КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ПУБЛІЧНОГО УПРАВЛІННЯ ТА ДЕРЖАВНОЇ СЛУЖБИ
КАФЕДРА ЄВРОІНТЕГРАЦІЙНОЇ ПОЛІТИКИ

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА
на тему

«РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УКРАЇНІ ТА ЄС»

Студентки 2 року навчання ОР «Магістр» заочної форми спеціальності 281 «Публічне управління та адміністрування» освітньо-професійної програми «Європейські студії для публічних управлінців (для державних службовців за замовленням Національного агентства України з питань державної служби)»
Науменко Яни Олександрівни

Науковий керівник:
в.о. завідувача кафедри євроінтеграційної політики, кандидат економічних наук, доцент
Гура Вікторія Леонідівна

Засвідчую, що в цій кваліфікаційній роботі немає запозичень із праць інших авторів без відповідних посилань.
Студентка _____
(підпис)

Робота допущена до захисту в екзаменаційній комісії рішенням кафедри євроінтеграційної політики від «21» листопада 2025 р., протокол № 7 .

В.о. завідувача кафедри євроінтеграційної політики, кандидат економічних наук, доцент
Гура Вікторія Леонідівна _____
(підпис)

КИЇВ – 2025

АНОТАЦІЯ

Науменко Я.О. **Регулювання використання штучного інтелекту в Україні та ЄС.** – Кваліфікаційна магістерська робота на правах рукопису.

Кваліфікаційна магістерська робота на здобуття ступеня вищої освіти другого (магістерського) рівня галузі знань 28 – Публічне управління та адміністрування, спеціальності 281 – Публічне управління та адміністрування. Навчально-науковий інститут публічного управління та державної служби Київського національного університету імені Тараса Шевченка, Київ, 2025.

Актуальність теми полягає в необхідності створення ефективної моделі правового регулювання штучного інтелекту в публічному секторі України в умовах стрімкої цифрової трансформації, євроінтеграційних процесів та безпекових викликів воєнного часу. Впровадження новітніх технологій потребує балансу між стимулюванням інновацій та захистом фундаментальних прав людини, забезпеченням принципів належного врядування та національної безпеки. У роботі проведено комплексний порівняльно-правовий аналіз підходів до регулювання ШІ в Україні та ЄС, досліджено виклики для прозорості та підзвітності влади, спричинені використанням алгоритмічних систем. Особливу увагу приділено аналізу ризик-орієнтованого підходу, закріпленого в Акті про ШІ (EU AI Act), та механізмам його імплементації. Ідентифіковано ключові адміністративно-правові та управлінські бар'єри впровадження ШІ в Україні та розроблено комплексну дорожню карту гармонізації державної політики з європейськими стандартами. Представлені результати можуть бути використані органами державної влади для вдосконалення законодавства та формування стратегії розвитку сфери штучного інтелекту.

Ключові слова: штучний інтелект, публічне управління, EU AI Act, ризик-орієнтований підхід, належне врядування, цифрова трансформація, національна безпека.

ANNOTATION

Naumenko Y.O. **Regulation of the Use of Artificial Intelligence in Ukraine and the EU**. – Qualifying master's thesis in the form of a manuscript.

Qualifying master's thesis for the award of a higher education degree of the second (master's) level in the field of knowledge: 28 Public administration, specialties: 281 Public administration. – The Educational and Scientific Institute of Public Administration and Civil Service of Taras Shevchenko National University of Kyiv, Kyiv, 2025.

The relevance of the topic lies in the need to create an effective model for the legal regulation of artificial intelligence in the public sector of Ukraine in the context of rapid digital transformation, European integration processes, and wartime security challenges. The implementation of emerging technologies requires balancing innovation incentives with the protection of fundamental human rights, ensuring good governance principles, and national security. The thesis conducts a comprehensive comparative legal analysis of AI regulation approaches in Ukraine and the EU, examining the challenges to transparency and accountability of power caused by the use of algorithmic systems. Special attention is paid to the analysis of the risk-based approach enshrined in the EU AI Act and the mechanisms of its implementation. Key administrative, legal, and managerial barriers to AI adoption in Ukraine are identified, and a comprehensive roadmap for harmonizing state policy with European standards is developed. The findings can be utilized by state authorities to improve legislation and formulate a strategy for the development of the artificial intelligence sector.

Keywords: artificial intelligence, public administration, EU AI Act, risk-based approach, good governance, digital transformation, national security.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Сучасний світ переживає четверту промислову революцію, рушійною силою якої є технології штучного інтелекту (ШІ). Проникаючи в усі сфери суспільного життя, від економіки до повсякденних комунікацій, ШІ створює не лише можливості для прогресу, а й фундаментальні виклики для існуючих соціальних, етичних та правових інститутів. Особливої гостроти це питання набуває у сфері публічного управління, де використання ШІ має на меті підвищення ефективності, прозорості та якості надання послуг, але, водночас, створює ризики для порушення прав людини, демократичних процесів та самої суті верховенства права.

Для України, яка обрала стратегічний курс на цифрову трансформацію та європейську інтеграцію, питання адекватного регулювання ШІ має виняткову актуальність. З одного боку, в умовах повномасштабної агресії технології ШІ стали критично важливим інструментом для забезпечення національної безпеки та оборони. З іншого боку, отримання статусу кандидата на вступ до Європейського Союзу покладає на Україну зобов'язання щодо гармонізації національного законодавства з європейським *acquis communautaire*. Ухвалення в ЄС першого у світі комплексного законодавчого акту EU AI Act – встановлює новий глобальний стандарт («Брюссельський ефект») у цій сфері, базуючись на людиноцентричному та ризик-орієнтованому підході.

Таким чином, перед Україною постає подвійне завдання: стимулювати розвиток інноваційних технологій для перемоги та повоєнної відбудови, і водночас – розробити та імплементувати таку модель правового регулювання, яка б відповідала європейським цінностям та захищала фундаментальні права громадян. Відсутність на сьогодні в Україні комплексного законодавства у сфері ШІ, наявність значних адміністративних та управлінських бар'єрів, а також нагальна потреба в гармонізації з правом ЄС зумовлюють актуальність даного дослідження.

Стан наукової розробки проблеми. Проблематика правового та етичного регулювання штучного інтелекту, а також його впровадження у публічний сектор, є предметом активних досліджень зарубіжних науковців. Фундаментальні аспекти впливу цифрових технологій, алгоритмів та «наглядового капіталізму» на суспільство і право висвітлено у працях Ш. Зубофф [91], Ф. Паскуале [68], Дж. Тернера [82] та В. Барфілда [39]. Етичні принципи функціонування ШІ досліджували Л. Флоріді та Дж. Коулз [50].

Значна увага у західній літературі приділена саме регламентації штучного інтелекту в Європейському Союзі, зокрема аналізу EU AI Act. Критичний огляд цього законодавства, питання стандартизації, ризик-орієнтованого підходу та взаємодії з GDPR розробляли М. Віль та Ф. З. Боргезіус [84; 85], Н. Смуга [76], М. Егеланд [47], О. Тамбу [79], М. Алмада [37], М. Еберс [46] та П. Фойт [86].

Окремий потужний пласт досліджень присвячено цифровізації та імплементації ШІ в систему публічного управління та адміністрування. Питання ефективності, прийняття рішень, організаційних змін та ризиків у цій сфері вивчали А. Таїхаг [78], А. Зудервайк [92], Р. Медалья та Л. Тангі [62; 80; 81], П. Мікалеф [64; 65], І. Мергель [63], Т. К. Сун [77] та інші. Проблеми цифрового суверенітету та кібердипломатії аналізували Д. Брудерс [40], М. Мюллер [66], Р. Крімерс [43].

У вітчизняній науці також спостерігається посилення інтересу до цієї проблематики. Загальнотеоретичні питання визначення та сутності ШІ, а також концептуальні моделі його регулювання досліджували О. А. Баранов [2], Р. Є. Еннан [9]. Особливості впровадження ШІ та принципів належного врядування в умовах цифровізації публічного адміністрування розглядали К. О. Гавриленко та А. В. Петровський [5], Р. Р. Марутян [15], О. В. Карпенко [12], К. В. Єсенніков [10], Н. О. Максіменцева [14].

Питання стратегії розвитку ШІ, гармонізації законодавства України з міжнародними стандартами та захисту прав людини висвітлено у працях Г. О. Андрощука [1], В. М. Тарасюка [29], О. В. Турути [31], Ю. І. Тюрі [32].

Специфіку використання ШІ в юриспруденції та окремих галузях аналізували В. І. Гришко [6], В. Ю. Цьомра [34] та інші.

Однак більшість наявних вітчизняних праць мають переважно галузевий або оглядовий характер, а значна частина була написана ще до ухвалення фінальної редакції європейського законодавства. На сьогодні відсутнє комплексне дослідження, яке б системно поєднувало аналіз затвердженого Акту про ШІ (2024 року) з практичними викликами для системи публічного управління та національної безпеки України.

Мета і завдання дослідження. *Метою* магістерської роботи є здійснення комплексного порівняльно-правового аналізу регулювання штучного інтелекту в публічному управлінні України та Європейського Союзу для розробки науково обґрунтованої дорожньої карти гармонізації державної політики України з європейськими стандартами.

Для досягнення поставленої мети було визначено такі **завдання:**

1. Дослідити теоретико-правові засади регулювання штучного інтелекту в публічному управлінні та ідентифікувати ключові виклики, які технології ШІ створюють для принципів належного врядування.
2. Проаналізувати європейську модель правового регулювання ШІ, розкривши сутність ризик-орієнтованого підходу (EU AI Act) та механізми його застосування в публічному секторі ЄС.
3. Здійснити аналіз поточного стану використання ШІ в системі публічного управління України, виявивши ключові адміністративно-правові та управлінські бар'єри на шляху його відповідального впровадження.
4. Провести порівняльний аналіз підходів до регулювання ШІ в Україні та ЄС для визначення основних розбіжностей та пріоритетних напрямів гармонізації національного законодавства.
5. Розробити пропозиції щодо адаптації державної політики України у сфері ШІ до європейських стандартів.

Об’єкт і предмет дослідження. *Об’єктом* дослідження є теоретичні та практичні аспекти правового регулювання штучного інтелекту в Україні та ЄС,

а також шляхи його гармонізації. *Предметом* дослідження є регулювання використання штучного інтелекту в Україні та ЄС.

Методи дослідження. Для досягнення мети та виконання завдань дослідження використано комплекс загальнонаукових та спеціально-юридичних методів, зокрема: порівняльно-правовий метод (при зіставленні норм EU AI Act та законодавства України); системний метод (при аналізі системи регулювання як сукупності взаємопов'язаних елементів); формально-юридичний метод (при тлумаченні норм права); історико-правовий метод (при аналізі еволюції регуляторних підходів); прогностичний метод (при розробці дорожньої карти).

Наукова новизна одержаних результатів полягає в тому, що магістерська робота є одним з комплексних досліджень, присвячених порівняльному аналізу регулювання ШІ в Україні та ЄС після фінального узгодження тексту EU AI Act. Зокрема, наукова новизна конкретизується в таких положеннях:

– *проведено* комплексний аналіз ризик-орієнтованої моделі регулювання, закладеної в EU AI Act, та деталізовано її ключові елементи (класифікація ризиків, обов’язки суб’єктів, система управління) в контексті їх можливої імплементації в Україні;

– *систематизовано* виклики, які створює ШІ для фундаментальних принципів належного врядування (прозорість, підзвітність, справедливість, верховенство права);

– *набуло подальшого розвитку* розуміння комплексу обов'язків, які покладаються на органи публічної влади як користувачів систем ШІ високого ризику;

– *розроблено* проєкт комплексної дорожньої карти гармонізації державної політики України з підходами ЄС, яка охоплює законодавчі, інституційні, освітні та інноваційні аспекти.

Практичне значення одержаних результатів. Результати дослідження можуть бути використані:

– *у законотворчій діяльності* – при розробці проєкту Закону України «Про штучний інтелект» та внесенні змін до секторального законодавства;

– *у правозастосовній діяльності* – для методичного забезпечення органів державної влади, суддів, адвокатів з питань відповідального використання ШІ;

– *у науково-дослідній сфері* – як основа для подальших досліджень окремих аспектів правового регулювання ШІ;

– *у навчальному процесі* – при викладанні курсів з публічного управління та адміністрування, менеджменту, інформаційного права, адміністративного права, європейського права для студентів юридичних та управлінських спеціальностей.

Апробація результатів.

Науменко Я.О. Правове регулювання штучного інтелекту в Україні та ЄС: виклики і напрями гармонізації. Євроінтеграційний дизайн: стратегії відновлення України: матеріали Міжнар. наук.-практ. конф. (Київ, 6 трав. 2025 р.) / за заг. ред. Л. Г. Комахи, М. С. Орлів. Київ: ННІ ПУДС КНУ, 2025. С. 91-93. https://ipacs.knu.ua/pages/osn/2/news/2202/files/cc01cdf1-6c15-449b-bbb7-6977e3de8663.pdf.

Структура та обсяг роботи. Магістерська робота складається зі вступу, трьох розділів, висновків, списку використаних джерел. Загальний обсяг становить 84 сторінки, з яких основний текст – 66 сторінок. Робота містить 9 таблиць, 4 рисунки. Список використаних джерел налічує 94 найменування.

.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПУБЛІЧНОМУ УПРАВЛІННІ

1.1. Наукові підходи до визначення сутності та функцій штучного інтелекту

Феномен штучного інтелекту (далі – ШІ), що стрімко увірвався в усі сфери суспільного життя – від економічного сектору та медицини до державного управління та сфери національної безпеки, – поставив перед сучасною науковою думкою та юридичною практикою фундаментальне і складне завдання: визначення його сутності, меж застосування та функціонального призначення. На наше переконання, складність цього завдання полягає передусім у тому, що ШІ не можна розглядати як статичне явище чи якусь єдину монолітну технологію. Аналіз фахової літератури свідчить, що це динамічна сукупність методів, алгоритмів та систем, які постійно еволюціонують, розмиваючи усталені межі між інструментом, процесом та квазі-суб'єктом, здатним до автономних дій [2; 9; 78].

Слід зазначити, що відсутність єдиного, загальноприйнятого визначення ШІ на міжнародному рівні створює значну «сіру зону» для правового регулювання, оскільки, як слушно зауважують дослідники, неможливо ефективно регулювати те, що не має чітких концептуальних рамок [38; 84]. Саме тому детальний аналіз наукових підходів до визначення сутності та функцій ШІ є необхідною відправною точкою для будь-якого дослідження у сфері його правового регулювання, особливо в такій чутливій сфері, як публічне управління.

Історично термін «штучний інтелект» пов'язують із науковими пошуками середини XX століття, коли він визначався як наука та інженерія створення розумних машин. Це початкове визначення, хоч і було доволі широким, заклало фундамент для розуміння ШІ як наукової дисципліни, спрямованої на

моделювання людських інтелектуальних здібностей. Проте з бурхливим розвитком технологій ця лаконічна дефініція виявилася недостатньою для охоплення всього спектру сучасних систем.

У сучасній науковій літературі, зокрема у фундаментальних працях В. Барфілда [39] та Дж. Тернера [82], можна виокремити декілька ключових підходів до визначення ШІ. Їх умовно можна згрупувати за двома осями: «мислення проти поведінки» та «людиноподібність проти раціональності». Ця класична матриця дозволяє нам систематизувати різноманіття концепцій та виділити чотири основні напрями розуміння природи ШІ:

1. *Системи, що мислять як люди (підхід когнітивного моделювання).* Цей напрям фокусується на відтворенні процесів людського мислення. Метою тут є створення програми, яка моделює внутрішні механізми роботи людського мозку, включаючи нейронні зв’язки та когнітивні процеси. Прихильники цього підходу прагнуть не просто отримати правильний результат, а досягти його тим самим шляхом, яким це робить людина. Однак, з правової точки зору, цей підхід видається нам проблематичним, оскільки перевірити, чи справді машина «мислить» як людина, надзвичайно складно, а внутрішні процеси її роботи часто залишаються непрозорими, створюючи ефект «чорної скриньки» [68].

2. *Системи, що діють як люди (підхід тесту Тюрінга).* Цей напрям пропонує оцінювати інтелект машини за її здатністю імітувати людську поведінку в процесі комунікації настільки переконливо, щоб сторонній спостерігач не зміг відрізнити її від людини. Такий підхід лежить в основі розробки сучасних чат-ботів, віртуальних асистентів та інших систем взаємодії. Проте критики справедливо зазначають, що здатність успішно імітувати діалог не обов'язково свідчить про наявність справжнього інтелекту чи розуміння суті речей, а може бути лише результатом роботи складних алгоритмів розпізнавання патернів [39; 50].

3. *Системи, що мислять раціонально (підхід «законів мислення»).* Цей підхід ставить за мету створення систем, здатних до правильних, логічно обґрунтованих міркувань на основі формальної логіки. Такі системи можуть

робити дедуктивні висновки та вирішувати завдання з чіткою структурою. Однак цей підхід має суттєві обмеження: по-перше, не всі аспекти інтелектуальної діяльності (особливо в управлінні) можна формалізувати; по-друге, в реальному світі часто доводиться діяти в умовах неповної інформації [82].

4. *Системи, що діють раціонально (підхід раціонального агента).* Це домінуючий на сьогодні підхід у науці. Він визначає інтелект як здатність діяти раціонально – тобто обирати дії, які максимізують досягнення мети з урахуванням наявної інформації. «Раціональний агент» – це система, яка сприймає середовище і впливає на нього для реалізації своїх задач. На нашу думку, для юристів та управлінців цей підхід є найбільш прагматичним, оскільки він дозволяє оцінювати ШІ за його діями та наслідками, що є ключовим для визначення відповідальності та встановлення регуляторних меж [90; 92].

Зазначене демонструє, що науковці не мають єдиної відповіді на питання «що таке ШІ?». Проте для цілей правового регулювання та публічного управління такий рівень абстракції є недостатнім. Необхідне більш практичне, функціональне визначення, яке б дозволило чітко окреслити об'єкт регулювання. Усвідомлюючи цю потребу, міжнародні інституції почали розробляти власні робочі дефініції.

Особливо значущим у цьому контексті є підхід Європейського Союзу, який став орієнтиром для багатьох країн, включно з Україною. Експертна група високого рівня з питань штучного інтелекту (High-Level Expert Group on AI) запропонувала широке визначення: системи ШІ – це програмні (а іноді й апаратні) системи, розроблені людьми, які, маючи складну мету, діють у фізичному або цифровому вимірі, сприймаючи своє середовище через збір даних, інтерпретуючи їх та вирішуючи, які найкращі дії вжити для досягнення поставленої мети [53; 54].

Це визначення, яке згодом лягло в основу Акта про штучний інтелект (EU AI Act) [16; 68], є надзвичайно важливим з кількох причин. По-перше, воно є технологічно нейтральним і не прив'язане до конкретних методів, що робить його стійким до майбутніх змін. По-друге, воно акцентує на здатності системи

до певної автономії. По-третє, воно чітко окреслює функціональний цикл роботи ШІ, що подано на рис. 1.1.

Рис. 1.1. Функціональний цикл роботи ШІ

В правовому полі нашої держави також спостерігаються спроби сформулювати власне бачення. Схвалена у 2020 році «Концепція розвитку штучного інтелекту в Україні» визначає ШІ як автономну систему, що є результатом науково-технічної діяльності, яка за допомогою аналізу даних здатна для досягнення визначеної мети робити прогнози, давати рекомендації або приймати рішення [24]. Така дефініція значною мірою корелює з європейським підходом, що є кроком у напрямку гармонізації понятійного апарату з міжнародним. Однак, питання узгодження термінології залишається гострим, оскільки різні наукові школи та нормативні акти можуть вкладати різний зміст у поняття «автономність» чи «рішення» [32].

Таким чином, перший етап нашого аналізу показує еволюцію поняття ШІ від абстрактних філософських концепцій до прагматичних, функціонально-орієнтованих визначень. Саме такий підхід, що фокусується не на тому, чи «мислить» система, а на тому, як вона діє та які ризики створює, став основою для сучасних регуляторних моделей.

Після окреслення загальних концептуальних підходів, необхідно перейти до більш прикладного рівня та розглянути ключові технології, які складають основу сучасного ШІ. Розуміння цих технологій є критично важливим, оскільки саме їхні специфічні властивості породжують унікальні виклики для права [38]. Сучасний ШІ – це «парасольковий термін», що об’єднує ціле сімейство методів, серед яких центральне місце займає машинне навчання (machine learning).

Машинне навчання (МН) – це підрозділ ШІ, що фокусується на розробці алгоритмів, які дозволяють комп'ютерам навчатися на основі даних без прямого

програмування кожного кроку. Замість жорсткого коду з інструкціями, розробники створюють моделі, які самостійно виявляють закономірності. Як влучно зауважує О. А. Баранов, саме здатність до навчання на досвіді є тією якістю, що принципово відрізняє системи ШІ від традиційних програмних продуктів [2].

Варто виділити три основні типи машинного навчання, кожен з яких має свою специфіку застосування в публічному секторі:

1. **Навчання з учителем (supervised learning).** Це найпоширеніший тип. Модель «навчається» на наборі даних, де кожен приклад вже має правильну відповідь. Система аналізує дані й виявляє спільні риси. У публічному управлінні цей підхід може використовуватися для прогнозування рівня безробіття, виявлення типових схем ухилення від податків або класифікації звернень громадян [15; 63].

2. **Навчання без учителя (unsupervised learning).** Тут модель працює з даними без заздалегідь відомих міток. Завдання алгоритму – самостійно знайти приховані структури. Найпоширенішим застосуванням є кластеризація. Такий підхід корисний для сегментації населення при наданні послуг, аналізу суспільної думки або виявлення аномалій у даних, що можуть свідчити про кіберзагрози [12; 22].

3. **Навчання з підкріпленням (reinforcement learning).** Імітує процес навчання методом проб і помилок. Система (агент) взаємодіє з середовищем і отримує «винагороду» або «штраф» за свої дії, прагнучи максимізувати результат. Цей підхід є основою для створення систем управління трафіком або автоматизованих систем на фінансових ринках [78].

Окремим і надзвичайно потужним підрозділом машинного навчання є **глибоке навчання (deep learning)**. Воно базується на використанні штучних нейронних мереж зі складною, багатошаровою архітектурою. Кожен шар такої мережі відповідає за розпізнавання ознак різного рівня складності – від простих форм до абстрактних концепцій. Саме завдяки глибокому навчанню були досягнуті значні успіхи в розпізнаванні мови, зображень та генерації контенту.

Проте ця потужність має і зворотний бік – проблему «чорної скриньки» (black box). Як слушно зазначає Ф. Паскуале, через величезну кількість параметрів у глибоких нейронних мережах часто неможливо пояснити, чому система прийняла те чи інше рішення [68]. Ця непрозорість створює серйозні ризики, особливо коли такі системи використовуються в публічному управлінні для прийняття рішень, що впливають на права громадян, наприклад, у сфері правосуддя або правоохоронній діяльності.

З огляду на технологічні особливості, ми вважаємо за доцільне класифікувати функції штучного інтелекту в контексті публічного управління за кількома напрямами. Така класифікація допомагає зрозуміти, які саме завдання делегуються машинам і які регуляторні виклики при цьому виникають. Для наочності ми систематизували ці функції у табл. 1.1.

Таблиця 1.1

Класифікація функцій систем штучного інтелекту в публічному управлінні та пов'язані регуляторні виклики

Група функцій	Характеристика та приклади застосування	Ключові регуляторні виклики
А. Інформаційно-аналітичні та прогностичні	Обробка великих даних (Big Data), моніторинг суспільної думки, прогнозування соціально-економічних тенденцій, моделювання кризових ситуацій	Якість та репрезентативність даних; ризик алгоритмічної упередженості; захист інформації.
Б. Автоматизація рутинних процесів (роботизація)	Чат-боти для комунікації з громадянами, автоматична обробка кореспонденції, заповнення форм, оптимізація внутрішнього документообігу	Стандарти якості надання послуг; забезпечення доступності для вразливих груп населення (цифровий розрив)
В. Контрольно-наглядові	Виявлення податкового шахрайства, фіксація порушень правил дорожнього руху, митний контроль, системи розпізнавання облич	Втручання у приватне життя (privacy); дотримання принципу презумпції невинуватості; відповідність вимогам GDPR
Г. Автономне прийняття рішень	Автоматичне нарахування соціальних виплат, системи «предикативного правосуддя», автономне управління критичною інфраструктурою	Проблема підзвітності та розподілу відповідальності (responsibility gap); право на оскарження рішення

Джерело: розроблено автором на основі аналізу [5; 15; 35; 61; 78]

Варто детальніше зупинитися на кожній групі:

А. Інформаційно-аналітичні та прогностичні функції. Це одна з найбільш поширених сфер застосування ШІ. Системи здатні обробляти масиви даних, які органи влади збирають у процесі діяльності. До цієї групи належать моніторинг суспільної думки та прогнозування процесів (наприклад, бюджетних надходжень). Як зазначають К. О. Гавриленко та А. В. Петровський, використання ШІ для аналітики дозволяє перейти до принципів належного врядування в умовах цифровізації, забезпечуючи проактивне реагування на проблеми [5].

Б. Автоматизація та оптимізація рутинних процесів. Значна частина роботи держслужбовців пов'язана зі стандартизованими завданнями. ШІ дозволяє автоматизувати документообіг та обробку звернень громадян через віртуальних асистентів. Впровадження таких інструментів, як зазначає Р. Р. Марутян, може суттєво скоротити час надання послуг та зменшити ризик людських помилок [15]. Дослідження Г. Мараньйо підтверджують, що чат-боти стають ефективними «організаційними агентами» в публічному секторі [61].

В. Контрольно-наглядові функції. ШІ слугує потужним інструментом для виявлення порушень. Це одна з найбільш чутливих сфер, оскільки вона безпосередньо зачіпає права людини. Сюди відносяться виявлення фінансового шахрайства та автоматична фіксація правопорушень. Використання ШІ в цій сфері вимагає особливо ретельного регулювання для запобігання дискримінації, про що попереджають європейські регулятори у своїх рекомендаціях щодо технологій розпізнавання облич.

Г. Автономне або напівавтономне прийняття рішень. Це найбільш складна функція, що передбачає делегування машині повноважень приймати юридично значущі рішення (наприклад, призначення соціальних виплат). Делегування таких повноважень машинам ставить під сумнів фундаментальні принципи правової держави, зокрема принципи відповідальності та підзвітності. Саме тому системи, що виконують такі функції, в EU AI Act здебільшого віднесені до категорії «високого ризику» [16; 69].

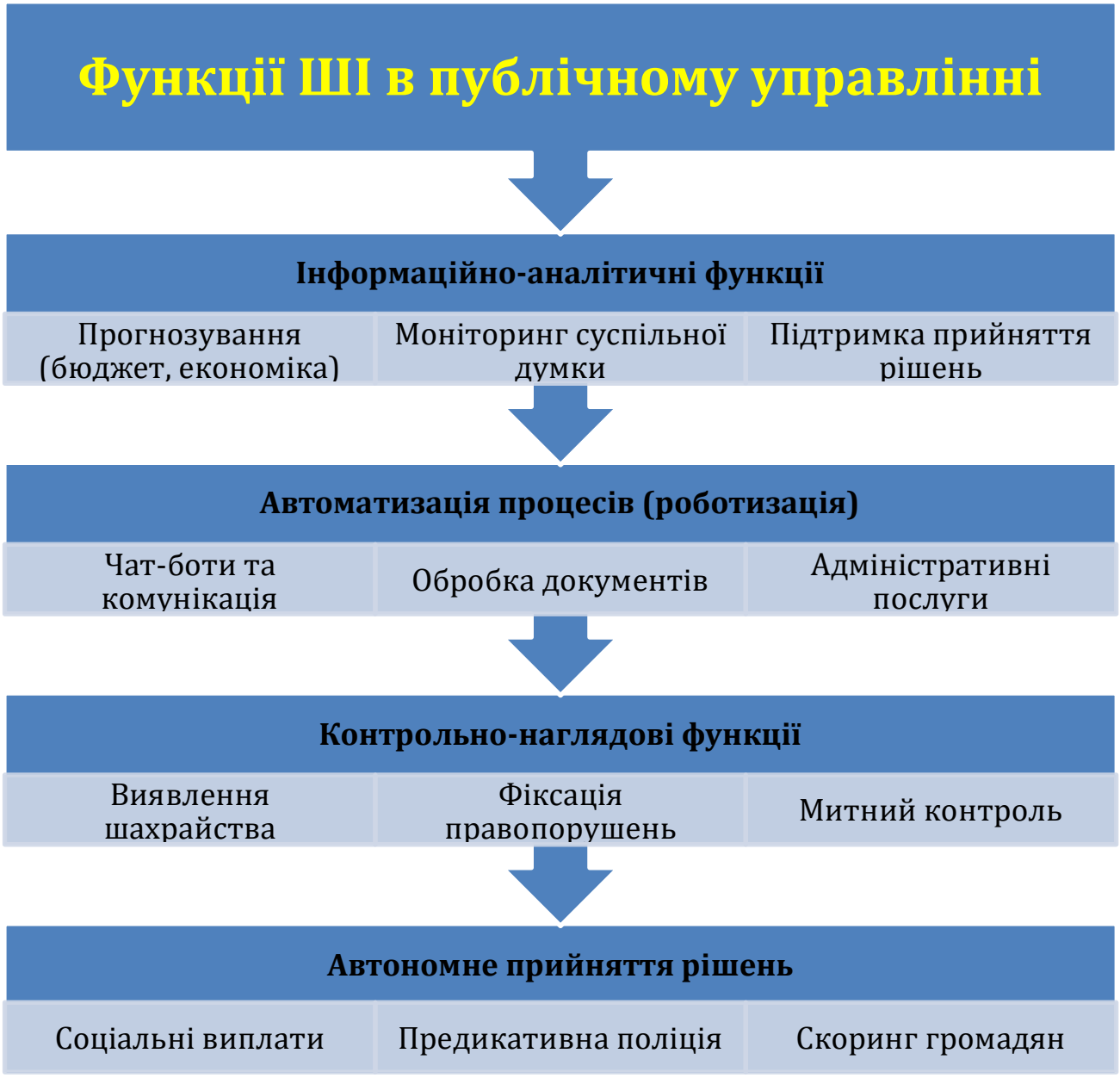

Рис. 1.2. Класифікація функцій систем штучного інтелекту в публічному управлінні

Отже, аналіз наукових підходів до визначення сутності ШІ та його технологічних основ дозволяє нам зробити висновок, що це не просто новий інструмент, а технологія, яка змінює саму природу управлінських процесів. Розуміння цієї функціональної різноманітності є передумовою для розробки адекватних моделей регулювання.

Підсумовуючи цей підрозділ, необхідно наголосити на ключових характеристиках феномену ШІ, які безпосередньо впливають на формування правової політики. Саме ці властивості відрізняють ШІ від попередніх поколінь

цифрових технологій і створюють унікальні виклики. До таких визначальних характеристик, на нашу думку, належать: автономність, непрозорість (складність) та здатність до навчання.

Автономність систем ШІ означає їхню здатність виконувати завдання без постійного контролю людини. Зростання рівня автономії є джерелом як переваг, так і ризиків. Коли автономна система завдає шкоди, виникає фундаментальна правова проблема, яку Г. Зек та інші дослідники називають «прогалиною у відповідальності» (responsibility gap): хто має відповідати – розробник, користувач чи сама система? [89; 90; 92].

Складність та непрозорість («чорна скринька») є другою іманентною властивістю. Внутрішня логіка прийняття рішень може бути незрозумілою навіть для розробників. Це створює перешкоди для забезпечення права на обґрунтоване рішення. Якщо громадянину відмовлено в послузі на підставі алгоритму, неможливість пояснити причини підриває довіру до влади. Тому вимога до пояснення ШІ стає ключовою в сучасних регуляторних актах. Водночас, варто погодитися з думкою дослідників, що «чорна скринька» не завжди є неминучою властивістю – часто це наслідок неналежної розробки та ігнорування процедур верифікації.

Здатність до навчання та адаптації є третьою рисою. Системи ШІ не є статичними; вони можуть змінювати поведінку, навчаючись на нових даних. Це породжує проблему передбачуваності. Система, сертифікована на момент запуску, може з часом діяти у непередбачуваний спосіб. Це створює виклик для механізмів нагляду: як забезпечити відповідність системи протягом усього життєвого циклу? [47; 51].

Усвідомлення цих трьох властивостей призводить до висновку, що традиційні підходи до регулювання є недостатніми. Неможливо регулювати ШІ так само, як звичайне програмне забезпечення. Регулювання має бути комплексним і включати не лише правові норми, а й технічні стандарти та етичні кодекси.

Таким чином, проведений аналіз дозволяє зрозуміти:

1. Для цілей правового регулювання найбільш продуктивним є функціональний, а не онтологічний підхід до визначення ШІ. Важливо оцінювати ризики, які система створює для прав людини та суспільства.

2. Технологічна основа ШІ (машинне навчання) породжує специфічні властивості – автономність та непрозорість, які вимагають нових правових механізмів (зокрема, щодо відповідальності).

3. Різноманіття функцій ШІ в публічному управлінні вимагає диференційованого, ризик-орієнтованого підходу до регулювання.

1.2. Концептуальні моделі регулювання цифрових технологій у публічному секторі

Впровадження штучного інтелекту в публічне управління створює не лише нові технологічні можливості, а й глибокі регуляторні дилеми. Унікальні характеристики ШІ, такі як автономність, здатність до самонавчання та непрозорість («чорна скринька»), ставлять під сумнів адекватність традиційних правових інструментів, розроблених для регулювання більш статичних та передбачуваних об'єктів. Цей розрив між швидкістю технологічного розвитку та інертністю правових систем отримав у науковій літературі назву «проблема темпу» (pacing problem). Як слушно зазначають дослідники Г. Мараньйо та Л. Тангі, державні інституції часто просто не встигають адаптувати нормативну базу під нові реалії [61].

Держави по всьому світу опинилися перед складним вибором: як встановити ефективний контроль над потенційно ризикованими технологіями, не придушивши при цьому інновації, що є рушієм економічного зростання?. Пошук відповіді на це питання призвів до формування та активного обговорення кількох концептуальних моделей регулювання. Кожна з них пропонує свій унікальний баланс між контролем та свободою, безпекою та розвитком.

На наше переконання, аналіз цих моделей є ключовим для розуміння глобальних тенденцій у сфері регулювання ШІ та для розробки адекватної національної стратегії для України. Умовно їх можна класифікувати на кілька основних типів, що варіюються від максимального державного втручання до покладання на саморегуляцію ринку. Розглянемо кожну з них детально.

1. Модель жорсткого регулювання («зверху вниз», top-down command-and-control)

Ця модель є класичним і найбільш звичним для континентальної правової системи підходом. В її основі лежить переконання, що держава, як представник суспільних інтересів, повинна встановлювати чіткі та обов'язкові для всіх правила поведінки через імперативні нормативно-правові акти. Цей підхід передбачає розробку детальних законів, регламентів та стандартів, які прямо наказують або забороняють певні дії.

Теоретичне підґрунтя цієї моделі ґрунтується на концепції державного суверенітету та ієрархічній природі права. Основними інструментами тут виступають:

- *Прямі заборони:* встановлення табу на розробку чи використання технологій, які визнаються суспільно небезпечними.
- *Обов'язкова сертифікація та ліцензування:* вимога до розробників отримувати дозвіл від державного органу перед виведенням продукту на ринок.
- *Імперативні стандарти:* законодавче закріплення вимог до архітектури системи та якості даних.

Головною перевагою жорсткого регулювання є високий рівень правової визначеності. Усі учасники ринку мають чітке розуміння того, що дозволено, а що заборонено. Це створює рівні умови для конкуренції та захищає громадян від свавілля. Такий підхід є незамінним для регулювання сфер, де ризики є надзвичайно високими, а потенційна шкода – незворотною (наприклад, національна безпека чи медицина).

Однак, ця модель зазнає серйозної критики в контексті цифрових технологій. Її головною вадою є низька адаптивність. Законодавчий процес є

тривалим, і поки закон проходить всі етапи ухвалення, технологія може кардинально змінитися. Це призводить до появи «мертвих норм», які не працюють на практиці. Крім того, надмірна регульованість може пригнічувати інновації, створюючи бар'єри для стартапів.

Найбільш яскравим прикладом застосування цієї моделі є запропоновані в європейському законодавстві (EU AI Act) прямі заборони на системи ШІ, що створюють неприйнятний ризик. Зокрема, йдеться про заборону систем, які використовують підсвідомі маніпулятивні техніки, експлуатують вразливості певних груп осіб або здійснюють соціальне рейтингування. У цих випадках законодавець діє безкомпромісно, визнаючи певні практики несумісними з цінностями демократичного суспільства [38; 69].

2. Модель «м'якого права» (soft law) та саморегулювання

На противагу жорсткому регулюванню, у сучасному управлінському дискурсі все більшої популярності набувають гнучкіші підходи. Модель «м'якого права» об'єднує інструменти, які не мають юридично обов'язкової сили в традиційному розумінні, але здатні впливати на поведінку суб'єктів через переконання та репутаційні механізми.

Теоретично ця модель ґрунтується на ідеях партнерства між державним і приватним секторами. Інструментарій тут різноманітний:

- *Етичні кодекси:* документи, що встановлюють моральні орієнтири (наприклад, принципи прозорості та недискримінації).
- *Технічні стандарти:* розробляються організаціями стандартизації (ISO, IEEE) і часто стають де-факто обов'язковими через вимоги ринку.
- *Рекомендації (guidelines):* поради щодо найкращих практик розробки.

Головною перевагою гнучких моделей є їхня швидкість та адаптивність. Стандарти можуть оновлюватися значно швидше за закони. Другою важливою перевагою, на яку вказують дослідники, є залучення експертизи: до розробки правил долучаються інженери та науковці, що робить норми технічно

обґрунтованими [46]. Крім того, коли індустрія сама бере участь у створенні правил, зростає ймовірність їх добровільного дотримання.

Проте підхід «м'якого права» має суттєві вади. Ключова проблема – відсутність механізмів примусу. Якщо дотримання правил суперечить комерційним інтересам, компанії можуть їх ігнорувати. Також існує ризик «етичного відмивання» (ethics washing), коли компанії публічно декларують прихильність до етичних принципів лише з маркетинговою метою, не змінюючи реальних бізнес-практик.

Незважаючи на критику, інструменти «м'якого права» відіграли важливу роль у формуванні глобального дискурсу. Яскравими прикладами є «Етичні рекомендації для надійного ШІ» (2019), розроблені Експертною групою високого рівня ЄС [54], та Принципи ШІ ОЕСР, які підтримала й Україна. Вони стали фундаментом, на якому пізніше почало будуватися «тверде» законодавство.

3. Модель співрегулювання (co-regulation)

Співрегулювання є гібридним підходом, який намагається поєднати переваги жорсткого та м'якого права. У цій моделі держава не відмовляється від своєї регуляторної ролі, але ділить її з представниками індустрії. Загальна схема виглядає наступним чином: законодавець встановлює в законі рамкові цілі, принципи та основні вимоги, а також визначає відповідальність за їх порушення. Однак детальні технічні специфікації та стандарти делегуються для розробки спеціалізованим саморегулівним або стандартизаційним організаціям.

Класичним механізмом тут є посилання в законі на технічні стандарти. Наприклад, закон може встановити загальну вимогу: «система ШІ високого ризику повинна мати високий рівень кібербезпеки». А що саме означає «високий рівень» і як його досягти, визначається у відповідному стандарті, розробленому європейськими організаціями (CEN/CENELEC). Дотримання такого гармонізованого стандарту створює презумпцію відповідності вимогам закону, що значно спрощує життя бізнесу [43].

Перевагою співрегулювання є те, що воно забезпечує баланс між юридичною обов'язковістю (від держави) та технічною компетентністю (від індустрії). Саме ця модель, поєднана з ризик-орієнтованим підходом, лежить в основі нової регуляторної філософії Європейського Союзу [62].

4. Принципо-орієнтована модель (principles-based regulation)

Еволюція регуляторної думки призвела до появи моделі, яка є відповіддю на проблему швидкого застарівання правил. Замість того, щоб намагатися передбачити всі можливі сценарії, законодавець встановлює низку високорівневих принципів, які мають слугувати дороговказом.

В основі моделі лежить ідея, що право має встановлювати кінцеву мету. Ключовими механізмами є:

- *Законодавче закріплення принципів:* прозорість, справедливість, підзвітність.
- *Обов'язок доведення відповідності (accountability):* компанії повинні демонструвати регулятору, як саме їхні процеси забезпечують дотримання принципів.
- *Privacy/Ethics by Design:* вимога інтегрувати етичні міркування в процес розробки.

Головною перевагою є гнучкість та довговічність норм. Принцип «справедливості» залишатиметься актуальним незалежно від технології. Однак, як зазначають критики, абстрактність принципів може створювати правову невизначеність: бізнесу важко зрозуміти, які саме заходи є достатніми для виконання вимог закону. Найяскравішим прикладом цієї моделі є GDPR, який базується на принципах обробки даних та відповідальності контролера [11].

5. Ризик-орієнтована модель (risk-based approach)

Ця модель є, по суті, синтезом попередніх підходів. Вона визнає, що штучний інтелект не є монолітним явищем, і різні його застосування несуть абсолютно різний рівень небезпеки. Тому застосовувати універсальні правила до всіх систем було б неефективно. Ідея полягає в диференціації вимог залежно від рівня потенційної шкоди.

В основі моделі лежить принцип пропорційності. EU AI Act пропонує чотирирівневу піраміду ризиків, яка стала глобальним стандартом [38; 41]:

1. *Неприйнятний ризик:* системи, що суперечать цінностям (наприклад, соціальний скоринг). Вони підлягають повній забороні (елемент жорсткого регулювання).

2. *Високий ризик:* системи в критичних сферах (медицина, транспорт, правосуддя). Вони підлягають суворим вимогам щодо сертифікації, якості даних та нагляду.

3. *Обмежений ризик:* системи, що несуть ризик маніпуляції (чат-боти, діпфейки). Для них встановлюються вимоги прозорості (інформування користувача).

4. *Мінімальний ризик:* переважна більшість систем. Для них заохочується добровільне прийняття етичних кодексів.

Головна перевага цього підходу – збалансованість. Він дозволяє сконцентрувати ресурси держави на найбільш небезпечних ділянках. Однак ключовою проблемою залишається складність класифікації ризиків у динамічному середовищі, про що попереджають дослідники.

Для наочності та систематизації розглянутих підходів ми узагальнили їх у порівняльній таблиці.

Таблиця 1.2

Порівняльна характеристика концептуальних моделей регулювання цифрових технологій

Модель регулювання	Сутність та інструменти	Переваги	Недоліки та ризики
Жорстке регулювання (Command-and-Control)	Імперативні норми, прямі заборони, ліцензування.	Висока правова визначеність, захист публічних інтересів, рівні умови для всіх.	Низька гнучкість, «проблема темпу», гальмування інновацій, ризик появи «мертвих норм»
М'яке право (Soft Law)	Етичні кодекси, рекомендації, добровільні стандарти.	Адаптивність, швидкість розробки, використання технічної експертизи бізнесу.	Відсутність примусу, ризик ігнорування правил, феномен «ethics washing»

Співрегулювання (Co-regulation)	Рамкові закони + технічні стандарти галузі.	Баланс між стабільністю закону та технічною актуальністю стандартів.	Ризик домінування великих корпорацій при розробці стандартів, складність нагляду.
Принципо-орієнтована (Principles-based)	Встановлення цілей та принципів (прозорість, підзвітність).	Технологічна нейтральність, довговічність регулювання, стимулювання відповідальності.	Правова невизначеність для бізнесу, складність перевірки відповідності
Ризик-орієнтована (Risk-based)	Диференціація вимог залежно від рівня ризику (піраміда).	Пропорційність втручання, ефективний розподіл ресурсів, підтримка інновацій.	Складність класифікації систем, ризик помилкової оцінки рівня небезпеки

Джерело: складено автором на основі [43; 48; 50; 61]

Таким чином, проведений аналіз показує чітку еволюцію від простих ієрархічних моделей до складних, гібридних систем. Сучасний регуляторний мейнстрім, яскраво представлений політикою ЄС, базується саме на ризик-орієнтованій моделі. Вона інтегрує в себе елементи всіх інших підходів: заборони для найнебезпечнішого, жорсткі вимоги для ризикованого, принципи прозорості для потенційно оманливого і саморегулювання для безпечного.

На наше переконання, саме ця модель, найімовірніше, стане основою і для майбутньої системи регулювання ШІ в Україні в процесі її гармонізації з європейським правовим полем. Вона дозволяє врахувати як потребу в захисті прав громадян, так і необхідність цифрового розвитку держави.

1.3. Виклики для забезпечення принципів належного врядування в умовах використання ШІ

Концепція належного врядування (good governance) є, без перебільшення, наріжним каменем сучасної демократичної правової держави. Як зазначають вітчизняні дослідники, вона охоплює низку фундаментальних принципів, що визначають характер взаємовідносин між державою та громадянином, і

спрямована на те, щоб діяльність органів публічної влади була прозорою, підзвітною, ефективною, справедливою та орієнтованою на захист прав людини [12].

Ці принципи, вироблені століттями політико-правового розвитку, включають верховенство права, прозорість, участь громадськості та недискримінацію. Однак, на наше переконання, стрімке впровадження систем штучного інтелекту в процеси прийняття державних рішень створює безпрецедентні виклики для кожного з них, змушуючи переосмислити їхній зміст та механізми забезпечення в нових цифрових реаліях.

Аналіз світової практики показує, що інтеграція ШІ відбувається стрімко. Наприклад, Міністерство фінансів США розпочало використовувати машинне навчання для автоматизації аналізу фінансових даних ще наприкінці 2022 року. Це дозволило виявляти приховані закономірності та шахрайство. У Франції технології на базі ШІ використовуються для автоматизації процесів отримання ліцензій, що прискорює адміністративні процеси. Безперечно, така інтеграція обіцяє значні переваги: підвищення ефективності, зменшення корупційних ризиків та прийняття більш обґрунтованих рішень на основі аналізу великих даних.

Проте, як слушно зауважують дослідники, ці переваги не є автоматичними і супроводжуються серйозними ризиками ерозії фундаментальних засад врядування. На нашу думку, варто детально розглянути, як саме унікальні властивості ШІ – автономність, складність та здатність до навчання – створюють виклики для ключових принципів належного врядування.

1. Виклик для принципу прозорості та права на обґрунтоване рішення

Принцип прозорості (транспарентності) передбачає, що діяльність органів влади має бути відкритою. Важливою складовою цього є право особи знати, на яких підставах було прийнято управлінське рішення. Однак саме цей принцип опиняється під найбільшою загрозою через властивість непрозорості («чорної скриньки»), притаманну сучасним системам ШІ.

Ми виділяємо декілька аспектів цієї проблеми:

- *Технічна непрозорість.* Мільярди параметрів у нейронній мережі унеможливлюють відстеження логічного ланцюжка від вхідних даних до результату. Коли система відмовляє особі у наданні соціальної допомоги, державний службовець часто не може пояснити логіку алгоритму, оскільки сам її не розуміє. Це явище, яке дослідники називають «автоматизованим бездумним виконанням», становить серйозну загрозу [63].
- *Комерційна таємниця.* Навіть якщо логіку можна пояснити, розробники часто відмовляються розкривати її, посилаючись на захист інтелектуальної власності. В результаті державний орган використовує систему, повний контроль над якою він не має, а громадянин позбавлений можливості перевірити її справедливість.

Наслідком ерозії прозорості є підрив довіри до державних інституцій та неможливість ефективного оскарження рішень у суді. Відповіддю на цей виклик є концепція пояснюваного ШІ (Explainable AI), яка вимагає, щоб рішення системи можна було пояснити у зрозумілій для людини формі, що відображено і в рекомендаціях європейських інституцій [38; 41].

2. Виклик для принципів підзвітності та відповідальності

Принцип підзвітності (accountability) означає, що державні органи зобов'язані звітувати за свої рішення. Впровадження ШІ розмиває традиційні лінії відповідальності, створюючи так звану «прогалину у відповідальності» (responsibility gap) [89; 90].

Проблема полягає у розподіленій відповідальності. У життєвому циклі системи беруть участь розробник, постачальник даних, оператор (державний орган) та кінцевий користувач. Кожен з них може перекладати провину за помилку на іншого. Крім того, здатність систем до самонавчання означає, що їхня поведінка може змінюватися у непередбачуваний спосіб. Чи може розробник відповідати за систему, яка еволюціонувала після випуску? Це питання залишається відкритим для науковців.

На нашу думку, розмивання відповідальності є вкрай небезпечним, оскільки може призвести до «алгоритмічного урядування», де рішення

приймаються без людської участі та відповідальності. Для подолання цього виклику EU AI Act встановлює чіткі обов'язки для всіх учасників ланцюжка.

3. Виклик для принципів справедливості, рівності та недискримінації

Поширена віра в те, що алгоритми є об'єктивними та нейтральними, часто виявляється ілюзією. На практиці системи ШІ можуть відтворювати та посилювати існуючі в суспільстві упередження (algorithmic bias).

- *Упередженість у даних (data bias).* Системи навчаються на історичних даних. Якщо в цих даних існують системні упередження (наприклад, щодо арештів певних меншин), модель неминуче їх засвоїть. Це створює замкнене коло дискримінації.
- *Упередженість у проєктуванні (model bias).* Розробники можуть обрати параметри, які опосередковано корелюють із захищеними ознаками (наприклад, поштовий індекс як замінник расової приналежності), що призводить до прихованої дискримінації [60].

Це явище отримало назву «відмивання упереджень через технологію». Воно легітимізує дискримінацію, маскуючи її під технічну об'єктивність. У результаті ШІ може стати інструментом для створення цифрової нерівності.

4. Виклик для принципу верховенства права

Принцип верховенства права (rule of law) означає, що дії влади мають бути передбачуваними та базуватися на законі. Впровадження ШІ створює загрозу правовій визначеності. Системи, що постійно навчаються, можуть вносити елемент непередбачуваності у прийняття рішень.

Також існує ризик заміни верховенства права «верховенством коду» (rule of code), про що попереджав Дж. Левіс [61]. Алгоритми можуть застосовувати правила автоматично, без врахування контексту та пом'якшувальних обставин, що призводить до дегуманізації права. Крім того, проблема «чорної скриньки» ускладнює судовий контроль, роблячи його формальним.

5. Виклик для принципу участі громадськості (public participation)

Демократичне врядування передбачає, що громадяни мають право брати участь у прийнятті рішень. Однак, на наше переконання, впровадження ШІ може

призвести до формування технократичної елітарності. Існує ризик, що рішення будуть прийматися вузьким колом експертів та алгоритмів, які нібито володіють «об'єктивним знанням». У такій моделі громадська думка може розглядатися як ірраціональний «шум», що заважає оптимізації процесів. Це може призвести до деполітизації важливих питань, коли вони подаються як суто технічні завдання.

З іншого боку, технології ШІ можуть використовуватися для маніпуляції громадською думкою. Алгоритми здатні аналізувати профілі людей, визначати їхні вразливості та поширювати таргетовану дезінформацію, впливаючи на вибори. Використання ботів може створювати ілюзію масової підтримки певних ініціатив, спотворюючи реальну картину [62].

6. Виклик для права на приватність та захист персональних даних

Ефективне функціонування ШІ нерозривно пов'язане зі збором величезних масивів даних. Це створює загрозу всеохоплюючого нагляду. Як зазначає Ш. Зубофф, людський досвід перетворюється на сировину для алгоритмів [91]. Коли ці механізми використовуються державою, виникає ризик побудови системи тотального контролю (наприклад, через соціальний рейтинг), що є неприйнятним для демократичних суспільств.

Навіть анонімні дані можуть бути розшифровані потужними алгоритмами, що дозволяє створювати детальні цифрові профілі громадян (про їхні погляди, здоров'я, поведінку) без їхньої згоди [15]. Це має «охолоджуючий ефект» на демократію: люди, знаючи про стеження, стають менш схильними до висловлення незгодних думок.

Ми узагальнили основні виклики у табл. 1.3.

Таблиця 1.3

Вплив технологій штучного інтелекту на принципи належного врядування

Принцип належного врядування	**Сутність виклику з боку ШІ**	**Потенційні негативні наслідки**	**Шляхи мінімізації ризиків (регуляторна відповідь)**
Прозорість (Transparency)	Технічна непрозорість («чорна скринька») та комерційна таємниця алгоритмів.	Неможливість обґрунтувати рішення громадянину;	Впровадження вимог до пояснюваності (Explainable AI);

		підрив довіри до влади	відкритість коду для публічного сектору.
Підзвітність (Accountability)	Розмивання відповідальності між розробником, постачальником даних та користувачем.	«Прогалина у відповідальності» (responsibility gap); уникнення покарання за помилки	Чіткий законодавчий розподіл ролей та обов'язків (як в EU AI Act); механізми аудиту алгоритмів.
Справедливість та недискримінація	Алгоритмічна упередженість (bias) через неякісні історичні дані або дизайн моделі.	Дискримінація вразливих груп; «відмивання упереджень» через технологію	Вимоги до якості та репрезентативності даних; тестування на упередженість перед запуском.
Верховенство права (Rule of Law)	Непередбачуваність рішень самонавчальних систем; автоматичне застосування жорстких правил.	Правова невизначеність; заміна права кодом (rule of code); формальний судовий контроль	Заборона повної автоматизації у чутливих сферах; обов'язковий людський нагляд (human-in-the-loop).
Приватність (Privacy)	Масовий збір даних для навчання моделей; ризик розкриття даних та профайлінгу.	Тотальний нагляд; втручання в особисте життя; «охолоджуючий ефект» для демократії	Мінімізація даних; суворе дотримання GDPR; заборона неприйнятних практик (соц. рейтинг).

Джерело: розроблено автором на основі [40; 48; 60]

Комплексний аналіз дозволяє нам зробити висновок, що ми маємо справу з фундаментальним зрушенням у природі управління. Ці виклики є взаємопов'язаними: непрозорість ускладнює підзвітність, а відсутність підзвітності робить дискримінацію безкарною. У сукупності це створює ризик формування алгократії – влади алгоритмів, яка є формально ефективною, але непрозорою та непідконтрольною суспільству.

Відповідь на ці виклики не може полягати у відмові від технологій. На нашу думку, вона має полягати у розробці парадигми «цифрового конституціоналізму», де права людини технологічно «вбудовані» (by design) в архітектуру державних систем. Саме в цьому контексті слід розглядати регуляторні ініціативи Європейського Союзу, які є спробою дати системну відповідь на ці екзистенційні загрози.

Висновки до Розділу 1

У першому розділі магістерської роботи нами було сформовано теоретико-методологічний базис для подальшого дослідження правового регулювання штучного інтелекту в публічному секторі. Узагальнення проведеного аналізу дозволяє зробити наступні висновки.

По-перше, дослідження наукових підходів до розуміння ШІ засвідчило, що для цілей правового регулювання абстрактні філософські концепції («машина, що мислить») є малоефективними. На наше переконання, найбільш продуктивним є функціональний підхід (зокрема, концепція «раціонального агента»), який розглядає ШІ через призму його здатності автономно сприймати середовище та діяти для досягнення мети. Ми з'ясували, що саме технологічна специфіка сучасного ШІ – передусім використання машинного навчання – породжує три ключові властивості, які створюють виклики для права: автономність (що призводить до розмивання відповідальності), непрозорість (проблема «чорної скриньки») та здатність до адаптації (непередбачуваність поведінки після запуску).

По-друге, аналіз регуляторних моделей через призму «проблеми темпу» (pacing problem) продемонстрував еволюцію від жорсткого адміністративного регулювання до більш гнучких форм. Ми дійшли висновку, що класична модель «command-and-control» є занадто повільною для динамічних технологій, а модель «м'якого права» не забезпечує належного примусу та породжує ризик «етичного відмивання». Враховуючи це, найбільш збалансованою стратегією на сьогодні видається ризик-орієнтована модель, поєднана з елементами співрегулювання. Саме цей підхід, що передбачає диференціацію вимог залежно від рівня загрози (від повної заборони до мінімального нагляду), став фундаментом європейської політики та є орієнтиром для України.

По-третє, ми встановили, що інтеграція ШІ в систему публічного управління несе не лише ефективність, а й системні загрози для принципів

належного врядування. Зокрема, ідентифіковано конфлікт між технологічними можливостями та демократичними цінностями:

- технічна непрозорість алгоритмів підриває право на обґрунтоване рішення;
- дифузія ролей між розробником і користувачем створює «прогалину у відповідальності» (responsibility gap);
- алгоритмічна упередженість загрожує принципам справедливості та недискримінації;
- ризик технократизму та маніпуляцій нівелює реальну участь громадськості.

Підсумовуючи, можна стверджувати, що без належного правового запобіжника цифровізація державного сектору ризикує перетворитися на алгократію – систему, де рішення приймаються непрозорими алгоритмами поза демократичним контролем. Це актуалізує необхідність впровадження принципів «цифрового конституціоналізму» та гармонізації законодавства України з європейськими стандартами, аналіз яких стане предметом нашого дослідження у наступному розділі.

РОЗДІЛ 2
ОСОБЛИВОСТІ РЕГУЛЮВАННЯ ШІ В ЄВРОПЕЙСЬКОМУ СОЮЗІ

2.1. Ризик-орієнтований підхід EU AI Act як основа регулювання ШІ

Акт про штучний інтелект Європейського Союзу (EU AI Act) є першою у світі спробою створити всеохоплюючу, горизонтальну законодавчу рамку для регулювання штучного інтелекту. Цей амбітний проєкт, запропонований Європейською Комісією у квітні 2021 року та остаточно узгоджений наприкінці 2023 року, став результатом багаторічних дискусій, консультацій та наукових досліджень, що відображено у таких програмних документах, як «Біла книга про штучний інтелект» [88] та «Скоординований план з питань штучного інтелекту» [36]. Фундаментальною філософією, що лежить в основі всієї архітектури Акту, є ризик-орієнтований підхід (risk-based approach). На наше переконання, цей вибір не був випадковим; він став свідомою відповіддю на подвійний виклик, що стояв перед європейськими інституціями: з одного боку, необхідність захистити фундаментальні права, безпеку та демократичні цінності громадян ЄС від потенційних загроз з боку потужних та непрозорих технологій, а з іншого – прагнення не стримувати інновації та зберегти конкурентоспроможність європейської економіки на глобальному технологічному ринку.

Ризик-орієнтована модель, як було проаналізовано в попередньому розділі, базується на принципі пропорційності: регуляторне навантаження повинно бути прямо пропорційним рівню ризику, який несе конкретне застосування ШІ. Замість того, щоб намагатися врегулювати «штучний інтелект» як єдине абстрактне явище, європейський законодавець вирішив класифікувати системи ШІ за їхнім потенційним впливом на суспільство. Ця класифікація утворює чітку ієрархічну структуру, яку умовно можна зобразити у вигляді чотирирівневої «регуляторної піраміди». Кожен рівень цієї піраміди відповідає певному ступеню ризику та передбачає свій, відмінний режим правового регулювання – від повної заборони на вершині до мінімального втручання біля її

основи [6; 50]. Такий підхід дозволяє сконцентрувати увагу та ресурси регуляторів, розробників та громадськості на тих сферах, де загрози є найбільш серйозними, водночас створюючи сприятливі умови для розвитку переважної більшості безпечних та корисних застосувань ШІ.

На найвищому рівні регуляторної піраміди знаходяться системи ШІ, використання яких вважається таким, що становить «явну загрозу безпеці, засобам до існування та правам людей». Такі системи, за логікою Акта, є несумісними з фундаментальними цінностями Європейського Союзу, закріпленими в Хартії основних прав ЄС, такими як людська гідність, свобода, демократія та верховенство права. Тому, замість того, щоб намагатися мінімізувати їхні ризики, законодавець обирає найрадикальніший інструмент – повну заборону (стаття 5 AI Act) [88]. Цей перелік заборон є відносно коротким, але має величезне символічне та практичне значення, оскільки він проводить чіткі «червоні лінії», перетинати які в демократичному суспільстві є неприпустимим.

До категорії заборонених належать, насамперед, використання маніпулятивних або підсвідомих технік. Забороняються системи ШІ, які використовують підсвідомі техніки, що виходять за межі свідомості людини, або цілеспрямовано маніпулятивні чи оманливі техніки з метою суттєвого спотворення поведінки особи. Ключовою умовою є те, що таке спотворення має призводити або з високою ймовірністю може призвести до фізичної чи психологічної шкоди для цієї особи або іншої особи. Ця норма спрямована на захист людської автономії та свободи волі від технологій, що можуть непомітно змушувати людей діяти всупереч їхнім інтересам [76].

Також забороняється використання вразливостей певних груп. Йдеться про системи ШІ, які використовують будь-які вразливості певної групи осіб, пов'язані з їхнім віком, фізичною чи психічною інвалідністю, з метою суттвого спотворення поведінки особи з цієї групи у спосіб, що завдає або може завдати шкоди. Ця норма є конкретизацією принципу недискримінації та посиленого захисту вразливих категорій населення.

Особливу увагу привертає заборона систем соціального рейтингування органами публічної влади. Забороняється використання систем ШІ для оцінки або класифікації надійності фізичних осіб протягом певного періоду часу на основі їхньої соціальної поведінки або відомих чи прогнозованих особистих характеристик. Ця норма є прямою відповіддю на практику побудови систем «соціального кредиту» в деяких країнах та розглядається в ЄС як фундаментально несумісна з принципами демократії [30; 43]. Вона покликана запобігти виникненню суспільства тотального контролю.

Ще однією, чи не найбільш обговорюваною забороною, є використання «реальночасової» дистанційної біометричної ідентифікації в громадських місцях для правоохоронних цілей. Така практика вважається надзвичайно інвазивною для права на приватність. Однак, розуміючи потреби безпеки, законодавець передбачив вичерпний перелік вузьких винятків (пошук жертв викрадення, запобігання тероризму), використання яких вимагає судової санкції [48].

Якщо вершина регуляторної піраміди є відносно вузькою, то наступний рівень – системи штучного інтелекту високого ризику (High-Risk AI Systems) – становить концептуальне та практичне ядро всього Акту про ШІ. Саме для цієї категорії систем розроблено найбільш детальний та вимогливий режим регулювання. На відміну від заборонених практик, системи високого ризику не вважаються апріорі шкідливими; навпаки, вони можуть приносити значну суспільну користь у таких критично важливих сферах, як медицина, освіта, правосуддя. Однак, через специфіку свого застосування, вони несуть значний потенційний ризик заподіяння шкоди. Тому основна мета регулятора полягає не в тому, щоб їх заборонити, а в тому, щоб гарантувати їхню безпеку та прозорість [21].

Процес ідентифікації систем ШІ як високоризикових є складним. Законодавець обрав контекстно-залежний підхід: ризик оцінюється не на основі технології, а на основі її призначення. Акт про ШІ встановлює два основні шляхи класифікації (стаття 6 AI Act) [88]. Перший стосується систем ШІ, які є компонентами безпеки продуктів, що вже підпадають під дію секторального

законодавства ЄС (ліфти, автомобілі, медичні вироби). Другий шлях – це автономні системи ШІ у визначених критичних сферах (Додаток ІІІ документу).

Цей перелік є результатом ретельного аналізу тих застосувань ШІ, де помилка або збій системи може мати найбільш серйозні наслідки. До цих сфер належать: біометрична ідентифікація (крім забороненої), управління критичною інфраструктурою, освіта та професійна підготовка, зайнятість та управління персоналом (де упереджені алгоритми можуть призвести до дискримінації [69]), доступ до основних приватних та державних послуг (наприклад, кредитний скоринг), правоохоронна діяльність, управління міграцією та відправлення правосуддя. Важливим нововведенням є «фільтр значного ризику», який дозволяє не вважати систему високоризиковою, якщо вона не несе суттєвої загрози правам людини, що додає механізму необхідної гнучкості.

Після детального аналізу систем з неприйнятним та високим ризиком, які становлять вершину та серцевину регуляторної піраміди EU AI Act, для повноти картини необхідно розглянути її нижні, але не менш важливі рівні. Це системи з обмеженим ризиком (Limited Risk) та мінімальним або нульовим ризиком (Minimal or No Risk). Саме ці категорії охоплюють переважну більшість систем ШІ, які вже сьогодні використовуються громадянами та бізнесом.

Третій рівень піраміди об'єднує системи ШІ, які, хоч і не становлять прямої загрози для безпеки чи фундаментальних прав, проте несуть специфічний ризик обману, маніпуляції або введення в оману. Основна проблема полягає в тому, що користувач може не усвідомлювати, що він взаємодіє з машиною, а не з людиною. Тому єдиною, але важливою вимогою до таких систем є обов'язок забезпечення прозорості (стаття 52 AI Act) [88].

Цей обов'язок реалізується через кілька правил:

1. *Системи взаємодії з фізичними особами (чат-боти).* Користувачі повинні бути поінформовані, що вони спілкуються з ШІ. Це дозволяє людині розуміти контекст і не стати жертвою маніпуляції.

2. *Системи розпізнавання емоцій.* Особи, які піддаються впливу таких систем, мають бути про це повідомлені.

3. *Генеративний ШІ та діпфейки.* Контент, що зображує реальних людей або події і є штучно створеним, має бути відповідним чином маркований. Ця вимога є критично важливою для боротьби з дезінформацією в епоху пост-правди.

Основою піраміди є системи з мінімальним або нульовим ризиком. Ця категорія включає переважну більшість застосувань: спам-фільтри, відеоігри, системи рекомендацій. Для цієї категорії Акт не встановлює жодних юридично обов'язкових вимог, щоб не створювати перешкод для інновацій. Однак, як зазначається у «Білій книзі про штучний інтелект», навіть тут заохочується добровільне прийняття етичних кодексів поведінки [28; 88]. Це може стати інструментом для компаній, щоб продемонструвати свою соціальну відповідальність.

Для систематизації ризик-орієнтованого підходу ми розробили узагальнюючу таблицю.

Таблиця 2.1

Класифікація систем штучного інтелекту за рівнем ризику згідно з EU AI Act

Рівень ризику	Характеристика систем	Приклади застосування	Регуляторний режим (вимоги)
Неприйнятний (Unacceptable Risk)	Системи, що створюють явну загрозу правам людини та безпеці. Несумісні з цінностями ЄС.	Соціальний скоринг, маніпулятивні системи, біометрична ідентифікація в реальному часі (з винятками).	**Повна заборона** на розміщення на ринку та використання
Високий (High Risk)	Системи, що можуть завдати значної шкоди здоров'ю, безпеці або правам людини.	ШІ в медицині, транспорті, освіті, правосудді, управлінні міграцією, рекрутингу.	**Суворі вимоги:** оцінка відповідності, управління ризиками, якість даних, прозорість, людський нагляд, кібербезпека
Обмежений (Limited Risk)	Системи, що несуть ризик маніпуляції або введення в оману (impersonation).	Чат-боти, системи розпізнавання емоцій, діпфейки (deepfakes).	**Вимоги прозорості:** інформування користувача про взаємодію з ШІ; маркування

			згенерованого контенту
Мінімальний (Minimal Risk)	Системи з незначним впливом на права людини.	Спам-фільтри, відеоігри, інструменти оптимізації логістики.	**Відсутність обов'язкових вимог.** Заохочення добровільних кодексів поведінки

Джерело: розроблено автором на основі [14; 16; 69; 88]

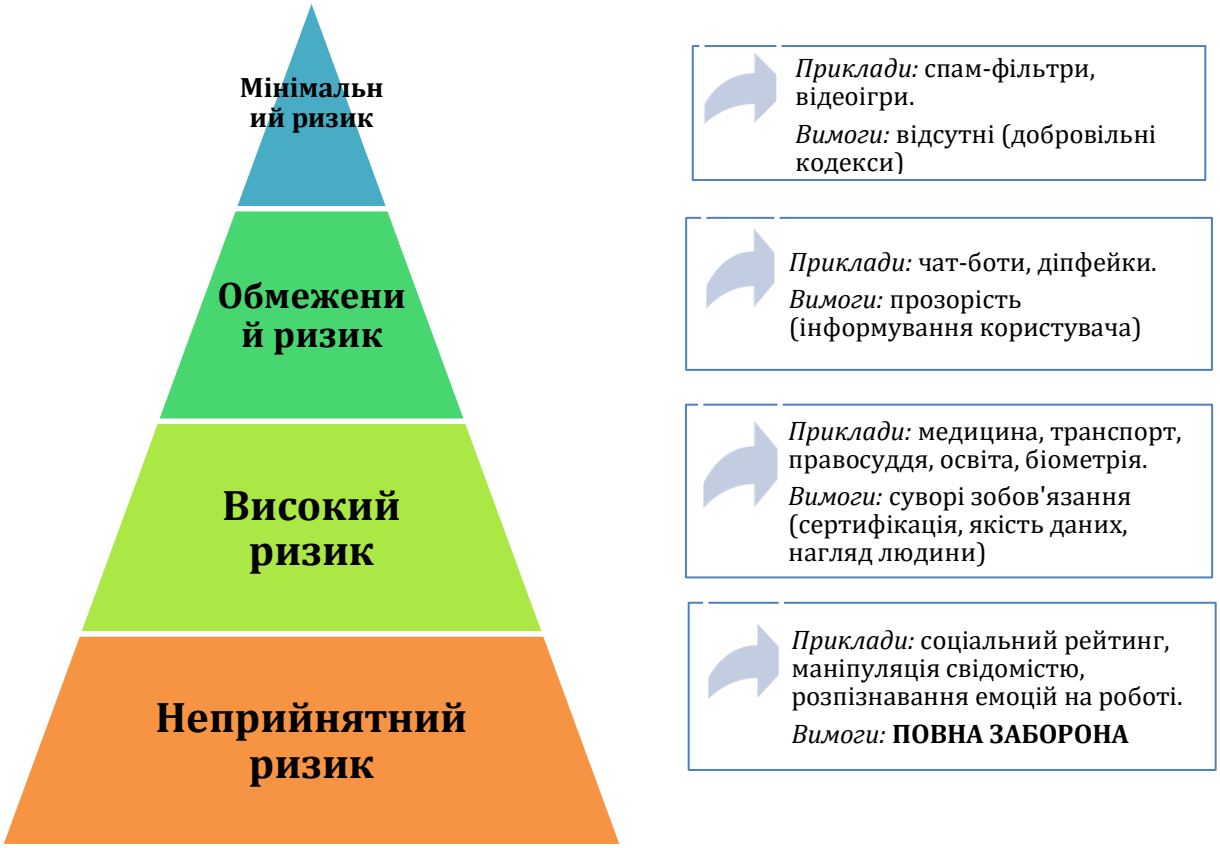

Рис. 2.1. Ризик-орієнтована модель регулювання згідно з Актом про ШІ (EU AI Act).

Проаналізувавши всі чотири рівні регуляторної піраміди EU AI Act, можна зробити висновок про її комплексність. Ризик-орієнтований підхід дозволив європейському законодавцю створити гнучку систему, яка встановлює етичні межі, гарантує безпеку в критичних сферах та захищає користувачів від обману, водночас не блокуючи інновації.

Ця модель є спробою знайти «золоту середину» і позиціонується ЄС як шлях побудови надійного та людиноцентричного ШІ. Звісно, вона не позбавлена критики: дослідники вказують на потенційну складність класифікації ризиків та

адміністративний тягар. Проте, безсумнівно, EU AI Act став найвпливовішою спробою врегулювати цю технологію і слугуватиме зразком для України на її шляху до євроінтеграції.

2.2. Обов’язки органів публічної влади у використанні систем ШІ високого ризику

Після того, як ми визначили, що ризик-орієнтований підхід є фундаментом європейського регулювання, логічним наступним кроком є детальний аналіз конкретних обов’язків, які Акт про ШІ покладає на суб’єктів, що працюють із системами високого ризику. Цей підрозділ ми фокусуємо на обов’язках органів публічної влади, оскільки саме вони є одночасно потужними користувачами таких систем і гарантами дотримання прав громадян.

Важливо зазначити, що EU AI Act створює комплексну систему розподіленої відповідальності. Хоча головний тягар вимог покладається на провайдера (розробника), значні обов'язки виникають і у користувача (оператора) системи. Цей підхід є вкрай важливим, оскільки, як зазначають дослідники, навіть ідеально розроблена система може завдати шкоди, якщо її неправильно впровадити або використовувати в непередбаченому контексті.

Спочатку коротко окреслимо фундаментальні вимоги до систем високого ризику (обов'язки провайдера), оскільки саме вони є базою для подальших дій користувача. Згідно з Главою 2 Розділу III Акту [88], провайдер зобов'язаний забезпечити:

1. **Систему управління ризиками (стаття 9).** Це безперервний процес ідентифікації, оцінки та мінімізації ризиків протягом усього життєвого циклу системи.
2. **Якість даних (Data Governance) (стаття 10).** Набори даних повинні бути репрезентативними та вільними від помилок. Це критично важливо для

боротьби з алгоритмічною дискримінацією, про яку ми згадували в першому розділі.

3. **Технічну документацію (стаття 11).** Створення детального опису архітектури та логіки системи.

4. **Ведення журналів (стаття 12).** Автоматична фіксація подій (логування) для можливості розслідування інцидентів.

5. **Прозорість (стаття 13).** Надання інструкцій, які дозволяють користувачам розуміти та інтерпретувати результати роботи системи [88].

Ці вимоги є основою безпеки. Однак, коли система потрапляє до органу публічної влади, виникає новий набір обов'язків, викладених у статті 29 Акта. Розглянемо їх детально.

1. Обов'язок використання за призначенням та належний людський нагляд

Це два фундаментальні та взаємопов'язані обов'язки.

- *Використання відповідно до інструкцій.* Орган влади зобов'язаний використовувати систему суворо відповідно до цілей, визначених провайдером. Наприклад, систему, розроблену для аналізу медичних знімків, не можна використовувати для інших цілей. Також необхідно забезпечити якість вхідних даних [21].
- *Забезпечення ефективного людського нагляду (Human Oversight).* На наше переконання, це найважливіший обов'язок. Законодавець виходить з принципу, що фінальне рішення, яке має наслідки для людини, ніколи не повинно прийматися машиною повністю автономно. Завжди має залишатися «людина в циклі» (human-in-the-loop). Орган влади повинен:
  - Призначити компетентних осіб для нагляду.
  - Забезпечити розуміння ними можливостей та обмежень системи.
  - Надати їм повноваження втручатися в роботу системи або скасовувати її рішення.

- Впровадити заходи для уникнення «автоматизаційної упередженості» (automation bias), коли людина схильна надмірно довіряти машині [54].

2. Обов'язки щодо моніторингу та звітності

Орган влади виступає «очима та вухами» регулятора на місцях. Він зобов'язаний:

- Моніторити роботу системи та негайно припинити її використання у разі виявлення серйозних ризиків.
- Повідомляти провайдера та національні наглядові органи про серйозні інциденти або збої. Це дозволяє своєчасно реагувати на системні проблеми [44].

3. Обов'язок ведення журналів (Record-keeping)

Користувач зобов'язаний зберігати автоматично згенеровані журнали (логи) роботи системи протягом щонайменше шести місяців. Це є критично важливим для пост-фактум контролю. Наприклад, у разі скарги громадянина на несправедливе рішення, саме логи дозволять перевірити, на основі яких параметрів воно було прийнято.

4. Оцінка впливу на фундаментальні права (FRIA)

Це одна з найважливіших новел фінальної версії Акта (стаття 29а), яка має особливе значення саме для публічного сектору. Перед введенням в експлуатацію системи високого ризику державний орган зобов'язаний провести оцінку її впливу на фундаментальні права (Fundamental Rights Impact Assessment). Вона включає опис процесів, категорій осіб, на яких впливатиме система, та конкретних ризиків дискримінації чи порушення приватності. Результати цієї оцінки мають бути опубліковані, що забезпечує громадський контроль ще до початку використання технології [88].

На додаток до фундаментальних обов'язків щодо належного використання та оцінки впливу, Акт про ШІ встановлює ще кілька важливих процедурних гарантій, які посилюють прозорість та підзвітність органів влади.

5. Обов'язок реєстрації у загальноєвропейській базі даних (стаття 51)

Для забезпечення прозорості ринку Акт передбачає створення публічної бази даних ЄС. Важливо, що обов'язок реєстрації покладається не лише на провайдерів, а й на користувачів, які є державними органами.

Органи публічної влади зобов'язані зареєструвати інформацію про системи ШІ високого ризику, які вони використовують. Ця вимога є ключовим інструментом громадського контролю. Вона дозволяє будь-якому громадянину чи журналісту перевірити, які саме системи використовує, наприклад, поліція чи міністерство соціальної політики. Це сприяє публічним дебатам та підвищує політичну відповідальність влади [88].

6. Обов'язки щодо прозорості стосовно фізичних осіб

Хоча пряма норма про індивідуальне інформування для систем високого ризику сформульована не так чітко, як для систем обмеженого ризику, цей обов'язок випливає із загальної логіки Акту та європейського адміністративного права.

Якщо рішення, прийняте органом влади за допомогою ШІ, має негативні наслідки для особи, вона має право отримати пояснення. Це право базується на:

- Обов'язку провайдера забезпечити прозорість системи (стаття 13) [91].
- Вимогах GDPR (статті 13–15, 22), які надають особі право на втручання людини та отримання інформації про логіку автоматизованої обробки [11].
- Хартії основних прав ЄС (право на належне адміністрування).

Таким чином, орган влади не може просто послатися на «рішення комп'ютера». Він зобов'язаний надати зрозуміле пояснення причин прийнятого рішення, що є необхідною умовою для його оскарження.

Для систематизації розглянутих вимог ми розробили таблицю, що узагальнює обов'язки різних суб'єктів.

Таблиця 2.2

Розподіл обов'язків між провайдером та користувачем (органом влади) щодо систем ШІ високого ризику

Категорія обов'язку	Провайдер (розробник)	Користувач (орган публічної влади)
Управління ризиками	Створення системи управління ризиками (Risk Management System); тестування системи.	Моніторинг роботи системи; припинення використання у разі виявлення ризиків.
Дані та документація	Забезпечення якості та репрезентативності даних; створення технічної документації	Використання якісних вхідних даних; збереження автоматично згенерованих журналів (логів)
Людський нагляд	Проектування системи з можливістю людського нагляду (Human Oversight by design)	Призначення компетентних наглядачів; забезпечення реального втручання в роботу системи
Прозорість та звітність	Надання інструкцій користувачу; реєстрація системи в базі даних ЄС	Реєстрація факту використання системи в базі ЄС; повідомлення про серйозні інциденти; проведення оцінки впливу (FRIA)
Захист прав осіб	Забезпечення точності, надійності та кібербезпеки системи	Інформування осіб, щодо яких приймаються рішення; забезпечення права на оскарження

Джерело: розроблено автором на основі статей 9–15, 29, 51 EU AI Act [88]

Аналіз обов'язків дозволяє зробити висновок про створення багаторівневої системи запобіжників. Вона включає:

1. *Технологічні запобіжники* (якість даних, кібербезпека), що забезпечуються провайдером.

2. *Організаційні запобіжники* (людський нагляд, FRIA), що забезпечуються органом влади.

3. *Інституційні запобіжники* (публічна база даних, звітність), що забезпечують громадський контроль.

Ця модель відображає розуміння того, що відповідальність за використання потужних технологій має бути розподілена. Орган влади перетворюється з пасивного споживача на активного суб'єкта, відповідального

за безпечну інтеграцію ШІ. Водночас, практична реалізація цих вимог вимагатиме значних зусиль: підвищення цифрової грамотності службовців та зміни культури прийняття рішень.

2.3. Інституційно-правові механізми нагляду та контролю в ЄС

Розробка детального переліку обов'язків для провайдерів та користувачів систем ШІ високого ризику є лише першим кроком у побудові ефективної регуляторної рамки. Другим, і не менш важливим, є створення дієвої системи управління (governance), яка б забезпечувала дотримання цих правил на практиці. Акт про ШІ передбачає створення складної, багаторівневої архітектури нагляду та контролю, що поєднує в собі елементи централізації на рівні ЄС та децентралізації на рівні держав-членів. Ця система покликана виконувати кілька ключових функцій: забезпечувати належну оцінку відповідності систем перед їх виходом на ринок, здійснювати постійний ринковий нагляд, розслідувати інциденти та гарантувати однакове застосування Акту на всій території Союзу [88].

На наше переконання, цю інституційну рамку можна розділити на чотири ключові елементи: (1) система оцінки відповідності; (2) національні наглядові органи; (3) новостворені інституції ЄС (Офіс з питань ШІ та Рада); (4) механізми захисту прав фізичних осіб. Розглянемо кожен з них детально.

1. Система оцінки відповідності (Conformity Assessment)

Перш ніж система ШІ високого ризику може бути легально розміщена на ринку, вона повинна пройти процедуру оцінки відповідності. Результатом успішного проходження є складання декларації про відповідність та нанесення маркування CE, яке слугує своєрідним «технічним паспортом» [44]. Акт передбачає два основні шляхи проведення цієї оцінки (стаття 43):

- **Внутрішній контроль (самооцінка).** Для більшості систем високого ризику (Додаток III) провайдер може самостійно провести оцінку. Цей

підхід покладає на нього величезну відповідальність. Важливою умовою є використання гармонізованих стандартів, що створює презумпцію відповідності.

- **Оцінка відповідності третьою стороною.** Для найбільш критичних систем (наприклад, дистанційна біометрична ідентифікація) самооцінки недостатньо. Акт вимагає залучення незалежного нотифікованого органу (notified body), який проводить аудит системи управління якістю та технічної документації [91].

2. Національні наглядові органи (National Supervisory Authorities)

Після того, як система потрапила на ринок, контроль переходить до національних органів. Акт зобов'язує кожну державу-члена призначити компетентні органи, які відповідатимуть за ринковий нагляд. Їхні повноваження є надзвичайно широкими:

- Проведення планових та позапланових перевірок;
- Доступ до інформації (включно з вихідним кодом та даними);
- Вжиття коригувальних заходів (аж до відкликання системи з ринку);
- Накладення штрафів, які можуть сягати 35 млн євро або 7% від світового обороту компанії [69]. Це створює потужний економічний стимул для дотримання правил.

3. Наднаціональні інституції ЄС

Щоб уникнути фрагментації регулювання, коли в одній країні правила застосовуються суворо, а в іншій – поблажливо, європейський законодавець створив два ключові органи на рівні ЄС.

Європейська рада з питань штучного інтелекту (European AI Board). Це координаційний орган, що складається з керівників національних наглядових органів та представника Європейської Комісії. Її роль нагадує EDPB у сфері захисту даних. Основні завдання Ради включають:

- Сприяння узгодженому застосуванню Акта (видання рекомендацій та guidelines).

- Координація діяльності національних органів при розслідуванні транскордонних справ.
- Консультування Комісії щодо оновлення переліку систем високого ризику [88].

Офіс з питань ШІ (AI Office). Якщо Рада координує, то Офіс, створений у структурі Європейської Комісії, має прямі виконавчі повноваження. Його створення стало відповіддю на стрімкий розвиток моделей ШІ загального призначення (GPAI), таких як GPT-4. До речі, у жовтні 2024 року Єврокомісія анонсувала запуск власного інструменту *GPT@EC* для внутрішнього використання. Ключові повноваження Офісу:

- Нагляд за моделями ШІ загального призначення (GPAI). Це ексклюзивна компетенція Офісу. Він контролюватиме дотримання провайдерами таких моделей спеціальних вимог.
- Управління центральною базою даних ЄС.
- Моніторинг виконання Акту та виявлення системних ризиків.

Таким чином, Рада та Офіс створюють дворівневу систему управління: Рада забезпечує координацію «знизу вверх», а Офіс – нагляд «зверху вниз» за найбільш стратегічними сегментами.

Останнім, але, на нашу думку, чи не найважливішим елементом системи контролю є механізми захисту прав фізичних осіб. Адже кінцевою метою всього регулювання є не просто відповідність стандартам, а захист людей від шкоди. Акт про ШІ створює низку інструментів, що дозволяють громадянам відстоювати свої права. Ми розглядаємо ці механізми як «третю лінію оборони», яка активується, коли превентивні заходи не спрацювали.

5. Механізми захисту та правові засоби для фізичних осіб

- *Право на подання скарги (Right to lodge a complaint).* Акт прямо закріплює право будь-якої особи подати скаргу до національного наглядового органу, якщо вона вважає, що система ШІ порушує вимоги законодавства (стаття 63). Це ключовий інструмент громадського контролю «знизу вверх». Орган

зобов'язаний розглянути скаргу та поінформувати про результати. Цей механізм аналогічний до GDPR і вже довів свою ефективність [11; 88].

- *Право на пояснення (Right to an explanation).* Як зазначалося в попередніх підрозділах, користувачі систем високого ризику зобов'язані здійснювати людський нагляд. Нова стаття 68c фінальної версії Акту встановлює, що особи, щодо яких приймається рішення системою високого ризику, мають право отримати «чітке та змістовне пояснення» щодо ролі системи та її основної логіки. Це критично важливо для подолання проблеми «чорної скриньки» та реалізації права на ефективний захист [63].
- *Право на ефективний засіб правового захисту.* Це право, гарантоване Хартією основних прав ЄС, дозволяє особі звернутися до суду для оскарження рішення або відшкодування шкоди. Для полегшення доказування в складних технічних справах Директива про відповідальність за ШІ вводить презумпцію причинно-наслідкового зв'язку: якщо доведено невиконання обов'язків провайдером, суд може припустити, що саме це призвело до шкоди [86].

Для наочності ми систематизували інституційну архітектуру нагляду в табл. 2.3.

Таблиця 2.3

Інституційно-правові механізми нагляду та контролю в ЄС

Рівень нагляду	Ключові суб'єкти	Основні функції та повноваження
Превентивний (Ex-ante)	Провайдер (самооцінка) та нотифіковані органи (третя сторона)	Оцінка відповідності системи перед виходом на ринок; видача сертифікатів ЄС; нанесення маркування CE
Національний (Ex-post)	Національні наглядові органи держав-членів	Ринковий нагляд; перевірки систем на місцях; розслідування інцидентів; накладення штрафів; розгляд скарг громадян
Наднаціональний (ЄС)	Європейська рада з ШІ (координація) та Офіс з питань ШІ (виконавчий орган)	Забезпечення єдиного застосування Акта; нагляд за моделями загального призначення (GPAI); управління базою даних ЄС

Громадський / Індивідуальний	Фізичні особи (суб'єкти даних), громадські організації	Подання скарг; вимога надання пояснень; судові позови про відшкодування шкоди

Джерело: розроблено автором на основі [15; 38; 43]

Отже, ми розуміємо, що Акт про ШІ створює комплексну систему:

1. *Превентивний етап:* система оцінки відповідності гарантує, що на ринок потрапляють лише безпечні продукти.
2. *Поточний етап:* дворівнева система нагляду (національні органи + інституції ЄС) забезпечує моніторинг ринку та координацію.
3. *Етап захисту:* право на скаргу та судовий захист надає громадянам інструменти для відновлення порушених прав.

Ця багатогранна архітектура є відповіддю на складність об'єкта регулювання. Вона визнає, що жоден окремий механізм не впорається з викликами ШІ. Лише синергія технічних стандартів, державного примусу та активної участі громадян може створити екосистему надійного ШІ. Практична ефективність цієї конструкції залежатиме від якості імплементації, але концептуально вона закладає міцний фундамент, який слугуватиме орієнтиром і для України.

Висновки до Розділу 2

У другому розділі магістерської роботи нами було проведено комплексний аналіз правового регулювання штучного інтелекту в Європейському Союзі, стрижнем якого є Акт про ШІ (EU AI Act).

По-перше, ми з’ясували, що фундаментом європейської регуляторної архітектури є ризик-орієнтований підхід. Ця модель є свідомим вибором, спрямованим на пошук балансу між захистом прав громадян та підтримкою інновацій. Шляхом класифікації систем ШІ за чотирма рівнями ризику («регуляторна піраміда») європейський законодавець створив гнучку систему:

- найсуворіші заходи (повна заборона) застосовуються лише до практик, що суперечать цінностям ЄС (соціальний скоринг, маніпуляція);
- детальні вимоги встановлюються для критичних сфер (медицина, правосуддя);
- для систем з ризиком обману (чат-боти) діє лише вимога прозорості;
- більшість безпечних технологій залишається поза межами жорсткого регулювання.

По-третє, ми проаналізували обов'язки суб'єктів, що працюють із системами високого ризику. Встановлено, що Акт запроваджує модель розподіленої відповідальності. Провайдери відповідають за технічну безпеку («design for safety»), якість даних та документацію. Натомість на користувачів, особливо органи публічної влади, покладається критично важлива роль у забезпеченні безпечної експлуатації. Ми довели, що ключовими запобіжниками тут виступають:

- обов'язок ефективного людського нагляду («human-in-the-loop»);
- проведення оцінки впливу на фундаментальні права (FRIA) перед впровадженням системи;
- реєстрація у публічній базі даних ЄС, що забезпечує прозорість держави перед суспільством.

По-третє, дослідження інституційного механізму показало, що ЄС будує ешелоновану систему нагляду, яка поєднує:

- Превентивний контроль: через процедури оцінки відповідності та сертифікацію.
- Поточний нагляд: через діяльність національних органів та централізовану координацію з боку новостворених Офісу з питань ШІ та Європейської ради з ШІ.
- Захист прав: через надання громадянам права на скаргу, пояснення та судовий захист.

Таким чином, у цьому розділі доведено, що Акт про ШІ є не просто набором технічних правил, а цілісною екосистемою, яка встановлює новий глобальний стандарт. Розуміння цієї логіки є критично важливим для України в контексті євроінтеграції.

РОЗДІЛ 3
ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ТА РЕГУЛЮВАННЯ ШІ В ПУБЛІЧНОМУ УПРАВЛІННІ УКРАЇНИ

3.1. Поточний стан та перспективи застосування ШІ в органах влади України

Після детального аналізу передового європейського досвіду у сфері регулювання штучного інтелекту, на нашу думку, критично важливим є звернення до українських реалій. Україна, обравши стратегічний курс на європейську інтеграцію, демонструє значний прогрес у цифровій трансформації, що особливо яскраво проявилося в умовах повномасштабної агресії. Розвиток сфери ШІ та його інтеграція в публічне управління є невід'ємною частиною цього процесу. Водночас, цей процес відбувається в умовах унікальних викликів, пов'язаних з війною, економічними труднощами та необхідністю швидкої гармонізації законодавства [28].

Аналіз поточного стану застосування ШІ в органах влади України доцільно проводити у двох площинах: по-перше, розглядаючи стратегічне та нормативне підґрунтя, і, по-друге, аналізуючи конкретні практичні кейси.

Усвідомлення важливості штучного інтелекту на найвищому державному рівні відбулося відносно нещодавно. Першим і на сьогодні головним стратегічним документом є Концепція розвитку штучного інтелекту в Україні, схвалена розпорядженням Кабінету Міністрів України від 2 грудня 2020 року № 1556-р [24]. Цей документ заклав основи, що значною мірою корелюють з європейськими підходами. Концепція визначає пріоритетні сфери застосування ШІ: публічне управління, національна безпека, правосуддя, охорона здоров'я та економіка.

Важливо, що Концепція наголошує на необхідності дотримання людиноцентричного підходу, вказуючи, що технології мають сприяти дотриманню прав людини. На її виконання було схвалено План заходів на 2021–

2024 роки [30]. Окрім цього, розвиток ШІ вписується в контекст «Дорожньої карти з інтеграції України до Єдиного цифрового ринку ЄС» [7; 8].

Знаковим етапом у формуванні сучасної державної політики стала презентація Міністерством цифрової трансформації у червні 2024 року «Білої книги з регулювання ШІ в Україні». У цьому документі запропоновано перехід до так званого «Bottom-up» підходу (від меншого до більшого), який передбачає поступовий рух до обов'язкового законодавчого регулювання. Суть концепції полягає у розділенні процесу на два етапи: підготовчий (2–3 роки), під час якого бізнесу надаються інструменти для добровільної адаптації (регуляторна пісочниця, маркування, кодекси поведінки), та фінальний — імплементація закону-аналогу EU AI Act.

Важливо підкреслити, що з огляду на умови воєнного стану, у Білій книзі чітко зафіксовано позицію щодо сфери оборони: вона залишається поза межами пропонованого регулювання. Це зумовлено національними інтересами та необхідністю безперешкодного впровадження інновацій для відсічі агресії, щоб не ставити Україну в менш вигідне становище порівняно з ворогом [3]

Але зважаючи на те, що в Україні відсутнє комплексне законодавство, подібного до EU AI Act, державні органи вже активно впроваджують рішення на основі ШІ. Розглянемо найбільш показові кейси.

1. Сфера надання публічних послуг та взаємодії з громадянами

Флагманом тут є екосистема «Дія». Більше того, у 2025 році було зафіксовано світовий рекорд: *Дія.AI* став першим у світі ШІ-асистентом, який надає державні послуги на національному рівні [7].

Більше того, Книга світових рекордів визнала створення Дія.AI досягненням у категоріях «Вперше» та «Винаходи». Це перший у світі ШІ-асистент, який надає громадянам державні послуги на національному рівні. Рекорд зафіксували під час WINWIN Summit у Києві 4 листопада 2025 року. Міжнародне визнання рекорду підтвердило унікальність української цифрової розробки — ШІ-асистента Дія.AI, запущеного у вересні 2025 року. Це перший у світі приклад використання штучного інтелекту на національному рівні для

надання держпослуг. Дія.AI розроблено за сприяння проєкту «Цифровізація для зростання, доброчесності та прозорості» (UK DIGIT), що виконується Фондом Євразія і фінансується UK Dev, та за підтримки швейцарсько-української програми EGAP, що виконується Фондом Східна Європа [33].

Крім того планується інтегрувати голосовий штучний інтелект у Дію та інші сервіси. У цьому допоможе ElevenLabs — світовий лідер у сфері голосового ШІ та багатомовних голосових агентів. Ключовий напрям — інтеграція передових голосових ШІ- та агентивних технологій компанії в державні сервіси, які розвиває команда Мінцифри. Технології дозволять громадянам отримувати послуги та консультації, просто озвучивши свій запит у чаті. Мінцифри уже використовує технології ElevenLabs: перший продукт — відтворення голосу міністра Михайла Федорова для його цифрового двійника. Планується інтегрувати інноваційні голосові технології в Дію, Мрію та Дія.Освіта. У підсумку Україна тепер прагне увійти до трійки лідерів у сфері ШІ до 2030 року, рухаючись до проактивної «агентивної держави» [17].

2. Сфера національної безпеки та оборони

Повномасштабне вторгнення стало каталізатором впровадження ШІ у секторі безпеки. Україна стала полігоном для тестування innovative рішень:

- *Аналіз розвідувальних даних:* платформи на кшталт Palantir допомагають обробляти супутникові знімки та дані OSINT для ідентифікації цілей.
- *Безпілотні системи:* ШІ забезпечує автономну навігацію БПЛА та морських дронів (наприклад, MAGURA V5) в умовах дії РЕБ.
- *Кібербезпека:* алгоритми машинного навчання використовуються для виявлення аномалій у трафіку та захисту критичної інфраструктури [22].

3. Сфера правосуддя та правоохоронної діяльності

Впровадження ШІ тут відбувається обережніше. У рамках ЄСІТС розробляються модулі для автоматичного розподілу справ. Системи «Безпечне місто» використовують комп'ютерний зір для розпізнавання номерних знаків та пошуку осіб, хоча це викликає дискусії щодо приватності [15].

4. Антикорупційна діяльність

НАЗК та Держаудитслужба використовують аналітичні інструменти для виявлення ризиків у деклараціях та системі Prozorro. Алгоритми автоматично знаходять невідповідності у доходах або зв'язки між учасниками тендерів. Держфінмоніторинг застосовує ШІ для виявлення підозрілих транзакцій [23].

Для наочності ми узагальнили ключові сфери застосування ШІ в Україні в табл. 3.1.

Таблиця 3.1

Сфери та приклади застосування систем ШІ в органах публічної влади України

Сфера	*Приклади застосування ШІ*	*Мета впровадження*
Публічні послуги	Асистент Дія.AI; чат-боти держорганів; ШІ-аватар МЗС.	Підвищення якості сервісу, швидкості обслуговування, автоматизація консультацій
Оборона та безпека	Аналіз розвідданих (Palantir); автономні дрони; системи кіберзахисту.	Досягнення асиметричної переваги на полі бою; захист критичної інфраструктури
Аграрний сектор	Аналіз супутникових знімків (Cropwise Operations); прогнозування врожайності.	Моніторинг земельних ресурсів, продовольча безпека.
Правосуддя та правопорядок	Авторозподіл судових справ; системи відеоаналітики «Безпечне місто»	Забезпечення неупередженості розподілу справ; громадська безпека
Антикорупція	Автоматичний аналіз декларацій та тендерів (Prozorro); фінмоніторинг.	Виявлення корупційних ризиків та відмивання коштів

Джерело: складено автором на основі [7; 9; 30]

Отже, практичне застосування ШІ в Україні вже не є питанням майбутнього. Технології активно використовуються, проте цей процес є фрагментарним. Відсутність єдиної правової рамки створює ризики, про які йшлося в першому розділі.

Проведений аналіз стратегічного бачення та конкретних кейсів застосування ШІ в Україні малює картину динамічного, хоча й дещо хаотичного процесу. Україна перебуває на роздоріжжі, де величезні перспективи стикаються

із серйозними викликами, посиленими війною. На нашу думку, для повноцінного розуміння ситуації необхідно системно розглянути як можливості, так і ризики.

Подальше стратегічне впровадження штучного інтелекту в публічне управління може стати для України потужним драйвером розвитку та одним з ключових елементів повоєнної відбудови. Ми виділяємо такі перспективи:

1. *Створення сервісної держави.* ШІ дозволяє перейти до проактивного врядування. Завдяки аналізу даних держава зможе прогнозувати потреби громадян і надавати послуги ще до звернення за ними (як це частково реалізовано в «єМалятко»). Це мінімізує корупційні ризики та підвищує довіру до інституцій [12].

2. *Асиметрична перевага у безпеці.* В умовах протистояння з ворогом, що переважає у ресурсах, технології стають ключовим фактором. Розвиток ШІ для аналізу розвідданих та автономних систем може надати Україні перевагу на полі бою, а також допомогти у повоєнному розмінуванні.

3. *Економічне зростання.* Створення сприятливих правових режимів (як-от Дія.City [7]) може перетворити Україну на регіонального лідера у сфері ШІ, залучаючи інвестиції та створюючи робочі місця.

4. *Прискорення євроінтеграції.* Успішна імплементація стандартів ШІ, гармонізованих з EU AI Act, продемонструє зрілість інституцій та наблизить нас до Єдиного цифрового ринку ЄС [3; 8; 88].

Попри величезний потенціал, шлях до реалізації цих можливостей не є простим. Україна стикається з низкою серйозних викликів та бар'єрів:

1. *Правова невизначеність.* Як було показано, наразі відсутній комплексний закон про ШІ. Існуючі документи є стратегічними, а не нормативними. Це створює проблеми як для розробників, так і для громадян, чиї права не захищені від алгоритмічних ризиків [32].

2. *Проблема даних (Data Challenge).* ШІ потребує якісних даних. Публічний сектор все ще страждає від проблеми ізольованих реєстрів та неузгодженості даних. Без належної політики data governance розвиток ШІ буде обмеженим.

3. *Кадровий дефіцит.* Державі потрібні фахівці, здатні формувати технічні завдання для ШІ та оцінювати етичні ризики. В умовах конкуренції з бізнесом та відтоку кадрів через війну, цей дефіцит є критичним.

4. *Етичні ризики в умовах війни.* Війна створює запит на технології нагляду. Існує ризик, що держава може надмірно розширити використання таких систем (розпізнавання облич) без належних запобіжників, що загрожує приватності [14].

5. *Ресурсні обмеження.* Війна вимагає колосальних коштів, що обмежує інвестиції у довгострокові цифрові проєкти.

Підсумовуючи, поточний стан застосування ШІ в Україні можна охарактеризувати як етап прагматичного, але фрагментарного розвитку. Існує політична воля та вражаючі практичні результати (особливо в оборонній та сервісній сферах), але цей процес відбувається за відсутності цілісної правової рамки. Україна успішно вирішує нагальні завдання за допомогою технологій, але ще не перейшла до побудови стійкої екосистеми надійного ШІ. Подолання цих бар'єрів та гармонізація з нормами ЄС є ключовим завданням, аналіз якого буде продовжено у наступних підрозділах.

3.2. Адміністративно-правові та управлінські бар’єри впровадження ШІ в Україні

Попри очевидний прогрес та наявність політичної волі до цифрової трансформації, шлях до повноцінної та відповідальної інтеграції штучного інтелекту в систему публічного управління України стикається з низкою глибоких та системних бар'єрів. Ці перешкоди мають як суто правовий характер (пов'язаний із застарілістю або відсутністю необхідних норм), так і управлінський (що стосується інституційної спроможності). Ідентифікація та аналіз цих бар'єрів є необхідною умовою для розробки ефективної «дорожньої карти» реформ [8].

На наше переконання, ці бар'єри можна умовно згрупувати у кілька взаємопов'язаних блоків: (1) нормативно-правові прогалини; (2) проблеми управління даними; (3) інституційні та кадрові обмеження; (4) соціокультурні виклики. Розглянемо кожен з них детальніше.

1. Прогалини та недоліки нормативно-правового регулювання

Це, мабуть, найбільш фундаментальний бар'єр. Правова невизначеність створює ризики для всіх учасників процесу: державних органів, розробників та громадян.

- *Відсутність комплексного законодавчого акту.* В Україні наразі відсутній єдиний закон, який би регулював сферу ШІ за зразком EU AI Act. Існуючі стратегічні документи не встановлюють конкретних механізмів відповідальності. Це призводить до відсутності єдиного понятійного апарату та класифікації ризиків. Потенційно небезпечні системи (наприклад, у правоохоронній сфері) та прості чат-боти де-юре перебувають в однаковому правовому полі.
- *Проблема відповідальності.* Це одна з найскладніших дилем. Чинне цивільне законодавство розраховане на ситуації, де є чіткий людський діяч. У випадку зі складними автономними системами традиційні моделі вини не працюють, створюючи «прогалину у відповідальності» [90; 94].
- *Неадаптованість законодавства про захист даних.* Закон України «Про захист персональних даних» не містить інструментів, специфічних для ризиків ШІ, таких як обов'язкова оцінка впливу (DPIA) або чітке регулювання автоматизованого прийняття рішень [15; 42].
- *Недосконалість законодавства про доступ до інформації.* Невизначеним залишається питання доступу громадськості до технічної документації або інформації про навчальні дані систем ШІ. Державні органи часто відмовляють у наданні такої інформації, посилаючись на комерційну таємницю, що унеможливлює контроль [32].

2. Проблеми у сфері управління даними (Data Governance)

Вимоги EU AI Act до якості даних є надзвичайно високими [88]. На жаль, поточний стан державних даних в Україні далекий від цих стандартів.

- *Фрагментованість та «силосність» реєстрів.* Дані про один об'єкт часто зберігаються в ізольованих базах без належної координації. Це призводить до неповноти даних та дублювання ресурсів. Проєкт «Трембіта» є важливим кроком, але він ще не вирішив проблему повністю.
- *Низька якість даних.* Багато реєстрів містять помилки та неактуальні записи. Навчання моделей на таких даних призводить до отримання ненадійних результатів (принцип «garbage in, garbage out»).
- *Ризики упередженості.* Історичні дані можуть містити приховані упередження щодо певних соціальних груп. Без попереднього аудиту використання таких даних призведе до створення дискримінаційних алгоритмів.
- *Проблема доступу та анонімізації.* Для розвитку інновацій потрібен доступ до знеособлених даних. Однак в Україні бракує як правового регулювання, так і технічних стандартів надійної анонімізації, що створює ризики для приватності [10].

Подолання цих бар'єрів вимагає розробки цілісної політики управління даними, що включає стандарти верифікації та створення безпечних «пісочниць» для дослідників.

Навіть за наявності досконалого законодавства та якісних даних, успішне впровадження ШІ неможливе без відповідної інституційної спроможності. Саме на цьому рівні в Україні спостерігається низка серйозних управлінських бар'єрів.

3. Інституційні та кадрові обмеження

Цей блок стосується «людського виміру» цифрової трансформації.

- *Дефіцит цифрових компетенцій.* Для відповідального впровадження ШІ державні службовці повинні мати базову «алгоритмічну грамотність». Вони мають розуміти принципи роботи ШІ, ризики упередженості та свою роль у системі людського нагляду. Наразі рівень таких компетенцій є низьким, що

призводить або до страху перед інноваціями, або до їх бездумного впровадження.

- *Проблема залучення IT-фахівців.* Державна служба не може конкурувати з приватним сектором за рівнем зарплат. Це призводить до тотальної залежності від зовнішніх підрядників та нездатності органу сформулювати якісне технічне завдання або проконтролювати результат.
- *Інституційна невизначеність.* В Україні відсутні спеціалізовані органи нагляду за ШІ. Незрозуміло, хто відповідає за розробку стандартів, аудит алгоритмів чи розслідування інцидентів. Це створює вакуум відповідальності.
- *Застарілі процедури закупівель.* Законодавство про публічні закупівлі розраховане на стандартні товари. Закупівля інноваційних IT-рішень, що вимагають гнучкого (Agile) підходу, є складною, що гальмує пілотні проєкти.

4. Соціокультурні та етичні виклики

- *Низький рівень довіри.* Традиційно невисока довіра до державних інституцій створює ризик, що впровадження непрозорих алгоритмів буде сприйнято як спроба посилення контролю. Без прозорості будь-які ініціативи можуть зіткнутися з опором суспільства.
- *Відсутність етичного діалогу.* В Україні бракує широкої дискусії щодо етичних аспектів ШІ (баланс безпеки та приватності, автоматизація правосуддя). Рішення часто приймаються технократично, без залучення правозахисників та громадськості [15].

Виявлені проблеми систематизовано у табл. 3.2.

Таблиця 3.2

Системні бар'єри впровадження штучного інтелекту в публічне управління України

Група бар'єрів	*Сутність проблеми*	*Негативні наслідки*
Нормативно-правові	Відсутність комплексного закону про ШІ; неврегульованість відповідальності; застарілість норм про захист даних	Правова невизначеність; ризики порушення прав людини; відсутність захисту від помилок ШІ

Управління даними (Data Governance)	«Силосність» реєстрів; низька якість та неактуальність даних; відсутність стандартів анонімізації	Неможливість створення надійних моделей (garbage in, garbage out); ризик алгоритмічної упередженості
Інституційно-кадрові	Дефіцит цифрових компетенцій у держслужбовців; залежність від вендорів; негнучкі процедури закупівель	Неефективне впровадження; нездатність здійснювати нагляд; ризик корупції при закупівлях
Соціокультурні	Низька довіра до державних інституцій; відсутність публічного діалогу з етичних питань	Опір суспільства інноваціям; технократизм у прийнятті рішень; ігнорування етичних ризиків

Джерело: розроблено автором на основі аналізу [10; 32; 42]

Отже, адміністративно-правові та управлінські бар'єри є системними і взаємопов'язаними. Неможливо вирішити проблему якості даних, не вирішивши проблему міжвідомчої взаємодії. Неможливо підвищити якість закупівель без підвищення компетенцій службовців. Подолання цих бар'єрів вимагає комплексного підходу, який і має лягти в основу «дорожньої карти» реформ.

3.3. Дорожня карта гармонізації державної політики України з підходами ЄС

Проведений у попередніх розділах аналіз теоретичних засад, передового європейського досвіду та українських реалій дозволяє перейти до найважливішого, на наше переконання, завдання цієї роботи – формування комплексної «дорожньої карти» для гармонізації державної політики України у сфері штучного інтелекту з підходами Європейського Союзу.

Ця дорожня карта не має бути просто набором рекомендацій. Це системний план дій, що охоплює законодавчі, інституційні, освітні та технологічні аспекти. Її кінцевою метою є побудова в Україні екосистеми ШІ, яка б, з одного боку, сприяла інноваційному розвитку та підвищенню ефективності держави, а з іншого – базувалася на фундаментальних цінностях

прав людини, демократії та верховенства права, що є наріжним каменем європейської інтеграції [42].

Враховуючи складність завдання, ми пропонуємо представити дорожню карту у вигляді кількох взаємопов'язаних стратегічних напрямів. Першим і фундаментальним з них є створення сучасної нормативно-правової бази.

Напрям 1. Формування всеохопної нормативно-правової рамки

Це основа всієї подальшої роботи. Без чіткого, сучасного та гармонізованого з ЄС законодавства будь-які інші заходи не матимуть міцного підґрунтя. Робота в цьому напрямі, на нашу думку, має включати кілька послідовних кроків.

Крок 1.1. *Розробка та ухвалення рамкового Закону України «Про штучний інтелект»*

Це пріоритетне завдання. Україна має розробити та ухвалити власний комплексний закон про ШІ, який би базувався на філософії та структурі EU AI Act, але водночас враховував національну специфіку. Цей закон не повинен бути сліпою копією, але має імплементувати ключові підходи:

- **Запровадження ризик-орієнтованого підходу.** Закон має чітко закріпити класифікацію систем ШІ за рівнями ризику (неприйнятний, високий, обмежений, мінімальний). Це дозволить застосовувати пропорційне регулювання.
- **Визначення переліку заборонених практик.** Закон має містити перелік заборонених систем, аналогічний статті 5 EU AI Act [88]. Це включає заборону на соціальний скоринг та маніпулятивні техніки. Щодо «реальночасової» біометричної ідентифікації, то в умовах війни потрібна чітка регламентація з вузькими винятками [44; 48].
- **Встановлення критеріїв для систем високого ризику.** Необхідно визначити перелік сфер, де застосування ШІ вважається високоризиковим (за аналогією з Додатком III до EU AI Act) [88]. Цей перелік має бути адаптований до українських реалій: наприклад, системи для верифікації ВПО, надання статусу учасника бойових дій та системи у сфері відбудови.

- **Закріплення обов'язкових вимог.** Закон має встановити вимоги до систем високого ризику, що дзеркально відображають вимоги ЄС: система управління ризиками, якість даних, технічна документація, прозорість та людський нагляд.
- **Визначення обов'язків.** Чітке розмежування ролей провайдерів та користувачів (особливо органів влади), покладаючи на останніх відповідальність за моніторинг та людський контроль.

Крок 1.2. *Адаптація секторального законодавства*

Ухвалення рамкового закону має супроводжуватися змінами до інших актів:

- *Закон «Про захист персональних даних».* Необхідно привести його у відповідність до GDPR, зокрема в частині регулювання автоматизованих рішень, запровадження DPIA та посилення повноважень Омбудсмана [11; 20].
- *Законодавство про відповідальність за шкоду.* Необхідно імплементувати норми щодо відповідальності за шкоду від ШІ (за аналогією з AI Liability Directive), зокрема запровадити презумпцію причинно-наслідкового зв'язку [90; 94].
- *Законодавство про публічні закупівлі.* Розробка механізмів для гнучкої закупівлі інноваційних рішень, включаючи обов'язкові критерії етичності та надійності при оцінці тендерів.
- *Процесуальне законодавство.* Зміни до кодексів щодо використання доказів, згенерованих ШІ, та оскарження алгоритмічних рішень.

Крок 1.3. *Розробка технічних стандартів*

Паралельно із законодавством, необхідно розвивати систему стандартів. Доцільно створити Національний технічний комітет зі стандартизації ШІ для гармонізації ДСТУ з європейськими стандартами (CEN/CENELEC). Це спростить для бізнесу процедуру доведення відповідності. Також держава має стимулювати розробку добровільних кодексів поведінки.

Напрям 2. Розбудова інституційної спроможності та системи управління (Governance)

Після закладення правового фундаменту, наступним кроком є побудова дієвої інституційної архітектури. Найкращі закони залишаться деклараціями без компетентних інституцій.

Крок 2.1. *Визначення та посилення Національного наглядового органу*

Україна має визначити орган, який виконуватиме функції нагляду (National Supervisory Authority). Ми розглядаємо кілька сценаріїв:

- *Сценарій А (найбільш реалістичний):* покладення функцій на Мінцифри. Переваги: наявність експертизи. Виклик: потенційний конфлікт інтересів (одночасно розвиває і контролює).
- *Сценарій Б:* розширення повноважень Уповноваженого ВРУ з прав людини. Переваги: фокус на правах людини. Виклик: брак технічних ресурсів.
- *Сценарій В:* створення нового незалежного регулятора. Переваги: незалежність. Виклик: тривалий процес і витрати.

Незалежно від моделі, орган має отримати широкі повноваження (доступ до коду, аудити, санкції) та ресурси.

Крок 2.2. *Створення міжвідомчої координаційної платформи*

За аналогією з Європейською радою з питань ШІ, доцільно створити Міжвідомчу раду при Кабінеті Міністрів. До її складу мають увійти представники Мінцифри, Міноборони, СБУ, Мін'юсту, Омбудсмана та наукової спільноти. Її завдання – стратегічна координація та вирішення міжвідомчих проблем.

Крок 2.3. *Впровадження Національної стратегії управління даними*

Якість даних є критичною. Стратегія має включати:

- Стандартизацію реєстрів та розвиток системи «Трембіта»;
- Запровадження посад «Головного офіцера з даних» (Chief Data Officer) у міністерствах;
- Процедури Data Quality Assurance для верифікації даних;

- Створення платформи відкритих даних 2.0 із безпечними «пісочницями» для дослідників [41].

Крок 2.4. *Створення системи оцінки відповідності*

Необхідно створити інфраструктуру, аналогічну європейській: визначити орган з акредитації, розробити критерії для незалежних аудиторів та створити публічний реєстр систем високого ризику.

Побудова такої рамки є складним завданням, але без неї процес впровадження ШІ залишиться неконтрольованим.

Після формування законодавчої бази та інституційної архітектури, успіх «дорожньої карти» залежить від наявності кваліфікованих кадрів та сприятливого середовища для інновацій. Тому завершальні напрями нашого плану дій фокусуються саме на цьому.

Напрям 3. Розвиток людського капіталу та підвищення «алгоритмічної грамотності»

Технології створюють та використовують люди, тому інвестиції в освіту є ключовими. Цей напрям має бути всеохопним.

Крок 3.1. *Національна програма з цифрової та алгоритмічної грамотності*

- **Для державних службовців:** обов'язкові програми підвищення кваліфікації (НАДС). Вони мають включати модулі з етики ШІ, правових вимог та практичні тренінги з людського нагляду.
- **Для правничої спільноти:** спеціалізовані курси для суддів, прокурорів та адвокатів. Правники повинні розуміти роботу алгоритмів, щоб оцінювати докази та захищати права клієнтів.
- **Для громадян:** інформаційні кампанії (через «Дія.Освіта») про права людини у взаємодії з ШІ [8; 12].

Крок 3.2. *Модернізація освіти*

- *IT-спеціальності:* інтеграція курсів з етики та права («Responsible AI»). Розробники мають розуміти соціальні наслідки своїх продуктів.

- *Гуманітарні спеціальності:* впровадження курсів з основ цифрових технологій.
- *Міждисциплінарні дослідження:* створення центрів, що об'єднують інженерів, юристів та соціологів.

Напрям 4. Стимулювання відповідальних інновацій та міжнародна співпраця

Метою регулювання є не стримування, а спрямування інновацій у безпечне русло.

Варто зазначити, що запропоновані нами кроки щодо стимулювання інновацій корелюють із баченням Мінцифри, викладеним у «Білій книзі». Зокрема, держава планує впровадити інструмент добровільного маркування систем ШІ, що дозволить розробникам демонструвати прозорість та відповідальність ще до запровадження обов'язкових вимог. Крім того, для захисту прав громадян у цифровому просторі пропонується використати механізм Trusted Flagger (довіреного спостерігача). Цей підхід, запозичений з європейського Digital Services Act, передбачає залучення компетентних громадських організацій для виявлення та пріоритетного розгляду скарг на порушення прав людини алгоритмами великих платформ [3].

Крок 4.1. *Створення регуляторних «пісочниць» (Regulatory Sandboxes)*

За зразком країн ЄС, доцільно створити правові режими для тестування інноваційних продуктів (особливо високого ризику) під наглядом регулятора. Це дозволить безпечно експериментувати ще до виходу на ринок.

Крок 4.2. *Державна підтримка етичного ШІ*

- Грантові програми для досліджень у сфері пояснюваного ШІ (XAI) та усунення упередженості.
- Переваги у публічних закупівлях для компаній, що дотримуються етичних кодексів.

Крок 4.3. *Активна міжнародна співпраця*

Україна має поглиблювати діалог з інституціями ЄС (зокрема з Офісом з питань ШІ), приєднуватися до глобальних ініціатив (GPAI) та співпрацювати з країнами-лідерами (США, Велика Британія) для залучення інвестицій.

Для наочності етапи дорожньої карти ми систематизували у табл. 3.3.

Таблиця 3.3

Стратегічні напрями гармонізації політики України у сфері ШІ з підходами ЄС

Напрям	*Ключові заходи (кроки)*	*Очікуваний результат*
Нормативно-правовий	Ухвалення рамкового Закону про ШІ (за моделлю EU AI Act); адаптація законів про захист даних та відповідальність; розробка стандартів	Створення чіткої правової рамки; запровадження ризик-орієнтованого підходу; захист прав громадян
Інституційний	Визначення наглядового органу; створення Міжвідомчої ради; впровадження стратегії управління даними.	Забезпечення ефективного нагляду; покращення якості даних; координація політики
Освітній (людський капітал)	Програми навчання для держслужбовців та суддів; модернізація університетських курсів; підвищення грамотності населення	Формування компетентного кадрового резерву; здатність здійснювати людський нагляд
Інноваційний	Створення регуляторних «пісочниць»; державні гранти на етичний ШІ; міжнародна співпраця	Безпечне тестування технологій; підтримка стартапів; інтеграція у глобальний ринок.

Джерело: розроблено автором на основі аналізу [7; 26; 37]

Рис. 3.1. Структурно-логічна схема дорожньої карти гармонізації державної політики України у сфері ШІ

Запропонована дорожня карта є амбітним, але реалістичним планом дій. Вона вимагає скоординованих зусиль влади, бізнесу та громадянського суспільства. Послідовна реалізація цих чотирьох напрямів дозволить Україні не просто формально скопіювати європейське законодавство, а й побудувати власну стійку екосистему ШІ. Це стане потужним інструментом для перемоги, повоєнної відбудови та утвердження України як лідера цифрової епохи.

Висновки до розділу 3

У третьому розділі магістерської роботи нами було здійснено комплексний аналіз поточного стану, бар'єрів та перспектив регулювання штучного інтелекту в публічному управлінні України в контексті євроінтеграції. Узагальнення проведеного дослідження дозволяє сформулювати такі ключові висновки.

По-перше, ми встановили, що Україна демонструє значний прогрес у цифровізації та має чітке стратегічне бачення, закріплене у Концепції розвитку ШІ. Вже сьогодні технології активно, хоч і фрагментарно, застосовуються у публічному секторі. Яскравими прикладами є екосистема «Дія» (зокрема, запуск ШІ-асистента Дія.AI) та сектор національної безпеки, де ШІ став інструментом досягнення асиметричної переваги на полі бою. Це свідчить про високий адаптивний потенціал держави. Однак, на наше переконання, цей розвиток є переважно прагматичним і відбувається за відсутності цілісної правової рамки.

По-друге, попри досягнення, ми ідентифікували низку системних адміністративно-правових та управлінських бар'єрів, які гальмують відповідальне впровадження ШІ:

- Правовий вакуум: відсутність комплексного закону, що регулював би ШІ за ризик-орієнтованим підходом, та неврегульованість відповідальності за шкоду.
- Проблеми Data Governance: фрагментованість («силосність») державних реєстрів, низька якість даних та відсутність стандартів їх анонімізації.
- Інституційна слабкість: дефіцит «алгоритмічної грамотності» у держслужбовців, залежність від зовнішніх підрядників та невизначеність щодо наглядового органу.
- Етичні виклики: ризики порушення приватності в умовах воєнного стану та відсутність широкого суспільного діалогу.

По-третє, для подолання цих перешкод нами було розроблено комплексну «дорожню карту» гармонізації державної політики України з підходами ЄС. Вона базується на чотирьох стратегічних напрямах:

1. Формування нормативної рамки: ухвалення рамкового Закону «Про штучний інтелект» (за моделлю EU AI Act), адаптація законодавства про захист даних та публічні закупівлі.

2. Розбудова інституцій: визначення Національного наглядового органу, створення міжвідомчої координаційної платформи та впровадження стратегії управління даними.

3. Розвиток людського капіталу: реалізація національної програми навчання для держслужбовців та модернізація освіти.

4. Стимулювання інновацій: створення регуляторних «пісочниць» (regulatory sandboxes) для безпечного тестування технологій.

Таким чином, у третьому розділі доведено, що Україна перебуває на етапі переходу від точкових експериментів до системної політики. Запропонована дорожня карта є планом дій, реалізація якого дозволить не лише виконати євроінтеграційні зобов'язання, а й перетворити ШІ на інструмент для перемоги та повоєнної відбудови, побудувавши екосистему, що базується на довірі та правах людини.

ВИСНОВКИ

Дане магістерське дослідження присвячене порівняльно-правовому аналізу регулювання штучного інтелекту в публічному управлінні України та Європейського Союзу, що дозволило досягти поставленої мети, реалізувати всі поставлені завдання та сформулювати висновки, зокрема.

1. Було досліджено теоретико-правові засади регулювання ШІ. Доведено, що стрімка імплементація систем ШІ спричиняє тектонічний зсув у традиційних правових парадигмах. Встановлено, що унікальні властивості ШІ як об'єкта регулювання – автономність у прийнятті рішень, непрозорість («чорна скринька») та здатність до самонавчання – роблять застарілі моделі правового впливу неефективними. На нашу думку, найбільш адекватною відповіддю на ці виклики є перехід до ризик-орієнтованого підходу. Також нами аргументовано, що неконтрольоване впровадження ШІ в публічне управління загрожує системною ерозією принципів належного врядування (прозорості, підзвітності, недискримінації), створюючи реальну небезпеку формування «алгократії».

2. Було проаналізовано європейську модель правового регулювання. Розкрито сутність та архітектуру Акту про ШІ (EU AI Act), який визначено як новий глобальний стандарт. Доведено, що його структура у вигляді чотирирівневої «піраміди ризиків» (неприйнятний, високий, обмежений, мінімальний) дозволяє ефективно збалансувати захист прав та інновації. Ми детально систематизували комплекс обов'язків органів публічної влади як користувачів систем високого ризику, серед яких ключовими є забезпечення ефективного людського нагляду («human-in-the-loop») та проведення оцінки впливу на фундаментальні права (FRIA). Також охарактеризовано ешелоновану систему нагляду в ЄС, що поєднує повноваження національних органів та централізовану координацію з боку Офісу з питань ШІ.

3. Здійснено аналіз поточного стану використання ШІ в Україні. Встановлено, що ситуація характеризується глибокою дихотомією. З одного боку, Україна демонструє виняткову цифрову стійкість та ефективне

впровадження технологій (екосистема «Дія», оборонний сектор). З іншого – цей розвиток відбувається за відсутності належної правової рамки. Нами ідентифіковано ключові бар'єри: правовий вакуум (відсутність закону про ШІ та неврегульованість відповідальності), проблеми Data Governance («силосність» реєстрів та низька якість даних), а також інституційна слабкість та дефіцит цифрових компетенцій у держслужбовців.

4. Проведено порівняльний аналіз підходів України та ЄС. Виявлено, що стратегічні документи (Концепція розвитку ШІ) хоч і декларують прихильність європейським цінностям, проте не містять дієвих механізмів їх реалізації. Головною розбіжністю є відсутність в Україні юридично обов’язкової класифікації ризиків та процедур оцінки відповідності, що створює ризики для прав громадян. Це підтверджує необхідність невідкладної гармонізації національного законодавства з нормами EU AI Act.

5. Розроблено проєкт комплексної дорожньої карти гармонізації державної політики України з підходами ЄС. Запропонована карта базується на чотирьох стратегічних напрямах:

- Нормативно-правовий: ухвалення рамкового Закону «Про штучний інтелект» (із закріпленням ризик-орієнтованого підходу) та адаптація законодавства про захист даних і публічні закупівлі.
- Інституційний: чітке визначення компетентного наглядового органу, створення міжвідомчої координаційної платформи та впровадження національної стратегії управління даними.
- Освітній: розвиток людського капіталу через впровадження програм з «алгоритмічної грамотності» для держслужбовців та правників.
- Інноваційний: стимулювання відповідальних інновацій через створення регуляторних «пісочниць» та грантову підтримку етичного ШІ.

Реалізація запропонованих заходів дозволить Україні побудувати цифрову державу, засновану на європейських цінностях, де технології слугують людині, а не навпаки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андрощук Г. О. Політика і стратегії розвитку штучного інтелекту в країнах світу: quo vadis? *Журнал «НТІ» – Наука Технології Інновації.* 2023. № 1. URL: https://nti.ukrintei.ua/wp-content/uploads/2024/03/Андрощук_1-2023.pdf

2. Баранов О. А. Визначення терміну «штучний інтелект». *Інформація і право.* 2023. № 1(44). С. 32–49. URL: http://il.ippi.org.ua/article/view/287537.

3. Біла книга з регулювання ШІ в Україні: бачення Мінцифри. Версія для консультацій. 2024. 30 с. URL: https://storage.thedigital.gov.ua/files/d/9d/0bbc3a705c821a197bedfcdfe00899d9.pdf.

4. Володимир Зеленський зустрівся з президентом корпорації Microsoft. Офіційне інтернет-представництво Президента України. 22 вересня 2021 року. URL: https://www.president.gov.ua/news/volodimir-zelenskij-zustrivsya-z-prezidentom-korporaciyi-mic-70761.

5. Гур'єва М. Штучний інтелект та «нова дискримінація»: як технології впливають на права та життя людини? *Inspired.* URL: https://inspired.com.ua/creative/technology/shtuchnyj-intelekt-ta-nova-dyskryminatsiya-yak-tehnologiyi-vplyvayut-na-prava-ta-zhyttya-lyudyny/

6. Гришко В. І., Вознюк С. С. Проблемні аспекти впровадження штучного інтелекту у сфері юриспруденції. *Аналітично-порівняльне правознавство.* 2024. № 2. С. 3. URL: https://doi.org/10.24144/2788-6018.2024.02.3

7. Дія.City. Законодавство. URL: https://city.diia.gov.ua/uk/tax-system/legislation

8. Дорожня карта з інтеграції України до Єдиного цифрового ринку ЄС / Міністерство цифрової трансформації України. Київ, 2021. 78 с. URL: https://mon.gov.ua/static-objects/mon/sites/1/kolegiya-ministerstva/2018/05/1-dorozhnya-karta-integratsii-ukraini-do-evro.pdf.

9. Еннан Р. Є. Право віртуального простору / цифрове право / інтернет-право та «цифровізація» права: загальні засади. *Актуальні проблеми інтелектуального, інформаційного, IT та Інтернет права:* матеріали Сьомої

всеукраїнської науково – практичної конференції (Львів, 25 травня 2023 р.). – Львів: Юрид. ф–т Львів. нац. ун–ту ім. І. Франка, 2023. С. 67-73. URL: https://law.lnu.edu.ua/wp-content/uploads/2015/09/Zbirnyk_7_Lviv_IPconference.pdf

10. Єсенніков К. В. Штучний інтелект як елемент системи державного управління: ризики і можливості. *Наукові перспективи (Naukovì perspektivi).* 2024. № 9(51). С. 115–126. URL: https://doi.org/10.52058/2708-7530-2024-9(51)-115-126

11. Загальний регламент про захист даних (GDPR). Regulation (EU) 2016/679 of the European Parliament and of the Council. URL: https://gdpr-info.eu

12. Карпенко О. В. Штучний інтелект як інструмент публічного управління соціально-економічним розвитком: смарт-інфраструктура, цифрові системи бізнес-аналітики та трансферти. *Державне управління: удосконалення та розвиток.* 2021. № 10. URL: http://www.dy.nayka.com.ua/pdf/10_2021/4.pdf

13. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр

14. Максіменцева Н. О., Максіменцев М. Г. Штучний інтелект у публічному управлінні: переваги цифрових технологій та загрози суверенному інформаційному простору. *Державне управління: удосконалення та розвиток:* ел.журн. 2024. URL: https://www.researchgate.net/publication/378525811_STUCNIJ_INTELEKT_U_PUBLICNOMU_UPRAVLINNI_PEREVAGI_CIFROVIH_TEHNOLOGIJ_TA_ZAGROZI_SUVERENNOMU_INFORMACIJNOMU_PROSTORU

15. Марутян Р. Р. Інформаційні технології інтелектуального управління у публічно-управлінській практиці: зарубіжний та вітчизняний досвід. *Вісник Національного університету цивільного захисту України.* 2018. № 2. С. 146–153. URL: http://nbuv.gov.ua/j-pdf/VNUCZUDU_2018_2_22.pdf.

16. Михальчук В. М., Шевченко Я. О. Розвиток штучного інтелекту у сфері державного управління: міжнародний досвід та перспективи впровадження в державних закладах охорони здоров'я в Україні. *Успіхи і досягнення у науці.*

2025. № 3 (13). URL: http://ir.nuozu.edu.ua:8080/bitstream/lib/5079/1/21706-Текст%20статті-25832-1-10-20250403.pdf

17. Мінцифри: Інтегруємо голосові технології в держсервіси. Міністерство цифрової трансформації України. Урядовий портал. 2025. URL: https://www.kmu.gov.ua/news/mintsyfry-intehruiemo-holosovi-tekhnolohii-v-derzhservisy.

18. Поради з відповідального використання штучного інтелекту публічними службовцями. Міністерство цифрової трансформації України, НАДС, Вища школа публічного управління. 2025. URL: https://storage.thedigital.gov.ua/files/f/bf/a9595e0dcd238ab2b3602909107aabf9.pdf. С. 14-15 (6).

19. Про адміністративну процедуру : Закон України від 17.02.2022 № 2073-IX. URL: https://zakon.rada.gov.ua/laws/show/2073-20

20. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17

21. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12

22. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

23. Про особливості надання публічних (електронних публічних) послуг: Закон України від 15.07.2021 № 1689-IX. URL: https://zakon.rada.gov.ua/laws/show/1689-20

24. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р#TexT

25. Регламент Європейського Парламенту і Ради ЄС 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

26. Результати всеукраїнського дослідження про перспективи ШІ в загальній середній освіті. Міністерство освіти і науки України. 2023. 20 грудня. URL: https://mon.gov.ua/news/rezultati-vseukrainskogo-doslidzhennya-pro-perspektivi-shi-v-zagalniy-seredniy-osviti.

27. Рекомендації з використання технологій штучного інтелекту в обробці персональних даних: найкращі практики ЄС. / Міжнародний проєкт EU4DigitalUA у співробітництві з Офісом Омбудсмена України та Міністерством цифрової трансформації України. 2024. С. 41. URL: https://eu4digitalua.eu/wp-content/uploads/2025/01/ai_guidelines_ua.pdf. (63)

28. Сова М., Дєніжна С. Міжнародний досвід правового регулювання небезпеки штучного інтелекту в реаліях воєнного часу: етико-філософський аспект. *Філософські та методологічні проблеми права.* 2024. № 1 (27). URL: https://elar.navs.edu.ua/server/api/core/bitstreams/175239c5-0b59-46e7-8a1b-7812964f061c/content

29. Тарасюк В. М. Правове регулювання застосування штучного інтелекту в Україні: сучасний стан та перспективи гармонізації з міжнародними стандартами. *Політологічний вісник.* 2024. № 93. С. 94–113. URL: https://www.zpv.knu.ua/index.php/pb/article/view/257/242.

30. Ткаленко О. М., Макаренко А. О., Полоневич О. В. Інтелектуальні технології та системи штучного інтелекту для підтримки прийняття рішень. *Телекомунікаційні та інформаційні технології.* 2019. № 2. С. 53–59. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/vduikt_2019_2_9.pdf

31. Турута О. В., Турута О. П. Штучний інтелект крізь призму фундаментальних прав людини. *Науковий вісник Ужгородського національного університету.* 2022. № 71. С. 49–54. URL: https://doi.org/10.24144/2307-3322.2022.71.7.

32. Тюря Ю. І. Деякі аспекти побудови нормативної бази адміністративно-правового регулювання діяльності зі створення, впровадження та використання

штучного інтелекту в Україні. *JURIS EUROPENSIS SCIENTIA.* 2022. № 5. С. 25–28. URL: http://jes.nuoua.od.ua/archive/5_2022/5.pdf

33. Україна встановила світовий рекорд: Дія.AI визнали першим національним ШІ-асистентом із державних послуг. Прес-офісу Міністерства цифрової трансформації України. 2025. URL: https://thedigital.gov.ua/news/progress/ukrayina-vstanovyla-svitovyy-rekord-diiaai-vyznaly-pershym-natsionalnym-shi-asystentom-iz-derzavnykh-posluh.

34. Цьомра В. Ю., Корильчук С. Т., Оленюк Д. О. Розвиток штучного інтелекту в сучасній юриспруденції. *Наукові записки Львівського університету бізнесу та права.* 2023. № 38. С. 100–108. URL: https://nzlubp.org.ua/index.php/journal/article/view/875.

35. Ahn M. J., Chen Y.-C. Digital transformation toward AI-augmented public administration: The perception of government employees and the willingness to use AI in government. Government Information Quarterly. 2022. Vol. 39(2). Art. 101664. URL: https://doi.org/10.1016/j.giq.2021.101664.

36. AI Act: MEPs adopt landmark law. European Parliament News. 13.03.2024. URL: https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/ai-act-meps-adopt-landmark-law

37. Almada M. The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy. *German Law Journal, FirstView.* 2023. Vol. 14, Iss. 2. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4592006.

38. Artificial Intelligence Act : Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (consolidated text agreed on 2 February 2024). URL: https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf.

39. Barfield W. The Cambridge Handbook of the Law of the A.I. *Cambridge : Cambridge University Press,* 2021. 780 p. URL: https://assets.cambridge.org/97811084/81960/frontmatter/9781108481960_frontmatter.pdf.

40. Broeders D., Cristiano F., Kaminska M. In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions. *JCMS: Journal of Common Market Studies.* 2023. Vol. 61(5). P. 1123–1431. URL: https://doi.org/10.1111/jcms.13462

41. Co-ordinated Plan on Artificial Intelligence (2021 Review) / European Commission. COM(2021) 205 final. *Brussels*, 21.04.2021. URL: https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review

42. Cordella A., Hesse J. E-government in the making: An actor network perspective. *Transforming Government: People, Process and Policy.* 2015. Vol. 9(1). P. 104–125. URL: https://doi.org/10.1108/TG-02-2014-0006

43. Creemers R. China's conception of cyber sovereignty: rhetoric and realization. *Governing cyberspace: Behaviour, power and diplomacy*. London: Rowman & Littlefield, 2020. URL: https://dx.doi.org/10.2139/ssrn.3532421

44. Criado J. I., Ode Zarate-Alcarazo L. Technological frames, CIOs, and artificial intelligence in public administration: A socio-cognitive exploratory study in Spanish local governments. *Government Information Quarterly.* 2022. Vol. 39(3). Art. 101688. URL: https://doi.org/10.1016/j.giq.2022.101688

45. Douzet F. et al. Measuring the fragmentation of the Internet: The case of the Border Gateway Protocol (BGP) during the Ukrainian crisis. *2020 12th international conference on cyber conflict (CyCon).* 2020. P. 157–182. URL: https://doi.org/10.23919/CyCon49761.2020.9131726

46. Ebers M. et al. The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). *J – Multidisciplinary Scientific Journal.* 2021. Vol. 4(4). P. 589–603. URL: https://www.mdpi.com/2571-8800/4/4/43/pdf

47. Egeland M. A. A risk-based approach to regulating AI: A viable compliance strategy for the European Union's proposed Artificial Intelligence Act? *Computer Law & Security Review.* 2022. Vol. 46. Art. 105721. URL: https://www.researchgate.net/publication/366007800_The_Risk-

Based_Approach_of_the_European_Union's_Proposed_Artificial_Intelligence_Regulation_Some_Comments_from_a_Tort_Law_Perspective

48. European Data Protection Board. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. 2022. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en

49. Fleck J. Reading between the lines of Ursula von der Leyen's ambitious vision for the EU. *Atlantic Council, New Atlanticist.* September 14, 2023. URL: https://www.atlanticcouncil.org/blogs/new-atlanticist/reading-between-the-lines-of-ursula-von-der-leyens-ambitious-vision-for-the-eu/

50. Floridi L., Cowls J. A Unified Framework of Five Principles for AI in Society. *Harvard Data Science Review.* 2019. Vol. 1, Iss. 1. URL: https://hdsr.mitpress.mit.edu/pub/l0jsh9d1/release/8

51. Gaozhao D., Wright J. E., Gainey M. K. Bureaucrat or artificial intelligence: people's preferences and perceptions of government service. *Public Management Review.* 2023. P. 1–28. URL: https://doi.org/10.1080/14719037.2022.2160488

52. Gesk T. S., Leyer M. Artificial intelligence in public services: When and why citizens accept its usage. *Government Information Quarterly.* 2022. Vol. 39(3). Art. 101704. URL: https://doi.org/10.1016/j.giq.2022.101704

53. High-Level Expert Group on AI. A definition of AI: Main capabilities and scientific disciplines. *Brussels : European Commission,* 2019. 16 p. URL: https://www.bdo.be/en-gb/insights/articles/2025/the-eu-ai-act?gad_source=1&gad_campaignid=23147171515&gbraid=0AAAADyL5g54JSst9gQXz8E9j1vh0Od4A&gclid=Cj0KCQiAuvTJBhCwARIsAL6DemifIWxIJdZxwVIGB_FrfBkln9HUu3I3kdUUgLbSwfdNy5RdH8eO-yEaAjYEEALw_wcB.

54. High-Level Expert Group on AI. Ethics Guidelines for Trustworthy AI. *Brussels : European Commission,* 2019. 41 p. URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

55. Horowitz M. C. Artificial Intelligence, International Competition, and the Balance of Power. *Texas National Security Review.* 2018. Vol. 1(3). P. 37–57. URL: https://doi.org/10.15781/T2639KP49

56. Krasner S. D. Sovereignty: Organized hypocrisy. *Princeton: Princeton University Press*, 1999. URL: https://archive.org/details/sovereigntyorgan0000kras

57. Kurowska X. What does russia want in cyber diplomacy? A primer. *Governing cyberspace: behaviour, power and diplomacy*. London: Rowman & Littlefield, 2020. P. 85–106. URL: https://www.researchgate.net/publication/392042089_What_Does_Russia_Want_In_Cyber_Diplomacy_A_Primer_1.

58. Lewis J. M., Ricard L. M., Klijn E. H. How innovation drivers, networking and leadership shape public sector innovation capacity. *International Review of Administrative Sciences.* 2018. Vol. 84(2). P. 288–307. URL: https://doi.org/10.1177/0020852317694085.

59. Madan R., Ashok M. AI adoption and diffusion in public administration: A systematic literature review and future research agenda. *Government Information Quarterly*. 2023. Art. 101774. URL: https://doi.org/10.1016/j.giq.2022.101774.

60. Mantelero A. AI and Big Data: A Blueprint for a Human Rights, Democracy and the Rule of Law Framework. *Council of Europe*, 2018. 57 p. URL: https://www.sciencedirect.com/science/article/pii/S0267364918302012

61. Maragno G., Tangi L., Gastaldi L., Benedetti M. AI as an organizational agent to nurture: Effectively introducing chatbots in public entities. *Public Management Review.* 2022. P. 1–31. URL: https://doi.org/10.1080/14719037.2022.2063935

62. Medaglia R., Tangi L. The adoption of artificial intelligence in the public sector in Europe: Drivers, features, and impacts. Icegov 2022. *Association for Computing Machinery.* 2022. Vol. 1, Iss. 1. URL: https://doi.org/10.1145/3560107.3560110

63. Mergel I., Dickinson H., Stenvall J., Gasco M. Implementing AI in the public sector. *Public Management Review.* 2023. P. 1–13. URL: https://doi.org/10.1080/14719037.2023.2231950.

64. Mikalef P., Gupta M. Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance. *Information & Management.* 2021. Vol. 58(3). Art. 103434. URL: https://doi.org/10.1016/j.im.2021.103434.

65. Mikalef P., Lemmer K., Schaefer C., Ylinen M., Fjørtoft S. O., Torvatn H. Y., Niehaves B. Enabling AI capabilities in government agencies: A study of determinants for European municipalities. *Government Information Quarterly.* 2021. Vol. 39. Art. 101596. URL: https://doi.org/10.1016/j.giq.2021.101596

66. Mueller M. Will the Internet fragment? Sovereignty, globalization and cyberspace. *John Wiley & Sons,* 2017. URL: https://ijoc.org/index.php/ijoc/article/viewFile/8202/2198

67. Neumann O., Guirguis K., Steiner R. Exploring artificial intelligence adoption in public organizations: A comparative case study. *Public Management Review.* 2022. P. 1–27. URL: https://doi.org/10.1080/14719037.2022.2048685

68. Pasquale F. The Black Box Society: The Secret Algorithms That Control Money and Information. *Cambridge : Harvard University Press,* 2015. 320 p. URL: https://easypdf.live/downloads/4990275-the-black-box-society-english-edition

69. Proposal for a Regulation on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) / European Commission. COM(2021) 206 final. Brussels, 21.04.2021. 108 p. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206.

70. Ranerup A., Henriksen H. Z. Digital discretion: Unpacking human and technological Agency in Automated Decision Making in Sweden's social services. *Social Science Computer Review.* 2022. Vol. 40(2). P. 445–461. URL: https://doi.org/10.1177/0894439320980434

71. RIPE Network Coordination Centre, RIPEstat, Historical WHOIS. 2023. URL: https://stat.ripe.net/widget/historical-

whois?pk_vid=fac55c350f3d8fa31607272904a2e27b#w.resource=80.245.112.0/20&w.time=2013–04-04T05:57:03

72. Sanina A., Balashov A., Rubtcova M. The socio-economic efficiency of digital government transformation. *International Journal of Public Administration.* 2021. P. 1–12. URL: https://doi.org/10.1080/01900692.2021.1988637.

73. Schiff D. S., Schiff K. J., Pierson P. Assessing public value failure in government adoption of artificial intelligence. *Public Administration.* 2021. P. 1–21. URL: https://doi.org/10.1111/padm.12742

74. Shollo A., Hopf K., Thiess T., Müller O. Shifting ML value creation mechanisms: A process model of ML value creation. *Journal of Strategic Information Systems.* 2022. Vol. 31(3). Art. 101734. URL: https://doi.org/10.1016/j.jsis.2022.101734

75. Sienkiewicz-Małyjurek K. Whether AI adoption challenges matter for public managers? The case of polish cities. *Government Information Quarterly.* 2023. Art. 101828. URL: https://doi.org/10.1016/j.giq.2023.101828

76. Smuha N. A. An Introduction to the Law, Ethics and Policy of Artificial Intelligence. *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence.* URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5121517

77. Sun T. Q., Medaglia R. Mapping the challenges of artificial intelligence in the public sector: Evidence from public healthcare. *Government Information Quarterly.* 2019. Vol. 36 (2). P. 368–383. URL: https://doi.org/10.1016/j.giq.2018.09.008

78. Taeihagh A. Governance of artificial intelligence. *Policy and Society.* 2021. Vol. 40, Iss.2. P.137–157. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3931469

79. Wolfram Burgard. The Draft AI Act and the GDPR: A Compliance Nightmare? *European Data Protection Law Review.* 2022. Vol. 8, Iss. 1. P. 3–14. URL: https://www.researchgate.net/publication/365517477_17_-_Artificial_Intelligence_as_a_Challenge_for_Data_Protection_Law

80. Tangi L., van Noordt C., Combetto M., Gattwinkel D., Pign Pignatelli F. AIwatch European landscape on the use of artificial intelligence by the public sector. 2022. URL: https://doi.org/10.2760/39336

81. Tangi L., van Noordt C., Rodriguez Müller A. P. The challenges of AI implementation in the public sector. An in-depth case studies analysis. *Proceedings of the 24th annual international conference on digital government research.* 2023. P. 414–422. URL: https://doi.org/10.1145/3598469.3598516

82. Turner J. Robot Rules: Regulating Artificial Intelligence. *Cham : Palgrave Macmillan*, 2019. 254 p. URL: https://www.law.kuleuven.be/citip/en/docs/hot-news/conferences/j-turner-robot-rules-regulating-artificial.pdf

83. van Noordt C., Misuraca G. Evaluating the impact of artificial intelligence technologies in public services: Towards an assessment framework. *International conference on theory and practice of electronic governance* (ICEGOV 2020). 2020. P. 8–16. URL: https://www.researchgate.net/publication/345015726_Evaluating_the_impact_of_artificial_intelligence_technologies_in_public_services_towards_an_assessment_framework.

84. Veale M., Borgesius F. Z. Demystifying the Draft EU Artificial Intelligence Act. Computer Law Review International. 2021. Vol. 22, Iss. 4. P. 97–112. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852

85. Veale M., Brass I. Administration by algorithm? Public management meets public sector machine learning. *Algorithmic Regulation.* 2019. P. 1–30. URL: https://doi.org/10.31235/OSF.IO/MWHNB

86. EU Artificial Intelligence Act: A Guide. 2025. URL: https://www.twobirds.com/-/media/new-website-content/pdfs/capabilities/artificial-intelligence/european-union-artificial-intelligence-act-guide.pdf

87. Wade M., Hulland J. The resource-based view and information systems research: Review, extension, and suggestions for future research. *MIS Quarterly: Management Information Systems.* 2004. Vol. 28(1). URL: https://www.researchgate.net/publication/220260051_The_Resource-

Based_View_and_Information_Systems_Research_Review_Extension_and_Suggestions_for_Future_Research

88. White Paper on Artificial Intelligence – A European approach to excellence and trust / European Commission. COM(2020) 65 final. Brussels, 19.02.2020. 27 p. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0065

89. Yeung K. A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility. *Brussels : European Parliament*, 2020. 60 p. URL: https://rm.coe.int/a-study-of-the-implications-of-advanced-digital-technologies-including/168096bdab.

90. Zech, H. Liability for AI: Public policy considerations. ERA Forum, 22(1), 147–158. URL: https://doi.org/10.1007/s12027-020-00648-0; https://www.weizenbaum-library.de/server/api/core/bitstreams/80b10854-3aed-4d55-8e4d-5276f11ecb97/content

91. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York : *PublicAffairs*, 2019. 704 p. URL: https://www.hbs.edu/faculty/Pages/item.aspx?num=56791

92. Zuiderwijk A., Chen Y.-C., Salem F. Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Government Information Quarterly*. 2021. Vol. 38. Art. 101577. URL: https://doi.org/10.1016/j.giq.2021.101577

93. Buiten M., de Streel A., Peitz M. EU liability rules in the age of Artificial Intelligence. Centre on Regulation in Europe, 2021. DOI:10.2139/ssrn.3817520; URL: https://www.researchgate.net/publication/350785164_EU_Liability_Rules_for_the_Age_of_Artificial_Intelligence

94. Roman A. Maydanyk, Nataliia I. Maydanyk, Maryna M. Velykanova. LIABILITY FOR DAMAGE CAUSED USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES. Journal of the National Academy of Legal Sciences of Ukraine, Vol. 28, No. 2, 2021. 151-159 p. DOI: 10.37635/jnalsu.28(2).2021.150-159. URL:

https://visnyk.kh.ua/uk/journals/visnik-naprnu-2-2021-r/vidpovidalnist-za-shkodu-zavdanu-vikoristannyam-tekhnologiy-shtuchnogo-intelektu