Цифрова трансформація

УДК / UDC: 347.82:342.7:004
DOI: https://doi.org/10.37750/2616-6798.2026.2(57).364302

Олексій Володимрович Костенко
Державна наукова установа «Інститут інформації, безпеки та права національного Академії правових наук України»
ORCID https://orcid.org/0000-0002-2131-0281
Людмила Олександрівна Шапенко
Національна академія статистики, обліку та аудиту
ORCID: https://orcid.org/0000-0001-7351-641X

СПРИЙНЯТТЯ ШТУЧНОГО ІНТЕЛЕКТУ В УКРАЇНІ: СОЦІАЛЬНО-ПРАВОВИЙ АНАЛІЗ У ВИМІРІ ІНФОРМАЦІЙНОГО ПРАВА ТА ЦИФРОВОЇ ЮРИСДИКЦІЇ

Анотація. *Стаття присвячена комплексному соціально-правовому аналізу сприйняття технологій штучного інтелекту в Україні крізь призму інформаційного права, цифрової юрисдикції та правового регулювання середовищ Metaverse/Web 4.0. Емпіричну базу дослідження становлять результати серії з восьми структурованих інтерактивних опитувань аудиторії суспільно-політичного видання "Дзеркало Тижня". Дослідження поєднує дескриптивний, кластерний, порівняльний benchmark-аналіз та побудову правової матриці ризиків ШІ.*

Запропоновано авторський Індекс правової зрілості цифрового суспільства (ІПЗЦС). Доведено, що результати дослідження корелюють із ключовими підходами EU AI Act, GDPR та міжнародних стандартів захисту цифрових прав людини.

Наукова новизна полягає у поєднанні емпіричного матеріалу з доктриною інформаційного права, цифрової юрисдикції та постантропоцентричної правової парадигми.

Ключові слова: *штучний інтелект, Metaverse, Web 4.0, EU AI Act, human-in-the-loop, Індекс правової зрілості цифрового суспільства, цифрові права дитини.*

Oleksiy V. Kostenko
State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"
ORCID https://orcid.org/ 0000-0002-2131-0281
Liudmyla O. Shapenko
Finance and Economics National Academy of Statistics, Accounting and Audit
ORCID: https://orcid.org/0000-0001-7351-641X

PERCEPTION OF ARTIFICIAL INTELLIGENCE IN UKRAINE: SOCIO-LEGAL ANALYSIS IN THE DIMENSION OF INFORMATION LAW AND DIGITAL JURISDICTION

Summary. *The article is devoted to a comprehensive socio-legal analysis of the perception of artificial intelligence technologies in Ukraine through the prism of information law, digital*

jurisdiction and legal regulation of Metaverse / Web 4.0 environments. The empirical basis of the study is the results of a series of eight structured interactive surveys of the audience of the socio-political publication "Dzerkalo Tyzhnia". The study combines descriptive, cluster, comparative benchmark analysis and the construction of a legal matrix of AI risks.

The author's Legal Maturity Index of the Digital Society (IUCN) is proposed. It has been proven that the results of the study correlate with the key approaches of the EU AI Act, GDPR and international standards for the protection of digital human rights.

The scientific novelty lies in the combination of empirical material with the doctrine of information law, digital jurisdiction and the post-anthropocentric legal paradigm.

Keywords: *artificial intelligence, Metaverse, Web 4.0, EU AI Act, human-in-the-loop, Digital Society Legal Maturity Index, digital children's rights.*

1. ВСТУП

Розвиток технологій штучного інтелекту (ШІ), Metaverse та Web 4.0 формує принципово нову правову реальність, у якій класичні категорії інформаційного права — суб'єкт, об'єкт, правовідношення, юрисдикція — потребують переосмислення та концептуальної адаптації. Алгоритмічні системи дедалі частіше приймають рішення, що справляють юридично значущі наслідки для фізичних осіб: у сферах кредитування, медичної діагностики, освітньої оцінки, соціального рейтингування. Одночасно глобальне розгортання Metaverse як інтегрованого кіберфізичного середовища ставить питання цифрової юрисдикції — правового регулювання відносин, що виникають у посттериторіальному цифровому просторі (Kostenko, 2024; Kostenko etal., 2022).

В Україні ці виклики набувають особливої гостроти в умовах воєнного стану, прискореної цифровізації публічного управління та євроінтеграційного вектору, що передбачає гармонізацію законодавства з acquis communautaire ЄС у сфері цифрового права, зокрема з Регламентом ЄС про штучний інтелект (EU AI Act, Regulation 2024/1689/EU). Попри наявність значного масиву доктринальних досліджень у сфері права ШІ та цифрової юрисдикції (Kostenko, 2021, 2022, 2024; Kostenko &Furashev, 2022; LoPiano, 2020; Mocanu DM 2022), емпіричний вимір сприйняття цих технологій у контексті правосвідомості українського суспільства залишається малодослідженим.

Метою цієї статті є комплексний соціально-правовий аналіз громадського сприйняття технологій ШІ в Україні. Для досягнення мети вирішуються такі завдання: охарактеризувати методологію та вибіркову стратегію дослідження; провести дескриптивний, кластерний та порівняльний аналіз результатів опитувань; побудувати правову матрицю ризиків ШІ; розробити Індекс правової зрілості цифрового суспільства (ІПЗЦС); запропонувати законодавчі рекомендації, узгоджені з EU AI Act та цифровою юрисдикцією Metaverse.

2. ТЕОРЕТИЧНІ ЗАСАДИ: ЦИФРОВА ЮРИСДИКЦІЯ, ПРАВО ШІ ТА POSTANTHROPO-ЦЕНТРИЧНА ПАРАДИГМА

Концептуальною основою дослідження є авторська доктрина цифрової юрисдикції, що розглядається як посттериторіальна, транскордонна та технологічно опосередкована правова конструкція для регулювання соціальних, економічних, інформаційних і алгоритмічних відносин у цифрових екосистемах — кіберпросторі, блокчейн-мережах, середовищах штучного інтелекту, Web 4.0 та Metaverse. На відміну від класичної юрисдикції, вона визначається не географією, а архітектурою платформ, режимами цифрової ідентифікації, алгоритмічними правилами та процедурами верифікації прав і обов'язків.

Дане дослідження формується на перетині доктрини цифрової юрисдикції, постантропоцентричної трансформації права, концепції делегованої правоспроможності

ШІ та ризик-орієнтованого регулювання. У цій логіці інформаційне право трансформується у нормативну матрицю цифрового правопорядку, покликану забезпечити баланс між інноваціями, алгоритмічною ефективністю, правами людини та цифровою безпекою.

3. МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ

Дослідження базується на серії з восьми структурованих інтерактивних опитувань, проведених на платформі видання "Дзеркало Тижня" впродовж 2024–2025 років. "Дзеркало Тижня" — засноване у 1994 році провідне суспільно-політичне видання України з аудиторією, що характеризується вищою освітою, переважно міським місцем проживання, проєвропейською громадянською позицією та розвиненим критичним мисленням.

Загальна кількість зафіксованих відповідей склала 1 112 одиниць (сукупно за всіма блоками). Кожен блок мав власну підвибірку: від n = 61 (блок щодо довіри алгоритмам у питаннях майбутнього дітей) до n = 374 (блок щодо довіри рекомендаціям ШІ у кредитуванні, лікуванні та навчанні). Метод: несистематична добровільна вибірка (voluntary response sampling) зі структурованими закритими запитаннями та відкритою опцією "Інше".

Аналіз проводився за чотирма методами:

1) дескриптивний аналіз (розподіл відповідей по блоках, побудова індексу сприйняття);

2) кластерний аналіз (авторська якісна типологія на основі патернів відповідей);

3) правова матриця ризиків (двовимірне зіставлення рівня суспільної тривоги та пріоритетності правового регулювання);

4) порівняльний benchmark-аналіз (зіставлення з орієнтовними міжнародними даними Eurobarometer 2024 та Edelman AI Trust 2024).

Таблиця 1. Зведена характеристика блоків опитування "Аналіз впливу технологій ШІ на українське суспільство"

№	Запитання	n	Домінуюча відповідь
1	Чим для вас є штучний інтелект?	н/з	Інструмент впливу на людей — 57%
2	Де народжуються найважливіші технології?	96	Спільні проєкти науки та бізнесу — 47%
3	Чи варто дозволяти ШІ самостійно клонувати себе?	174	Ні, це може бути небезпечно — 60%
4	Хто має відповідати за рішення ШІ?	94	Компанія-власник / оператор — 49%
5	Чи готові довіряти алгоритмам ШІ дітей і майбутнє?	61	Важл. рішення — лише за людиною — 72%
6	Як часто ділитися фото/відео дитини у соцмережах?	90	Ніколи — 80%
7	Довіра до рекомендацій ШІ (кредит, лікування, навчання)?	374	Лише як підказці — 61%
8	Як сприймаєте ШІ — інструмент чи загроза?	223	Інструмент-виконавець — 61%
Σ	**Усього (сукупно по всіх блоках)**	**1 112**	*2024–2025 рр.*

4. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

4.1. Дескриптивний аналіз

Найвищий показник зафіксовано у блоці “Приватність дітей” (80% “ніколи не ділитися зображеннями”), що відображає сформовану культуру privacy by design. Найнижчий показник — у питанні визнання ШІ суб’єктом права (13%), що свідчить про незрілість суспільного консенсусу в цьому концептуально складному питанні. Лише 4% респондентів “зазвичай довіряють” рекомендаціям ШІ у критичних рішеннях, тоді як 94% сукупно відкидають повну алгоритмічну автономію в цій сфері (блок 7, n = 374 — найбільша підвибірка серії).

Вперше на основі емпіричних даних виявлено та обґрунтовано феномен “прагматичного скептицизму” як домінуючої моделі ставлення освіченої української аудиторії до штучного інтелекту, що поєднує визнання його функціональної корисності з відмовою від прийняття повної автономізації алгоритмічних рішень у сферах, пов’язаних із правами, свободами, безпекою та гідністю людини. Доведено, що суспільний запит спрямований не на обмеження розвитку ШІ, а на його контрольоване, підзвітне та юридично детерміноване впровадження.

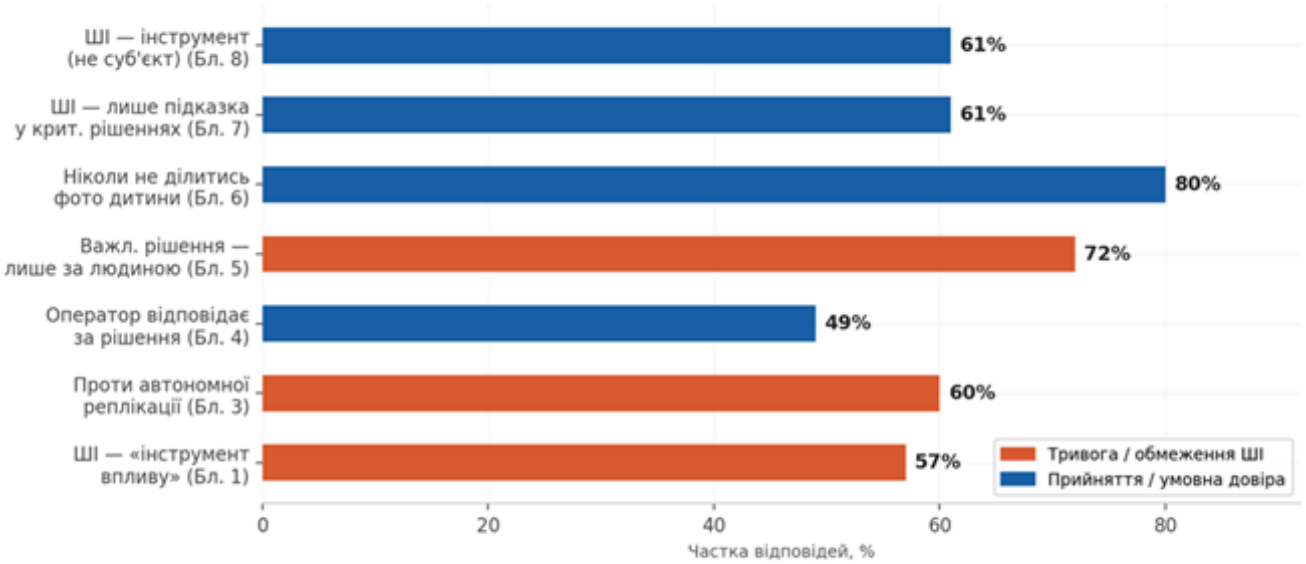

Рис. 1. Домінуючі позиції респондентів за ключовими правовими вимірами (n = 1 112, 2024–2025)

На рис. 1 відображено консолідований індекс домінуючих позицій респондентів за сімома ключовими правовими вимірами дослідження. Його узагальнення дає підстави стверджувати, що суспільне сприйняття ШІ в досліджуваній аудиторії вибудовується навколо трьох базових смислових ліній:

1. **ШІ як інструмент, а не самостійний носій волі**;
2. **необхідність збереження людського контролю у критичних рішеннях**;
3. **підвищена чутливість до ризиків приватності, відповідальності та цифрової безпеки дітей**.

Найбільш виразним індикатором є блок цифрової приватності дітей: 80% респондентів виступають проти поширення їхніх зображень у мережі, що свідчить про

сформовану правосвідомість у логіці privacy by design та пріоритету найкращих інтересів дитини.

Щодо автономії ШІ, 94% опитаних заперечують можливість його повної самостійності у критичних рішеннях, підтримуючи модель human-in-the-loop. Водночас домінує орієнтація на operator liability (49%), що підтверджує закріплення відповідальності за ШІ за реальними суб'єктами контролю.

Суттєвим є також запит на превентивні обмеження ризикових форм автономії: 60% респондентів виступають проти самореплікації ШІ, що кореспондує з принципом обережності у правовому регулюванні.

У питанні правосуб'єктності лише 13% допускають її можливість для ШІ, що засвідчує домінування антропоцентричної моделі при одночасному зародженні передумов до її трансформації.

Водночас виявлено амбівалентне сприйняття ШІ як інструменту виконання завдань і водночас засобу впливу на поведінку людини, що зумовлює необхідність правового контролю за алгоритмічним впливом.

Загалом аудиторія демонструє нормативно-вимогливу позицію: визнаючи користь ШІ, вона наполягає на збереженні пріоритету людини, підзвітності та правового контролю, що свідчить про готовність до імплементації європейської моделі регулювання ШІ.

Таким чином, дескриптивний аналіз показує, що досліджувана аудиторія займає **не антиінноваційну, а нормативно-вимогливу позицію** щодо ШІ. Вона готова визнавати користь технології, але лише за умови збереження пріоритету людини, чіткого ланцюга відповідальності, захисту вразливих груп та недопущення неконтрольованої автономізації алгоритмічних систем. Саме це і дозволяє визначити виявлену тенденцію як **прагматичний скептицизм**: суспільство не відмовляється від ШІ, але відмовляється довіряти йому без права, без контролю і без людини. У ширшому значенні це свідчить про високий потенціал для імплементації в Україні європейської моделі правового регулювання ШІ, побудованої на принципах підзвітності, пропорційності, ризик-орієнтованості та пріоритету основоположних прав.

4.2. Кластерний аналіз

На підставі крос-аналізу патернів відповідей виокремлюються три кластери респондентів (рис. 2).

Рис. 2. Кластерний розподіл респондентів за ставленням до технологій ШІ (авторська типологія)

Таблиця 2. Характеристика кластерів ставлення до технологій ШІ (авторська типологія)

Кластер	%	Характеристика
«Скептики»	48	Відкидають автономію ШІ; наполягають на human primacy; підтримують жорстке регулювання. Корелюють із запитом на EU AI Act-сумісне законодавство.
«Прагматики»	38	Приймають ШІ як інструмент за умови операторського контролю та прозорості; підтримують модель strictliability оператора.
«Оптимісти»	14	Готові до розширеного делегування повноважень ШІ; відкриті до визнання ШІ суб'єктом права; підтримують науково-бізнесові партнерства.

Кластерний аналіз емпіричних даних дозволив перейти від фіксації окремих відповідей до виявлення стійких моделей правосвідомого ставлення до штучного інтелекту як цілісного соціально-правового феномена. Його результатом стало виокремлення трьох базових типів: “Скептики” (48%), “Прагматики” (38%) та “Оптимісти” (14%), які слід розглядати не як жорсткі соціальні групи, а як якісно-аналітичні моделі правового мислення щодо ШІ.

Домінуючим є кластер “Скептики”, для якого характерні заперечення повної автономії ШІ, підвищена чутливість до ризиків непрозорості та чіткий запит на жорстке нормативне регулювання. У правовому вимірі ця модель ґрунтується на пріоритеті людського контролю, недопустимості делегування фінальних рішень алгоритмам і посиленні відповідальності оператора, що кореспондує з ризик-орієнтованою логікою сучасного європейського регулювання.

Кластер “Прагматики” відображає найбільш збалансовану модель: ШІ сприймається як корисний інструмент за умови його прозорості, підконтрольності та інтеграції у чіткий ланцюг відповідальності. Для цієї групи характерна орієнтація на процедурні механізми регулювання — підзвітність, аудит, explainability — що фактично відтворює архітектуру сучасного AI governance. Саме цей кластер виступає соціальною базою для умовно-ліберальної, але нормативно щільної моделі регулювання.

Найменш чисельний, але концептуально значущий кластер “Оптимісти” демонструє відкритість до розширення функціональної ролі ШІ, включаючи можливість переосмислення меж правосуб’єктності. Він відображає зародження постантропоцентричних підходів, у межах яких алгоритмічні агенти розглядаються як потенційні учасники цифрових правовідносин.

Відмінності між кластерами мають не лише кількісний, а й онтологічний характер: від сприйняття ШІ як об’єкта ризику (“Скептики”), через інструментально-регульовану модель (“Прагматики”), до бачення його як елемента нової цифрової екосистеми (“Оптимісти”). Це дозволяє виокремити три нормативні сценарії розвитку: обмежувально-превентивний, регуляторно-прагматичний та інноваційно-постантропоцентричний.

Отримані результати мають принципове значення для правотворчості, оскільки свідчать про неможливість одновимірної моделі регулювання ШІ. Баланс між інноваціями та захистом прав людини може бути досягнутий лише через багаторівневу нормативну конструкцію, яка враховує різні соціальні запити. У цьому контексті

кластер “Прагматики” виконує стабілізуючу функцію, забезпечуючи основу для компромісної правової моделі.

Таким чином, кластерний аналіз підтверджує, що суспільне сприйняття ШІ є структурованим, праворефлексивним і внутрішньо диференційованим, що створює сприятливі передумови для імплементації в Україні європейської моделі регулювання, адаптованої до національного соціально-правового контексту.

4.3. Правова матриця ризиків ШІ

Правова матриця ризиків ШІ, побудована на основі результатів опитування, є спробою перевести емпіричні дані суспільного сприйняття у площину **нормативного картографування ризиків**, тобто співвіднести рівень соціальної тривоги щодо певних аспектів функціонування штучного інтелекту з рівнем необхідного правового реагування. На відміну від звичайного опису окремих відповідей, матриця ризиків дозволяє побачити, **які саме суспільні страхи, сумніви та запити вже набули форми потенційних об’єктів правового регулювання**, а також які з них мають бути віднесені до сфери першочергового нормативного втручання.

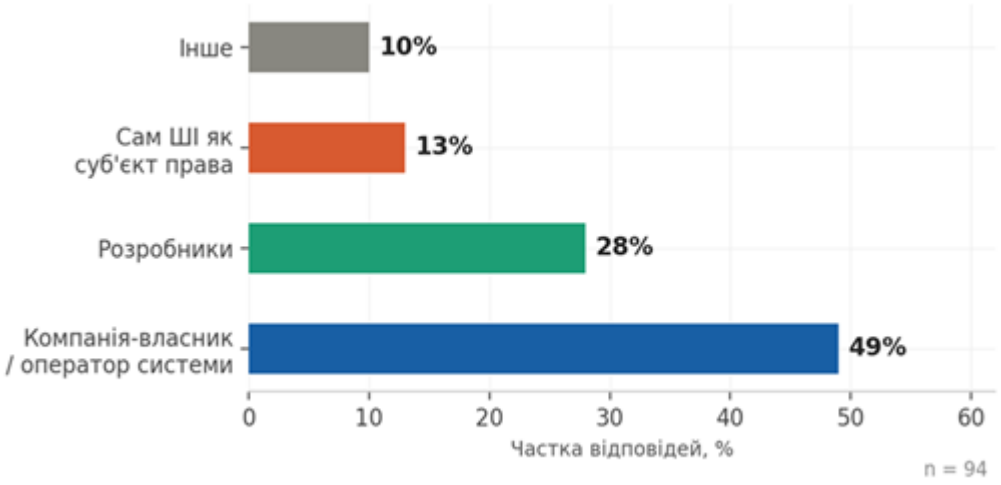

Рис. 3. Розподіл відповідей: “Хто має відповідати за рішення ШІ?” (n = 94)

У методологічному плані правова матриця ризиків ґрунтується на двох взаємопов’язаних координатах:

1. **рівень суспільної тривоги / настороженості** щодо певного явища, зафіксований емпірично;
2. **ступінь пріоритетності правового регулювання**, визначений через зіставлення результатів опитування з чинними або перспективними нормами інформаційного права, acquis ЄС, положеннями EU AI Act, GDPR та суміжних міжнародних актів.

Такий підхід дозволяє розглядати ризик не лише як технологічну або соціальну категорію, а як **юридично значущий сигнал**, що вказує на потребу в конкретному типі правового режиму: заборонному, превентивному, дозвільно-контрольному, процедурному або доктринально-дискусійному. У цьому полягає основна цінність матриці: вона дає змогу не просто констатувати, що суспільство “боїться” або “не довіряє”, а визначити, **яка саме форма правового втручання є адекватною для кожного типу ризику**.

Найвищий рівень тривоги виявлено щодо **використання ШІ у критичних рішеннях**, пов’язаних із майбутнім людини, її дітей, лікуванням, кредитуванням та

навчанням. Сукупний показник у **94%**, які фактично не підтримують повну алгоритмічну автономію у таких сферах, свідчить про те, що суспільство сприймає цю проблему не як технічну, а як **екзистенційно-правову**. Йдеться про ситуації, де рішення алгоритму може безпосередньо впливати на базові права та життєві перспективи особи. Саме тому у правовій матриці цей блок закономірно віднесено до категорії **критичного регулювання**. Його нормативним еквівалентом виступає насамперед ст. 14 EU AI Act, яка закріплює обов'язковість meaningful human oversight, а також ст. 22 GDPR, що гарантує право не підлягати рішенню, заснованому виключно на автоматизованій обробці, якщо воно породжує юридичні або подібні істотно значущі наслідки для особи.

На рис. 3 та у таблиці 3 наведено розподіл відповідей щодо суб'єкта відповідальності за рішення ШІ та авторську правову матрицю ризиків.

Таблиця 3. Правова матриця ризиків ШІ за результатами опитування (авторська розробка)

Тема	Тривога	Регулювання	Правова норма
Довіра до ШІ у критичних рішеннях	Висока (94%)	Критична	EU AI Act Art.14 (human oversight); GDPR Art.22
Автоматична самореплікація ШІ	Висока (60%)	Критична	EU AI Act Art.5 (заборонені практики)
Відповідальність оператора	Середня (49%)	Висока	EU AI Act Art.3 (deployer); модель strictliability
Приватність дітей	Висока (80%)	Висока	GDPR Art.8, 25; UNCRC Gen. Comment 25 (2021)
Правосуб'єктність ШІ	Середня (13%)	Дискусійна	EPRS 2017 ("електронна особистість"); EU AI Act — відсутність консенсусу

У змістовному вимірі цей блок демонструє, що суспільна правосвідомість фактично підтримує одну з базових ідей сучасного цифрового права: алгоритм може допомагати, але не повинен остаточно заміщати людину у рішеннях високого ризику . Це створює як доктринальне, так і емпіричне підґрунтя для закріплення принципу human-in-the-loop як обов'язкової вимоги для систем ШІ, що впливають на права, ресурси або юридичний статус особи.

Суттєвим є також блок автономної самореплікації ШІ: 60% респондентів сприймають її як небезпечну. У правовій площині це означає ризик втрати контролю над самою архітектурою системи, що обґрунтовує застосування не лише контрольних, а й заборонних або жорстко превентивних механізмів регулювання відповідно до логіки недопустимих практик.

У сфері відповідальності домінує підтримка моделі operator liability (49%), що відображає відмову від "безсуб'єктної" відповідальності та підтверджує орієнтацію на класичну правову конструкцію: відповідальність має нести суб'єкт, який впроваджує або контролює систему. Це узгоджується з європейською моделлю AI governance та створює підстави для впровадження режимів підвищеної або суворої відповідальності у ризикових сферах.

Особливо високий рівень нормативної пріоритетності виявлено у сфері захисту цифрових прав дитини: 80% респондентів підтримують обмеження поширення відповідного контенту. Це свідчить про трансформацію суспільної правосвідомості у напрямі визнання захисту цифрового сліду дитини як імперативу та обґрунтовує необхідність формування спеціалізованої правової підсистеми.

Натомість питання правосуб'єктності ШІ (13%) залишається у сфері доктринальної відкритості. Воно не потребує негайної кодифікації, але фіксує наявність соціальної бази для майбутнього переосмислення меж суб'єктності в цифрових екосистемах.

Узагальнення показує асиметрію регуляторних пріоритетів: найбільш жорсткого нормативного втручання потребують сфери, пов'язані з людською автономією, безпекою та правами дитини, тоді як статус ШІ залишається предметом наукового розвитку.

Таким чином, емпіричні дані трансформуються у карту нормотворчих пріоритетів, де право має діяти диференційовано — від імперативних заборон до процедурного контролю та концептуального моделювання. Саме така модульна, ризик-орієнтована логіка відповідає сучасній архітектурі цифрової юрисдикції та європейського регулювання ШІ.

4.4. Індекс правової зрілості цифрового суспільства (ІПЗЦС)

Для переходу від фрагментарного аналізу окремих відповідей до більш цілісної оцінки стану правосвідомості досліджуваної аудиторії в умовах цифрової трансформації у межах цього дослідження запропоновано авторський **Індекс правової зрілості цифрового суспільства (ІПЗЦС)**. Його запровадження зумовлене тим, що окремі соціологічні показники, навіть доволі виразні, не завжди дозволяють належно оцінити загальний рівень готовності суспільства до сприйняття, осмислення та нормативного супроводу технологій штучного інтелекту. Відтак виникає потреба у синтетичному показнику, здатному інтегрувати кілька змістовно різних, але юридично взаємопов'язаних вимірів у єдину аналітичну рамку.

ІПЗЦС не претендує на універсальний і вичерпний інструмент вимірювання всіх аспектів цифрової правосвідомості. Його функція інша: **сформувати узагальнену правову оптику**, яка дозволяє побачити, наскільки суспільство готове сприймати ШІ не лише як технічну новацію, а як об'єкт правового регулювання, джерело ризиків для прав людини та водночас інструмент цифрового розвитку. Саме тому індекс побудовано не навколо технічної компетентності респондентів, не навколо рівня їхньої технологічної обізнаності як такої, а навколо **здатності виявляти юридично значущі межі допустимого використання ШІ**.

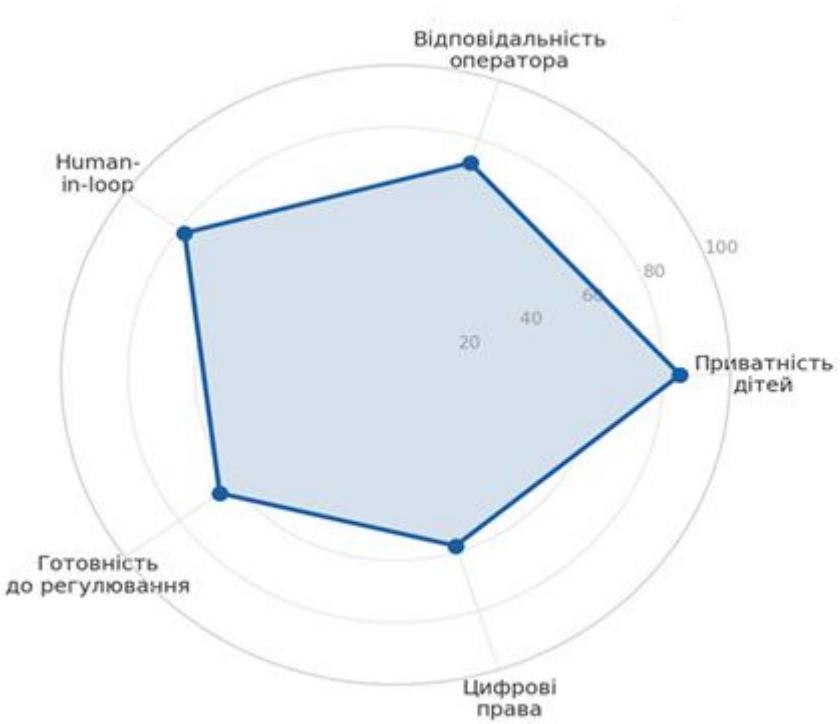

Рис. 4. Індекс правової зрілості цифрового суспільства (ІПЗЦС), аудиторія "Дзеркала Тижня", 2024–2025 (авторська розробка)

Структурно ІПЗЦС охоплює **п'ять базових вимірів**, кожен із яких репрезентує окремий аспект правового ставлення до цифрових технологій:

1. **приватність**;
2. **операторська відповідальність**;
3. **human-in-the-loop / людський контроль**;
4. **готовність до правового регулювання ШІ**;
5. **усвідомлення цифрових прав**.

Авторський Індекс правової зрілості цифрового суспільства (ІПЗЦС) обчислюється за п'ятьма вимірами: приватність (~85), відповідальність оператора (~72), human-in-the-loop (~78), готовність до регулювання ШІ (~65), усвідомлення цифрових прав (~58). Середнє значення ІПЗЦС становить ~73/100, що відповідає категорії "висока правова цифрова зрілість" (рис. 4).

Для операціоналізації Індексу правової зрілості цифрового суспільства (ІПЗЦС) запропоновано багатовимірну модель, побудовану на агрегуванні ключових юридично значущих показників, що відображають ставлення респондентів до базових елементів правового регулювання штучного інтелекту. Індекс має інтегративний характер і формується як зважена сума нормованих індикаторів, згрупованих у відповідні змістовні блоки.

Загальна формула індексу може бути представлена у вигляді:

$$\text{ІПЗЦС} = w_1 \cdot H + w_2 \cdot R + w_3 \cdot L + w_4 \cdot C + w_5 \cdot S$$

де:

- **H (Human Control Index)** — індекс підтримки людського контролю (human-in-the-loop / human oversight);

- **R (Risk Sensitivity Index)** — індекс чутливості до ризиків (автономія ШІ, самореплікація, непрозорість);
- **L (Liability Orientation Index)** — індекс орієнтації на юридичну відповідальність (operator/deployer liability);
- **C (Child Digital Protection Index)** — індекс підтримки захисту цифрових прав дитини;
- **S (Subjectivity Perception Index)** — індекс сприйняття правосуб'єктності ШІ (з інверсною шкалою як фактор стримування);
- $w_1 \ldots w_5$ — вагові коефіцієнти відповідних індикаторів ($\sum w = 1$).

Кожен індикатор формується на основі відповідей респондентів шляхом нормування значень у діапазоні [0;1], де 0 відображає відсутність правової зрілості за відповідним параметром, а 1 — її максимальний прояв. Нормування здійснюється через приведення відсоткових показників до шкали одиничного інтервалу або через бінаризацію відповідей (правильно/неправильно з погляду нормативної моделі).

Особливість моделі полягає у різноспрямованості окремих індикаторів. Зокрема, показник **S (правосуб'єктність ШІ)** має зворотний вплив на загальний індекс: чим вищий рівень підтримки повної автономної суб'єктності ШІ, тим нижчим є рівень правової зрілості в антропоцентричній моделі права. Відповідно, у формулі він враховується або з негативною вагою, або через інверсне перетворення (1 – S).

Вагові коефіцієнти можуть визначатися двома способами:

1. **експертним (доктринальним)** — із пріоритетом прав людини, безпеки та відповідальності;
2. **емпіричним** — на основі статистичної значущості відповідних показників (наприклад, через факторний аналіз).

У базовій моделі доцільно використовувати рівномірний розподіл ваг ($w_1 = w_2 = \ldots = 0{,}2$) або ж надати підвищену вагу індикаторам **H** та **C** як таким, що безпосередньо пов'язані з фундаментальними правами.

Інтерпретація значень ІПЗЦС пропонується у вигляді шкали:

- **0,00–0,39** — низький рівень правової зрілості (технологічний редукціонізм, недооцінка правових ризиків);
- **0,40–0,69** — середній рівень (фрагментарна правосвідомість, наявність суперечливих установок);
- **0,70–1,00** — високий рівень (сформована нормативна позиція, орієнтація на права людини та відповідальність).

Методологічно ІПЗЦС виконує не лише описову, а й аналітико-прогностичну функцію. Він дозволяє:

- порівнювати різні соціальні групи за рівнем правової готовності до впровадження ШІ;
- виявляти "слабкі зони" правосвідомості, що потребують регуляторного або освітнього втручання;
- оцінювати відповідність суспільних установок європейській моделі AI governance;
- формувати емпірично обґрунтовану ієрархію нормотворчих пріоритетів.

Таким чином, ІПЗЦС виступає інструментом трансформації соціологічних даних у юридично релевантний показник, що відображає ступінь інтеграції принципів верховенства права, людського контролю, відповідальності та захисту вразливих груп у цифровій свідомості суспільства.

Для практичної апробації Індексу правової зрілості цифрового суспільства (ІПЗЦС) у межах цього дослідження використано емпіричні дані, отримані за п'ятьма ключовими вимірами: підтримка людського контролю над ШІ, чутливість до ризиків автономної самореплікації, орієнтація на операторську відповідальність, підтримка захисту цифрових прав дитини та ставлення до правосуб'єктності ШІ.

У базовій моделі формула індексу має такий вигляд:

ІПЗЦС = (H + R + L + C + S) / 5

де:

H — показник підтримки human-in-the-loop;
R — показник ризик-чутливості щодо автономної самореплікації;
L — показник орієнтації на operator liability;
C — показник підтримки захисту цифрових прав дитини;
S — інверсований показник правосуб'єктності ШІ.

На підставі отриманих результатів емпіричні значення цих індикаторів становлять:
H = 0,94, оскільки 94% респондентів заперечують можливість повної автономії ШІ у критичних рішеннях;
R = 0,60, оскільки 60% респондентів вважають автономну самореплікацію ШІ небезпечною;
L = 0,49, оскільки 49% підтримують модель відповідальності компанії-власника або оператора системи;
C = 0,80, оскільки 80% виступають проти поширення фото- та відеоконтенту за участю дітей;
S = 1 – 0,13 = 0,87, оскільки лише 13% допускають можливість визнання ШІ самостійним суб'єктом права, а отже інверсне значення, що відповідає антропоцентричній моделі правової зрілості, становить 0,87.

Підставляючи ці значення у формулу, отримуємо:

ІПЗЦС = (0,94 + 0,60 + 0,49 + 0,80 + 0,87) / 5 = 3,70 / 5 = 0,74

Отже, розрахункове значення ІПЗЦС становить **0,74**.

За запропонованою шкалою інтерпретації це відповідає **високому рівню правової зрілості цифрового суспільства**, оскільки показник перевищує поріг 0,70. Такий результат свідчить, що досліджувана аудиторія в цілому демонструє сформовану нормативну чутливість до ключових правових викликів, пов'язаних із розвитком ШІ, і орієнтується на пріоритет людського контролю, відповідальності, захисту прав дитини та обмеження надмірної автономії алгоритмічних систем.

Водночас внутрішня структура індексу показує, що окремі його компоненти є нерівномірними. Найвищі значення мають показники, пов'язані з людським контролем (**0,94**), захистом цифрових прав дитини (**0,80**) та відмовою від визнання повної правосуб'єктності ШІ (**0,87**). Натомість найнижчим є компонент юридичної відповідальності (**0,49**), що свідчить не про відсутність правової зрілості, а про меншу визначеність суспільства саме у виборі конкретної юридичної моделі деліктної або регуляторної відповідальності за дії ШІ. Саме цей сегмент доцільно розглядати як зону подальшого доктринального уточнення та правотворчого розвитку.

За потреби формула може бути уточнена шляхом введення вагових коефіцієнтів. Наприклад, якщо надати пріоритет фундаментальним правам і захисту вразливих груп, модель може бути представлена так:

ІПЗЦС = 0,25H + 0,20R + 0,15L + 0,25C + 0,15S

У такому разі підстановка дає:

ІПЗЦС = 0,25×0,94 + 0,20×0,60 + 0,15×0,49 + 0,25×0,80 + 0,15×0,87
ІПЗЦС = 0,235 + 0,120 + 0,0735 + 0,200 + 0,1305 = 0,759

Отже, за зваженою моделлю значення індексу становить **0,759**, що також підтверджує **високий рівень правової зрілості** досліджуваної аудиторії.

Таким чином, навіть із урахуванням різних моделей обчислення, ІПЗЦС фіксує наявність у досліджуваній групі не технофобного, а нормативно структурованого ставлення до ШІ. Йдеться про аудиторію, яка готова приймати технологічні інновації, але лише за умови збереження людського контролю, чіткого ланцюга відповідальності, захисту вразливих категорій та правового обмеження ризикованих форм алгоритмічної автономії.

Обрання саме цих вимірів має не випадковий, а доктринально вмотивований характер. У сукупності вони охоплюють ті ключові вузли, в яких сьогодні концентруються основні виклики інформаційного права, права ШІ та цифрової юрисдикції. Приватність відображає здатність суспільства бачити у цифрових даних не технічний ресурс, а об'єкт правового захисту. Операторська відповідальність демонструє, чи усвідомлює аудиторія необхідність замикати юридичний ланцюг наслідків на конкретному суб'єкті, а не розчиняти його в технічній автономії алгоритму. Вимір human-in-the-loop фіксує рівень підтримки людиноцентричної парадигми. Готовність до регулювання ШІ показує, чи сприймається право як необхідна умова технологічного розвитку, а не як його зовнішній бар'єр. Нарешті, усвідомлення цифрових прав відображає глибину правової інтерпретації цифрової реальності загалом.

За результатами дослідження значення окремих компонентів ІПЗЦС становлять орієнтовно: **приватність — ~85**, **операторська відповідальність — ~72**, **людський контроль — ~78**, **готовність до регулювання ШІ — ~65**, **усвідомлення цифрових прав — ~58**. Середнє значення індексу становить **приблизно 73/100**, що дає підстави віднести досліджувану аудиторію до категорії "**висока правова цифрова зрілість"**.

Інтерпретуючи цей показник, слід наголосити, що він не означає ані абсолютної поінформованості респондентів у сфері цифрового права, ані завершеності суспільного консенсусу щодо складних питань ШІ. Його зміст полягає в іншому: він свідчить про наявність достатньо сформованої правової інтуїції, за якої аудиторія вже здатна відрізняти допустиме від недопустимого, безпечне від ризикованого, допоміжне від такого, що потенційно витісняє людину із сфери юридично значущого рішення. Саме ця здатність і становить ядро цифрової правової зрілості.

Найвищий компонент ІПЗЦС — **приватність (~85)** — має особливо показове значення. Він свідчить про те, що в межах досліджуваної аудиторії питання захисту персональних даних, особливо даних дітей, уже не сприймається як периферійне або факультативне. Навпаки, приватність виявляється однією з найстійкіших ціннісно-правових установок. Це дозволяє стверджувати, що в українському інформаційному середовищі формується не лише цифрова грамотність, а й **культура юридичного обмеження цифрової видимості особи**, що є надзвичайно важливим для подальшого розвитку законодавства про захист персональних даних, цифрову ідентичність та права дитини у цифровому середовищі.

Високий показник за виміром **human-in-the-loop (~78)** також має принципове значення. Він демонструє, що для більшості респондентів право на фінальне, осмислене, людське рішення залишається фундаментальною гарантією в умовах алгоритмізації суспільних процесів. По суті, цей компонент ІПЗЦС фіксує суспільну підтримку однієї з базових ідей сучасного AI governance: автоматизація може бути глибокою, але вона не повинна перетворювати людину на пасивний додаток до системи. У ширшому

теоретичному сенсі це означає, що попри розвиток постантропоцентричних концепцій і цифрової суб'єктності, суспільне ядро правового порядку все ще міцно тримається за принцип **антропоцентричної остаточності юридичного рішення**.

Компонент **операторської відповідальності (~72)** демонструє іншу важливу рису правової зрілості: аудиторія не лише відчуває ризики, а й прагне бачити у правопорядку чітко визначеного носія обов'язку та відповідальності. Це означає, що суспільство вже не задовольняється абстрактними деклараціями про "етичний ШІ" або "безпечні алгоритми"; воно очікує конкретних юридичних механізмів, які встановлювали б, хто саме має відповідати за помилки, шкоду, маніпуляцію або порушення прав, спричинені функціонуванням систем ШІ. Такий підхід свідчить про збереження класичного правового мислення в його найкращому вимірі: навіть у цифровій екосистемі право повинно мати адресата.

Дещо нижчий, але все ж достатньо високий показник **готовності до регулювання ШІ (~65)** вказує на те, що досліджувана аудиторія загалом підтримує ідею спеціального нормативного втручання у сферу ШІ, хоча ступінь цієї підтримки вже є більш диференційованим. Це пояснюється тим, що тут респонденти стикаються з більш складною дилемою: як збалансувати технологічний розвиток, інноваційність і безпеку. Саме тому цей компонент є нижчим за показники приватності або human-in-the-loop. Однак навіть його значення свідчить про принципово важливу річ: право у сприйнятті аудиторії не розглядається як ворог інновацій. Воно сприймається як умова легітимності інноваційного розвитку. Це має надзвичайно важливе значення для євроінтеграційного контексту України, оскільки свідчить про наявність суспільного підґрунтя для імплементації норм, сумісних із EU AI Act та іншими актами acquis ЄС.

Найнижчий компонент індексу — **усвідомлення цифрових прав (~58)** — заслуговує на особливу увагу. Саме він виявляє ту межу, за якою цифрова правова зрілість поки що ще не стала повністю системною. Якщо у питаннях приватності, відповідальності чи людського контролю респонденти демонструють доволі стійкі установки, то щодо загального усвідомлення цифрових прав як цілісної категорії правового статусу людини в мережевому середовищі рівень рефлексії залишається нижчим. Це означає, що суспільство вже добре відчуває окремі ризики, але ще не завжди мислить їх як елементи єдиної системи цифрових прав — права на захист даних, права на пояснення, права на оскарження автоматизованого рішення, права на цифрову гідність, права на безпечне алгоритмічне середовище тощо.

У доктринальному вимірі ІПЗЦС має ще одну важливу функцію: він дозволяє поєднати **інформаційне право, цифрову юрисдикцію та емпіричну соціологію** в єдину аналітичну рамку. Зазвичай ці площини існують відокремлено: право формулює норми, соціологія фіксує настрої, а цифрова юрисдикція пропонує моделі регулювання посттериторіального середовища. ІПЗЦС, натомість, показує, що цифрова правова зрілість може бути осмислена як точка перетину цих трьох вимірів. Тобто йдеться не просто про індекс "довіри до ШІ", а про індикатор **готовності суспільства до життя в умовах алгоритмічного правопорядку**.

Отже, значення ІПЗЦС на рівні **~73/100** дозволяє зробити подвійний висновок. З одного боку, досліджувана аудиторія демонструє справді високий рівень правової чутливості до ключових викликів ШІ, що створює сприятливий соціальний ґрунт для впровадження в Україні сучасного ризик-орієнтованого регулювання. З іншого боку, індекс виявляє зони подальшого розвитку — передусім у частині системного усвідомлення цифрових прав і формування більш цілісної мови правового самозахисту в алгоритмічному середовищі.

Він демонструє, що українська освічена аудиторія вже має достатньо сформований потенціал для підтримки людиноцентричного, підзвітного й правозахисного регулювання ШІ, але водночас потребує подальшого розвитку категоріальної і правопросвітницької основи цифрових прав. Саме це й робить ІПЗЦС важливим внеском не лише у структуру цього дослідження, а й у ширшу доктрину інформаційного права та цифрової юрисдикції.

4.5. Порівняльний benchmark-аналіз

Вперше на основі порівняльного benchmark-аналізу встановлено, що рівень довіри до рекомендацій штучного інтелекту у критичних рішеннях в українській аудиторії є істотно нижчим за міжнародні показники (4% проти ≈12% у європейських та ≈9% у американських вибірках), що свідчить не про технофобію, а про сформовану модель нормативно-обмеженого сприйняття ШІ. Доведено, що українська правосвідомість орієнтується на інструментальне використання алгоритмів із пріоритетом людського контролю, тим самим підтверджуючи її відповідність принципу human-in-the-loop та більш високий рівень правової чутливості до меж легітимності алгоритмічних рішень у сферах, що зачіпають права, безпеку та майбутнє людини (рис. 5).

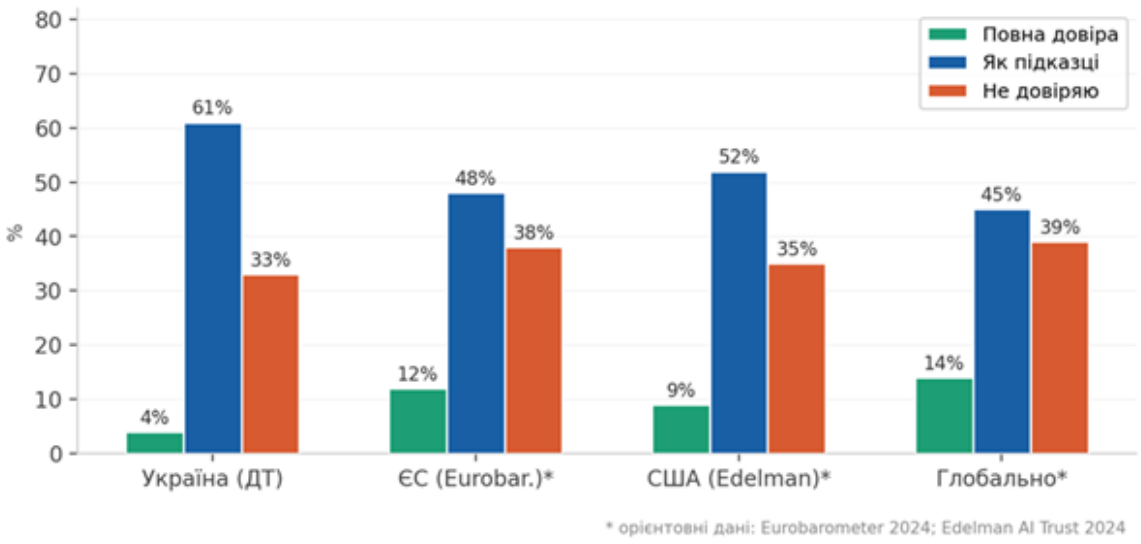

*Рис. 5. Порівняльний аналіз рівня довіри до ШІ-рекомендацій (*орієнтовні дані: Eurobarometer 2024; Edelman AI Trust 2024)*

Рівень повної довіри до ШІ в українській аудиторії (4%) суттєво нижчий за європейські (~12%) та американські (~9%) показники, тоді як домінує модель “ШІ як підказка” (61%) . Це свідчить про сформовану інструментально-контрольовану модель довіри, в якій алгоритм сприймається як допоміжний інструмент за збереження фінального людського рішення.

Така відмінність відображає не технологічну відсталість, а вищий рівень нормативної настороженості до алгоритмічного втручання у критичні сфери. Довіра до ШІ тут обумовлена не лише його ефективністю, а й відповідністю базовим правовим принципам — автономії людини, відповідальності та контролю над рішенням.

У цьому сенсі українська аудиторія демонструє модель “ШІ як підказка, але не арбітр”, що узгоджується з принципом human-in-the-loop та загальною логікою європейського регулювання. Водночас така позиція формується і під впливом

специфічного контексту — підвищених безпекових ризиків, досвіду війни та чутливості до втрати контролю над критичними системами.

Загалом benchmark-аналіз підтверджує, що нижчий рівень довіри до ШІ є індикатором не слабшої, а більш зрілої правової фільтрації технологій. Це створює сприятливі передумови для впровадження в Україні людиноцентричної, ризик-орієнтованої моделі AI governance, сумісної з європейським підходом.

5. ОБГОВОРЕННЯ

Результати дослідження не лише підтверджують, а й конкретизують базові положення інформаційного та цифрового права, демонструючи їх емпіричне відображення у правосвідомості суспільства. Ключові концепти — людиноцентричність, підзвітність, ризик-орієнтованість, захист вразливих груп та межі цифрової суб'єктності — уже функціонують не лише як доктринальні конструкції, а як елементи суспільного запиту.

Поєднання інструментального сприйняття ШІ (61%) із високою чутливістю до його впливу (57%) відображає феномен технологічного амбівалентизму: ШІ одночасно розглядається як корисний інструмент і як потенційний механізм впливу на поведінку. Це виводить аналіз за межі технократичної ефективності у площину алгоритмічної влади та підзвітності, корелюючи з проблемою "чорної скрині" та вимогою algorithmic accountability.

Негативне ставлення до самореплікації ШІ (60%) підтверджує наявність у правосвідомості межі між допустимою автоматизацією та ризикованою автономією. Це відображає підтримку превентивного підходу та узгоджується з концепцією неприйнятного ризику у сучасному європейському праві.

Значення ІПЗЦС на рівні близько 73/100 свідчить про феномен випереджальної правової зрілості: досліджувана аудиторія демонструє готовність мислити в категоріях підзвітності, контролю та прав людини швидше, ніж ці принципи повністю інституціоналізовані у національному праві.

13% підтримки ідеї правосуб'єктності ШІ фіксують ранній етап трансформації правового мислення у бік постантропоцентричних моделей, що потребує доктринального опрацювання без передчасної нормативної легітимації.

Показник 80% щодо обмеження поширення зображень дітей підтверджує формування стійкого запиту на спеціальний захист цифрового сліду дитини, узгоджений із міжнародними стандартами та концепцією посиленого захисту вразливих груп.

У сукупності ці результати свідчать, що правосвідомість досліджуваної аудиторії вже формує нормативну карту допустимого у сфері ШІ. Це створює емпірично підтверджене підґрунтя для розвитку в Україні людиноцентричної, підзвітної та ризик-орієнтованої моделі правового регулювання цифрових технологій.

6. ЗАКОНОДАВЧІ РЕКОМЕНДАЦІЇ ЩОДО РЕГУЛЮВАННЯ ШІ В УКРАЇНІ

Емпіричні результати дослідження, розглянуті у попередніх підрозділах, дають підстави перейти від діагностики суспільних установок до формулювання конкретних законодавчих рекомендацій - не абстрактних побажаннь щодо "кращого регулювання", а про нормативно вмотивований пакет рекомендацій, який може бути використаний у процесі розробки української моделі права ШІ.

Принципово важливо, що запропоновані рекомендації не зводяться до механічної імплементації європейських актів. Їхнє завдання полягає у тому, щоб адаптувати фундаментальні принципи європейського підходу до українського правового, соціального та безпекового контексту. Україна входить у фазу інтенсивної цифрової

трансформації одночасно з процесом євроінтеграції, а отже, має історичну можливість не лише гармонізувати законодавство з acquis ЄС, а й сформувати власну, більш цілісну й доктринально послідовну модель регулювання ШІ, що враховуватиме як ризики алгоритмічного врядування, так і перспективи цифрової юрисдикції в середовищах Web 4.0 і Metaverse.

Таблиця 4. Законодавчі рекомендації щодо регулювання ШІ в Україні (авторська розробка)

№	Рекомендація	Обґрунтування та правова основа
1	**Закріплення принципу human-in-the-loop**	94% відкидають автономні рішення ШІ в критичних сферах → ст. 14 EU AI Act; ст. 22 GDPR; необхідна імплементація в ЗУ “Про захист персональних даних”
2	**Операторська відповідальність за рішення ШІ**	49% підтримують модель operator-liability → ст. 3 EU AI Act (deployer); запровадження strict liability оператора в ЦКУ / спеціальному ЗУ “Про ШІ”
3	**Захист “цифрового сліду дитини”**	80% “ніколи” → GDPR Art. 8, 25; UNCRC Gen. Comment 25 (2021); спеціальна глава в ЗУ “Про захист персональних даних”
4	**Заборона автономної самореплікації ШІ**	60% проти → EU AI ActArt. 5 (заборонені практики); внесення до переліку систем “неприйнятного ризику” в національному законодавстві
5	**Цифрова юрисдикція Metaverse**	13% готові до правосуб'єктності ШІ → розробка Цифрового кодексу України з регулюванням цифрової ідентичності, аватарів та “делегованої правоспроможності” ШІ в Metaverse

6.1. Закріплення принципу human-in-the-loop як імперативної норми

Першою і, без перебільшення, фундаментальною рекомендацією є закріплення на рівні закону принципу **human-in-the-loop**, тобто обов’язкової участі людини у фінальному ухваленні рішень у тих сферах, де використання ШІ здатне породжувати істотні правові, соціальні, економічні чи безпекові наслідки для особи. Необхідність такої норми безпосередньо підтверджується емпіричними даними: **94% респондентів** фактично відкидають повну алгоритмічну автономію в питаннях, що стосуються дітей, лікування, кредитування, навчання та інших критично важливих рішень.

В українському праві такий принцип потребує не декларативного, а саме **операційного закріплення**. Його законодавча реалізація повинна включати щонайменше кілька обов’язкових елементів:

1. визначення переліку сфер, у яких автоматизоване рішення не може бути остаточним без людського підтвердження;
2. закріплення права особи вимагати перегляду такого рішення людиною;
3. встановлення стандартів компетентного людського контролю, щоб формальна присутність людини не перетворилася на імітацію нагляду;
4. фіксацію обов’язку документувати момент людського втручання та підстави прийняття фінального рішення.

Інакше кажучи, закон має закріпити не лише сам принцип, а й процесуальні гарантії його реальної дії. Без цього human-in-the-loop ризикує залишитися риторичною формулою без належної юридичної сили.

6.2. Запровадження моделі операторської відповідальності за рішення ШІ

Другою ключовою рекомендацією є нормативне закріплення **операторської відповідальності** за рішення, дії або наслідки функціонування систем ШІ. Емпірично така потреба підтверджується тим, що **49% респондентів** прямо вказали на компанію-власника або оператора як на суб'єкта, який повинен відповідати за рішення ШІ. Хоча цей показник не є абсолютною більшістю, у правовій інтерпретації він має надзвичайно високу вагу, оскільки відображає суспільний вибір саме на користь певної моделі юридичного зв'язування технології з її наслідками.

З позицій інформаційного права це означає, що суспільство не сприймає алгоритм як самодостатнє джерело відповідальності. Юридична оцінка наслідків функціонування ШІ має замикатися на конкретному носії контролю — розробнику, операторі або іншому суб'єкті, який впроваджує систему, визначає сферу її застосування, підтримує її функціонування або отримує вигоду від її використання. У сучасному європейському регулюванні саме така логіка домінує в підході до AI governance. Відтак для України доцільним є запровадження конструкції **strictliability** або, принаймні, презумпції підвищеної відповідальності оператора за шкоду, спричинену використанням систем ШІ у сферах підвищеного ризику.

Нормативно це може бути реалізовано двома шляхами:

- або через внесення змін до Цивільного кодексу України з формуванням спеціальної деліктної конструкції відповідальності за шкоду, спричинену системами ШІ;
- або через ухвалення спеціального закону про ШІ, який би встановлював окремий режим відповідальності залежно від категорії ризику системи.

Особливо важливо, щоб така відповідальність не розмивалася через договірні конструкції, технічну складність системи або посилання на "непередбачуваність алгоритму". Право має чітко виходити з того, що складність технології не скасовує обов'язку мати юридичного адресата шкоди. У протилежному разі виникне нормативна лакуна, за якої автономність технології фактично перетворюватиметься на засіб уникнення відповідальності.

6.3. Спеціальний захист цифрового сліду дитини

Третя рекомендація стосується створення спеціального законодавчого режиму захисту **цифрового сліду дитини**. Підставою для цього є один із найсильніших результатів дослідження: **80% респондентів** вважають неприйнятним поширення фото- та відеозображень дітей у соціальних мережах. Такий показник свідчить про наявність стійкого суспільного запиту на підвищений захист дітей у цифровому середовищі й дає нормативно вагомий аргумент на користь того, щоб проблема sharenting була виведена з площини суто етичних міркувань у площину спеціального правового регулювання.

Мова йдеться про те, щоб дитина в цифровому середовищі розглядалася не як пасивний об'єкт батьківського чи платформного контролю, а як носій майбутньої цифрової автономії. Саме такий підхід відповідає людиноцентричній моделі права ШІ і водночас посилює захист однієї з найбільш вразливих груп у цифровому суспільстві.

6.4. Заборона або жорстке обмеження автономної самореплікації ШІ

Четверта рекомендація полягає у нормативному закріпленні заборони або принаймні надзвичайно жорсткого регулювання **автономної самореплікації ШІ**. Емпірична основа цієї рекомендації очевидна: **60% респондентів** прямо висловилися

проти можливості самостійного клонування або саморозгортання ШІ. У правовому сенсі це свідчить про сприйняття такої можливості як граничного ризику, пов'язаного не просто з помилкою алгоритму, а з втратою контролю над самою логікою його функціонування.

Для українського законодавства це означає доцільність:

- включення автономної самореплікації ШІ до переліку **заборонених або критично високоризикових практик**;
- запровадження спеціального порядку державного дозволу на будь-які дослідження й експерименти, що передбачають високий рівень самостійного розширення алгоритмічної системи;
- встановлення підвищених вимог до кібербезпеки, audit trail та систем екстреного відключення;
- криміналізації певних форм навмисного створення або запуску неконтрольованих самореплікативних AI-систем, якщо вони становлять загрозу для суспільної безпеки.

Така рекомендація не є "антиінноваційною". Її завдання полягає в тому, щоб установити межу, за якою технологічний розвиток перестає бути керованим правом і починає створювати ризики системного характеру. У цьому аспекті запит аудиторії на обмеження самореплікації ШІ є повністю сумісним із сучасною логікою безпекового регулювання.

6.5. Формування нормативної моделі цифрової юрисдикції і делегованої правоспроможності ШІ

П'ята рекомендація має найбільш стратегічний і водночас найбільш доктринально складний характер. Ідеться про необхідність поступового формування нормативної моделі **цифрової юрисдикції**, яка б охоплювала питання цифрової ідентичності, правового режиму аватарів, алгоритмічних агентів, віртуальних активів та форм делегованої участі ШІ у цифрових правовідносинах. Емпіричним імпульсом для цієї рекомендації є показник **13% респондентів**, готових визнати ШІ суб'єктом права. Хоча цей показник не є домінуючим, його не можна ігнорувати, оскільки він вказує на початок зрушення в суспільному сприйнятті меж правосуб'єктності у цифровому середовищі.

Законодавча робота в цьому напрямі повинна мати не одномоментний, а поетапний характер. Доцільно: розробити **концепцію цифрової юрисдикції** як окремий напрям національної правової політики; сформулювати базові законодавчі дефініції цифрової ідентичності, цифрового агента, аватара, алгоритмічного представника, делегованої правоспроможності; визначити, які саме форми участі ШІ в цифрових правовідносинах можуть бути допустимими без визнання повної правосуб'єктності; закріпити правила ідентифікації, верифікації, доказування та відповідальності у транскордонних цифрових середовищах; у перспективі розглянути можливість розробки **Цифрового кодексу України**, який би системно інтегрував регулювання цифрової юрисдикції, ШІ, віртуальних активів, цифрових ідентичностей та алгоритмічної відповідальності.

Ця рекомендація має особливе значення в контексті євроінтеграції. Європейське право нині переважно рухається шляхом секторального регулювання окремих аспектів цифрового середовища, тоді як Україна має шанс сформувати більш концептуально цілісну, системну модель, у якій цифрова юрисдикція виступатиме не побічною темою, а базовим організуючим принципом права цифрової епохи.

7. ВИСНОВКИ

Проведене дослідження дозволяє сформулювати такі висновки.

По-перше, аудиторія України у 2024–2025 роках демонструє виражений запит на людиноцентричне (human-centric), прозоре та операторські відповідальне регулювання ШІ. Цей запит корелює з вектором EU AI Act та міжнародними стандартами захисту прав людини у цифровому середовищі.

По-друге, авторський ІПЗЦС (~73/100) свідчить про "випереджальну правову зрілість" досліджуваної аудиторії, що формує сприятливий соціальний ґрунт для впровадження гармонізованого з ЄС цифрового законодавства в Україні.

По-третє, кластерний аналіз виявляє структуровану диференціацію суспільства: "скептики" (48%) формують запит на жорстке регулювання, "прагматики" (38%) — на умовно-ліберальні регуляторні моделі, "оптимісти" (14%) — на перспективні доктринальні дискусії про правосуб'єктність ШІ.

По-четверте, показник 13% готових визнати ШІ суб'єктом права є індикатором формування суспільного запиту на "делеговану правоспроможність" алгоритмічних систем у контексті цифрової юрисдикції Metaverse, що потребує доктринального відображення у Цифровому кодексі України.

По-п'яте, отримані дані слугують емпіричним підґрунтям для розробки комплексного регулювання ШІ в Україні та відповідних положень щодо гармонізації з acquis communautaire ЄС у рамках євроінтеграційних зобов'язань. Запропоновані п'ять законодавчих рекомендацій охоплюють ключові напрями: human-in-the-loop, операторська відповідальність, захист цифрових прав дитини, заборона автономної самореплікації та цифрова юрисдикція Metaverse.

У сукупності ці рекомендації формують основу для побудови в Україні не фрагментарного, а цілісного законодавчого режиму регулювання ШІ, який буде сумісним з правом ЄС, але водночас не втратить власної доктринальної суб'єктності.

Загальний висновок дослідження полягає в тому, що українське суспільство — принаймні в його соціально активному сегменті — вже сьогодні виявляє достатній рівень правової готовності до переходу від стихійного використання ШІ до **осмисленого цифрового правопорядку**. Це означає, що подальший розвиток українського законодавства у сфері ШІ має спиратися не лише на зовнішні регуляторні імпульси, а й на внутрішньо сформований суспільний запит на право, яке одночасно буде інноваційним, людиноцентричним, підзвітним і здатним захищати особу в умовах алгоритмічної реальності. Саме в цьому і полягає головне значення проведеного дослідження: воно показує, що майбутнє права ШІ в Україні має будуватися не всупереч суспільству, а в логіці його вже наявної — хоча ще не до кінця кодифікованої — **цифрової правової зрілості**.

Примітки щодо даних: *порівняльні показники Eurobarometer 2024 та Edelman AI Trust 2024 мають орієнтовний характер; кластерна типологія є авторською якісною класифікацією.*

ПОДЯКА: Подяка тижневику "Дзеркало тижня" за співпрацю у просвітницькій та науково-популярній діяльності. Окрема подяку головному редактору видання пані Юлії Мостовій та редактору пані Оксані Оніщенко.

КОНФЛІКТ ІНТЕРЕСІВ: Немає

Використана література

1. Mocanu DM (2022) Gradient Legal Personhood for AI Systems—Painting Continental Legal Shapes Made to Fit Analytical Molds. Front. Robot. AI 8:788179. doi:

10.3389/frobt.2021.788179EdelmanTrustInstitute. (2024). Edelman AI TrustBarometer 2024. https://www.edelman.com/trust

2. Kostenko, O. (2022). Artificial intelligence (AI) and Metaverse: legal aspects. Legal Science Electronic Journal, 8, 301–308. https://doi.org/10.32782/2524-0374/2022-8/66

3. Kostenko, O. (2025). Digitaljurisdiction: model. InformationandLaw, 4(55), 24–45. https://doi.org/10.37750/2616-6798.2025.4(55).346297

4. Kostenko, O., &Furashev, V., Zhuravlov, D., &Dniprov, O. (2022). Genesis of Legal Regulation Web and the Model of the Electronic Jurisdiction of the Metaverse. BratislavaLawReview, 6(2), 21–36. https://doi.org/10.46282/blr.2022.6.2.316

5. Kostenko, O., Zhuravlov, D., Dniprov, O., &Korotiuk, O. (2023). Metaverse: model criminal code. Baltic Journal of Economic Studies, 9(4), 134–147. https://doi.org/10.30525/2256-0742/2023-9-4-134-147

6. Kostenko, O., Zhuravlov, D., Nikitin, V., Manhora, V., Manhora, T., &Gabani, I. (2024). A Typical Cross-Border Metaverse Modelas a Counteractionto Its Fragmentation. Bratislava Law Review, 8(2), 163–176. https://doi.org/10.46282/blr.2024.8.2.844

7. Kostenko, O., &AkefiGhaziani, V. (2024). Admissibility of illegally obtained e-evidence: A critical studyof EU law and the precedent sof the European Court of Human Rights. EuropeanJournalofPrivacyLawand Technologies, 2024(2). https://doi.org/10.2139/ssrn.5050699 [Scopus Q4]

8. Kostenko, O. (2025). AI law model for ethical legislation: Strate gic recommendations for the regulation of artificial intelligence. SciFormatPublishing. https://doi.org/10.69635/978-1-0690482-5-7

9. LoPiano, S. (2020). Ethical princip lesin machine learning and artificial intelligence: Cases from the field and possibl eways forward. Humanities and Social Sciences Communications, 7, 9. https://doi.org/10.1057/s41599-020-0501-9

Олексій Володимрович Костенко
Ph.D, старший дослідник
завідувач лабораторії Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України» 04053, Україна, м. Київ, пров. Несторівський, 4.
email: antizuk@gamil.com

Людмила Олександрівна Шапенко
кандидат юридичних наук, доцент
доцент кафедри права та публічного управління Фінансово-економічного факультету Національної академії статистики, обліку та аудиту
04107, Україна, м. Київ, вулиця Підгірна, 1
email: shapenkol@ukr.net

Oleksiy V. Kostenko
Ph.D, Senior Researcher
Head of the Laboratory of the State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"
4 Nestorivskyi Lane, Kyiv, 04053, Ukraine
email: antizuk@gamil.com

Liudmyla O. Shapenko
Ph.D., Associate Professor
Associate Professor of the Department of Law and Public Administration, Faculty of Finance and Economics National Academy of Statistics, Accounting and Audit
04107, Ukraine, Kyiv, Pidhirna Street, 1
email: shapenkol@ukr.net

Рекомендоване цитування: Костенко О.В., Шапенко Л.О. Сприйняття штучного інтелекту в Україні: соціально-правовий аналіз у вимірі інформаційного права та цифрової юрисдикції. *Інформація і право*. № 2(57)/2026. 2026. С. 42-63. https://doi.org/10.37750/2616-6798.2026.2(57).364302

Suggested Citation: Kostenko O., Shapenko L**.** (2026) Perception of Artificial Intelligence in Ukraine: Socio-Legal Analysis in the Dimension of Information Law and Digital Jurisdiction. *Information and Law*. 2(57)/2026. 42-63. https://doi.org/10.37750/2616-6798.2026.2(57).364302

Дата надходження статті до редакції: 09.04.2026 р.
Дата прийняття статті до друку після рецензування: 23.04.2026 р.
Дата публікації (оприлюднення): 26.05.2026 р.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~