https://doi.org/10.26565/2075-1834-2025-40-12
УДК 340.5:004.8]:341.17(4-675ЄС)]

ГУРА М. В.
кандидат юридичних наук,
старший викладач кафедри цивільно-правових дисциплін
E-mail: m.gura@karazin.ua ORCID: https://orcid.org/0000-0002-7695-7672
Харківський національний університет імені В.Н. Каразіна
м. Харків, 61022, майдан Свободи, 4

АДАПТАЦІЯ ЗАКОНОДАВСТВА УКРАЇНИ ДО НОРМ EU ARTIFICIAL INTELLIGENCE ACT: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

АННОТАЦІЯ. *Вступ.* У статті проведено аналіз процесу адаптації законодавства України до норм Регламенту (ЄС) 2024/1689. Метою дослідження є ідентифікація ключових викликів, що постають перед українською правовою системою на шляху імплементації цього акта, та розробка пропозицій щодо напрямів гармонізації. Методологічну основу дослідження становлять загальнонаукові та спеціальні методи пізнання, зокрема порівняльно-правовий, системно-структурний, формально-догматичний та метод прогнозування.

Короткий зміст. Автором досліджено ключові принципи та структуру AI Act, з акцентом на ризик-орієнтованому підході, що класифікує системи штучного інтелекту за рівнями ризику. Проведено аудит поточного стану правового регулювання ШІ в Україні, який виявив його фрагментарний характер та відсутність комплексного, що створює нормативну невідповідність законодавству ЄС. Наукова новизна дослідження полягає у систематизації викликів для України, які класифіковано на чотири групи: нормотворчі, інституційні, технікоюридичні та економічні.

Висновки. Обґрунтовано, що інституційний виклик, пов'язаний із відсутністю компетентного національного наглядового органу, є ключовим. Автором запропоновано дорожню карту адаптації, що передбачає поетапний підхід.

КЛЮЧОВІ СЛОВА: *штучний інтелект, EU AI Act, правове регулювання, ризик-орієнтований підхід, адаптація законодавства, цифрова євроінтеграція, гармонізація права.*

Як цитувати: Гура М. В. Адаптація законодавства України до норм EU artificial intelligence act: виклики та перспективи. *Вісник Харківського національного університету імені В. Н. Каразіна, серія «Право».* 2025. Вип. 40. С.119-128 https://doi.org/10.26565/2075-1834-2025-40-12

In cites: M.V.Hura (2025). Adaptation of Ukrainian legislation to the norms of the EU artificial intelligence act: challenges and prospects. *The Journal of V.N. Karazin National University, Series "Law"*, (40), P. 119-128 https://doi.org/10.26565/2075-1834-2025-40-12 (in Ukrainian)

Постановка проблеми та її зв'язок із важливими науковими та практичними завданнями. Регламент ЄС 2024/1689 (EU Artificial Intelligence Act) став першою спробою комплексного врегулювання штучного інтелекту. Цей Регламент можна вважати наслідком «ефекту Брюсселя», коли регуляторні стандарти, розроблені Європейським Союзом, отримають глобальне значення, поза межа однієї юрисдикції.

Однак, у наукових колах існує дискусія щодо актуальності цього ефекту в контексті ШІ. А. Бредфорд наголошує, що, як і у випадку з GDPR, величезний ринок ЄС та екстериторіальний принцип дії AI Act змусять компанії з різних країн уніфікувати свої продукти відповідно до європейських стандартів, оскільки підтримувати різні версії продукту для різних ринків економічно невигідно [15, с. 15]. Ч. Сабель та Дж. Цайтлін висувають альтернативну концепцію «експериментального врядування». Вони стверджують, що через фундаментальну невизначеність, пов'язану з розвитком ШІ, AI Act слід розглядати не як остаточний міжнародний стандарт, а як один із багатьох регуляторних експериментів, а різні юрисдикції розглядаються як учасники глобального процесу взаємного моніторингу та навчання, що з часом може призвести до конвергенції на основі найбільш ефективних практик [23, с. 280]. На нашу думку, хоча «ефект Брюсселя» може мати місце, його вплив матиме обмежений та опосередкований характер через активну регуляторну політику інших країн та міжнародних об'єднань. Це робить «експериментальне врядування» більш реалістичною моделлю майбутнього міжнародного регулювання ШІ.

Для України, яка знаходиться на шляху євроінтеграції, адаптація національного законодавства до норм AI Act є не просто бажаною, а обов'язковою умовою. Цей імператив має подвійну природу. По-перше, це необхідність гармонізації національного законодавства з acquis communautaire. По-друге, це економічна необхідність, адже український IT-сектор значною мірою орієнтований на ринок ЄС. Екстериторіальний принцип дії AI Act означає, що будь-яка українська IT-компанія, яка має намір постачати свої AI-рішення на європейський ринок, повинна дотримуватися вимог європейського законодавства, незалежно від стану національного регулювання. Ігнорування цих правил загрожує не лише втратою доступу до європейського ринку, а й фінансовими втратами, що можуть сягати 35 мільйонів євро або 7% від загального світового річного обороту компанії [20].

Перед українською правовою системою постає складне завдання: у стислі терміни та в умовах воєнного стану здійснити масштабну рецепцію інноваційного та комплексного європейського законодавства. Але нормативних змін може бути не достатньо для всебічної імплементації європейських норм, адже необхідн інституційна розбудова та впровадження нових економічних стимулів для українських компаній. Адекватна та швидка реакція українських регуляторів визначатиме не лише майбутнє правового регулювання ШІ в Україні, а й конкурентоспроможність її технологічного сектору у майбутньому.

Аналіз останніх досліджень і публікацій, в яких розглядаються різні аспекти даної проблеми і на які спирається автор. Проблематика правового регулювання ШІ перебуває у фокусі уваги як вітчизняних та зарубіжних науковців. Основним питанням, що стало предметом наукової дискусії є визначення правового статусу ШІ.

Тут можна виокремити дві основні позиції. О. Баранов наголошує, що найбільш прийнятним на сучасному етапі є розгляд ШІ як об'єкта права [1, с. 29]. Такий підхід, на його думку, дозволяє уникнути надмірної теоретизації та вирішити практичне питання відповідальності за шкоду, завдану діями ШІ, покладаючи її на людських агентів – розробників, власників чи операторів системи. Інші дослідники висловлюють протилежну думку, пропонуючи наділити «сильний» ШІ спеціальним правовим статусом «електронної особи» [10, с. 68]. Ця концепція актуалізує проблему відповідальності автономних систем, які здатні приймати рішення без прямого втручання людини.

На нашу думку, хоча концепція «електронної особи» наразі є передчасною, визначення ШІ лише як пасивного об'єкта не враховує його унікальних властивостей, зокрема здатності до самонавчання та автономії. Важливо зауважити, що європейський законодавець в AI Act уникнув цього філософсько-правового питання та зосередив увагу на регулюванні ШІ як продукту та покладанні чітких обов'язків на його провайдерів та користувачів [9, с. 147]. Аналізуючи стан національного законодавства у сфері регулювання ШІ, О. Турецька та Т. Яворська, доходять висновку про його фрагментарність та недостатність [7, с. 13]. Дослідники наголошують на відсутності узгодженої нормативної бази та стандартів, що створює правову невизначеність [12; 13; 19].

Попри наявність наукових праць, в яких досліджуються окремі аспекти правового статусу ШІ та виклики його регулювання, на сьогодні відсутнє комплексне дослідження, яке б системно аналізувало виклики та перспективи адаптації законодавства України до специфічної, ризик-орієнтованої моделі, запропонованої в EU AI Act. Залишаються недостатньо дослідженими питання інституційного забезпечення імплементації, техніко-юридичні аспекти розробки стандартів та економічний вплив нового регулювання на український IT-ринок.

Формулювання мети статті (постановка завдання). Метою даного дослідження є ідентифікація головних нормативних, інституційних, техніко-юридичних та економічних викликів для правової системи України в процесі його імплементації та розробка обґрунтованих пропозицій щодо шляхів адаптації національного законодавства.

Виклад основного матеріалу. *Ризик-орієнтований підхід та структура EU AI Act.*

В основі архітектури AI Act лежить ризик-орієнтований підхід (risk-based approach), що є спробою знайти пропорційний баланс між стимулюванням інновацій та захистом фундаментальних прав, здоров'я та безпеки громадян [17, с. 2-4]. Замість позитивістського регулювання ШІ, європейський нормотворець диференціював вимоги залежно від рівня потенційної шкоди, яку може завдати та чи інша AI-система. Цей підхід відображається у чотирирівневій «піраміді ризиків».

Хоча ризик-орієнтований підхід отримав широке схвалення як прагматична та пропорційна модель регулювання, він не уникнув і гострої наукової критики. М. Еберс стверджує, що, попри декларації, AI Act не завжди дотримується справді ризик-орієнтованого підходу

[17, с. 10]. На його думку, у Регламенті часто відбувається категоризація за сферами застосування (наприклад, Додаток ІІІ), а індивідуальна оцінка ризику конкретної системи, що може призводити до надмірного або недостатнього регулювання [17, с. 10]. А. Барічелла наголошує на недостатній гнучкості такого статичного підходу до класифікації ризиків в умовах стрімкого технологічного розвитку, що може призвести до «регуляторного застаріванння» [14, с. 4].

На наш погляд, більш обґрунтованою є позиція, що ризик-орієнтований підхід є концептуально правильною відправною точкою, однак його ефективність буде залежати від гнучкості механізмів імплементації, зокрема від здатності регуляторів швидко переглядати списки систем високого ризику та адаптувати вимоги до нових технологічних реалій.

Системи ШІ розмежовуються в залежності від рівню потенційного ризику: неприйнятний, високий, обмежений та мінімальний ризик.

Неприйнятний ризик визначається для систем ШІ які становлять настільки очевидну загрозу для основоположних цінностей ЄС та прав людини, що підлягають повній забороні (Стаття 5 Регламенту). До них належать, зокрема:

1) системи, що використовують підсвідомі, маніпулятивні чи обманні техніки для спотворення поведінки людини, завдаючи їй значної шкоди;

2) системи, що експлуатують вразливості певних груп осіб (наприклад, дітей чи людей з інвалідністю);

3) системи соціального скорингу (social scoring), що використовуються державними органами для оцінки надійності громадян;

4) системи віддаленої біометричної ідентифікації в режимі реального часу в публічних місцях з правоохоронною метою (за деякими суворо визначеними винятками) [22, ст. 5].

Високий ризик становлять системи ШІ, використання яких може створити значні ризики для здоров'я, безпеки або фундаментальних прав людини. Стаття 6 та Додаток ІІІ Регламенту відносять до цієї категорії дві групи систем:

1) системи, що є компонентами безпеки продуктів, які підпадають під дію іншого секторального законодавства ЄС (наприклад, медичні вироби, іграшки, автомобілі, ліфти та ін.).

2) системи у восьми специфічних сферах, зокрема: біометрична ідентифікація та категоризація фізичних осіб; управління критичною інфраструктурою; освіта та професійна підготовка; працевлаштування та управління персоналом; доступ до основних приватних та публічних послуг (включно з кредитним скорингом); правоохоронна діяльність; управління міграцією та прикордонний контроль; відправлення правосуддя та демократичні процеси [22, ст. 6].

До провайдерів таких систем висуваються суворі вимоги:

1) система управління ризиками: обов'язок впровадити та підтримувати безперервний процес ідентифікації, оцінки та мінімізації ризиків протягом усього життєвого циклу системи [22, ст. 9];

2) управління даними: вимоги до якості, релевантності та репрезентативності наборів даних, що використовуються для тренування, валідації та тестування, з метою запобігання дискримінаційним упередженням (bias) [22, ст. 10];

3) технічна документація: обов'язок створювати та постійно оновлювати детальну документацію, що демонструє відповідність системи ШІ всім вимогам Регламенту [22, ст. 11];

4) ведення записів: системи повинні мати можливість автоматично реєструвати події (вести логи) для відстежування їх функціонування [22, ст. 12];

5) прозорість та надання інформації: користувачі мають бути забезпечені чіткою та зрозумілою інформацією про можливості, обмеження та правильне використання системи ШІ [22, ст. 13];

6) людський нагляд: системи мають бути розроблені таким чином, щоб забезпечити можливість ефективного контролю з боку людини, включно з можливістю втручання або його повної зупинки [22, ст. 14];

7) точність, надійність та кібербезпека: системи повинні досягати належного рівня продуктивності та бути стійкими до помилок і спроб зловмисного втручання [22, ст. 15].

Обмежений ризик охоплює системи ШІ, які несуть переважно ризики, пов'язані з прозорістю. До них застосовуються специфічні зобов'язання щодо інформування. Наприклад, користувачі чат-ботів повинні знати, що вони спілкуються з машиною, а контент, згенерований ШІ, має бути відповідно позначений.

Переважна більшість систем ШІ, що використовуються сьогодні в ЄС (спам-фільтри, рекомендаційні системи, ШІ у відеоіграх), належать до категорії «мінімального ризику» і не підпадають під дію жорстких регуляторних вимог. Для них Регламент заохочує добровіль-

не прийняття кодексів поведінки [12].

Для забезпечення однакового застосування Регламенту на всій території ЄС створюється нова інституційна архітектура, ключовими елементами якої є Європейський офіс зі штучного інтелекту (European AI Office) та Європейська рада зі штучного інтелекту (European Artificial Intelligence Board), що складається з представників національних наглядових органів.

Правове поле для ШІ в Україні.

На відміну від комплексного та проактивного підходу ЄС, поточний стан правового регулювання сфери ШІ в Україні можна охарактеризувати як фрагментарний, реактивний та переважно декларативний.

Ключовим стратегічним документом в цьому напрямку є Концепція розвитку штучного інтелекту в Україні, схвалена Розпорядженням Кабінету Міністрів України від 2 грудня 2020 року № 1556-р [6; 8].

Цей документ був необхідним кроком, адже він вперше на урядовому рівні визначив пріоритети та окреслив основні виклики, що потребують вирішення. Серед них – «відсутність або недосконаліть правового регулювання штучного інтелекту», «недостатній рівень інформаційної безпеки» та «складність перевірки відповідності роботи систем штучного інтелекту законодавству та етичним принципам» [6; 8]. Однак, за своєю правовою природою, Концепція є документом політичного планування і не містить норм прямої дії, залишаючи відкритим питання про механізми її реалізації.

Спеціальне законодавство, яке б комплексно врегулювало розробку, впровадження та використання систем ШІ, наразі відсутнє в Україні.

Окремі аспекти опосередковано охоплюються чинними нормативно-правовими актами, зокрема, ЗУ «Про захист персональних даних», ЗУ «Про основні засади забезпечення кібербезпеки України» та ЗУ «Про електронні комунікації». Проте зазначені закони не враховують особливостей, пов’язаних з технологіями ШІ.

Певним кроком на шляху до гармонізації українського та європейського законодавства у сфері ШІ є законопроєкт № 8153 «Про захист персональних даних», який має на меті імплементацію норм GDPR, зокрема щодо автоматизованого прийняття рішень [3]. Показовими є спроби галузевого регулювання, зокрема, законопроєкт № 10392 про академічну доброчесність, в якому передбачено відповідальність за використання ШІ при написанні наукових робіт [5].

Врегулювання окремих, найбільш актуальних проявів використання нової технології, є характерним для початкових етапів регламентації нового явища або суспільних відносин. Проте, це принципово відрізняється від комплексної, ризик-орієнтованої позиції відображеній в EU AI Act. Таким чином, можна підтвердити наявність істотної нормативної та концептуальної прогалини, яка потребує якнайшвидшого заповнення.

Ця ситуація не є унікальною для України та відображає загальносвітовий виклик, що постає перед правовими системами в епоху цифрової трансформації.

Цифрові інновації, зокрема технології штучного інтелекту та Big Data, спричиняють фундаментальну зміну в системі створення, передачі та зберігання документів, що, своєю чергою, трансформує саму природу правових відносин [25, с. 175]. Водночас, аналізуючи досвід інших країн, науковці доходять висновку, що наявні законодавчі рамки часто виявляються неготовими до забезпечення належного захисту даних та кібербезпеки в умовах, що стрімко змінюються [16, с. 268].

Українська проблема фрагментарності нормативного регулювання ШІ є проявом глобального «розриву» між швидкими темпами технологічного розвитку та реактивністю правових інститутів, що підкреслює необхідність швидкої розробки та впровадження адаптивного законодавства у сфері регулювання ШІ.

Імплементація AI Act є складним завданням, що зумовлює для України низку викликів, які можна об’єднати у чотири категорії.

1. Нормотворчі виклики. Масштаб необхідних законодавчих змін потребує переосмислення значної частини чинного законодавства. Недостатньо розробити та впровадити спеціальний закон «Про штучний інтелект», який би відтворював структуру та основні положення європейського Регламенту.

Необхідно провести комплексний аналіз та внести зміни до чинних нормативних актів у сферах захисту прав споживачів, технічного регулювання, оцінки відповідності, цивільної та кримінальної відповідальності, щоб забезпечити їх узгодженість та уникнути правових колізій.

2. Інституційні виклики. Ефективне функціонування моделі, закладеної в AI Act, неможливе без розгалуженої та компетентної інституційної інфраструктури, яка включає створення національних наглядових та нотифікованих органів з оцінки відповідності. В Ук-

раїні на сьогодні відсутній єдиний державний орган, який би мав мандат, ресурси та технічну експертизу для виконання функцій нагляду за ринком систем ШІ, проведення розслідувань, накладення санкцій та сертифікації систем високого ризику [24].

Створення такого органу є предметом чисельних обговорень. Прихильники «м'якого», бізнес-орієнтованого формату, що знаходить підтримку в Міністерстві цифрової трансформації, наголошують на пріоритеті саморегуляції та уникненні надмірного тиску на ІТ-сектор на початкових етапах [27].

Ця модель передбачає поступовий перехід від добровільних інструментів до обов'язкових стандартів. Водночас, представники правозахисних організацій та частина експертної спільноти висловлюють занепокоєння, що такий підхід може призвести до недостатнього захисту прав громадян [26]. Вони наголошують на доцільності створення незалежного та централізованого регулятора з чіткими повноваженнями з самого початку, за аналогією з антикорупційними чи антимонопольними органами, щоб уникнути «захоплення» регулятора галузевими інтересами.

На нашу думку, оптимальним є компромісний варіант: створення єдиного координаційного та наглядового органу з поетапним збфльшенням його повноважень (від моніторингу, надання рекомендацій та управління «регуляторними пісочницями», і до поступово переходу до функцій ринкового нагляду та правозастосування).

3. Техніко-юридичні виклики. AI Act встановлює низку високотехнологічних вимог, проте залишає деталізацію їх реалізації на рівень гармонізованих європейських стандартів. Для України це означає необхідність розробки або адаптації національних стандартів (ДСТУ), методологій оцінки ризиків та процедур аудиту відповідності. Це завдання ускладнюється гострим дефіцитом кваліфікованих фахівців на перетині права, етики та комп'ютерних наук, здатних проводити такий складний технічний аудит.

Ініціатива Міністерства цифрової трансформації щодо розробки відповідної методології є кроком у правильному напрямку, але її масштабування на всю країну залишається серйозним викликом [4].

У цьому контексті виникає наукова дискусія щодо першочерговості викликів. З одного боку, вважається, що ключовим завданням є саме узгодження технологічного прогресу з міжнародними правовими стандартами та практиками кібербезпеки, особливо в частині функціонування електронного документообігу, який є аналогом вимог AI Act до технічної документації та ведення записів [25, с. 174]. Цей підхід пріоритезує розробку досконалих технічних та правових норм.

З іншого боку, Е. Ксіхо та співавтори висувають тезу про те, що навіть ідеально розроблені стандарти залишаться «мертвими» без належної інституційної спроможності для їх впровадження та контролю, пропонуючи як рішення створення національного центру кібербезпеки [16, с. 269]. На наш погляд, ці два підходи не суперечать, а доповнюють один одного.

Ефективна імплементація AI Act в Україні неможлива ані без розробки деталізованих національних стандартів, ані без створення компетентного органу, здатного забезпечити їх дотримання. Це дві невід'ємні складові єдиного процесу.

4. Економічні виклики. Імплементація AI Act неминуче може створити фінансове та адміністративне навантаження на бізнес. Це питання є центральним у дискусії між регуляторами та ІТ-компаніями.

Представники європейських стартапів та венчурних інвесторів висловлювали занепокоєння, що жорсткі вимоги можуть «задушити інновації», підвищити вартість розробки та зробити європейські компанії неконкурентоспроможними у порівнянні з американськими та китайськими [18; 26]. Дослідження, проведене appliedAI, показало, що 50% AI-стартапів вважають, що AI Act значно сповільнить інновації в Європі.

Проте, прихильники регулювання, вважають, що впровадження чітких та узгоджених норм збільшать довіру споживачів та бізнесу до технологій ШІ, що в середньостроковій перспективі стимулюватиме їх впровадження та інвестиції, а правова визначеність є не бар'єром, а передумовою для сталого розвитку ринку [21, с. 5]. На наш погляд, обидві позиції мають раціональне підґрунтя.

Але, ризик сповільнення інновацій є реальним, особливо для малих та середніх підприємств. З огляду на зазначене, ключовим завданням для України є не копіювання, а розумна адаптація, що передбачає створення спеціальних механізмів підтримки для стартапів, використання «регуляторних пісочниць» та диференційований підхід до накладення санкцій, як це передбачено в AI Act.

Для демонстрації нормативної неузгодженості між нормами AI Act та українським законодавством, доцільно навести порівняльну таблицю.

Таблиця 1. Порівняльний аналіз ключових вимог до систем ШІ високого ризику.
Table 1. Comparative analysis of key requirements for high-risk AI systems

Вимога EU AI Act (Статті 9-15)	Наявність аналогічної норми в законодавстві України	Прогалини та невідповідності
Система управління ризиками (ст. 9)	Відсутня	Немає системної вимоги до розробників проводити та документувати оцінку ризиків для фундаментальних прав протягом життєвого циклу системи.
Управління даними та якість даних (ст. 10)	Частково в ЗУ «Про захист персональних даних»	Чинні норми стосуються персональних даних, але не охоплюють вимоги до репрезентативності, повноти та відсутності помилок у тренувальних та тестових датасетах для уникнення упередженості.
Технічна документація (ст. 11)	Відсутня	Немає обов'язку створювати та підтримувати детальну технічну документацію, що демонструє відповідність системи ШІ вимогам безпеки та прозорості.
Ведення журналів (ст. 12)	Відсутня	Немає вимоги до систем високого ризику автоматично генерувати логи для забезпечення відстежуваності операцій.
Прозорість та надання інформації (ст. 13)	Відсутня	Відсутні чіткі зобов'язання надавати користувачам детальну інформацію про можливості, обмеження та призначення системи ШІ.
Людський нагляд (ст. 14)	Відсутня	Законодавство не встановлює конкретних вимог до проєктування систем для забезпечення ефективного людського контролю, включаючи можливість втручання та зупинки.
Точність, надійність, кібербезпека (ст. 15)	Частково в ЗУ «Про основні засади забезпечення кібербезпеки України»	Існують загальні вимоги до кібербезпеки, але відсутні специфічні норми щодо надійності та точності саме для систем ШІ.

Перспективи та стратегічні напрями адаптації. Оптимальним шляхом для України є поетапний підхід, що поєднує інструменти «м'якого» та «жорсткого» права, як це, зокрема, передбачено Дорожньою картою з регулювання ШІ в Україні, розробленою Міністерством цифрової трансформації.Складність полягає в тому, що ефективній імплементації «жорсткого права» у вигляді обов'язкового до виконання закону має передувати етап активного

застосування інструментів «м'якого права». Такий порядок дозволить підготувати ринок, розбудувати інституційну спроможність та накопичити необхідну експертизу, мінімізуючи регуляторний шок для економіки.На першому (підготовчому) етапі адаптації ключову роль мають відіграти два інструменти: «регуляторні пісочниці» та розробка та поширення добровільних стандартів і методологій. «Регуляторні пісочниці», створення спеціальних правових режимів для інноваційних проєктів у сфері ШІ, є однією з найбільш перспективних ідей, прямо передбачених AI Act [22, ст. 57]. «Регуляторна пісочниця» – це контрольоване середовище, в якому компанії (передусім стартапи) можуть тестувати свої продукти на відповідність майбутнім вимогам законодавства під наглядом та за методичної підтримки регулятора [2]. Це дозволяє стимулювати інновації, розвивати культуру «відповідності через проєктування» та накопичувати практичний досвід для бізнесу і майбутнього наглядового органу.Другий інструмент - розробка та поширення добровільних стандартів і методологій. Необхідно активно підтримати роботу Міністерства цифрової трансформації щодо розробки національної методології оцінки ризиків систем ШІ, адаптуючи найкращі європейські практики, зокрема методологію HUDERIA [11, с. 157]. Паралельно слід заохочувати бізнес до добровільного прийняття кодексів поведінки та галузевих стандартів.Після завершення підготовчого етапу, слід розпочати повноцінну імплементацію норм AI Act. Це потребує наступних кроків: 1) створення міжвідомчої робочої групи за участі представників Міністерства цифрової трансформації, Міністерства юстиції, профільних комітетів Верховної Ради України, наукової спільноти та асоціацій ІТ-бізнесу для розробки проєкту рамкового закону про ШІ; 2) пріоритетне вирішення інституційного питання та а розробка законопроєкту, яка має йти паралельно з визначенням моделі, повноважень та джерел фінансування Національного наглядового органу у сфері ШІ; 3) забезпечення широкого публічного обговорення законопроєкту для досягнення суспільного консенсусу та збалансування інтересів усіх стейкхолдерів; 4) поетапне введення в дію норм закону, починаючи з регулювання систем високого ризику, щоб надати бізнесу достатньо часу для адаптації.

Висновки. Адаптація законодавства України до норм EU Artificial Intelligence Act є складним, багатовимірним, але безальтернативним процесом, що відповідає стратегічному курсу держави на європейську інтеграцію. Проведене дослідження дозволяє зробити висновок, що цей процес генерує для української правової системи низку викликів: нормотворчих, інституційних, техніко-юридичних та економічних. Найбільш критичним серед них є інституційний, що обумовлюється відсутністю в Україні компетентного наглядового органу, здатного забезпечити ефективне виконання майбутнього законодавства. Водночас, ці виклики створюють унікальну можливість для побудови в Україні сучасної, гнучкої та ефективної системи правового регулювання ШІ, що відповідатиме найкращим європейським стандартам. В цьому контексті доцільно відмовитись від поспішної та механічної рецепції європейських норм на користь поміркованої, поетапної стратегії. Новизна даного дослідження полягає у систематизації викликів гармонізації українського законодавства з EU AI Act за чотирма ключовими напрямами та запропоновано дорожню карту адаптації, яка ґрунтується на прагматичному підході, що передбачає використання інструментів «м'якого права» (зокрема «регуляторних пісочниць») на підготовчому етапі для мінімізації ризиків та розбудови інституційної спроможності перед повноцінним впровадженням «жорсткої» нормативної регламентації.

Перспективи подальших наукових досліджень у цьому напрямі вбачаються у поглибленому дослідженні окремих аспектів імплементації, зокрема: розробці детальної моделі функціонування національного наглядового органу; аналізі питань цивільно-правової відповідальності за шкоду, завдану системами ШІ, в контексті проєкту європейської Директиви про відповідальність у сфері ШІ; а також у дослідженні довгострокових правових наслідків розвитку автономних систем та їх потенційного впливу на доктрину правосуб'єктності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1.Баранов О. А. Особливості визначення правового статусу робота із штучним інтелектом. *Інформація і право.* 2023. № 4 (47). С. 40–54. DOI: https://doi.org/10.37750/2616-6798.2023.4(47).291581 (дата звернення: 15.10.2025).

2.Варинський В. О. Правосуб'єктність штучного інтелекту: критичний погляд на автономність. *Інформація і право.* 2024. № 4 (51). С. 83–94. DOI: https://doi.org/10.37750/2616-6798.2024.4(51).317919 (дата звернення: 15.10.2025).

3.В Україні анонсували запуск «регуляторної пісочниці» для розробників штучного інтелекту. *Bazilik Media*. URL: https://bazilik.media/v-ukraini-anonsuvaly-zapusk-rehuliatornoi-pisochnytsi-dlia-rozrobnykiv-shtuchnoho-intelektu/ (дата звернення: 15.10.2025).

4.Захист персональних даних і ШІ: Законопроєкт №8153, GDPR та Закон ЄС про ШІ у контексті технологій штучного інтелекту. *Центр Дністрянського*. URL: https://dc.org.ua/news/zahyst-personalnyh-danyh-i-shi-zakonoproekt-8153-gdpr-ta-zakon-es-pro-shi-u-konteksti-tehnologiy-shtuchnogo-intelektu (дата звернення: 15.10.2025).

5.Майбутнє регулювання штучного інтелекту в Україні: аналіз Білої книги з регулювання ШІ. *Центр Дністрянського*. URL: https://dc.org.ua/news/maybutne-regulyuvannya-shtuchnogo-intelektu-v-ukrayini-analiz-biloyi-knygy-z-regulyuvannya-shi (дата звернення: 15.10.2025).

6.Новий законопроєкт про використання штучного інтелекту в навчальних закладах. *Українська студентська ліга*. URL: https://www.usl.org.ua/usl-news/noviy-zakonoproekt-pro-vikoristannya-shtuchnogo-intelektu-v-navchalnih-zakladah (дата звернення: 15.10.2025).

7.Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядж. Каб. Міністрів України від 02.12.2020 № 1556-р : станом на 29 груд. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р#Text (дата звернення: 16.10.2025).

8.Турецька О. В., Яворська Т. М. Стан нормативно-правового регулювання штучного інтелекту в Україні та світі. *Вісник студентського наукового товариства ДонНУ імені Василя Стуса*. 2025. № 17 (1). С. 215–219. URL: https://jvestnik-sss.donnu.edu.ua/article/view/17334 (дата звернення: 18.10.2025)

9.Уряд затвердив Концепцію розвитку штучного інтелекту в Україні. *Лабораторія цифрової безпеки*. 2020. URL: https://dslua.org/publications/uriad-zatverdyv-kontseptsiiu-rozvytku-shtuchnoho-intelektu-v-ukraini-z-urakhuvanniam-propozytsiy-tsyfrolaby/ (дата звернення: 15.10.2025).

10. Харитонов Є., Харитонова О. ШІ як бінарна категорія ІТ. *ІТ-право під час гібридної війни: від пошуку парадигми до прагматичних рішень : кол. монографія* / за заг. ред. Є. Харитонова, О. Харитонової, І. Давидової. – Одеса : Фенікс, 2025. – С. 93–118. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/c56cc38a-029c-457e-9732-20efe8ff1d6b/content (дата звернення: 18.10.2025)

11. Яновицька Г. Б. Гармонізація процесів нормативного регулювання використання штучного інтелекту в Україні та інших країнах Європи. *Наукові інновації та передові технології*. 2024. № 4 (32). С. 593–602. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/7950 (дата звернення: 18.10.2025)

12. AI Act Explorer. *Artificialintelligenceact.eu*. URL: https://artificialintelligenceact.eu/ai-act-explorer/ (дата звернення: 15.10.2025).

13. AI governance: EU and US converge on risk-based approach amid stark differences. *Hertie School*. URL: https://www.hertie-school.org/en/digital-governance/research/blog/detail/content/ai-governance-eu-and-us-converge-on-risk-based-approach-amid-stark-differences (дата звернення: 15.10.2025).

14. Barichella A. Regulating artificial intelligence at the EU level: obstacles and prospects. *Jacques Delors Institute*. 2023. 12 p. URL: https://institutdelors.eu/content/uploads/2025/04/PP294_Regulation_IA_Barichella_EN.pdf (дата звернення: 18.10.2025).

15. Bradford A. The Brussels Effect: How the European Union Rules the World. Oxford : Oxford University Press, 2020. 424 p. URL: https://academic.oup.com/book/36491/chapter-abstract/321182245 (дата звернення: 18.10.2025).

16. Digital Transformation in the Legal Sector: Challenges and Opportunities for Cybersecurity and Data Protection / E. Xhixho et al. *Law, State and Telecommunications Review*. 2025. Vol. 17, no. 1. P. 250–271. DOI: doi.org/10.26512/lstr.v17i1.56176 (дата звернення: 18.10.2025).

17. Ebers M. Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act. *European Journal of Risk Regulation*. 2024. No. 16 (2). P. 684–703. DOI: doi.org/10.1017/err.2024.78 (дата звернення: 18.10.2025).

18. EU AI Act takes effect, and startups push back. Here's what you need to know. *Vestbee*. 2025. URL: https://www.vestbee.com/insights/articles/eu-ai-act-takes-effect-what-you-need-to-know (дата звернення: 15.10.2025).

19. EU AI Act: first regulation on artificial intelligence. *European Parliament*. URL: (https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence) (дата звернення: 15.10.2025).

20. How the EU AI Act affects US-based companies. *KPMG*. 2024. URL: https://kpmg.com/us/en/articles/2024/how-eu-ai-act-affects-us-based-companies.html (дата звернення: 15.10.2025).

21. 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). *Official Journal of the European Union*. L, 2024/1689.

22. Sabel C., Zeitlin J. Learning from Difference: The New Architecture of Experimentalist Governance in the EU. *European Law Journal*. 2008. Vol. 14(3). P. 271–327.

23. Safeguarding human rights in the sphere of AI in Ukraine. *ECNL*. URL: https://ecnl.org/impact-story/safeguarding-human-rights-sphere-ai-ukraine (дата звернення: 15.10.2025).

24. The transformation of legal frameworks through secure digitisation / V. Savchenko et al. *African journal of applied research*. 2025. Vol. 11, no. 1. P. 173–193. DOI: https://doi.org/10.26437/ajar.v11i1.835 (дата звернення: 15.10.2025).

25. Threat to innovation? Survey of European start-ups on the EU AI Act. *appliedAI Initiative GmbH.* 2023. URL: https://www.unternehmertum.de/en/topics/ai/threat-to-innovationsurvey-european-start-ups-on-eu-ai-act (дата звернення: 15.10.2025).

26. Ukraine's AI road map seeks to balance innovation and security. *Atlantic Council*. URL: https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-ai-road-map-seeks-to-balance-innovation-and-security/ (дата звернення: 15.10.2025).

27. Veale M., Borgesius F. Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*. 2021. Vol. 22(4). P. 97–112. DOI: https://doi.org/10.48550/arXiv.2107.03721 (дата звернення: 15.10.2025).

Стаття надійшла до редакції 06.10.2025 Переглянуто 09.11.2025.
Стаття рекомендована до друку 24.11.2025 Опубліковано 30.12.2025

M. V. HURA
PhD in Law,
Senior Lecturer of the Department of Civil Law Disciplines,
E-mail: m.gura@karazin.ua , ORCID: https://orcid.org/0000-0002-7695-7672
V.N. Karazin Kharkiv National University
Kharkiv, 61022, Svobody square, 4

ADAPTATION OF UKRAINIAN LEGISLATION TO THE NORMS OF THE EU ARTIFICIAL INTELLIGENCE ACT: CHALLENGES AND PROSPECTS

ANNOTATION. *Introduction.* This paper provides a comprehensive analysis of the adaptation process of Ukraine's national legislation to Regulation (EU) 2024/1689, known as the EU Artificial Intelligence Act (AI Act). The study aims to identify the key challenges facing the Ukrainian legal system in implementing this act and to develop grounded proposals for strategic directions of harmonisation. The methodological basis of the work consists of general scientific and special methods of cognition, including comparative-legal, systemic-structural, formal-dogmatic, and forecasting methods.

Summary of the main results of the study. The key principles and structure of the AI Act are examined, emphasising a risk-based approach that classifies artificial intelligence (AI) systems into four risk levels. An audit of the current state of AI legal regulation in Ukraine was conducted, revealing its fragmented nature and the absence of a comprehensive, systemic approach, which creates a significant normative gap with EU legislation. The novelty of the research lies in the systematisation of challenges for Ukraine, which are classified into four groups: normative, institutional, technical-legal, and economic.

Conclusion. It is substantiated that the most critical challenge is institutional, related to the absence of a competent national supervisory authority. For the first time, a comprehensive roadmap for adaptation is proposed, envisioning a phased approach. The research results are of practical importance for legislative bodies, scholars, and representatives of the IT industry.

KEYWORDS: *artificial intelligence, EU AI Act, legal regulation, risk-based approach, adaptation of legislation, digital European integration, harmonisation of law.*

REFERENCES

1. Baranov O. A. (2023). Peculiarities of determining the legal status of an artificial intelligence robot. *Information and law*. № 4 (47). P. 40–54. DOI: https://doi.org/10.37750/2616-6798.2023.4(47).291581 (accessed: 15.10.2025) (in Ukrainian).
2. Varynskyi V. O. (2024). Legal personality of artificial intelligence: a critical view of autonomy. *Information and Law*. № 4 (51). P. 83–94. DOI: https://doi.org/10.37750/2616-6798.2024.4(51).317919. (accessed: 15.10.2025) (in Ukrainian).
3. Ukraine announces the launch of a "regulatory sandbox" for artificial intelligence developers. (2024). *Bazilik Media*. URL: https://bazilik.media/v-ukraini-anonsuvaly-zapusk-rehuliatornoi-pisochnytsi-dlia-rozrobnykiv-shtuchnoho-intelektu/ (accessed: 15.10.2025) (in Ukrainian).
4. Personal data protection and AI: Draft Law No. 8153, GDPR and the EU AI Law in the context of artificial intelligence technologies. (2025). *Dniester Center*. URL: https://dc.org.ua/news/zahyst-personalnyh-danyh-i-shi-zakonoproekt-8153-gdpr-ta-zakon-es-pro-shi-u-konteksti-tehnologiy-shtuchnogo-intelektu (accessed: 15.10.2025) (in Ukrainian).
5. The future of artificial intelligence regulation in Ukraine: analysis of the White Paper on AI regulation. (2024). *Dniester Center*. URL: https://dc.org.ua/news/maybutne-regulyuvannya-shtuchnogo-intelektu-v-ukrayini-analiz-biloyi-knygy-z-regulyuvannya-shi (accessed: 15.10.2025) (in Ukrainian).
6. A new bill on the use of artificial intelligence in educational institutions. (2024). *Ukrainian Student League.* URL: https://www.usl.org.ua/usl-news/noviy-zakonoproekt-pro-vikoristannya-shtuchnogo-intelektu-v-navchalnih-zakladah (accessed: 15.10.2025) (in Ukrainian).
7. On Approval of the Concept of Artificial Intelligence Development in Ukraine: Decree of the Cabinet of Ministers of Ukraine. of Ministers of Ukraine dated 02.12.2020 No. 1556-r: as of December 29. 2021 p. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text (accessed: 16.10.2025) (in Ukrainian).
8. Turetska O. V., Yavorska T. M. (2025). The state of regulatory and legal frameworks for artificial intelligence in Ukraine and worldwide. *Bulletin of the Vasyl Stus DonNU Student Scientific Society*. No. 17 (1). C. 215–219. URL: https://jvestnik-sss.donnu.edu.ua/article/view/17334 (accessed: 18.10.2025) (in Ukrainian).
9. The government approved the Concept of Artificial Intelligence Development in Ukraine. *Digital Security Laboratory.* 2020. URL: https://dslua.org/publications/uriad-zatverdyv-kontseptsiiu-rozvytku-shtuchnoho-intelektu-v-ukraini-z-urakhuvanniam-propozytsiy-tsyfrolaby/ (accessed: 15.10.2025) (in Ukrainian).
10. Kharytonov Ye., Kharytonova O. (2025). AI as a binary category of IT. *In* IT Law During the Hybrid War: From Paradigm Search to Pragmatic Solutions : collective monograph. Ed. by Ye. Kharytonov, O. Kharytonova, I. Davydova. Odesa : Feniks. P. 93–118. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/c56cc38a-029c-457e-9732-20efe8ff1d6b/content (accessed: 18.10.2025) (in Ukrainian).
11. Yanovytska H. (2024). Harmonisation of the processes of regulatory regulation of the use of artificial intelligence in Ukraine and other European countries. *Scientific Innovations and Advanced Technologies*. № 3. C. 156–159. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/7950 (accessed: 18.10.2025) (in Ukrainian).
12. AI Act Explorer. *Artificialintelligenceact.eu*. URL: https://artificialintelligenceact.eu/ai-act-explorer/ (accessed: 15.10.2025).
13. AI governance: EU and US converge on risk-based approach amid stark differences. *Hertie School*. URL: https://www.hertie-school.org/en/digital-governance/research/blog/detail/content/ai-governance-eu-and-us-converge-on-risk-based-

approach-amid-stark-differences (accessed: 15.10.2025).

14. Barichella A. (2023). Regulating artificial intelligence at the EU level: obstacles and prospects. *Jacques Delors Institute*. 2023. 12 p. URL: https://institutdelors.eu/content/uploads/2025/04/PP294_Regulation_IA_Barichella_EN.pdf (accessed: 18.10.2025).

15. Bradford A. The Brussels Effect: How the European Union Rules the World. Oxford : Oxford University Press, 2020. 424 p. URL: https://academic.oup.com/book/36491/chapter-abstract/321182245 (accessed: 18.10.2025).

16. E. Xhixho et al. (2025). Digital Transformation in the Legal Sector: Challenges and Opportunities for Cybersecurity and Data Protection. *Law, State and Telecommunications Review*. Vol. 17, no. 1. P. 250–271. DOI: doi.org/10.26512/lstr.v17i1.56176 (accessed: 18.10.2025).

17. Ebers M. (2024). Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act. *European Journal of Risk Regulation*. No. 16 (2). P. 684–703. DOI: doi.org/10.1017/err.2024.78 (accessed: 18.10.2025).

18. EU AI Act takes effect, and startups push back. Here's what you need to know. *Vestbee*. 2025. URL: https://www.vestbee.com/insights/articles/eu-ai-act-takes-effect-what-you-need-to-know (accessed: 15.10.2025).

19. EU AI Act: first regulation on artificial intelligence. *European Parliament*. URL:(https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence) (accessed: 15.10.2025).

20. How the EU AI Act affects US-based companies. *KPMG*. 2024. URL: https://kpmg.com/us/en/articles/2024/how-eu-ai-act-affects-us-based-companies.html (accessed: 15.10.2025).

21. 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). *Official Journal of the European Union*. L, 2024/1689.

22. Sabel C., Zeitlin J. (2008). Learning from Difference: The New Architecture of Experimentalist Governance in the EU. *European Law Journal*. Vol. 14(3). P. 271–327.

23. Safeguarding human rights in the sphere of AI in Ukraine. *ECNL*. URL: https://ecnl.org/impact-story/safeguarding-human-rights-sphere-ai-ukraine (accessed: 15.10.2025).

24. Savchenko V. et al. (2025). The transformation of legal frameworks through secure digitisation / V. Savchenko et al. *African journal of applied research*. 2025. Vol. 11, no. 1. P. 173–193. DOI: https://doi.org/10.26437/ajar.v11i1.835 (accessed: 15.10.2025).

25. Threat to innovation? Survey of European start-ups on the EU AI Act. *appliedAI Initiative GmbH.* 2023. URL: https://www.unternehmertum.de/en/topics/ai/threat-to-innovationsurvey-european-start-ups-on-eu-ai-act (accessed: 15.10.2025).

26. Ukraine's AI road map seeks to balance innovation and security. *Atlantic Council*. URL: https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-ai-road-map-seeks-to-balance-innovation-and-security/ (accessed: 15.10.2025).

27. Veale M., Borgesius F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*. Vol. 22 (4). P. 97–112. DOI: https://doi.org/10.48550/arXiv.2107.03721 (accessed: 15.10.2025)

The article was received by the editors 06.10.2025 The article was revised 09.11.2025
The article is recommended for printing 24.11.2025 This article published 30.12.2025