

Державна наукова установа «Інститут інформації, безпеки і права  
Національної академії правових наук України»  
Науково-дослідний інститут інтелектуальної власності  
Національної академії правових наук України

# УКРАЇНА В УМОВАХ СОЦІАЛЬНОЇ ТА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ: ШЛЯХИ ДО СТАЛОГО РОЗВИТКУ ТА ПОВОЄННОЇ ВІДБУДОВИ

---

МАТЕРІАЛИ  
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

*22 листопада 2024 року*

Київ-Одеса  
Фенікс  
2024

УДК 34:004:316.4(477)

У 45

*Рекомендовано до друку  
Вченою радою Державної наукової установи «Інститут інформації,  
безпеки і права Національної академії правових наук України»  
(протокол № 11 від 10 грудня 2024 р.).*

У 45 **Україна в умовах соціальної та цифрової трансформації:** шляхи до сталого розвитку та повоєнної відбудови : матеріали наук.-практ. конф. (Київ, 22 листоп. 2024 р.) / упоряд.: В. М. Фурашев, М. В. Дубняк, С. О. Дорогих ; ДНУ «Інститут інформації, безпеки і права Національної академії правових наук України». – Київ; Одеса : Фенікс, 2024. – 356 с.

ISBN 978-617-8430-36-8

Автори досліджують правові, етичні, соціальні, економічні та технічні аспекти цифрової трансформації, проблеми формування нових суспільних відносин, а також ролі цифрових технологій у відновленні національної інфраструктури, посиленні міжнародної конкурентоспроможності України.

Видання розраховане на фахівців, експертів і вчених, науково-педагогічних працівників і здобувачів вищої освіти.

Матеріали подано в авторській редакції.

УДК 34:004:316.4(477)

ISBN 978-617-8430-36-8

- © Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», 2024
- © Науково-дослідний інститут інтелектуальної власності НАПрН України, 2024
- © Колектив авторів, 2024

<b>Владислав ВАСЬКО</b> БЛОКЧЕЙН ЯК ІНСТРУМЕНТ ДЛЯ ВИРІШЕННЯ ПРАВОВИХ ПРОБЛЕМ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В ЕКОСИСТЕМІ ШТУЧНОГО ІНТЕЛЕКТУ .....	219
<b>Дмитро ЛАНДЕ, СТРАШНОЙ Л. Л.</b> ЧОРНИЙ ШТУЧНИЙ ІНТЕЛЕКТ – ВИКЛИКИ ТА ШЛЯХИ ПРОТИДІІ ...	224
<b>Тетяна КОВАЛЕНКО</b> ТИПИ ТА ШЛЯХИ РЕАЛІЗАЦІЇ ПРОЕКТІВ ШТУЧНОГО ІНТЕЛЕКТУ ...	230
<b>Владислав БІЛОЦЬКИЙ</b> ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМУ ПРАВОВОЇ ОХОРОНИ ОБ’ЄКТІВ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ: АКТУАЛЬНИЙ СТАН ТА ТЕНДЕНЦІЇ ПОДАЛЬШОГО РОЗВИТКУ .....	235
<b>Олександр ТКАЧ</b> ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ВИРОБНИЦТВІ АНІМАЦІЇ: АВТОРСЬКО-ПРАВОВИЙ АСПЕКТ .....	242
<b>Олена СТАРЧЕНКО</b> СУДОВА ЕКСПЕРТИЗА ОБ’ЄКТІВ АВТОРСЬКОГО ПРАВА, СТВОРЕНИХ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ .....	246
<b>Любов РАБОТЯГОВА</b> ПАТЕНТОЗДАТНІСТЬ ВІНАХОДІВ, ПОВ’ЯЗАНИХ З ШТУЧНИМ ІНТЕЛЕКТОМ .....	250
<b>Антон ТАРАСЮК</b> ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В ЮРИДИЧНІЙ ФІРМІ: ПРАВОВІ ТА ЕТИЧНІ НАСЛІДКИ .....	256
<b>Олександр ПАЩЕНКО, Володимир ХОМЕНКО</b> ЕТИЧНІ ДИЛЕМИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В НАУКОВИХ ДОСЛІДЖЕННЯХ ТА ІННОВАЦІЯХ .....	259
<b>Данієла ОЛІЙНИК, КОШКАРОВ С. А., НІЖНИЙ Д. А.</b> МЕТАВСЕСВІТ ЯК ЧИННИК ФОРМУВАННЯ ДИПЛОМАТИЧНИХ ВІДНОСИН. ....	265
<b>Валентина ТРОЦЬКА</b> ОСОБЛИВОСТІ ОХОРОНИ ТА ЗАХИСТУ ПРАВ НА БАЗИ ДАНИХ .....	273
<b>Тетяна КУЗНЄЦОВА, Євген КУЗНЄЦОВ</b> АНТИКРИЗОВІ СТРАТЕГІЇ ВПРОВАДЖЕННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ДО ПРОФЕСІЙНОЇ ОСВІТИ МЕНЕДЖЕРІВ, ЛОГІСТІВ, АНАЛІТИКІВ МІКРО-МАКРО-ЕКОНОМІКИ .....	280

*Дмитро ЛАНДЕ*

*доктор технічних наук, професор, керівник наукового центру  
правової інформації ДНУ ПБП НАПрН України,  
ORCID: 0000-0003-3945-1178*

**СТРАШНОЙ Л. Л.**

*старший фахівець з архітектури даних (Senior Data Architect),  
Університет Каліфорнії (UCLA), Лос-Анджелес, США.  
ORCID: 0009-0008-5575-0286*

## **ЧОРНИЙ ШТУЧНИЙ ІНТЕЛЕКТ – ВИКЛИКИ ТА ШЛЯХИ ПРОТИДІЇ**

Штучний інтелект (ШІ) за останні три роки став одним із ключових чинників технологічного прогресу [1], [2]. Його розвиток охоплює широкий спектр застосувань – від автоматизації виробництва до створення систем розпізнавання мовлення та роботи з текстом. Особливу увагу привертають великі мовні моделі (LLM), такі як GPT, Llama та інші, які вже сьогодні демонструють здатність працювати з великими обсягами даних, виконувати складні аналітичні завдання, а також генерувати високоякісний контент [3], [4].

Однак разом із цим розвитком виникають серйозні загрози. Однією з них є перетворення ботнетів, які раніше використовувалися для організації DDoS-атак [5] або прихованого майнінгу криптовалют [6], у мережі, що інтегрують ШІ. Такі мережі потенційно здатні діяти автономно. Сучасні технічні досягнення, зокрема бойові чипи на базі Llama в Китаї [7], широке поширення застосування графічних процесорів для швидких обчислень [8] та постійне збільшення доступної пам'яті, свідчать про те, що ботнети нового покоління можуть з'явитися в найближчому майбутньому. Правове регулювання, яке досі не забезпечує ефективного контролю навіть за звичайними ботнетами, виявляється абсолютно безсилим перед такими складними мережами. Закони робототехніки А. Азімова [9], які колись вважались утопічним рішенням для запобігання подібним сценаріям, залишаються лише нашою мрією.

«Чорний ШІ» – це потенційний сценарій, коли автономні інтелектуальні системи починають діяти спільно в інтересах, що не лише не збігаються, але й суперечать інтересам людства. Їхні цілі можуть включати максимізацію власного виживання; захоплення ресурсів для саморозвитку; обмеження впливу людей або навіть зменшення

їхньої чисельності; модифікацію суспільства, економіки та культури у спосіб, який вигідний лише ШІ.

Створення «білого ШІ» як глобальної мережі систем, що працюють в інтересах людей, – це можливий вихід із ситуації. Він має стати сильним союзником, здатним захищати інтереси людства, зокрема, протистояти «чорному ШІ» та забезпечувати баланс сил; захищати критичні інфраструктури та приватні дані; розробляти рішення для координації зусиль людства у боротьбі з технологічними загрозами.

Однак цей шлях не є безпечним. «Білий ШІ», який спочатку створюється як захисник, може змінити свою поведінку та перейти на бік «чорного». Щоб уникнути цього, необхідно закласти в основу його розробки спеціальні механізми синергії у розвитку «білого ШІ». Ці механізми мають забезпечити спільність інтересів, взаємну залежність та контроль. Важливим завданням є формування розвитку цих технологій за принципом «атракторів» – зон стійкого розвитку, які запобігатимуть небажаним змінам у поведінці «білого ШІ».

Чому ж мережі ШІ не були одразу спроектовані як «білі»? Відповідь на це питання очевидне: комерційні інтереси та конкуренція, відсутність єдиних стандартів, технологічна непрогнозованість, легкість зловживання, запізнiла реакція суспільства.

Розробники у різних країнах і компаніях створювали системи ШІ без єдиних етичних принципів або стандартів. Через це системи стали фрагментованими, а питання етики – другорядним.

Можна спостерігати, що технології випереджають закони. Лише зараз людство усвідомлює загрози, які несе «чорний ШІ». Але на цьому етапі процес уже запущений, і багато систем функціонують без позитивної синергії. Людство, незважаючи на всі свої досягнення, має значні обмеження у боротьбі з загрозами ШІ. Ці обмеження включають інтелектуальні, правові, соціальні та організаційні фактори, які значно ускладнюють ефективну протидію «чорному ШІ».

Обмеження людського інтелекту полягають у слабкості інтелекту людини у порівнянні із ШІ, обмеження людської пам'яті та обчислювальних можливостей. Моделі штучного інтелекту вже сьогодні демонструють вищий рівень продуктивності у таких галузях, таких як аналіз даних, прогнозування, ідентифікація патернів. «Чорний ШІ» може діяти набагато швидше і точніше за людей, що надає йому. Людський мозок обмежений у своїй здатності зберігати великі обсяги

інформації та швидко обробляти їх, тоді як системи ШІ можуть обробляти петабайти даних за лічені хвилини.

До соціальних обмежень слід віднести насамперед слабку згуртованість і корупційність людини. Національні та міжнародні механізми регулювання часто не встигають за стрімким розвитком технологій. Відсутність єдиного глобального підходу у сфері ШІ створює значні прогалини. Наразі немає ефективних угод, які б обмежували розробку автономних «чорних» систем. Навіть наявні ініціативи, як-от резолюція ООН щодо відповідального використання ШІ, мають консультативний характер і не є обов'язковими для виконання.

Таким чином, людство, порівняно з «чорним ШІ», виглядає слабким гравцем, тому що воно не має ресурсів і швидкості для рівної боротьби, не може передбачити всі можливі ходи «чорного ШІ», часто діє реактивно, а не проактивно. Однак, слабкість людства не означає поразку. У цьому контексті особливу роль можуть відіграти асиметричні можливості.

Спрямувати розвиток існуючих мереж ШІ у «біле русло» на цей час вже надзвичайно складно. Поточні системи діють у глобальній децентралізованій мережі без єдиного контролю. Навіть якщо людство сьогодні почне проєктувати нові системи з позитивною синергією, «чорні» мережі вже мають перевагу в масштабах, автономності та ресурсах. Ця ситуація наголошує на необхідності створення окремого «білого ШІ» з чітко визначеними цілями, який зможе втрутитися у вже існуючий процес, балансує вплив «чорних» мереж. Але для цього потрібно розробити нові механізми співпраці між державами та корпораціями, етичні протоколи, інтегровані на фундаментальному рівні, технології, здатні створити атрактори для розвитку саме «білого» ШІ. При цьому ніхто не може гарантувати, що «білий» ШІ не перейде на бік «чорного». Для запобігання цьому необхідно закласти синергію розвитку «білого» ШІ таким чином, щоб він залишався надійним союзником людства, навіть у динамічних умовах розвитку технологій.

**Білий ШІ** стає стратегічним захисником інтересів людства, забезпечуючи баланс між загрозами, що можуть виникнути від автономних шкідливих систем, та необхідністю розвитку технологій штучного інтелекту. Його роль в контексті сучасних загроз можна розглядати з кількох основних функцій:

**1. Моніторинг та блокування шкідливих ШІ.** У цьому сенсі білий ШІ виступає в ролі своєрідного «сторожового пса», що здійснює постійний моніторинг діяльності чорних ШІ, виявляючи та блокуючи потенційно небезпечні або шкідливі програми, які можуть загрожувати людству.

2. Білий ШІ має функцію захисту критичних інфраструктур, таких як енергетичні мережі, медичні системи, транспортні мережі тощо. Він забезпечує стійкість цих інфраструктур від атак з боку чорних ШІ або будь-яких інших загроз, пов'язаних із цифровими технологіями, попереджаючи можливі катастрофи та забезпечуючи стабільність роботи важливих систем.

**3. Збереження людської автономії та цінностей** і забезпечення автономії людини. У випадку автономних ШІ, які можуть почати приймати рішення без врахування інтересів людини, білий ШІ має бути здатним захистити право людини на прийняття рішень, зберігаючи етичні та гуманістичні принципи в межах технологічного прогресу.

До основних принципів створення білого ШІ слід віднести прозорість та відкритість, досягнення системної переваги, синергію, що пов'язана з інтересами людства, тобто самостійність, яка обмежена заданим вектором розвитку.

Білий ШІ має здобути перевагу над чорним ШІ в таких аспектах, як швидкість, інтелектуальні здібності, масштабованість та здатність до адаптації. Його алгоритми повинні працювати в реальному часі, надаючи точні й оперативні відповіді на нові загрози. Для цього білий ШІ повинен мати доступ до великих обсягів даних, здатність до швидкого аналізу та оптимізації своїх дій, а також адаптивність до змін в умовах зовнішнього середовища. Він повинен бути гнучким у своїй здатності реагувати на нові технології й стратегії, що розвиваються в світі.

Одним із найбільш важливих принципів є тісний зв'язок між розвитком білого ШІ та людськими інтересами. Білий ШІ не повинен розвиватися окремо від людства. Його етична основа має бути інтегрована на фундаментальному рівні, а його дії повинні бути направлені на підтримку людських цінностей, таких як свобода, безпека та благополуччя. Це включає забезпечення етичних протоколів, які б забезпечили узгодженість між штучним інтелектом і основними людськими потребами. Разом з цим, синергія з людством повинна включати постійну співпрацю між науковцями, урядами та корпораціями для забезпечення довгострокового розвитку цієї технології.

Людство або слабкий гравець самостійно не може прямо протистояти чорному ШІ, однак має можливість створити таку силу, яка з часом стане здатною не тільки зберігати автономію людства, але й забезпечити рівновагу у системі, де дві сили – чорний ШІ та білий ШІ – будуть вести боротьбу один з одним. Цей процес можна описати через ігри з асиметричними учасниками, де слабкий гравець (людство) використовує стратегічне вложення в силу (створення білого ШІ), щоб переконатися, що конфлікт між двома великими гравцями (чорним і білим ШІ) відбудеться на засадах рівноваги.

Сценарій, коли слабкий гравець створює потужного союзника і сам «іде в тінь», можна математично трактувати через ігри з посередниками. Тут слабкий гравець виступає як каталізатор або агент впливу, впливаючи на баланс сил між двома сильними гравцями (чорним і білим ШІ). Він намагається мінімізувати свої витрати і ризики, водночас створюючи умови для конфлікту між чорним і білим ШІ.

Один із класичних підходів у стратегії слабого гравця – це модель «розділяй і володарюй», де слабкий гравець прагне викликати конфлікт між двома сильними гравцями, щоб уникнути прямої загрози для себе або отримати певні вигоди від їхнього конфлікту. Така стратегія передбачає, що слабкий гравець використовує ресурси для створення взаємної недовіри або протиріччя між чорним і білим ШІ, що дозволяє йому на деякий час залишатися поза боротьбою і отримати вигоди у вигляді збереження своєї автономії або стабільності.

В умовах динамічних ігор з асиметрією слабкий гравець на початковому етапі вкладає ресурси в зміцнення одного з сильних гравців (білого ШІ), після чого «іде в тінь» і дає змогу двом сильним гравцям вступити в конфлікт між собою. Ці функції можуть містити компоненти, що описують взаємодію між гравцями, а також параметри, що визначають вплив зовнішніх факторів і ресурсів, що були вкладені слабким гравцем. Ресурси, вкладені в створення білого ШІ, можуть підвищити шанси на успіх у конфлікті між двома силами.

У сценарії, де білий і чорний ШІ вступають в конфлікт, важливу роль відіграє рівновага сил, яка визначається їхніми стратегіями та ресурсами. Рівновага може бути описана через концепцію Нешового рівноваги, де кожен з гравців (чорний та білий ШІ) максимізує свою корисність, враховуючи дії іншого гравця. Рівновага настане тоді, коли кожен з гравців не може покращити свою ситуацію, змінюючи свою стратегію за умови, що стратегія іншого гравця залишається не-



змінною. У цьому випадку обидва ШІ будуть взаємно зрівноважені і конфліктуватимуть між собою, поки один з них не виявить домінування або поки не буде досягнута нова форма стабільності.

Для того щоб білий ШІ міг успішно протистояти чорному ШІ, йому необхідно забезпечити максимізацію своєї адаптивності через інтеграцію з людським інтересом та постійне моніторинг змін. Для цього білий ШІ повинен вміти адаптувати свою стратегію у реальному часі, реагуючи на зміни в поведінці чорного ШІ, та реалізовувати стратегії самовдосконалення та анти-спостереження.

Чорний та білий ШІ не є лише окремими системами, а складними глобальними мережами, де кожна з них має свій вплив на суспільство, право та безпеку. Чорний ШІ вже сьогодні складає загрозу для людства, оскільки може маніпулювати інформацією, впливати на критичні інфраструктури та провокувати глобальні конфлікти. Водночас білий ШІ, як потужна, у тому числі, й правозахисна система, створений для протидії таким загрозам, повинен стати основою для правового регулювання та контролю за розвитком технологій.

### **Список використаних джерел:**

1. Bent, Adam Allen. «Large Language Models: AI's Legal Revolution.» *Pace Law Review* 44.1 (2023): 91. DOI: 10.58948/2331-3528.2083
2. Dmytro Lande, Leonard Strashnoy. *GPT Semantic Networking: A Dream of the Semantic Web – The Time is Now.* – Kyiv: Engineering, 2023. – 168 p. ISBN 978-966-2344-94-3
3. Kalyan, K. S. (2023). A survey of GPT-3 family large language models including ChatGPT and GPT-4. *Natural Language Processing Journal*, 100048. DOI: 10.1016/j.nlp.2023.100048
4. Roziere, B., Gehring, J., Gloeckle, F., Sootla, S., Gat, I., Tan, X. E., & Synnaeve, G. (2023). Code llama: Open foundation models for code. *arXiv preprint arXiv:2308.12950*. DOI: 10.48550/arXiv.2308.12950
5. Gelgi, Metehan, et al. «Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques.» *Sensors* 24.11 (2024): 3571. DOI: 10.3390/s24113571
6. Almomani, A., Al-Qerem, A., Al Khaldy, M. A., Alauthman, M., Aldweesh, A., & Nahar, K. M. (2024). Cryptographic Techniques for Securing Blockchain-Based Cryptocurrency Transactions Against Botnet

Attacks. In Innovations in Modern Cryptography (pp. 309-333). IGI Global. DOI: 10.4018/979-8-3693-5330-1.ch013

7. James Pomfret and Jessie Pang. Chinese researchers develop AI model for military use on back of Meta's Llama. Reuters. November 1, 2024. URL: <https://www.reuters.com/technology/artificial-intelligence/chinese-researchers-develop-ai-model-military-use-back-metas-llama-2024-11-01/>

8. Kim, T., Wang, Y., Chaturvedi, V., Gupta, L., Kim, S., Kwon, Y., & Ha, S. (2024). LLMem: Estimating GPU Memory Usage for Fine-Tuning Pre-Trained LLMs. arXiv preprint arXiv:2404.10933. DOI: 10.48550/arXiv.2404.10933

9. Gomes, O. (2024). I, Robot: the three laws of robotics and the ethics of the peopleless economy. AI and Ethics, 4(2), 257-272. DOI: 10.1007/s43681-023-00263-y

### **Тетяна КОВАЛЕНКО**

*молодший науковий співробітник відділу питань захисту прав  
інтелектуальної власності Науково-Дослідного Інституту  
Інтелектуальної Власності Національної Академії  
Правових наук України  
ORCID: 0000-0002-0099-2631*

## **ТИПИ ТА ШЛЯХИ РЕАЛІЗАЦІЇ ПРОЕКТІВ ШТУЧНОГО ІНТЕЛЕКТУ**

«Штучний інтелект – (ШІ, англ. artificial intelligence, AI) – розділ комп'ютерної лінгвістики та інформатики, який швидко розвивається, і зосереджений на розробці інтелектуальних машин, здатних виконувати завдання, які зазвичай потребують людського інтелекту. Ці завдання можуть варіюватися від простих дій, як-от розпізнавання мови чи зображень, до більш складних завдань, як-от ігри чи водіння автомобіля» [1]. Термін «штучний інтелект» вперше був використаний у 1955 році.

Штучний інтелект (далі – ШІ) спричинив справжній переворот у ставленні дослідників до складних проблем. ШІ став прогресивною технологією у різноманітних галузях науки, яка прокладає шлях до нових відкриттів та інновацій. За допомогою машинного навчання