваджують технології ІІІ для поліпшення ефективності своєї роботи в різних сферах — від безпеки до економіки. Це дозволяє оптимізувати процеси, автоматизувати рутинні завдання, покращити управління ресурсами та надати громадянам більш якісні послуги. Більшість підприємств, які застосовують ІІІ, відносяться до приватного сектору. Щодо державних підприємств в Україні, то кілька з них активно використовують технології ІІІ для вдосконалення своїх процесів, підвищення ефективності та покращення надання послуг, а також для виконання функцій державного контролю у сфері ІТ. Отже, головні державні підприємства, які впроваджують ІІІ:

- Державний центр інформаційних технологій (ДЦІТ) <https://qc.csi.cip.gov.ua/>. Головна задача — інформаційно-аналітичні системи для держорганів: ДЦІТ відповідає за впровадження ІІІ в державному управлінні для автоматизації аналізу даних, управління ресурсами та прийняття рішень. Це включає використання аналітичних систем для оптимізації роботи урядових органів.

- Центр стратегічних комунікацій та інформаційної безпеки <https://spravdi.gov.ua/czentr-strategichnyh-komunikacij-ta-informacijnoyi-bezpeky-otrymav-derzhavnu-reyestracziyu/>. Центр стратегічних комунікацій та інформаційної безпеки отримав державну реєстрацію нещодавно, одна з головних задач — аналіз медіапростору. Центр використовує ІІІ для моніторингу інформаційного простору та виявлення дезінформації чи пропаганди. Алгоритми аналізують великий обсяг текстових і відеоматеріалів для виявлення фейкових новин і маніпуляцій.

- Державна служба спеціального зв'язку та захисту інформації України (ДССЗІ). ДССЗІ працює над проєктами в сфері кібербезпеки, де використовуються ІІІ-технології для виявлення та реагування на кібератаки, захисту критичної інфраструктури та державних інформаційних систем.

- Вже 15 років в Україні реалізується проєкт для автоматизації надання державних послуг цифрова платформа «Дія» — онлайн-платформа для взаємодії громадян із державними органами. Частково в таких платформах застосовуються чат-боти і автоматизовані системи на базі ІІІ для обробки запитів громадян та автоматизації процесів видачі документів.

У роботі [24] наведена така класифікація учасників впровадження ІІІ та ІТ у державі: «...український GovTech сьогодні складається з Мінцифри, яка є трендсетером GovTech у країні; центральних органів влади, які впроваджують політику цифровізації; донорів, які мають експертизу і фінансують велику кількість проєктів; муніципалітетів, які ведуть проєкти цифровізації (серед них виділяється «Київ Цифровий»); GovTech-компаній — консультантів та виконавців у різних сферах, серед яких бізнес-аналіз, розробка, кібер-



безпека та ін.». При такому підході бачимо серед учасників процесу впровадження ІІІ центральні органи державної влади, приватні структури, але, на жаль, не бачимо НАН України, до речі, не має спогадів про НАНУ й у «Білій книзі» з впровадження ІІІ в Україні.

#### 2.1.4. Інші Державні організації та ініціативи, які використовують ІІІ

Система «Прозорро» — система електронних державних закупівель, де використовується ІІІ для аналізу даних і виявлення можливих корупційних ризиків, шахрайських схем та порушень. ІІІ також допомагає в оптимізації процесу закупівель і поліпшенні управління держбюджетом. «З 2016-го року компанія належить державному підприємству «Прозорро». У компанії є штатна ІТ-команда з 20 людей, ще 10 фахівців залучено на аутсорсі. ІТ-команда Prozorro працює за Agile, дотримується продуктового підходу та data-driven концепції. Використовує Jira і Confluence, керує розробкою за допомогою Kanban. Серед технологій переважно опенсорсні: MongoDB, HAProxy, nginx, Zabbix, Grafana, RabbitMQ, Kafka, ELK, Linux. Також застосовуються хмарні технології, PHP, JavaScript. Ядро платформи написано на Python» [24].

Система відеонагляду та аналізу даних для безпеки МВС. ІІІ застосовується для автоматичного моніторингу та аналізу відеозаписів із камер спостереження в громадських місцях для виявлення порушень та підтримки правопорядку.

Медична сфера — у рамках реформ в охороні здоров'я ІІІ використовується для аналізу медичних зображень (наприклад, рентгенівських знімків), що дозволяє лікарям швидше ставити діагнози. ІІІ також може використовуватись для передбачення поширення захворювань, моніторингу стану здоров'я населення. Найбільша ІТ-компанія «eZdorovya», або ДП «Електронне здоров'я», яка діє з 2017-го року та відповідає за адміністрування національних інформаційних систем у сфері охорони здоров'я України. Серед них: Центральна база даних електронної системи охорони здоров'я (ЦБД ЕСОЗ) і ГІКС «HealthNet». Компанія є розробником Державного реєстру дезінфекційних засобів і Державного реєстру харчових добавок, які реалізуються на платформі «Дія Engine». Планує взяти на адміністрування державні реєстри медвиробів, харчових добавок, косметики, дезінфекційних засобів, системи крові тощо [24]. З 2019-го року працюють за власним фреймворком SDLC, розробленим серед іншого на основі PMBok і адаптованим під eHealth-домен. Здебільшого працюють за каскадною моделлю, але з додаванням Agile-практик. Оскільки компанія працює з мікросервісною архітектурою, то використовують Kubernetes. Технологічний стек на базі Elixir також застосовує Kotlin.

Проекти в аграрній сфері в Україні активно використовують ІІІ-технології для моніторингу сільськогосподарських угідь (за допомогою дронів і супутникових знімків) та для оптимізації виробничих процесів у сільському господарстві, що покращує продовольчу безпеку.

В Україні працюють сотні компаній ІТ, більшість з яких є приватними структурами й використовують іноземні інвестиції [23]. Чисельність деяких сягає декілька тисяч висококваліфікованих спеціалістів ІТ, наприклад:

- SoftServe — одна з провідних українських ІТ-компаній, яка займається розробкою рішень на основі ІІІ. SoftServe працює над проектами, які включають використання ІІІ для аналізу великих даних, автоматизації процесів у банківському секторі, а також для покращення публічних послуг.
- Miratech — це українська компанія, яка спеціалізується на наданні ІТ-послуг. Вона використовує ІІІ для автоматизації обслуговування клієнтів, обробки даних і для підтримки громадських ініціатив, пов'язаних із цифровою трансформацією.
- DataRobot — це американська компанія, яка має представництво в Україні і використовує ІІІ для автоматизованого аналізу даних у різних сферах, включаючи фінанси, медицину та державне управління.

- Luxoft — ця компанія надає консультаційні послуги та рішення для урядів і бізнесу, використовуючи технології ШІ для аналізу великих даних, моніторингу економічної ситуації та виявлення шахрайських схем у фінансових установах.

- Intellias — це ще одна ІТ-компанія, яка активно займається впровадженням ШІ в різних секторах економіки, зокрема, в транспорті, енергетиці та державному управлінні. Вони працюють над проєктами, що включають оптимізацію транспортних потоків і розвиток інтелектуальних транспортних систем.

- Ciklum працює над розробкою рішень для автоматизації бізнес-процесів у державних установах та компаніях, що стосуються управління даними, фінансів, а також розробки системи ШІ для підтримки онлайн-сервісів та електронного урядування.

- Компанія Сідкон «Штучний інтелект і безпека».

Як висновок, впровадження ШІ в Україні активно розвивається і стає важливим елементом у поліпшенні державного управління, підвищенні якості державних послуг і забезпеченні безпеки. Водночас приватні компанії, які займаються розробкою та впровадженням технологій ШІ, значно сприяють інноваціям у різних секторах економіки, надаючи державі сучасні інструменти для ефективнішого управління.

В Україні, зокрема, в Києві, кілька медичних установ активно впроваджують технології штучного інтелекту (ШІ) для покращення діагностики, лікування та надання медичних послуг. Серед них є як приватні, так і державні клініки, які використовують ШІ в таких напрямках, як аналіз медичних зображень, прогнозування захворювань, автоматизація робочих процесів та покращення ефективності лікування. Ось деякі клініки та медичні установи в Києві, які впроваджують або використовують ШІ: Клініка «Борис», Універсальна клініка «Оберіг», Медична лабораторія «Діла», Інститут нейрохірургії імені А.П. Ромоданова НАМН України, Приватне підприємство «Стоматологія-Світ».

З нашої точки зору, значний потенціал має впровадження ШІ у цілях безпеки, цим має займатися Державна служба з надзвичайних ситуацій (ДСНС).

### **2.1.5. Роль ШІ у боротьбі з надзвичайними ситуаціями**

Світові держави-лідери активно розвивають та використовують технології ШІ для покращення ефективності роботи своїх служб у протидії надзвичайним ситуаціям (НС), аналізі даних і прогнозуванні можливих загроз. Ось кілька прикладів використання ШІ у цій сфері.

1. Прогнозування природних катастроф та небезпечних явищ для попередження наслідків природних катастроф, таких як повені, землетруси, лісові пожежі та сильні бурі. Системи з ШІ аналізують величезні обсяги даних, включаючи метеорологічні прогнози, історичні дані та супутникові знімки, для виявлення потенційних загроз і їхнього розвитку з метою забезпечення своєчасної евакуації та підготовки до реагування.

2. Аналіз відео з безпілотних літальних апаратів (БПЛА) для моніторингу ситуації на місці надзвичайних подій. ШІ допомагає автоматично обробляти відео та зображення, отримані з БПЛА, для виявлення осередків пожеж, затоплених територій або пошкоджених об'єктів, що дозволяє швидко оцінити масштаб катастрофи (наприклад, лісової пожежі) та координувати дії рятувальників.

3. Інтелектуальні системи для аналізу великих даних, таких як соціальні мережі, метеорологічні звіти, новини та інші джерела інформації для виявлення ранніх ознак НС або для моніторингу поточних подій із метою виявлення повідомлень про потенційні небезпеки або катастрофи в реальному часі.

4. Використання роботів та автономних систем для рятувальних операцій у важкодоступних місцях, таких як завали або постраждалих будівлі після землетрусів чи вибухів. Ці роботи здатні здійснювати пошук постраждалих, передавати дані в реальному часі та допомагати рятувальникам при виконанні небезпечних завдань. Як приклад використання

роботів, оснащених сенсорами і камерами, для визначення високих рівнів радіації на об'єкті «Укриття».

5. Системи з ШІ для управління та координації рятувальних операцій. Ці системи використовують алгоритми для оптимізації розподілу ресурсів, розрахунку часу прибуття рятувальних бригад, а також для прогнозування подальшого розвитку подій.

6. Аналіз і моніторинг екологічної ситуації із застосуванням ШІ — це моніторинг екологічної ситуації, зокрема, забруднення повітря, води та ґрунту після хімічних або промислових аварій. Алгоритми ШІ дозволяють автоматизувати обробку даних від датчиків і супутникових знімків для виявлення змін у навколишньому середовищі.

Як бачимо, ШІ активно використовується для покращення реакції на НС, прогнозування ризиків, обробки даних та моніторингу ситуацій у реальному часі. Ці технології дозволяють підвищити ефективність рятувальних операцій, забезпечити точність діагностики та пришвидшити процес прийняття рішень у критичних ситуаціях. Але, на жаль, в ДСНС України за даними сайту служби такі роботи ще не проводяться навіть теоретично, тобто, як було сказано у вступі, впровадження ШІ у сферу безпеки є однією з головних задач науки з безпеки в Україні.

### 2.1.6. Ринок праці та зайнятість

Зайнятість на ринку праці у сфері штучного інтелекту в Україні демонструє позитивну динаміку, однак є кілька аспектів при оцінці цього ринку, які варто враховувати.

Попит на спеціалістів зі ШІ в державі зростаючий. Ринок праці в Україні відчуває все більший попит на спеціалістів, які мають знання та навички в галузі ШІ. Враховуючи розвиток ІТ-сектору, стартапів і цифрових трансформацій у різних галузях, в Україні збільшується потреба у фахівцях, які можуть працювати з такими технологіями, як машинне навчання, поглиблене навчання, комп'ютерний зір, обробка природної мови та аналіз великих даних. Пропонуються типи робіт та спеціальності:

- Data Scientists (науковець з обробки даних). Це одна з найбільш затребуваних професій на ринку ШІ в Україні. Такі науковці працюють над збором, обробкою та аналізом великих обсягів даних для вирішення бізнес-завдань.

- Інженери машинного навчання. Потреба у фахівцях, які можуть розробляти і оптимізувати алгоритми машинного навчання, постійно зростає.

- Розробники програмного забезпечення для ШІ. Програмісти, які спеціалізуються на розробці рішень, що включають елементи штучного інтелекту.

- Аналітики даних. Ці спеціалісти збирають та аналізують дані для виявлення трендів і створення прогностичних моделей за допомогою ШІ.

- Експерти в області комп'ютерного зору, обробки природної мови, робототехніки. Розробка та впровадження ШІ в конкретні галузі потребує спеціалістів із глибокими знаннями в окремих підсистемах ШІ.

Звісно, немає названих професій у державних довідниках та й в учбових програмах більшості ВНЗ, тому негайно потрібно адаптувати та розвивати освіту й навчання технологіям ШІ відповідно до вимог ринку. Такі програми пропонують низку вищих навчальних закладів, як-от Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київський національний університет імені Тараса Шевченка, Львівський національний університет імені Івана Франка, Національний технічний університет «Харківський політехнічний інститут», а також приватні курси та онлайн-платформи (наприклад, Prometheus, Coursera, DataCamp, edX). Але тут також існує проблема кадрового дефіциту — значний дефіцит висококваліфікованих кадрів викладачів ВНЗ. Це пов'язано з високими вимогами до освіти, наявністю практичного досвіду в цій сфері із суттєвою різницею рівня заробітної плати у комерційних організаціях у порівнянні

із заробітною платою викладача ВНЗ, а також із дефіцитом спеціалістів у конкретних підгалузях ІІІ.

Ринок праці для ІІІ у стартапах та ІТ-компаніях дещо відрізняється від загальнодержавного. Багато українських ІТ-компаній активно працюють у сфері ІІІ. Технологічні стартапи, як-от Reface, Allset, Miratech, Luxoft, активно наймають спеціалістів для розробки рішень на основі ІІІ. Також українські компанії надають послуги великим міжнародним клієнтам. Україна є важливим аутсорсинговим хабом для багатьох іноземних компаній, які розробляють ІІІ-продукти. Це створює додаткові можливості для працевлаштування українських спеціалістів в міжнародних проєктах. Спеціалісти з ІІІ в Україні зазвичай мають високий рівень зарплати, їхні доходи часто можуть перевищувати середні зарплати в інших галузях. Зарплата інженерів машинного навчання або data scientist може варіюватися від 2 000 до 5 000 доларів США на місяць у залежності від досвіду та спеціалізації. Оскільки попит на спеціалістів з ІІІ зростає, конкуренція на ринку праці теж збільшується. Водночас компанії часто шукають кадри з міжнародним досвідом або глибокими спеціалізованими знаннями в конкретних підсистемах ІІІ.

Отже, ринок праці в Україні у сфері ІІІ активно розвивається і має великий потенціал для зростання у майбутньому. Попит на кваліфікованих спеціалістів з ІІІ в Україні високий і буде продовжувати зростати, однак дефіцит висококваліфікованих кадрів залишається значною проблемою. Тому для забезпечення сталого розвитку цієї галузі необхідно буде інвестувати в освіту, підвищення кваліфікації фахівців та створення додаткових стимулів для залучення талановитих людей.

### **3. Можливі ризики**

#### **3.1. Короткий огляд**

Відповідно до концепції ризик-орієнтованого підходу (РОП) та міжнародних стандартів для усіх технологій потрібно розглядати ризики для персоналу підприємств, населення та довкілля. Ризик, пов'язаний із впровадженням ІІІ відповідно до загальноприйнятої класифікації, позначатимемо як соціальний, довгостроковий, постійний, глобальний, колективний, примусовий (не добровільний для більшості) ризик, який може мати навіть катастрофічні наслідки. Наслідки, щодо яких є занепокоєння у суспільстві, вивчалися в Україні компанією Research.ua [1]: «...більшість респондентів (71 %) побоюються втратити роботу через конкуренцію зі штучним інтелектом. 57 % не хотіли б опинитися в залежності від технологій. І майже однаковою мірою українці оцінюють вірогідність таких негативних наслідків, як неконтрольований розвиток ІІІ, його неетичне використання та порушення приватності». Як бачимо, всі передбачувані негативні наслідки — це соціальні ризики. На нашу думку, останнє має ще більш негативні наслідки для освіти та глобального розвитку (п. 3.2).

Доктор С.М. Петько [2] наводить таку якісну класифікацію можливих ризиків:

«До групи неприйнятної ризику відносяться технології біометричної ідентифікації, які використовуються у громадських місцях, як-от: системи відеоспостереження з ідентифікацією обличчя.

До групи високого ризику відносяться програми ІІІ, які можуть нанести шкоду безпеці, здоров'ю людини, юридичному праву та навколишньому середовищу. Згадані технології ІІІ використовуються у критичній інфраструктурі, при наданні державних послуг, у навчальному процесі, при працевлаштуванні, управлінні персоналом. Окремо акцентується увага на технологіях, які можуть впливати на демократичні процеси в країні, емоціональну поведінку виборців, поширення дезінформації під час виборчого процесу.

До групи обмеженого ризику будуть застосовуватися лише правила прозорості. До таких систем відносяться цифрові додатки, що взаємодіють із людьми (чат-боти), системи

розпізнавання емоцій, а також системи, що генерують/маніпулюють зображеннями та створюють цифровий контент».

На нашу думку, з такою якісною (не кількісною) класифікацією у цілому можна погодитися, кількісні показники потребують ретельного дослідження. Але, як бачимо, автор не відносить до категорії високого ризику системи з використанням ШІ, які «створюють цифровий контент», що, з нашої точки зору, є дискусивним та докладно розглядається далі у розділі 3.2.

Не зважаючи на те, що існують стандарти і закони Євросоюзу щодо використання ШІ стосовно запобігання ризиків [16, 25–29], впровадження європейського підходу з питань безпеки ШІ є предметом дискусії у нашій державі. Так, у згаданій вище Білій книзі [23] рекомендуються «принципи етичного міркування та добровільного кодексу поведінки...». Але у доктора С.М. Петька [2] інша точка зору, з якою ми повністю погоджуємось: «У процесі аналізу міжнародних стандартів штучного інтелекту важливо згадати й Резолюцію 2015/2103 (INL) щодо цивільно-правового регулювання робототехніки з рекомендаціями для Європейської комісії (англ. «European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics» (2015/2103(INL))), ухвалену Європейським Парламентом 16 лютого 2017 р. Ця Резолюція заклала підвалини до розуміння робототехніки та штучного інтелекту і стала, не зважаючи на її рекомендаційний характер, основою для запровадження наступних міжнародних стандартів у сфері впровадження та розвитку ШІ. Зазначена Резолюція передбачила запровадження цивільно-правової відповідальності за шкоду, завдану робототехнікою і штучним інтелектом, на агентів, тобто фізичних осіб, які використовують такі технології».

Отож [26]: «Відповідно до Резолюції 2015/2103(INL) від 16 лютого 2017 р. відповідальність за завдану шкоду не може бути покладена на роботів (у тому числі, на штучний інтелект, який використовує робототехніка), а покладається виключно на людину, яка може бути виробником, оператором, власником або користувачем. Для встановлення юридичної відповідальності необхідне доведення провини людини, яка могла передбачити і попередити завдання такої шкоди роботом. У зв'язку з цим пропонується запровадження обов'язкової системи страхування від настання негативних наслідків і завдання шкоди у сфері впровадження робототехніки та штучного інтелекту». Отже, визнання особистості за робототехнікою разом зі штучним інтелектом на міжнародному рівні заперечується, що, скоріше за все, стане міжнародним стандартом на тривалий час. Тобто штучний інтелект та роботи не будуть у найближчій перспективі визнаватися як юридичні особи чи інші категорії, які можуть напяму нести юридичну відповідальність за заподіяну шкоду, що є ознакою обмеженого штучного інтелекту, потребує ретельного дослідження моніторингу та законодавчого регулювання в міру зростання та розвитку потужності обчислювальних ресурсів і технологій ШІ, зростання складності моделей ШІ та втрачання контрольованості процесу навчання ШІ у міру зростання складності моделей на фоні більш широкого впровадження ШІ у промислові технології, технології навчання, прийняття рішень на державному рівні та у повсякденне життя.

### **3.2. Недотримання стандартів як нова катастрофічна небезпека**

Стосовно безпеки генеративного ШІ. Як сказано вище, більшість фахівців і компаній вважають цю сферу застосування ШІ зоною малого ризику. На жаль, це не стосується України. Наприклад, на сьогодні маємо офіційно діючу «Академію статей», створену в Україні з метою (з офіційного сайту): «Академія статей — це провідна міжнародна консалтингова компанія, яка надає допомогу науковцям у написанні та публікації наукових статей у наукометричних базах даних. Ми успішно працюємо в Україні, Казахстані, Йорданії, Узбекистані, країнах Балтії та в Азербайджані». Й далі: «За час роботи ми опублікували більше 1095-ти статей у Scopus та Web of Science, завдяки співпраці з нами близько 100-та вчених



отримали докторський ступінь, а 73 % наших замовників стали постійними клієнтами і довіряють нам та нашому професіоналізму». Щоб зрозуміти напрям діяльності «Академії», достатньо подивитися на послуги, які вони пропонують (рис. 3 а).

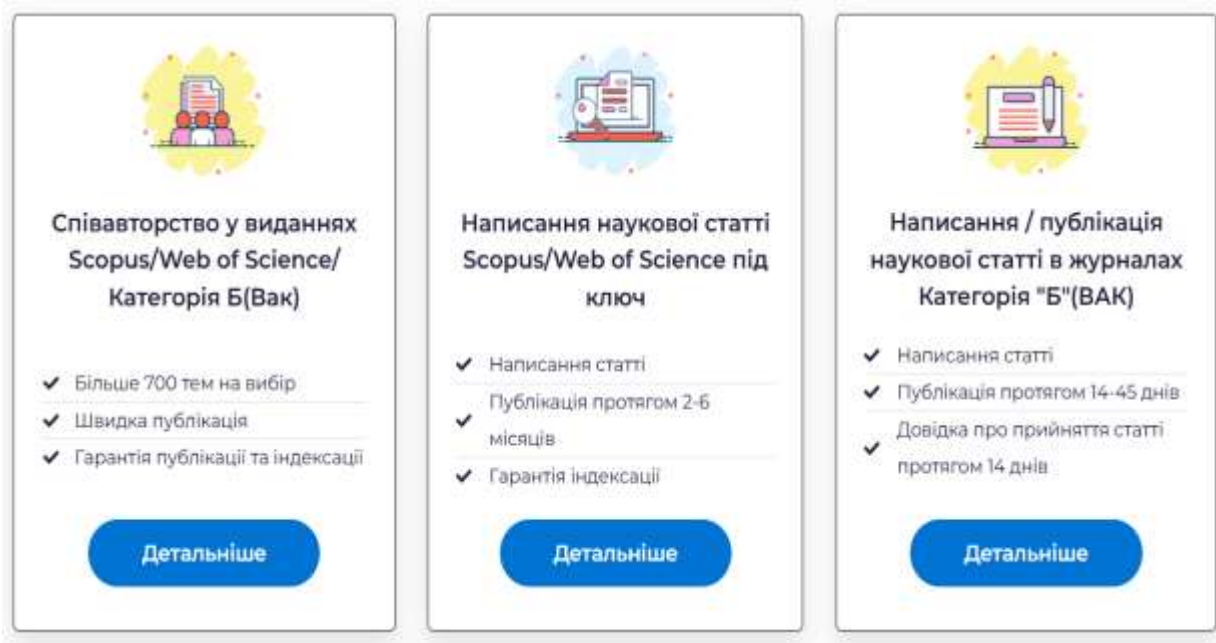


Рисунок 3 а — Послуги «Академії статей» з офіційного сайту організації, скриншоти, створені автором

Так, спектр послуг, які вони пропонують, містить повний комплекс робіт «під ключ» у становленні науковця від початкового рівня (нульового) до вищого рівня ОСВІТИ — доктора філософії та доктора наук! При цьому наводяться навіть розцінки (рис. 3 б). Плати й царствуй «лежачи на боку», як у відомій казці! Діяльність даної «Академії» у всіх галузях науки, техніки, адміністративного управління загалом охоплює більше 150 напрямів.

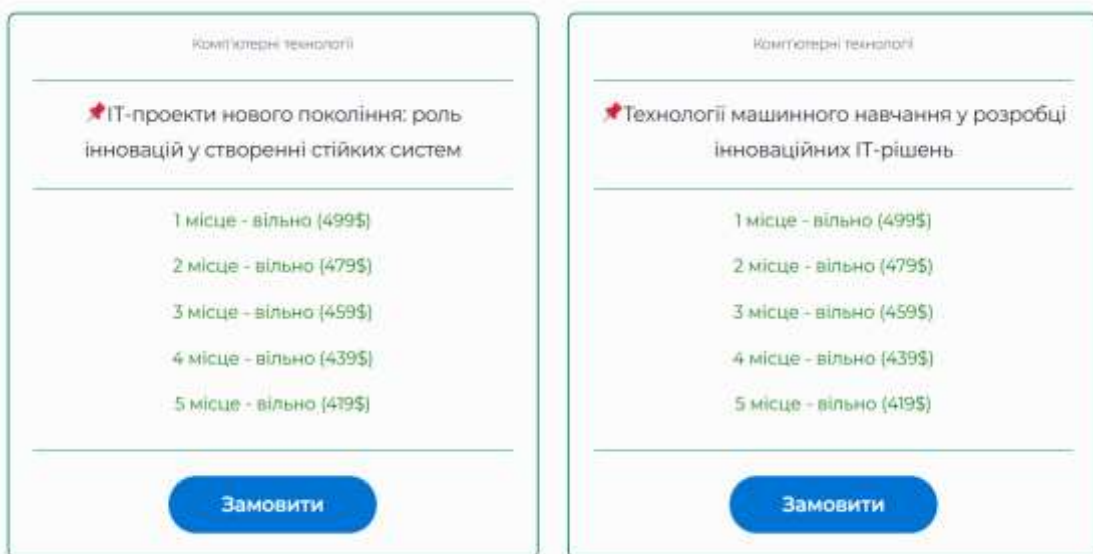


Рисунок 3 б — Приклад розцінок послуг «Академії статей» за співавторство у публікаціях за певними темами (скриншоти створені автором)

Дивно, що «Академією статей» не тільки надаються послуги з підготовки наукових публікацій для отримання наукового ступеня, а й можливість створювати наукові монографії й навчальні підручники. Звісно, таке було й раніше в Україні, наприклад, у 90-ті роки такі об'яви були на стовпах біля ВНЗ з набагато довшими термінами виконання на той час, тому що тоді роботи виконували на замовлення реальні вчені-спеціалісти без можливості використання ШІ. У ті часи це явище призвело майже до руйнування української науки та зниження престижності та визнання отриманих в Україні наукових звань та дипломів про освіту.

При цьому компанією «Академії статей» пропонується навіть написання підручника в будь-якому напрямі (160 напрямів!), два з яких із прикладами розцінок наведені на рис. 3 б з метою допомоги кар'єрному росту в науковій сфері, хоча засновником (директором) компанії, згідно з даними Google Scholar, за весь час написано дві статті, які не мають відношення до науки. Що правда, «Академія статей» проводить набір на роботу науковців із вченим ступенем. Й все це являє собою катастрофічну небезпеку.

Нині, внаслідок можливості застосування ШІ, суттєво зросли доступні темпи створення наукових робіт на замовлення псевдонауковців та пропорційно зросла можлива кількість псевдонауковців. Тому створення когорти таких псевдонауковців та псевдоспеціалістів, які часто навіть не знають змісту «своїх» наукових робіт внаслідок виконання їх на замовлення в організаціях на кшталт «Академії статей», на наш погляд, загрожує руйнуванню держав, на території яких функціонують такі організації. Тобто, очевидними є катастрофічні наслідки цієї небезпеки застосування генеративного ШІ для держави й народу. До речі, на запит про названу компанію у Google бачимо десятки сторінок інформації. Але ChatGPT надав таку відповідь: «Компанія «Академія статей» не є широко відомою або публічно зареєстрованою організацією на момент моїх останніх даних, тому мені важко сказати, хто є її засновником. Щодо ліцензії. В Україні компанії, які займаються публікацією контенту або надають подібні послуги, повинні дотримуватися відповідних норм законодавства, зокрема, у сфері авторських прав та інтернет-діяльності. Тому, якщо компанія має офіційну реєстрацію та надає послуги, вона, ймовірно, повинна мати ліцензії або інші дозволи, залежно від характеру її діяльності».

Цей приклад застосування ШІ в Україні, на наш погляд, являє собою глобальну катастрофічну небезпеку для держави в цілому. За фактом бачимо порушення не тільки норм наукової доброчесності, що вже є небезпекою, великим соціальним ризиком, але й згаданого міжнародного законодавства. У 90-ті роки подібна халтура часто робилася шляхом перекладу іншомовних наукових робіт, але потім, з часом, це виявлялося як плагіат, що іноді коштувало посади чиновникам у багатьох країнах. З появою генеративного ШІ з'являються проблеми виявлення недоброчесних псевдонауковців, аж поки їх некомпетентні рішення не призведуть до катастрофічних наслідків.

Крім того, на наш погляд, слід розглянути небезпеку у використанні ШІ учнями та студентами під час написання контрольних, курсових та дипломних робіт [30, 31]. Причому справа не тільки в тому, що людина не отримає необхідних у процесі подальшого життя знань та вмінь, хоча й це велика небезпека, але головна проблема полягає в тому, що людина з раннього віку не має стимулу та не вчиться думати з причин сподівання на ШІ. Отже, є можливість (ймовірність) отримати покоління громадян, не здатних логічно мислити й, як наслідок, виконувати складні сучасні роботи. Такі громадяни будуть здатні працювати тільки слугами, рабами цивілізованих сусідів.

Тому законодавство та стандартизація з впровадження ШІ має значення, хоча у «Білій книзі» це питання подається як дискусійне, хоча у цивілізованих державах такі норми існують.

### 3.3. Законодавство та стандарти з впровадження ШІ

З метою забезпечення безпеки [1] застосування технологій та систем ШІ на міжнародному рівні вироблені певні стандарти у галузі штучного інтелекту, а саме стандарти НАТО, ЄС та інших загальноєвропейських і світових інституцій щодо ШІ. Зокрема, Стратегія НАТО щодо штучного інтелекту [27], яка прийнята в жовтні 2021 р. та яка визначає ШІ як можливість досягнення технологічної переваги, але водночас і як джерело загроз, ставить таку мету щодо впровадження та розвитку ШІ:

- активне просування та прискорення впровадження ШІ;
- захист і моніторинг технологій ШІ та інноваційних можливостей з урахуванням міркувань політики безпеки, таких як практичне застосування принципів відповідального використання технологій ШІ;

- виявлення та захист від загроз зловмисного використання ШІ.

Стратегією НАТО щодо штучного інтелекту також сформульовано такі принципи відповідального використання ШІ: законність, відповідальність і підзвітність, пояснюваність і відстежуваність, надійність, керованість, зниження упередженості.

Водночас Рекомендації Ради Європи щодо штучного інтелекту (Recommendation of the Council on Artificial Intelligence) від 22 травня 2019 р. (OECD Legal Instruments) [28] встановлюють такі принципи діяльності з розвитку ШІ:

- Інклюзивне зростання, стійкий розвиток та загальний добробут. Будь-яка діяльність із розвитку ШІ має сприяти подоланню економічної, соціальної та інших видів нерівності, сталому розвитку та підвищенню добробуту і якості життя населення, захисту навколишнього середовища.

- Людиноцентричні цінності та верховенство права. Процес розвитку ШІ мусить забезпечувати верховенство права, демократичні цінності та права людини, у тому числі право на працю, захист особистої інформації (персональних даних), чесність, суспільну справедливість, а також надавати громадянам можливість отримувати знання та набувати навички для успішної адаптації до впровадження технологій ШІ.

- Прозорість і зрозумілість. Розробники ШІ мають бути відкритими та готовими пояснити зміст власних розробок щодо ШІ, сприяти подоланню соціального протистояння стосовно нових технологій ШІ.

- Безпека та надійність. Системи ШІ мають бути безпечними та надійними протягом усього життєвого циклу. Особи та організації, що займаються розвитком ШІ, мають забезпечити надійний ризик-менеджмент і контроль кожного етапу життєвого циклу технологій ШІ, аналіз їх стабільності та безпечності. Усі ризики виникнення негативних наслідків використання технологій ШІ повинні бути мінімізовані. Крім того, системи на базі ШІ не повинні мати можливостей умисного заподіяння шкоди громадянам і юридичним особам.

- Звітність. Усі сторони, що беруть участь у розвитку технологій ШІ, повинні бути підзвітними суспільству стосовно виконання зазначених принципів діяльності з розвитку ШІ.

- Цілісність інноваційного циклу у процесі наукових досліджень та економічної діяльності. Всі сторони, що беруть участь у розвитку технологій ШІ, повинні забезпечувати тісну взаємодію наукових досліджень і розробок у галузі ШІ з реальним сектором економіки.

- Технологічна незалежність. Держава повинна забезпечити необхідний рівень незалежності країни у галузі штучного інтелекту, зокрема, за допомогою переважного використання національних технологій і технологічних рішень, розроблених на основі ШІ.

Як бачимо, безпека та надійність технології ШІ є одними з основних принципів розвитку за міжнародними стандартами, а в цілому технологія має служити сталому розвитку та підвищенню добробуту і якості життя населення, захисту навколишнього середовища.

Початкові (основоположні) світові стандарти штучного інтелекту — це ISO/IEC 24668:2022(en) Information technology — Artificial intelligence — Process management framework for big data analytics [31] та NIST Trustworthy and Responsible AI NIST AI 600-1. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. 2024, 06 [26].

Як зазначено у передмові: «У цьому документі представлено еталонну модель процесу BDA (BDA PRM), а також модель оцінки процесу (BDA PAM). BDA PAM складається з двох вимірів: вимір процесу, який включає процеси, засновані на наборі PRM, включаючи BDA PRM, і вимір можливостей, заснований на структурі вимірювання процесу (PMF).

Цей документ визначає PRM та PAM як частину структури для аналізу великих даних, відповідно до вимог ISO/IEC 33004:2015 та ISO/IEC 33020:2019, для використання при проведенні оцінки відповідності згідно з вимогами ISO/IEC 33002:2015».

Міжнародні стандарти серії ISO/MEK встановлюють не тільки регулювання використання ШІ, але й наводять основні алгоритми створень моделей ШІ, що, безумовно, є корисним для практики й навчання як приклад (рис. 4).

На рис. 4 показано взаємозв'язок з еталонною моделлю процесу, процесом оцінювання та системою вимірювання відповідно до ISO/MEK 33001:2015 та ISO/MEK 33002:2015.

## Process capability determination

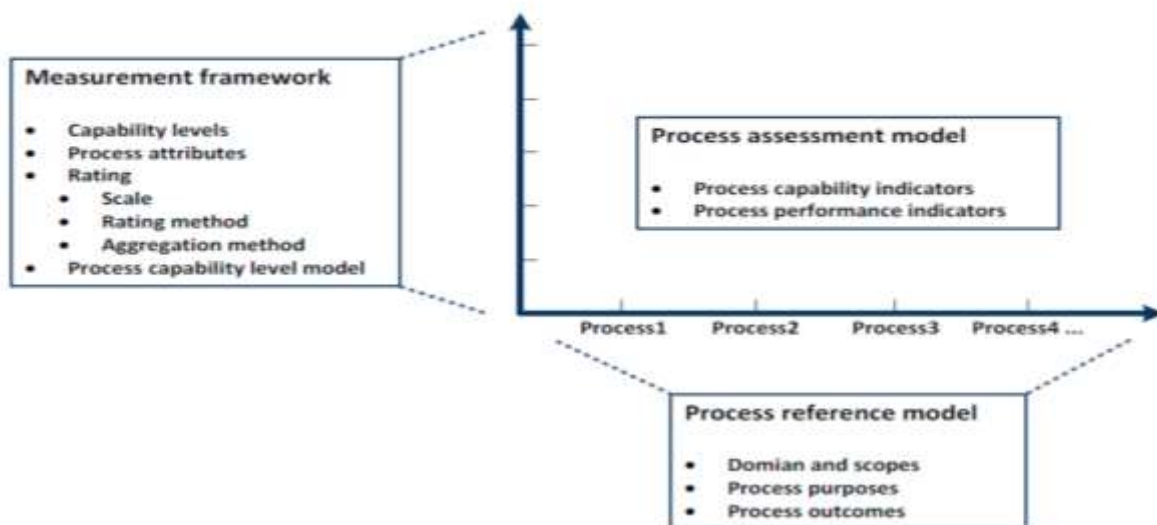


Рисунок 4 — Взаємозв'язки в моделі оцінювання процесу. Джерело [16]

Як бачимо, стандартизований на міжнародному рівні процес створення моделі з застосуванням ШІ повністю відповідає концепції РОП [4].

В Україні на сьогодні існують окремі ініціативи та нормативно-правові акти, що стосуються використання ШІ, однак чітко визначених комплексних державних стандартів для цієї сфери поки що немає. Проте в контексті розвитку технологій та необхідності адаптації до сучасних вимог Україна працює над створенням нормативної бази та відповідних стандартів для ШІ. У 2020 році Україна затвердила Національну стратегію розвитку штучного інтелекту до 2030 року. Вона є основним документом, що визначає загальні напрями розвитку ШІ в Україні, включаючи:

- Розвиток інфраструктури ІІІ та дослідницьких ініціатив.
- Створення національної нормативної бази для забезпечення безпеки, етики та правового регулювання ІІІ.
- Підготовку кадрів для ІІІ та розвитку освіти.
- Створення інноваційних екосистем для стартапів та ІТ-компаній, що займаються розробкою ІІІ.

В Україні також розглядаються проекти законів, які можуть регулювати використання ІІІ в різних сферах.

#### **4. Розробка програмного забезпечення для оцінки та аналізу ризиків**

Управління безпекою на об'єктах підвищеної небезпеки та критичної інфраструктури потребує використання сучасних програмних засобів, що дозволяють проводити комплексну оцінку ризиків і приймати обґрунтовані рішення щодо їх мінімізації. У цьому контексті розробка програмного забезпечення для оцінки та аналізу ризиків за допомогою ІІІ є одним із ключових елементів підвищення рівня безпеки на таких об'єктах.

Програмне забезпечення, розроблене в рамках проекту «Цифрові технології безпеки» [32], має бути орієнтоване на вирішення завдань моніторингу, аналізу та управління ризиками в реальному часі відповідно до концепції РОП. Основними функціональними можливостями такого ПЗ є моделювання ризиків — інструменти для створення математичних моделей ризиків, що враховують специфіку об'єктів підвищеної небезпеки та критичної інфраструктури; аналіз даних — модулі для збору, обробки та аналізу даних про поточний стан об'єктів, а також історичних даних про попередні інциденти та аварії; оцінка ризиків — автоматизовані алгоритми для оцінки ймовірності виникнення загроз і їхніх можливих наслідків на основі оброблених даних; розробка заходів реагування — інструменти для розробки планів реагування на надзвичайні ситуації, включаючи рекомендації щодо запобігання та мінімізації ризиків [7].

##### **4.1. Використання хмарних технологій для безпеки**

Однією з інноваційних складових розробленого програмного забезпечення є використання хмарних технологій. Хмарні обчислення дозволяють забезпечити доступ до обчислювальних ресурсів і даних у режимі реального часу, що є особливо актуальним для управління безпекою на великих об'єктах. Зокрема, це дозволяє оперативно реагувати на зміни в стані об'єкта та забезпечувати безперервний моніторинг [32].

Використання хмарних технологій також надає можливість знизити витрати на підтримку і розвиток ІТ інфраструктури, оскільки більшість обчислювальних процесів виконується на стороні хмарного провайдера. Це дозволяє компаніям зосередитися на основних бізнес-процесах, не відволікаючись на обслуговування складної ІТ інфраструктури [7]. Приклади застосування програмного забезпечення на ОПН та КІ.

Розроблене програмне забезпечення має широкий спектр застосувань на об'єктах підвищеної небезпеки та критичної інфраструктури. Це можуть бути промислові підприємства — автоматизовані системи для моніторингу стану обладнання та виявлення потенційних загроз, що дозволяють знизити ймовірність аварійних ситуацій; енергетичні об'єкти — системи управління ризиками для електростанцій та мережевої інфраструктури, що забезпечують безперервне постачання енергії й запобігають аваріям; транспортна інфраструктура — рішення для моніторингу стану транспортних мереж і об'єктів, що дозволяють підвищити безпеку перевезень та знизити ризики інцидентів [7].

#### **5. Висновки**

1. Потрібно більш широке поширення інформації щодо впровадження технології ІІІ у світі та в Україні, системне вивчення світового досвіду використання технологій штучного ін-

телекту в пріоритетних галузях економіки, кращих світових практик щодо безпеки. Академічним установам та ВНЗ потрібно проводити дослідження щодо безпеки з урахуванням особливостей розвитку та обставин в Україні.

2. Потрібно визначення потреб галузей критичної інфраструктури в технологіях штучного інтелекту, які необхідно й можливо провести з метою впровадження технологій штучного інтелекту в сфері безпеки; розроблення та затвердження вимог до інформаційної інфраструктури та інформаційної безпеки у разі впровадження та використання технологій штучного інтелекту в сфері безпеки.

3. Формування вимог до професійних компетентностей, переліків компетентностей та освітніх програм ВНЗ щодо розроблення, тестування, впровадження та використання технологій штучного інтелекту має стати на порядок денний та постійно оновлюватися. Зміни освіти з цього напрямку мають бути проведені терміново.

4. Наукова спільнота має клопотати щодо розробки пропозицій для внесення змін до чинного законодавства з метою доповнення відповідних нормативно-правових актів положеннями щодо технологій штучного інтелекту та гармонізації з актами Європейського Союзу відносно штучного інтелекту. Міжнародні стандарти технології мають бути також впроваджені найближчим часом.

## СПИСОК ДЖЕРЕЛ

1. Maslej N., Fattorini L., Perrault R., Parli V., Reuel A., Brynjolfsson E., Etchemendy J., Ligett K., Lyons T., Manyika J., Niebles J.C., Shoham Y., Wald R., Clark J. The AI Index 2024 Annual Report. AI Index Steering Committee, Institute for Human-Centered AI. Stanford: Stanford University, 2024. 502 p. URL: <https://aiindex.stanford.edu/report/> (дата звернення: 09.02.2025).
2. Петько С.М. Правове регулювання використання технологій штучного інтелекту в країнах — цифрових лідерах. *Економічний журнал Одеського політехнічного університету*. 2023. № 4 (26). С. 55–72. URL: <https://economics.net.ua/ejopu/2023/No4/55.pdf>. DOI: <https://doi.org/10.15276/EJ.04.2023.7>. DOI: <https://doi.org/10.5281/zenodo.10456760>.
3. Трамп анонсував створення ШІ-компанії з інвестиціями у 500 мільярдів доларів. URL: [https://lb.ua/economics/2025/01/22/656450\\_tramp\\_anonsuvav\\_stvorennnya.html](https://lb.ua/economics/2025/01/22/656450_tramp_anonsuvav_stvorennnya.html).
4. Іщенко О. Рік великих ідей: головні досягнення ШІ у 2024 році. URL: <https://fact-news.com.ua/rik-velikih-idey-golovni-dosyagnennya-shi-u-2024-rotsi/> 24.12.24.
5. Бегун В.В. Методологічні основи інформаційної технології управління безпекою на основі ризик-орієнтованого підходу: дис. ... д-ра техн. наук: 05.13.06. Київ, 2020. 553 с.
6. Бегун В.В. Розвиток парадигми РОП на основі теоретичних досліджень у сфері безпеки. *Математичні машини і системи*. 2023. № 2. С. 55–68.
7. Бегун В., Бегун С. Концепція інформаційної технології раннього розпізнавання відмов на основі нейронних мереж. *Інформаційні технології та комп'ютерне моделювання ІТКМ-2023*: міжнар. наук.-практ. конф. (м. Івано-Франківськ – Микуличин, 5–8 липня 2023 року). Івано-Франківськ – Микуличин, 2023. С. 6–8.
8. Бегун В.В. Впровадження цифрового управління у сферу безпеки. *Журнал обчислювальної та прикладної математики*. 2022. № 2. С. 7. URL: <https://scholar.google.com/>.
9. Смуток Б. Хто і як займався цифровізацією на державному рівні. Telegram: Contact @zedigital.
10. Інститут кібернетики. Напрямки досліджень. URL: <https://incyb.kiev.ua/doslidzennya/napryamki-doslidzennya>.
11. Іщенко О. Професії майбутнього: бізнес і держава повинні разом створювати нове покоління фахівців. URL: <https://fact-news.com.ua/profesii-maybutnogo-biznes-i-derzhava-povinni-razom-stvoryuvati-nove-pokolinnya-fahivtsiv/22.10.24>.
12. Постанова КМУ від 30 серпня 2024 р. № 1021 «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти».
13. Делюков О. Chat GPT, Siri тощо. Для чого українці використовують ШІ та яким сервісам довіряють? Дослідження. Chat GPT, Siri тощо. Для чого українці використовують ШІ та яким сервісам довіряють? Дослідження | MC.today.



14. Концепція Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року схвалено розпорядженням Кабінету Міністрів України від 13 квітня 2024 р. № 320.
15. ISO/IEC 24668:2022(en) Information technology — Artificial intelligence — Process management framework for big data analytics.
16. Словник термінів у сфері штучного інтелекту / упорядники: Чумаченко Д., Мішкін Д., Андрієнко О., Краковецький О., Турута О., Дубно О., Хрущова Д., Кобрін А., Авдєєва Т., Кравець І., Герасимяк В., Шабанов О., Бистрицька А. Київ: Міністерство цифрової трансформації України, 2024. 37 с. URL: [https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/Словник%20термінів%20у%20сфері%20ШІ%20\(1\).pdf](https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/Словник%20термінів%20у%20сфері%20ШІ%20(1).pdf) (дата звернення: 09.02.2025).
17. Yashchenko V.O. Neural-like growing networks in the development of general intelligence. neural-like growing networks (P. II). *Математичні машини і системи*. 2023. N 1. С. 3–29.
18. Yashchenko V.A. Neural-like growing networks in the development of general intelligence. Neural-like element (P. I). *Mathematical machines and systems*. 2022. N 4. P. 15–36.
19. XPeng's new electric air taxi can whisk you over traffic jams at up to 130 km/h. URL: <https://www.youtube.com/watch?v=G9xgvYDaIn0&pp=ygUzYWVybYB0YXhpIGNoaW5hIHJvdG9ycyB1cCB0byB0d28gcGFzc2VuZ2VycyAxMzAga21o>.
20. Погончук Я. Рекомендую її всім лідерам: Білл Гейтс назвав свою улюблену книгу про штучний інтелект. URL: [https://24tv.ua/trends24/bill-geyts-poradiv-pro-knigu-pro-shtuchniy-intelekt-shho-pro\\_n2737836](https://24tv.ua/trends24/bill-geyts-poradiv-pro-knigu-pro-shtuchniy-intelekt-shho-pro_n2737836).
21. Наступна хвиля: технології, влада і найбільша дилема XXI століття. URL: <https://www.gatesnotes.com/the-coming-wave>.
22. Компанія «Сідкон». Штучний інтелект і безпека. URL: <https://sidcon.com.ua/bookstest/tproduct/641995295-451537533371-shtuchnii-ntelekt-bezpeka>.
23. Біла книга з регулювання ШІ в Україні: бачення Мінцифри. URL: <https://cms.thedigital.gov.ua/storage/uploads/files/page/community>.
24. Pushkina V. Огляд українського GovTech: хто розробляє проєкти для державного сектора, у чому полягають виклики і які перспективи. URL: <https://dou.ua/lenta/articles/ukrainian-govtech-overview/>.
25. Світові стандарти штучного інтелекту. URL: <https://sidcon.com.ua/tpost/l31tdcc9f1-svtov-standarti-shtuchnogo-ntelektu>.
26. NIST Trustworthy and Responsible AI NIST AI 600-1. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. 2024. 06.
27. Стратегія НАТО щодо штучного інтелекту, яка прийнята в жовтні 2021 р.
28. Рекомендації Ради Європи щодо штучного інтелекту (Recommendation of the Council on Artificial Intelligence) від 22 травня 2019 р. (OECD Legal Instruments).
29. EU agrees 'historic' deal with world's first laws to regulate AI. URL: <https://www.theguardian.com/world/2023/dec/08/eu-agrees-historic-deal-with-worlds-first-laws-to-regulate-ai>.
30. AI Content Creator Workshop: Ваша можливість опанувати створення контенту за допомогою Штучного Інтелекту. URL: <https://www.facebook.com/61559587087077/videos/1182295422877045/?rdid=6iOOK3cUD6rnBThD#>.
31. Чи знаєте ви, як TikTok впливає на ваш мозок і національну безпеку? URL: [https://www.facebook.com/story.php?story\\_fbid=600607036169308&id=100086600513676&rdid=z2yUwFMgSu2zZxE0#](https://www.facebook.com/story.php?story_fbid=600607036169308&id=100086600513676&rdid=z2yUwFMgSu2zZxE0#).
32. Бегун В., Волошин О., Бегун С. Оптимізація контролю безпеки торговельно-розважальних комплексів на основі аналізу моделей визначення ризику. *Інформаційні технології та комп'ютерне моделювання: матеріали статей міжнар. наук.-практ. конф. (м. Івано-Франківськ, 15–16 грудня 2022 р.)*. Івано-Франківськ: п. Голіней О.М., 2022. С. 4–6.

Стаття надійшла до редакції 10.02.2025