

Адміністративне право і процес; фінансове право; інформаційне право
УДК 342.9:004.89

Дуліба Євгенія Володимирівна

доктор юридичних наук, професор,

професор кафедри конституційного права та галузевих дисциплін

Навчально-наукового інституту права

Національний університет водного господарства та природокористування

Duliba Yevheniia

Doctor of Science Law, Professor,

Professor of the Department of Constitutional Law and Field-Related Disciplines

Institute of Law

National University of Water and Environmental Engineering

ORCID:0000-0003-2651-4977

**ЗАКОН ПРО ШТУЧНИЙ ІНТЕЛЕКТ ЄС: У ПОШУКАХ БАЛАНСУ
МІЖ ПРОСУВАННЯМ ІННОВАЦІЙ ТА ВИЗНАННЯМ РИЗИКІВ
EU ARTIFICIAL INTELLIGENCE ACT: SEEKING A BALANCE
BETWEEN PROMOTING INNOVATION AND RECOGNIZING RISKS**

***Анотація.** Вступ. Динамічний розвиток штучного інтелекту призвів до глобальної цифрової трансформації суспільств та держав, посилив занепокоєння щодо безпеки, упередженості, особистих даних, прав інтелектуальної власності. Прийнятий Європейським парламентом Закон ЄС про штучний інтелект є першим у світі всеосяжним нормативно-правовим актом, що встановлює етичні принципи та гармонізовані правила для розробки, розміщення, введення в експлуатацію та використання систем штучного інтелекту в ЄС. Поза сумнівом, цей закон буде мати значний вплив на використання систем штучного інтелекту не лише в ЄС, але і за його межами, може стати основою для глобального стандарту*

етичної розробки та впровадження штучного інтелекту, впливаючи на нормативні акти різних країнах.

Мета. Метою дослідження є проведення ґрунтовного аналізу положень прийнятого та опублікованого Закону ЄС про штучний інтелект, а також висвітлення наявних можливостей та викликів для розвитку систем штучного інтелекту у ЄС.

Матеріали і методи. Матеріалами дослідження є : 1) Закон ЄС про штучний інтелект; 2) праці вітчизняних та зарубіжних науковців у сфері штучного інтелекту, зокрема щодо проєкту чи Закону ЄС про штучний інтелект в цілому, так і застосування цих положень в окремих сферах життєдіяльності держави; 3) статистичні та звіті матеріали ЄС.

В процесі здійснення дослідження було використано загальнонауковий діалектичний метод та метод системного аналізу, методи класифікації та групування, системно-функціональний метод.

Результати. У науковій статті проведено ґрунтовний аналіз положень прийнятого та опублікованого Закону ЄС про штучний інтелект. Зроблено висновок, що Закон ЄС про штучний інтелект вводить загальноєвропейські мінімальні вимоги до систем штучного інтелекту, що ґрунтується на застосуванні ризик-орієнтованого підходу до регулювання штучного інтелекту. Такий підхід спрямований на захист фундаментальних прав людини, верховенства права, демократії, навколишнього середовища від негативного впливу систем штучного інтелекту.

Виділено та проаналізовано системи штучного інтелекту за чотирма рівнями ризику: з неприйнятним ризиком, з високим ризиком, з обмеженим ризиком або спеціальними зобов'язаннями щодо прозорості, з мінімальним ризиком.

Аналіз положень Закону ЄС про штучний інтелект надав можливість виділити виклики для імплементації його положень та можливості для розвитку сфери штучного інтелекту в ЄС. До найбільших викликів

імплементції положень Закону віднесено: належне впровадження та забезпечення дотримання положень; створення послідовної та ефективної системи управління у цій сфері на всьому континенті; збільшення експлуатаційних витрат та цін на системи штучного інтелекту; вимкнення або обмеження певних функцій системи штучного інтелекту для забезпечення відповідності, затримка запуску нових продуктів штучного інтелекту, затрата часу на вихід на ринок, відставання європейських розробників від інших розробників з регіонів з менш суворими правилами для систем штучного інтелекту, виникнення розбіжностей між державами-членами щодо здійснення нагляду та застосування положень цього закону в межах своїх юрисдикцій. До можливостей європейських розробників систем штучного інтелекту віднесено: створення прецеденту для наслідування, формування репутації розробників надійних систем штучного інтелекту; забезпечення чесної конкуренції в регіоні.

Зазначено, що імплементція Закону ЄС про штучний інтелект залежатиме від того, наскільки ефективно його положення збалансують можливості та виклики, а також від того, як адаптуються суб'єкти господарювання, органи публічної влади та громадське суспільство до нового правового регулювання.

Ключові слова: штучний інтелект, системи штучного інтелекту, нові технології, правове регулювання, ЄС, ризики для фундаментальних прав людини.

Summary. Introduction. The dynamic development of artificial intelligence has led to a global digital transformation of societies and states, and increased concerns about security, bias, personal data, and intellectual property rights. Adopted by the European Parliament, EU Artificial Intelligence Act is the world's first comprehensive legal act establishing ethical principles and harmonised rules for the development, placement, putting into service and use of artificial

intelligence systems in the EU. Undoubtedly, this law will have a significant impact on the use of artificial intelligence systems not only in the EU but also abroad, and can become the basis for a global standard for the ethical development and implementation of artificial intelligence, influencing the regulations of different countries.

Purpose. The purpose of the issue is to conduct a thorough analysis of the provisions of the adopted and published EU Artificial Intelligence Law, as well as to highlight the existing opportunities and challenges for the development of artificial intelligence systems in the EU.

Materials and methods. The research materials are 1) EU Artificial Intelligence Act; 2) the works of domestic and foreign scientists in the field of artificial intelligence, in particular regarding the draft of EU Artificial Intelligence Law as a whole, and the application of these provisions in certain areas of the state; 3) EU statistical and reporting materials. In the research process, the general scientific dialectical method, the method of system analysis, classification and grouping methods, and the system-functional method were used.

Results. The issue provides a thorough analysis of the provisions of the adopted and published EU Artificial Intelligence Law. It is concluded that the EU Artificial Intelligence Law introduces pan-European minimum requirements for artificial intelligence systems, based on using a risk-based approach to regulating artificial intelligence. This approach is aimed at protecting fundamental human rights, the rule of law, democracy, and the environment from the negative impact of artificial intelligence systems.

Artificial intelligence systems are identified and analysed for four levels of risk: unacceptable risk, high risk, limited risk or special obligations for transparency, with minimal risk.

Analysis of the EU Artificial Intelligence Law provided an opportunity to highlight challenges to the implementation of its provisions and opportunities for

the development of artificial intelligence in the EU. The greatest challenges to the implementation include proper implementation and enforcement of the provisions; creation of a consistent and effective management system in this area throughout the continent; increase in operating costs and prices for artificial intelligence systems; disabling or restricting certain functions of the artificial intelligence system to ensure compliance, delaying the launch of new artificial intelligence products, wasting time on market entry, lagging European developers behind other developers from regions with less stringent rules for artificial intelligence systems, disagreements between Member States regarding the implementation of supervision and application of the provisions of this law within their jurisdictions. The capabilities of European developers of artificial intelligence systems include: creating a precedent for imitation, building the reputation of developers of reliable artificial intelligence systems; and ensuring fair competition in the region.

The implementation of the EU Artificial Intelligence Law will depend on how effectively its provisions balance opportunities and challenges, as well as on how business entities, public authorities and civil society adapt to the new legal regulation.

Key words: *artificial intelligence, artificial intelligence systems, new technologies, legal regulation, EU, risks for fundamental human rights.*

Вступ. Динамічний розвиток штучного інтелекту (далі – ШІ) призвів до глобальної цифрової трансформації суспільств та держав й посилив занепокоєння щодо безпеки, упередженості, особистих даних, прав інтелектуальної власності. Як наслідок цього сьогодні однією з найбільш актуальних проблем у світі є створення ефективного правового регулювання та управління системами ШІ, які зможуть забезпечити збалансований підхід до інновацій та захисту суспільних інтересів.

У той час як США і Китай борються у технологічному суперництві за лідерство у сфері ІІІ, Європейський Союз (далі – ЄС) приймає і опубліковує Закон про ІІІ (далі – Закон). Закон є першим у світі всеосяжним нормативно-правовим актом, що встановлює етичні принципи та гармонізовані правила для розробки, розміщення, введення в експлуатацію та використання систем ІІІ в ЄС. Поза сумнівом, цей закон буде мати значний вплив на використання систем ІІІ не лише в ЄС, але і за його межами, може стати основою для глобального стандарту етичної розробки та впровадження ІІІ. У цьому контексті проведення огляду основних положень Закону набуває неабиякої актуальності.

Аналіз останніх досліджень і публікацій. Сьогодні ІІІ знаходиться в центрі академічних і громадських дебатів. З моменту підготовки проєкту Закону, науковці зі всього світу аналізують його положення в цілому [1; 2; 3], а також вплив цих положень на світовий ринок ІІІ [4], політику інших країн світу у цій сфері [5]. Науковці також особливу увагу приділяють дослідженню застосування положень Закону у різних сферах життєдіяльності (наприклад, у сфері освіти [6], зайнятості населення [7], цифрової медицини [8] та економіки [9]). Поряд з цим метою цієї статті є здійснити ґрунтовний аналіз положень прийнятого та опублікованого Закону, а також висвітлити наявні можливості та виклики для розвитку систем ІІІ у ЄС.

Виклад основного матеріалу. 2 лютого 2024 року Європейська Рада одноголосно проголосувала за схвалення новаторського Закону [10], який був офіційно підписаний Європейським парламентом 13 березня 2024 року та опублікований 12 липня 2024 року. Закон набуває чинності з 02 серпня 2024 року. Однак більшість його положень почнуть діяти після дворічного пільгового періоду, який передбачений для підготовки до їх виконання, за винятком окремих положень, що набудуть чинності через 6 або 12 місяців.

В цілому, Закон є частиною правового регулювання цифрових технологій у ЄС поряд з Загальним регламентом про захист даних [11], Законом про цифрові послуги [12], Законом про цифрові ринки [13].

Визнаючи потенціал систем ШІ «поставити під загрозу» фундаментальні права людини, демократію та верховенство права, ЄС розглядає ШІ як потенційно високоризиковану технологію, яка потребує втручання. Закон переслідує подвійну мету: по-перше, сприяти розробці, використанню та поширенню ШІ в ЄС; по-друге, мінімізувати чи усунути ризики та шкоду суспільним інтересам та фундаментальним правам людини, гарантуючи, що системи ШІ – це технології, орієнтовані на людину.

Взявши за основу поняття «система ШІ», що визначене Організацією економічного співробітництва та розвитку [14], це поняття вживається у Законі у трьох аспектах як: машинна система, яка призначена для роботи з різним рівнем автономії; машинна система, що може проявляти адаптивність після впровадження, тобто така адаптивність відноситься до можливостей самонавчання, що дозволяє системі змінюватися під час використання; машинна система, яка для явних або неявних цілей робить висновок на основі вхідних даних, які вона отримує (прогнози, контент, рекомендації або рішення), які можуть впливати на фізичне або віртуальне середовище (п. 1 статті 3) [10].

Закон вводить загальноєвропейські мінімальні вимоги до систем ШІ, що ґрунтуються на застосуванні ризик-орієнтованого підходу до регулювання ШІ. Цей підхід спрямований на захист фундаментальних прав людини, верховенства права, демократії, навколишнього середовища від негативного впливу систем ШІ.

Закон класифікує системи ШІ за чотирма рівнями ризику:

1) системи ШІ з неприйнятним ризиком – це системи ШІ, які за своєю суттю порушують фундаментальні права або суперечать цінностям ЄС. Зокрема, відповідно до статті 2 Консолідованої версії Договору про ЄС,

цінностями ЄС є повага до людської гідності, свободи, демократії, рівності, верховенства права та поваги до прав людини [15]. Статтею 5 Закону передбачено перелік заборонених систем ШІ, до яких віднесено: системи ШІ, що використовують підсвідомі (виходять за межі свідомості людини) або маніпулятивні чи оманливі методи для спотворення поведінки людини та прийняття рішення, яке б вона не прийняла б в іншому випадку (пп. а п.1 стаття 5); системи ШІ, які використовують вразливості певної групи осіб через їхній вік, інвалідність або соціально-економічне становище з метою значного спотворення їх поведінки і завдання шкоди (пп. б п.1 стаття 5); системи ШІ для соціальної оцінки людей за їх поведінкою чи особистісними характеристиками, що призводять до несправедливого або непропорційного відношення (пп. с п.1 стаття 5); системи ШІ, що використовуються для оцінки ризиків або прогнозування ризиків вчинення фізичною особою кримінального правопорушення, крім випадків підтримки людської оцінки до причетності особи до злочинної діяльності (пп. d п.1 стаття 5); системи ШІ для створення або розширення бази даних розпізнання обличчя шляхом збору зображень з Інтернету або записів з камер спостереження (пп. і п. 1 стаття 5); системи ШІ, що використовуються для визначення емоцій на робочих місцях або освітніх закладах, крім медичних чи безпекових цілей (пп. f п.1 стаття 5); системи ШІ, що використовуються для категоризації людей за расою, політичними поглядами, релігійними переконаннями тощо (пп. g п.1 стаття 5); системи ШІ "реального часу" для біометричної ідентифікації в публічних місцях для цілей правоохоронних органів, крім випадків, коли це необхідно для запобігання загрозам життю, безпеці або терористичним актам (пп. h п. 1 стаття 5) [10]. Однак тут варто звернути увагу на той факт, що положення про заборонені системи ШІ можуть тлумачитися по-різному. Наприклад, який об'єктивний поріг заподіяння психологічної шкоди; чи ця чітка заборона систем ШІ буде застосовуватися до алгоритмів поведінкового підштовхування, які часто зустрічаються в

Інтернеті; чи виключає заборона систем ІІІ "реального часу" системи, які могли б біометрично аналізувати відеозапис [16].

2) системи ІІІ з високим ризиком – це системи ІІІ, що впливають на безпеку людей і їх фундаментальні права, та повинні підлягати суворій перевірці шляхом оцінки відповідності перед тим, як вони будуть випущені на ринок, і постійно контролюватися протягом усього їх життєвого циклу. Системи ІІІ з високим рівнем ризику поділяються на: системи, що є компонентами безпеки або продуктами, що підпадають під існуючі стандарти безпеки та оцінки (наприклад, медичні вибори, іграшки, радіоприлади) та системи, що призначені для використання у таких сферах життєдіяльності держави, як біометрична ідентифікація та категоризація фізичних осіб, критична інфраструктура, освіта, зайнятість та управління працівниками, доступ до основних приватних та державних послуг, правоохоронна діяльність, міграція, правосуддя та у виборчих процесах (стаття 6) [10].

3) системи ІІІ з обмеженим ризиком або спеціальними зобов'язаннями щодо прозорості – це системи ІІІ, що становлять мінімальні загрози, але вимагають певного рівня поінформованості користувачів, що вони взаємодіють з системою ІІІ, якщо це не є очевидним під кутом зору фізичної особи. Такі системи повинні відповідати вимогам прозорості. Наприклад, до таких систем слід віднести: чат-боти, які взаємодіють з клієнтами або діпфейки, які використовують у розважальних цілях.

4) системи ІІІ з мінімальним ризиком – це системи ІІІ практично без ризику для безпеки, конфіденційності чи основних прав людини. Ці системи не підпадають під жодні правила. Наприклад, відео-ігри на основі ІІІ або базові спам-фільтри. Втім, для впроваджувачів таких систем ІІІ рекомендується створювати кодекси поведінки для сприяння добровільному застосуванню деяких або всіх обов'язкових вимог, що застосовуються до

систем ІІІ з високим ризиком (стаття 56) [10]. Поява непередбачуваних ризиків для систем ІІІ з мінімальним ризиком внаслідок розвитку ІІІ, а також розвиток генеративного ІІІ, який може створювати дуже реалістичний і потенційно шкідливий контент, у майбутньому може вимагати врегулювання і цього види систем ІІІ.

5) Поряд з цим поява генеративного ІІІ, який може створювати дуже реалістичний і потенційно шкідливий контент, може вимагати майбутніх правил у цій категорії, так само як і поява непередбачуваних ризиків в категоріях мінімального ризику внаслідок розвитку ІІІ.

Варто звернути увагу, що класифікація систем ІІІ за ризиками тісно пов'язана з цільовим призначенням кожної системи ІІІ. Паралельно з цільовим призначенням законодавець ЄС розглядає так зване «обґрунтовано передбачене неправомірне використання», а саме випадки, коли система ІІІ використовується «... у спосіб, який не відповідає її прямому призначенню, але й який може бути результатом розумно передбачуваної поведінки людини або взаємодії з іншими системами, включаючи інші системи ІІІ...» (п.13 стаття 3) [10].

Таким чином, Закон встановлює межі дозволеного, обґрунтовуючи їх етичними ризиками та ризиками безпеки, які можуть призвести до негативних наслідків, а тому найбільше регулювання та здійснення нагляду зосереджено на заборонених системах ІІІ та системах ІІІ з високим ризиком.

Слід також акцентувати увагу на тому, що Закон поширюється не лише на суб'єктів господарювання ЄС, але й на тих суб'єктів, що розробляють системи ІІІ за межами ЄС, на постачальників, які розміщують на ринку або вводять в експлуатацію системи ІІІ під власним іменем або торговою маркою, імпортерів, дистриб'юторів, а також впроваджувачів систем ІІІ, тобто фізичних чи юридичних осіб, органів публічної влади, які використовують системи ІІІ. Запозичуючи концепцію із законодавства про

безпеку продукції, суть якої полягає в тому, щоб працювати у зворотному напрямку від певної шкоди до заходів, які зменшують ризик того, що ця шкода матеріалізується, Закон встановлює зобов'язання та обов'язки для операторів систем III з високим ризиком (постачальник, виробник продукції, розповсюджувач, уповноважений представник, імпортер, дистриб'ютор), пропорційні інтенсивності та масштабу шкоди, яку можуть завдати системи III.

Закон запроваджує низку зобов'язань для постачальників систем III з високим ризиком, які включають: створення, провадження, документування та підтримання системи управління ризиками (стаття 9); ефективне управління даними (стаття 10); виготовлення технічної документації для демонстрації відповідності (стаття 11); ведення обліку (автоматичних записів подій) (стаття 12); забезпечення достатньої прозорості та ефективного людського нагляду (ст. 13-14); проєктування та впровадження системи III таким чином, щоб досягти належної точності, надійності та кібербезпеки (стаття 15); впровадження системи управління якістю та ведення документації (стаття 17, 18), призначення уповноваженого представника в ЄС (стаття 22). До того ж постачальники систем III з високим рівнем ризику повинні пройти процедуру оцінки відповідності (стаття 43), скласти письмову декларацію про відповідність ЄС (стаття 47) та зареєструвати себе та свою систему в базі даних ЄС (стаття 49, 71) [10]. Як висновок з цього, слід зазначити, що наявність такої кількості зобов'язань про документування створює високе адміністративне навантаження на постачальників систем III.

Аналіз норм Закону надав можливість зробити висновок, що перш за все розробники, починаючи з етапу проєктування, повинні враховувати відповідність системи III нормативним вимогам. Надалі імпортери та дистриб'ютори зобов'язані переконатися, що система III з високим рівнем ризику відповідає конкретним положенням Закону. До того ж

постачальники, дистриб'ютори та впроваджувачі повинні постійно перевіряти відповідність системи ІІІ протягом усього її життєвого циклу. Вони також повинні інформувати постачальника та компетентні органи, що система ІІІ з високим ризиком становить ризики для здоров'я, безпеки та фундаментальних прав людини.

Таким чином, для досягнення успіху у використанні ІІІ на європейському ринку, суб'єкти господарювання та органи публічної влади повинні дотримуватися широкого спектру зобов'язань, формувати культуру довіри та забезпечувати прозорість протягом усього життєвого циклу ІІІ.

Сьогодні відомо непоодинокі випадки, коли генеративний ІІІ генерував певні факти сумнівної якості або засновані на вигаданій інформації, тому Закон встановлює обов'язок суб'єктів господарювання, які розробляють і випускають ботів, перевіряти і коригувати світогляд ІІІ, щоб не допустити подібних прецедентів (стаття 53). До того ж Закон встановлює правила, які зобов'язують перевіряти джерела та достовірність інформації перед додаванням її до системи навчання ботів, а також перевіряти та контролювати інформацію користувачів та фільтрувати шкідливі тренди [10]. Наприклад, якщо бот отримує запит, який містить ключові слова, система повинна позначити його відповідним чином і виключити інформацію з системи індексації та навчання.

Заслуговує на увагу і нововведення щодо заборони збирання конфіденційної інформації про користувачів та зберігання її на публічних серверах. Закон суворо регулює численні ніші та їхні можливості застосування ІІІ. Наприклад, ботам тепер заборонено надавати інформацію про здоров'я, інформацію про методи лікування. Ці обмеження, на мій погляд, є не випадковими, а обґрунтованими потенційними ризиками, які можуть негативно вплинути на безпеку, об'єкти інфраструктури та життя і здоров'я людей.

Варто також звернути увагу на особливості публічного адміністрування цієї сфери. Держави-члени ЄС зобов'язані призначити принаймні один нотифікуючий орган та національний наглядовий орган (стаття 70). Нотифікуючий орган має бути зареєстрований у списку, створеному Європейською комісією, та відповідати за встановлення та проведення необхідних процедур для оцінки, призначення та повідомлення органів з оцінки відповідності систем ШІ та за їх моніторинг (статті 28). Нотифікуючий органи зможуть видавати сертифікати на відповідність обов'язковим вимогам систем ШІ з високим ризиком, які будуть дійсні протягом не більше 4 і 5 років в залежності від системи ШІ (стаття 44). Національний наглядовий орган діятиме як орган ринкового нагляду, контролюючи національний ринок і здійснюючи нагляд за дотриманням необхідних правил для систем ШІ з високим рівнем безпеки (стаття 70) [10].

До того ж Законом передбачено створення Офісу ШІ (стаття 64), як центру експертизи у галузі ШІ в ЄС та сприяння розробки та використання надійного ШІ [10; 17]; Європейської ради з питань ШІ у складі представників держав-членів, що відповідатиме за сприяння гармонізованому застосуванню положень Закону на всій території ЄС та забезпечення співпраці та координації дій між національними наглядовими органами (стаття 65); Консультативного форуму, як дорадчого органу для надання технічної експертизи та консультування Комісії та Правління Європейської Ради з питань ШІ, а також сприяння виконанню їхніх завдань, що має «...представляти збалансований вибір зацікавлених сторін, включаючи промисловість, стартапи, малі та середні підприємства, громадське суспільство та наукові кола» (стаття 67); наукової групи незалежних експертів для підтримки правозастосовної діяльності Комісії (стаття 68) [10].

За порушення Закону передбачено адміністративні штрафи, але вид та розмір таких штрафів залежатимуть від всіх обставин, що стосуються

даної ситуації, а саме: характеру, тяжкості і тривалості порушення та його наслідків із урахуваннями мети системи ШІ, кількості постраждалих осіб та рівня шкоди, якої вони зазнали; розмір, річний оборот і частка ринку оператора, який вчинив порушення; наявність пом'якшуючих чи обтяжуючих обставин; навмисний чи недбалий характер порушення; ступінь співпраці з національними компетентними органами з метою усунення порушення та пом'якшення негативних наслідків порушення, а також наявність чи відсутність застосованих національним компетентним органом адміністративних штрафів за це порушення (стаття 99). Наприклад, за порушення суб'єктами господарювання заборонених практик або невідповідності, пов'язану з вимогами до даних, може бути накладено штраф до 35 млн євро або 7% від його загального світового річного обороту за попередній фінансовий рік залежно від того, яке з цих значень вище; за порушення вимог або зобов'язань закону – до 15 млн євро або 3%; за надання неправильної, неповної або оманливої інформації – до 7,5 млн євро або 1% [10].

Без сумніву, прийнятий Закон може спричинити виникнення багатьох викликів для імплементації його положень у реальність, однак також відкрити нові можливості та перспективи розвитку сфери ШІ.

На мою думку, найбільшими викликами імплементації положень Закону є належне впровадження та забезпечення дотримання положень, а також створення послідовної та ефективної системи управління у цій сфері на всьому континенті. Заплутана мережа національних органів, яким доручено імплементацію, може зіткнутися з проблемами фінансування, технічної спроможності та наявністю кваліфікованого персоналу.

Не слід забувати і той факт, що імплементація Закону може призвести до виникнення потенційних викликів не лише для всіх суб'єктів господарювання, що розробляють, вводять в експлуатацію, використовують системи ШІ, але й для користувачів. Наприклад, імплементація положень

Закону призведе до збільшення експлуатаційних витрат та цін на системи ІІІ. Насамперед, мова йде про те, що системи ІІІ можуть мати вищу вартість порівняно з аналогічними системами ІІІ з регіонів із нижчими стандартами або без них, а підвищенні вимоги до безпеки цифрових рішень та алгоритмів використання ботів можуть збільшити витрати на розробку та підтримку таких систем, а також призвести до потенційного підвищення цін для споживачів. До того ж, Закон містить чимало положень щодо необхідності здійснення людського нагляду, моніторингу, повідомлення про серйозні інциденти та несправності, що збільшує експлуатаційні витрати. Підтвердженням моєї думки є дослідження оцінки впливу нормативних вимог до ІІІ в Європі, яке проведене для Європейської Комісії ще у 2021 році. Результати цього дослідження демонструють, що дотримання вимог щодо відповідності положенням Закону орієнтовно може коштувати 10 тисяч євро, тоді як придбання додаткових послуг або наймання додаткового персоналу може збільшити вартість до 30 тисяч євро [18]. З цього приводу керівники 150 великих європейських компаній (Airbus, Renault і Heineken, Siemens тощо) звернулися з відкритим листом до Європейської комісії, Європейської Ради та Європейського Парламенту про їх стурбованість таким суворим регулюванням систем ІІІ та базових моделей, незалежно від їх використання. На думку цих керівників імплементація положень Закону може призвести до збільшення вартості систем ІІІ та зниження продуктивності їхньої діяльності, а отже, конкурентоспроможності порівняно з іншими країнами світу [19].

Не слід залишати поза увагою і те, що наявність чітко прописаних положень щодо функціонування систем ІІІ можуть вимагати вимкнення або обмеження певних функцій систем ІІІ для забезпечення відповідності, результатом чого може бути запроваджено менш функціональні або персоналізовані продукти для кінцевих користувачів.

На жаль, виконання всіх вимог Закону може затримати запуск нових продуктів ІІІ, призвести до витрачання часу на вихід на ринок та ймовірного відставання європейських розробників від розробників з регіонів з менш суворими правилами для систем ІІІ. Також надмірно суворі положення Закону можуть перешкоджати дослідженням і розробкам, потенційно спонукаючи до розробки нових систем ІІІ в інших регіонах.

Врешті-решт, практичне застосування Закону може спричинити виникнення розбіжностей між державами-членами ЄС щодо здійснення нагляду та застосування положень Закону в межах своїх юрисдикцій.

Поряд з цим, європейські розробники системи ІІІ можуть скористатися низкою нових можливостей. По-перше, будучи першою глобальною правовою базою для постачальників систем ІІІ, Закон позиціонує європейських розробників як «першопрохідців», потенційно створюючи прецедент для інших країн, які будуть наслідувати цей приклад. По-друге, європейські розробники систем ІІІ можуть створити репутацію розробників надійних систем ІІІ, що забезпечують високий рівень безпеки та викликають довіру, підвищуючи попит на свої продукти та послуги. По-третє, Закон створює підґрунтя для чесної конкуренції в регіоні, адже усі суб'єкти господарювання, що займаються ІІІ, незалежно від походження, повинні дотримуватися положень Закону, щоб працювати в межах ЄС.

Висновки і перспективи подальших досліджень. Таким чином, підсумовуючи вищевикладене, варто зробити такі висновки:

1) Закон вводить загальноєвропейські мінімальні вимоги до систем ІІІ, що ґрунтується на застосуванні ризик-орієнтованого підходу до регулювання ІІІ. Такий підхід спрямований на захист фундаментальних прав людини, верховенства права, демократії, навколишнього середовища від негативного впливу систем ІІІ.

2) Закон розрізняє системи ІІІ за чотирма рівнями ризиками: з неприйнятним ризиком, з високим ризиком, з обмеженим ризиком або спеціальними зобов'язаннями щодо прозорості, з мінімальним ризиком.

3) До найбільших викликів імплементації положень Закону віднесено: належне впровадження та забезпечення дотримання положень; створення послідовної та ефективної системи управління у цій сфері на всьому континенті; збільшення експлуатаційних витрат та цін на системи ІІІ; вимкнення або обмеження певних функцій системи ІІІ для забезпечення відповідності, затримка запуску нових продуктів ІІІ, затрата часу на вихід на ринок, відставання європейських розробників від інших розробників з регіонів з менш суворими правилами для систем ІІІ, виникнення розбіжностей між державами-членами щодо здійснення нагляду та застосування положень цього закону в межах своїх юрисдикцій.

4) До можливостей європейських розробників систем ІІІ віднесено: створення прецеденту для наслідування, формування репутації розробників надійних систем ІІІ; забезпечення чесної конкуренції в регіоні.

Імплементація Закону залежатиме від того, наскільки ефективно його положення збалансують можливості та виклики, а також від того, як адаптуються суб'єкти господарювання, органи публічної влади та громадське суспільство до нового нормативно-правового регулювання. І лише після подолання всіх складнощів ЄС можна буде позиціонувати як світового лідера в етичному та відповідальному розвитку систем ІІІ.

В подальших наукових дослідженнях пропонується зосередити увагу на вивченні впливу положень Закону на функціонування правосуддя та адаптації законодавства до швидкоплинних змін у сфері правосуддя та технологій.

Література

1. Pavlidis G. Unlocking the black box: analysing the EU artificial intelligence act's framework for explainability in AI. *Law, Innovation and Technology*. 2024. 16(1). P. 293-308. doi: <https://doi.org/10.1080/17579961.2024.2313795>.
2. Enqvist L. «Human oversight» in the EU artificial intelligence act: what, when and by whom? *Law, Innovation and Technology*. 2023. 15(2). P. 508-535. doi: <https://doi.org/10.1080/17579961.2023.2245683>.
3. Kalodanis K., Rizomiliotis P., Anagnostopoulos D. European Artificial Intelligence Act: an AI security approach. *Information and Computer Security*. 2024. Vol. 32 No. 3. P. 265-281. doi: <https://doi.org/10.1108/ICS-10-2022-0165>.
4. Siegmännand Ch., Anderljung M. The Brussels Effect and Artificial Intelligence: How EU regulation will impact the global AI market. 2022. URL: <https://arxiv.org/pdf/2208.12645> (дата звернення: 29.07.2024).
5. Svantesson D. The European Union Artificial Intelligence Act: Potential implications for Australia. *Alternative Law Journal*. 2022. 47(1). P. 4-9. doi: <https://doi.org/10.1177/1037969X211052339>.
6. Teremetskyi V., Burylo Yu., Zozuliak O., Koshmanov M., Polyova N., Petruk O. Academic integrity in the age of artificial intelligence: world trends and outlook for Ukraine from the legal perspective. *Pakistan Journal of Life and Social Sciences*. 2024. 22(1). P. 2020-2029. doi: <https://doi.org/10.57239/PJLSS-2024-22.1.00147>.
7. Cefaliello A., Kullmann M. Offering false security: How the draft artificial intelligence act undermines fundamental workers' rights. *European Labour Law Journal*. 2022. 13(4). P. 542-562. doi: <https://doi.org/10.1177/20319525221114474>.
8. Gilbert S. The EU passes the AI Act and its implications for digital medicine are unclear. *npj Digit. Med.* 2024. 7. P. 135. doi: <https://doi.org/10.1038/s41746-024-01116-6>.

9. Mazur J., Włoch R. Embedding digital economy: Fictitious triple movement in the European Union's Artificial Intelligence Act. *Social & Legal Studies*. 2024. 33(1). P. 104-123. doi: <https://doi.org/10.1177/09646639231152866>.

10. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (дата звернення: 29.07.2024).

11. EU data protection rules. URL: https://commission.europa.eu/law/law-topic/data-protection/eu-data-protection-rules_en#library (дата звернення: 29.07.2024).

12. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj> (дата звернення: 29.07.2024).

13. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1925> (дата звернення: 29.07.2024).

14. Explanatory memorandum on the updated OECD definition of an AI system. URL: https://www.oecd-ilibrary.org/science-and-technology/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_623da898-en (дата звернення: 29.07.2024).

15. Консолідовані версії Договору про ЄС та Договору про функціонування ЄС з протоколами та деклараціями. URL:

https://zakon.rada.gov.ua/laws/show/994_b06#Text (дата звернення: 29.07.2024).

16. EU's AI law needs major changes to prevent discrimination and mass surveillance. URL: <https://edri.org/our-work/eus-ai-law-needs-major-changes-to-prevent-discrimination-and-mass-surveillance/> (дата звернення: 29.07.2024).

17. European AI Office. URL: <https://digital-strategy.ec.europa.eu/en/policies/ai-office> (дата звернення: 29.07.2024).

18. Renda A., Arroyo J., Fanni R., Laurer M., Sipiczki A., Yeung T., Maridis G., Fernandes M., Endrodi G., Milio S. Study to support an impact assessment of regulatory requirements for artificial intelligence in Europe. 2021. URL: <https://op.europa.eu/en/publication-detail/-/publication/55538b70-a638-11eb-9585-01aa75ed71a1/language-en/format-PDF/source-204305195> (дата звернення: 29.07.2024).

19. Open letter to the representatives of the European Commission, the European Council and the European Parliament. URL: <https://drive.google.com/file/d/1wrtxfvcD9FwfNfWGDL37Q6Nd8wBKXCkn/view> (дата звернення: 29.07.2024).

References

1. Pavlidis, G. (2024). Unlocking the black box: analysing the EU artificial intelligence act's framework for explainability in AI. *Law, Innovation and Technology*, 16(1), 293-308. doi: <https://doi.org/10.1080/17579961.2024.2313795>.

2. Enqvist, L. (2023). «Human oversight» in the EU artificial intelligence act: what, when and by whom? *Law, Innovation and Technology*, 15(2), 508-535. doi: <https://doi.org/10.1080/17579961.2023.2245683>.

3. Kalodanis, K., Rizomiliotis, P., & Anagnostopoulos, D. (2024). European Artificial Intelligence Act: an AI security approach. *Information and*

Computer Security, 32(3), 265-281. doi: <https://doi.org/10.1108/ICS-10-2022-0165>

4. Siegmännand Ch., & Anderljung, M. (2022). The Brussels Effect and Artificial Intelligence: How EU regulation will impact the global AI market. URL: <https://arxiv.org/pdf/2208.12645>.

5. Svantesson, D. (2022). The European Union Artificial Intelligence Act: Potential implications for Australia. *Alternative Law Journal*, 47(1), 4-9. doi: <https://doi.org/10.1177/1037969X211052339>.

6. Teremetskyi, V., Burylo, Yu., Zozuliak, O., Koshmanov, M., Polyova, N., & Petruk, O. (2024). Academic integrity in the age of artificial intelligence: world trends and outlook for Ukraine from the legal perspective. *Pakistan Journal of Life and Social Sciences*, 22(1), 2020-2029. doi: <https://doi.org/10.57239/PJLSS-2024-22.1.00147>.

7. Cefaliello, A., & Kullmann, M. (2022). Offering false security: How the draft artificial intelligence act undermines fundamental workers' rights. *European Labour Law Journal*, 13(4), 542-562. <https://doi.org/10.1177/20319525221114474>

8. Gilbert, S. (2024). The EU passes the AI Act and its implications for digital medicine are unclear. *npj Digit. Med.*, 7, 135. doi: <https://doi.org/10.1038/s41746-024-01116-6>.

9. Mazur, J., & Włoch, R. (2024). Embedding digital economy: Fictitious triple movement in the European Union's Artificial Intelligence Act. *Social & Legal Studies*, 33(1), 104-123. doi: <https://doi.org/10.1177/09646639231152866>

10. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.

11. EU data protection rules. URL: https://commission.europa.eu/law/law-topic/data-protection/eu-data-protection-rules_en#library.

12. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>.

13. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1925>.

14. Explanatory memorandum on the updated OECD definition of an AI system. URL: https://www.oecd-ilibrary.org/science-and-technology/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_623da898-en.

15. Konsolidovani versii Dohovoru pro YeS ta Dohovoru pro funktsionuvannia YeS z protokolamy ta deklaratsiiamy. URL: https://zakon.rada.gov.ua/laws/show/994_b06#Text [in Ukrainian].

16. EU's AI law needs major changes to prevent discrimination and mass surveillance. URL: <https://edri.org/our-work/eus-ai-law-needs-major-changes-to-prevent-discrimination-and-mass-surveillance/>.

17. European AI Office. URL: <https://digital-strategy.ec.europa.eu/en/policies/ai-office>.

18. Renda, A., Arroyo, J., Fanni, R., Laurer, M., Sipiczki, A., Yeung, T., Maridis, G., Fernandes, M., Endrodi, G., & Milio, S. (2021). Study to support an impact assessment of regulatory requirements for artificial intelligence in Europe. URL: <https://op.europa.eu/en/publication-detail/-/publication/55538b70-a638-11eb-9585-01aa75ed71a1/language-en/format-PDF/source-204305195>.

19. Open letter to the representatives of the European Commission, the European Council and the European Parliament. URL:

<https://drive.google.com/file/d/1wrtxfvcD9FwfNfWGDL37Q6Nd8wBKXCkn/view>.