

Міністерство освіти і науки України

Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

Навчально-науковий інститут фінансів, економіки,
управління та права
Кафедра фінансів, банківського бізнесу та оподаткування



ЕКОНОМІЧНА БЕЗПЕКА: ДЕРЖАВА, РЕГІОН, ПІДПРИЄМСТВО

Матеріали ІХ Міжнародної
науково-практичної конференції

15 травня 2025 р.

Полтава
2025

УДК 330.342:004.8

Онищенко Світлана Володимирівна,
доктор економічних наук, професор,
директор ННІ фінансів, економіки управління та права
Чумак Олександр Сергійович, аспірант
Національний університет «Полтавська політехніка імені
Юрія Кондратюка»

ЕКОНОМІЧНА БЕЗПЕКА В ЕПОХУ ШТУЧНОГО ІНТЕЛЕКТУ: РИЗИКИ, ПОТЕНЦІАЛ І ТОЧКИ БАЛАНСУ

Швидка еволюція технологій штучного інтелекту (ШІ) кардинально трансформує глобальну економічну архітектуру, створюючи принципово нові виклики, загрози та можливості для економічної безпеки. ШІ формує нову парадигму економічної безпеки, де традиційні загрози поступаються місцем техно-економічним викликам, а технологічне лідерство стає критичним чинником національної конкурентоспроможності. За прогнозами експертів McKinsey Global Institute, ШІ додасть близько 13 трильонів доларів до світового ВВП до 2030 року [1], а дослідження World Economic Forum показують, що технології штучного інтелекту трансформують 40% робочих місць протягом наступних 15 років [2].

Цифрова трансформація детермінує принципово нову парадигму забезпечення економічної безпеки в умовах глобалізованого технологічного середовища. Використання штучного інтелекту (ШІ) докорінно змінює характер економічних процесів, формуючи нову зміну загроз та можливостей для національної та глобальної економіки. Економічна безпека більше не може розглядатися в ізоляції від технологічної політики держави. Швидко поширюватимуться й основні ризики, пов'язані з розвитком ШІ, а саме: структурного безробіття через автоматизацію, концентрацію даних у транснаціональних корпораціях, кіберзагроз, зниження прозорості алгоритмічних рішень та потенційну втечу капіталу в юрисдикції з низьким рівнем регулювання.

Потенціал ШІ – це драйвер економічного зростання та стратегічної стійкості, але за умови правильного управління ШІ може підвищити продуктивність, оптимізувати логістичні та фінансові процеси, зміцнити економічну безпеку, а також забезпечити аналітичну підтримку кризовому менеджменту. ШІ має й геоеткономічний вимір: конкуренція технологічних платформ. Економічна безпека в епоху ШІ все більше визначається здатністю держав розвивати власні технологічні екосистеми. Важливо уникнути залежності від монопольних цифрових акторів (Google, Amazon, Meta, Microsoft, Apple, Alibaba, Tencent), зокрема у сфері обробки великих даних та хмарних інфраструктур. Виникає необхідність формування нової державної політики економічної безпеки в умовах розвитку ШІ, де ключовими напрямками стають: регулювання етичного використання алгоритмів, забезпечення прозорості цифрових рішень, надання кібергарантій для бізнесу, підготовка кадрів до нової структури ринку праці та міждержавна співпраця з управління ризиками. Водночас, забезпечення економічної безпеки потребує балансу між інноваційністю та інклюзивністю, між динамікою ринку та захистом соціально вразливих верств, саме тут формується головний виклик сучасної економічної політики.

Постає обґрунтована потреба у дослідженні європейського досвіду цифрового нормативного простору як зразка збалансованого підходу до поєднання інноваційного розвитку, захисту основоположних прав і забезпечення економічної безпеки. Європейський Союз демонструє унікальну модель цифрового врядування, де правове регулювання відіграє не стримувальну, а навпаки – формувальну функцію, створюючи передбачувані умови для розвитку штучного інтелекту, обробки великих даних, функціонування онлайн-платформ та кіберінфраструктури. Досвід ЄС у розробці таких актів, як Закон про цифрові послуги (DSA), Закон про цифрові ринки (DMA), Акт про штучний інтелект (AI Act) чи Європейська стратегія даних,

може слугувати орієнтиром для інших держав у формуванні власної цифрової політики. Ці документи не лише забезпечують конкурентне середовище, а й закладають основу для технологічного суверенітету, прозорості алгоритмічних систем та відповідальності цифрових акторів.

Наближення до 2030 року ознаменується формуванням інтегрованої цифрової екосистеми, у якій конвергенція 5G, Інтернету речей, периферійних обчислень, штучного інтелекту, робототехніки та доповненої реальності створить принципово нові архітектури створення доданої вартості. Ці трансформації перетворять традиційні виробничі ланцюги на високотехнологічні бізнес-моделі, засновані на етичному обміні даними та підтримані комплексною нормативно-правовою базою Європейського Союзу. Частину цифрового нормативного простору ЄС становлять:

- Стратегія кібербезпеки ЄС для Цифрового десятиліття (*EU Cybersecurity Strategy for the Digital Decade*, 2020) [6];

- Закон про цифрові послуги (*Digital Services Act*, 2022) [7];

- Закон про цифрові ринки (*Digital Markets Act*, 2022) [8];

- Європейська цифрова ідентичність (*European Digital Identity Framework*, запропонована у 2021 році, очікується набуття чинності до 2026) [9];

- План дій для медіа і аудіовізуального сектору (*Media and Audiovisual Action Plan*, 2020) [10];

- План дій для європейської демократії (*European Democracy Action Plan*, 2020) [11];

- Стратегія цифрових фінансів (*Digital Finance Strategy*, 2020) [12];

- Європейська стратегія даних (*European Data Strategy*, 2020) [13];

- Білий документ щодо штучного інтелекту (*White Paper on Artificial Intelligence*, 2020) [14] та пов'язаний із ним Акт про штучний інтелект (*AI Act*, погоджений у 2024 році) [15];

- Регламент щодо геоблокування (*Geo-blocking Regulation*, чинний з 2018 року) [16];

– Платформи для регулювання онлайн-бізнесу у межах *Regulation on platform-to-business (P2B) relations* (2019) [17-18].

На основі аналізу комплексної нормативно-правової бази ЄС у сфері цифрових технологій можна дійти висновку, що підхід Європейського Союзу до формування законодавства характеризується стратегічною цілісністю, превентивністю та людиноцентричністю. Європейська Комісія послідовно прагне забезпечити науковий прорив, зміцнити технологічне лідерство Європейського Союзу та гарантувати, що новітні технології слугують добробуту всіх європейців, сприяючи покращенню якості життя та повазі до фундаментальних прав.

У своїх Політичних настановах голова Комісії Урсула фон дер Ляєн окреслила необхідність скоординованого європейського підходу до розуміння людських та етичних наслідків штучного інтелекту (ШІ), а також підкреслила важливість ефективного використання великих даних задля посилення інноваційного потенціалу ЄС. У цьому контексті Комісія підтримує поєднання регуляторного та інвестиційно-орієнтованого підходу, що має на меті, з одного боку, сприяти широкому впровадженню ШІ, а з іншого – мінімізувати ризики, пов'язані з потенційно шкідливими або неприйнятними сферами його застосування. Презентована Біла книга з питань штучного інтелекту окреслює можливі політичні варіанти для досягнення зазначених цілей. Документ не охоплює аспектів розробки та використання ШІ у військових цілях [14]. Європейська Комісія запрошує держави-члени, інституції ЄС, представників промисловості, соціальних партнерів, організації громадянського суспільства, дослідницьку спільноту та широку громадськість взяти участь у консультаціях щодо запропонованих підходів і зробити внесок у формування майбутньої політики ЄС у сфері штучного інтелекту.

Таким чином, аналіз європейського нормативного ландшафту дозволяє окреслити потенційні моделі адаптації та впровадження правових механізмів, що сприятимуть розвитку національних цифрових екосистем, збереженню стійкості та зміцненню економічної безпеки у цифрову епоху.

Стратегічні підходи до балансування ризиків та потенціалу включають розробку комплексних національних стратегій ШІ, інвестиції в критичну інфраструктуру, перекваліфікацію робочої сили та міжнародне співробітництво у створенні етичних стандартів ШІ. Ключові точки балансу лежать між інноваціями та стабільністю через адаптивне регулювання, між відкритістю та безпекою через технологічний суверенітет, а також між ефективністю та справедливістю через інклюзивний розвиток ШІ. Успішне управління цими викликами вимагає координованих зусиль урядів, бізнесу та міжнародної спільноти для забезпечення відповідального розвитку ШІ, що максимізує економічні вигоди при мінімізації ризиків для національної безпеки.

Література

1. McKinsey Global Institute. (2018). *Notes from the AI frontier: Modeling the impact of AI on the world economy*. <https://www.mckinsey.com/>
2. World Economic Forum. (2023). *The future of jobs report 2023*. World Economic Forum. <https://www.weforum.org/>
3. Onyshchenko S., Hlushko A., Maslii O., Chumak O. (2024). Digital transformation of the national economy in the context of information environment development in Ukraine. Chapters of Monographs, in: "Transformations of national economies under conditions of instability", published by the Scientific Route OÜ. Tallinn, Estonia, chapter 6, pages 169–197. DOI: 10.21303/978-9916-9850-6-9.ch6
4. Onyshchenko, S., Maslii, O., Hlushko, A. (2025). Digital and Economic Security of the State Under Global Threats. In: Dovgyi, S., Siemens, E., Globa, L., Kopiika, O., Stryzhak, O. (eds) Applied Innovations in Information and Communication Technology. ICAIT 2024. Lecture Notes in Networks and Systems, vol 1338. Springer, Cham. https://doi.org/10.1007/978-3-031-89296-7_29
5. Haitan, O., Yanko, A., Zdorenko, Y., Rudenko, O. (2024) Method for detection of the modified DDoS cyber attacks on a web resource of an Information and Telecommunication Network based on

the use of intelligent systems. CEUR Workshop Proceedings, 3723, pp. 219-235.

6. European Commission. (2020). *EU's Cybersecurity Strategy in the Digital Decade*. <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade>

7. European Commission. (2022). *Digital Services Act package*. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>

8. European Commission. (2022). *Digital Markets Act*. https://digital-markets-act.ec.europa.eu/index_en

9. European Commission. (2022). *European Digital identity*. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

10. European Commission. (2020). *Media and Audiovisual Action Plan*. <https://digital-strategy.ec.europa.eu/en/policies/media-and-audiovisual-action-plan>

11. European Commission. (2020). *European Democracy Action Plan*. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020DC0790>

12. European Commission. (2020). *Digital Finance Strategy*. https://finance.ec.europa.eu/publications/digital-finance-package_en

13. European Commission. (2020). *European Data Strategy*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0066>

14. European Commission. (2020). *White Paper on Artificial Intelligence: A European approach to excellence and trust*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0065>

15. European Commission. (2024). *AI Act* <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

16. European Commission. (2024). *The EU's approach to artificial intelligence*. <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>

17. European Union. (2018). *Regulation (EU) 2018/302 on addressing unjustified geo-blocking and other forms of discrimination*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0302>

18. European Union. (2019). *Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services*. <https://eur-lex.europa.eu/eli/reg/2019/1150/oj/eng>