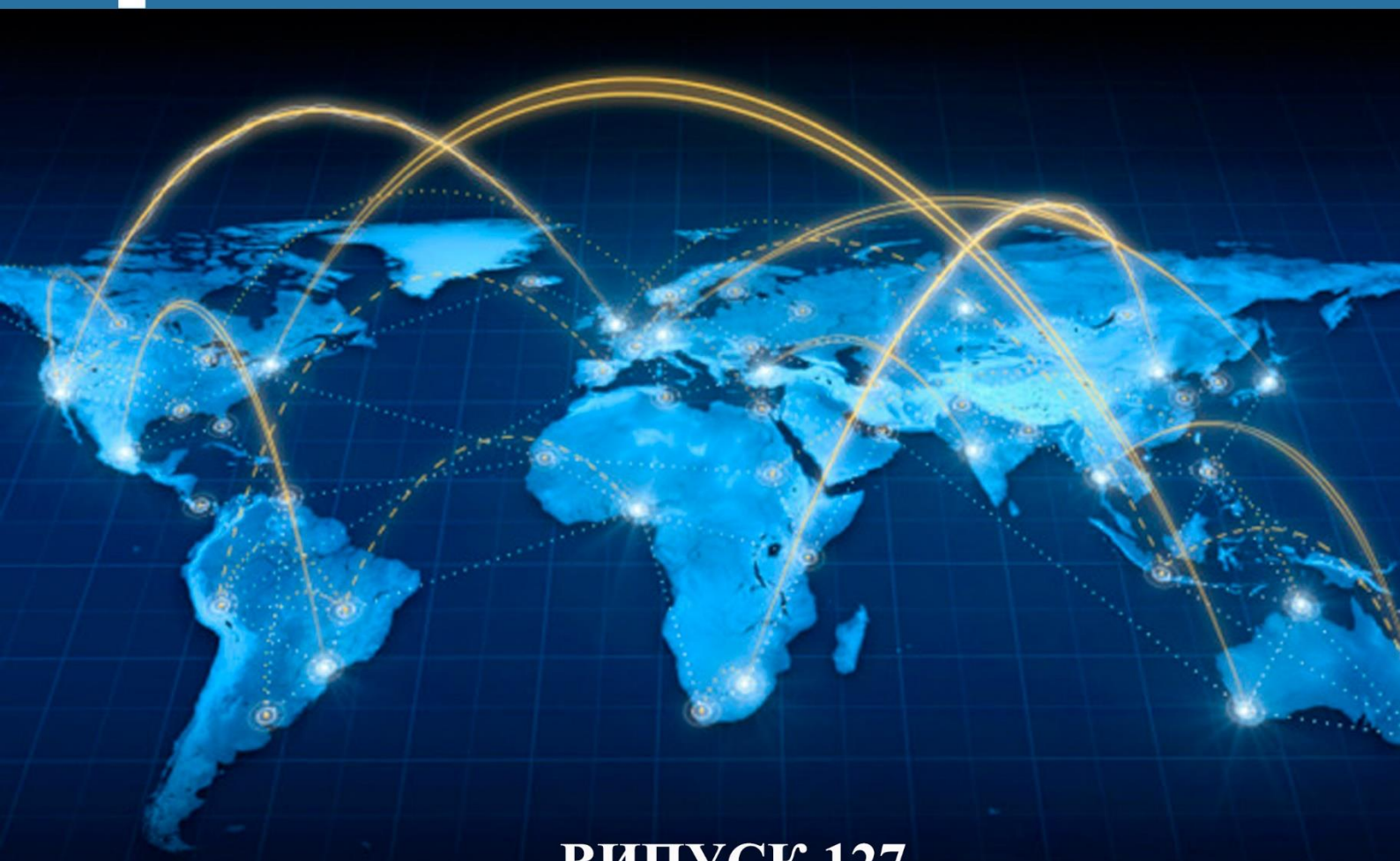
МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА
ІНТЕРНЕТ-КОНФЕРЕНЦІЯ

«ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ НАУКИ І ОСВІТИ В УМОВАХ ГЛОБАЛІЗАЦІЇ»



ВИПУСК 127

31 березня 2026 р.

м. Переяслав

УНІВЕРСИТЕТ ГРИГОРІЯ СКОВОРОДИ
В ПЕРЕЯСЛАВІ
РАДА МОЛОДИХ УЧЕНИХ УНІВЕРСИТЕТУ
ГО «ІНСТИТУТ СУСПІЛЬНОГО РОЗВИТКУ
І НАУКОВИХ ДОСЛІДЖЕНЬ»

Матеріали
Міжнародної науково-практичної інтернет-конференції

«ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ НАУКИ І ОСВІТИ В УМОВАХ ГЛОБАЛІЗАЦІЇ»

31 березня 2026 року
Вип. 127

Збірник наукових праць

Переяслав – 2026

УДК 001+37(100)
ББК 72.4+74(0)
Т 33

Матеріали Міжнародної науково-практичної інтернет-конференції «Тенденції та перспективи розвитку науки і освіти в умовах глобалізації»: зб. наук. праць. Переяслав, 2026. Вип. 127. 254 с.

ГОЛОВНИЙ РЕДАКТОР:
Кикоть С. М. – кандидат історичних наук, заступник голови ГО «Інститут суспільного розвитку і наукових досліджень»

РЕДАКЦІЙНА КОЛЕГІЯ:
Воловик Л. М. – кандидат географічних наук, доцент
Гузун А. В. – кандидат біологічних наук, доцент
Євтушенко Н. М. – кандидат економічних наук, доцент
Носаченко В. М. – кандидат педагогічних наук, доцент
Руденко О. В. – кандидат психологічних наук, доцент
Садиков А. А. – кандидат фізико-математичних наук, доцент (Казахстан)
Скляренко О. Б. – кандидат філологічних наук, доцент
Халматова Ш. С. – кандидат медичних наук, доцент (Узбекистан)
Юхименко Н. Ф. – кандидат філософських наук, доцент

Збірник матеріалів конференції вміщує результати наукових досліджень наукових співробітників, викладачів вищих навчальних закладів, докторантів, аспірантів, студентів з актуальних проблем гуманітарних, природничих і технічних наук

Відповідальність за грамотність, автентичність цитат, достовірність фактів і посилань несуть автори публікацій

© Університет Григорія Сковороди в Переяславі
© Рада молодих учених університету
© ГО «Інститут суспільного розвитку і наукових досліджень»

УДК 34:004.8

Nikita Linchak, Maryna Vyshnevska
(Kyiv, Ukraine)

RISK CLASSIFICATION OF ARTIFICIAL INTELLIGENCE SYSTEMS UNDER THE EU AI ACT: PRINCIPLES AND CHALLENGES

This article examines the risk-based classification system established by the EU Artificial Intelligence Act (Regulation (EU) 2024/1689), which entered into force in August 2024 as the world's first comprehensive legal framework governing AI. The analysis evaluates the four-tier risk structure, the methodological limitations of the current classification approach, and the key challenges affecting the Act's practical implementation, including enforcement gaps, difficulties in classifying general-purpose AI models, and the absence of harmonized technical standards. The article concludes with directions for strengthening the classification system and considers the Act's relevance as a governance model for countries developing their own AI regulation frameworks.

Keywords: *artificial intelligence regulation, EU AI Act, risk-based approach, AI risk classification, high-risk AI systems, AI governance, trustworthy AI.*

У статті досліджується система класифікації ризиків, запроваджена Законом ЄС про штучний інтелект (Регламент (ЄС) 2024/1689), який набрав чинності у серпні 2024 року як перший у світі комплексний правовий акт у сфері регулювання ШІ. Аналізуються чотирирівнева структура ризиків, методологічні обмеження чинного підходу до класифікації та ключові виклики практичної реалізації Закону. У висновках запропоновано напрями вдосконалення класифікаційної системи та розглянуто актуальність моделі ЄС для країн, що формують власне законодавство у сфері ШІ.

Ключові слова: *регулювання штучного інтелекту, Закон ЄС про ШІ, ризик-орієнтований підхід, класифікація ризиків ШІ, системи ШІ високого ризику, врядування ШІ, надійний штучний інтелект.*

For decades, artificial intelligence existed largely outside the scope of formal legal regulation. Governments issued ethical guidelines and technology companies adopted internal codes of conduct – yet binding rules were absent. That changed on 1 August 2024, when Regulation (EU) 2024/1689, the EU Artificial Intelligence Act (AI Act), entered into force as the world's first comprehensive legal framework governing AI systems [7, p. 8].

The Act's central mechanism is a risk-based approach: rather than regulating all AI uniformly, the legislation assigns obligations proportionate to the potential harm a system may cause. Four risk categories structure this logic: unacceptable, high, limited, and minimal [7, p. 11]. In practice, however, applying it raises difficult questions: how should risk be measured when the same model can serve radically different purposes, and who verifies compliance when third-party audits are not mandatory?

Scholars have already identified structural weaknesses in the classification methodology, including overreliance on static application domains and limited enforcement mechanisms [2, p. 4]. This article examines the principles underlying the risk classification system and the challenges that emerge in its practical implementation, drawing on the legislative text and recent academic literature.

The EU AI Act operates on a foundational assumption: that risks posed by AI systems differ significantly depending on what those systems do and where they are deployed. This translates into a tiered regulatory structure where the intensity of legal obligations scales with the severity of potential harm [7, p. 4]. At the top sits the unacceptable risk category - practices so fundamentally incompatible with EU values that they are outright prohibited. These include AI systems that manipulate human behaviour through subliminal techniques, enable mass surveillance through

real-time biometric identification in public spaces, and perform social scoring by public authorities. Below that lies the high-risk category, which forms the regulatory core. Article 6 defines high-risk AI systems along two axes: those embedded in products subject to EU safety legislation and those deployed in eight sensitive domains listed in Annex III, including critical infrastructure, education, employment, law enforcement, and migration [7, p. 50]. Systems in this category face mandatory risk management, data governance, technical documentation, human oversight, and conformity assessments.

Limited-risk systems – primarily chatbots and deepfake tools, must meet transparency requirements only, while minimal-risk systems face no specific obligations [1, p. 6]. The structure's key strength is its proportionality logic: calibrating regulation to actual risk exposure rather than applying uniform burdens. As Balciğlu and colleagues have argued, this reflects a European tradition of governance rooted in fundamental rights protection [1, p. 19]. The boundary between high-risk and non-high-risk is not always self-evident, however, and the Commission retains authority to expand Annex III through delegated acts – introducing regulatory uncertainty for developers [7, p. 16].

The European Commission popularized a pyramid representation of the risk system, with prohibited practices at the top narrowing down to minimal-risk applications at the base. This model, however, misrepresents the classification logic in the Act's actual text [4, p. 21]. The pyramid implies a clean linear hierarchy, whereas the AI Act's classification process is considerably more branching: a system must pass through the general scope of application, then category-specific criteria, before receiving a designation. Transparency obligations do not constitute a separate risk level they operate in parallel with the main classification framework [4, p. 34]. Gasiola proposes replacing the pyramid with a binary decision diagram, a structured sequence of yes/no questions that makes the process traceable and reduces interpretive ambiguity.

A related problem concerns how risk magnitude is estimated. The Act assigns risk categories based primarily on the application domain, treating any system used in employment as high-risk by default regardless of its specific function. This static logic can lead to both over- and under-regulation [5, p. 14]. Novelli and colleagues propose integrating a scenario-based assessment model adapted from the Intergovernmental Panel on Climate Change, evaluating risk through the interaction of hazard characteristics, exposure, vulnerability, and societal context [5, p. 6]. Applied to AI, two systems in the same domain could receive different risk assessments depending on deployment scale, affected population, and availability of human oversight. If national supervisory authorities adopt such a scenario-driven approach, the classification system becomes more responsive to actual risk – though also more resource-intensive [7, p. 77].

The risk-based framework represents a genuine regulatory achievement, yet the classification system faces four structural challenges that may limit its effectiveness. For most high-risk AI systems, the Act permits providers to conduct their own conformity assessments without independent third-party verification [2, p. 8]. Self-assessment in a technically complex domain creates obvious risks: organizations may lack expertise to identify blind spots, and competitive pressure may incentivize optimistic interpretations. Researchers argue that regulatory legitimacy depends on the credibility of the assessment process, not merely its existence.

Models like GPT-4 or Gemini do not fit cleanly into the classification logic their risk profile depends entirely on how they are used and by whom [2, p. 10]. The Act introduced a separate tier for general-purpose AI with systemic risk, but the criteria remain insufficiently precise. Measuring capability thresholds by computational training costs captures scale but not necessarily danger [2].

High-risk AI systems must meet demanding technical requirements, but harmonized standards providing concrete verification benchmarks are still under development [3, p. 16]. Developers face genuine uncertainty about what level of documentation and testing is sufficient, particularly for organizations outside the EU [2, p. 12].

Large technology companies headquartered in the US or China operate in less restrictive regulatory environments, gaining a structural advantage over EU-based competitors [2, p. 2].

Smaller European developers face compliance costs that represent a disproportionate share of their budgets. The Act includes provisions for SMEs – simplified conformity procedures and regulatory sandboxes, but whether these offset the competitive imbalance remains uncertain.

These four challenges, while distinct, share a common implication: they do not undermine the case for the risk-based approach, but point to where it needs to be strengthened.

Conclusion. The EU AI Act's risk classification system marks a significant shift in AI governance. By anchoring obligations to potential harm, the Act establishes a framework that is proportionate and adaptable in principle. The four-tier structure reflects a deliberate policy choice to enable innovation while protecting fundamental rights. In practice, however, the gap between principle and implementation is wider than anticipated. The domain-based classification assigns risk statically rather than dynamically a limitation that scenario-based models could address [5, p. 6]. The Commission's pyramid misrepresents the actual classification process [4, p. 17], and the self-assessment enforcement architecture raises questions about whether compliance will translate into genuine safety [2, p. 11].

Three directions for improvement emerge. First, integrating scenario-based risk assessment into the delegated acts process would allow classification to reflect actual deployment context. Second, accelerating harmonized technical standards is essential for meaningful verification [3, p. 13]. Third, expanding mandatory third-party audits for the highest-stakes applications would strengthen compliance credibility. Beyond the EU, the risk-based model offers a workable starting point for countries developing AI governance frameworks, including Ukraine – one worth adopting critically, with the limitations identified here in mind.

REFERENCES

1. Balciğlu Y. S., Çelik A. A., Altindağ E. A turning point in AI: Europe's human-centric approach to technology regulation. *Global Transitions.* 2025. Vol. 51(4). PP. 1-35.

2. Ballot Jones L., Thornton J., De Silva D. Limitations of risk-based artificial intelligence regulation: a structuration theory approach. *Discover Artificial Intelligence.* 2025. Vol. 5. P. 14. PP. 1-13.

3. Buscemi A., Deckenbrunnen T., Kabir F., Mishchenko K. et al. Assessing High-Risk AI Systems under the EU AI Act: From Legal Requirements to Technical Verification. 2025. P. 1-17.

4. Gasiola G. G. Rebuilding the pyramid: The AI Act's risk-based approach using a binary decision diagram. Computer Law & Security Review. 2025. Vol. 58. Article 106189. P. 1-13.

5. Novelli C., Casolari F., Rotolo A., Taddeo M., Floridi L. AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act. *Digital Society.* 2024. Vol. 3. Article 13. P. 5-29.

6. Novelli C., Casolari F., Rotolo A., Taddeo M., Floridi L. Taking AI risks seriously: a new assessment model for the AI Act. *AI & Society.* 2024. Vol. 39. No. 5. PP. 1-6.

7. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union.* 2024. P. 1-144.