УДК 351:004.8
DOI https://doi.org/10.32782/tnv-pub.2025.6.11

ШТУЧНИЙ ІНТЕЛЕКТ ТА АВТОМАТИЗОВАНЕ ПРИЙНЯТТЯ РІШЕНЬ У ПУБЛІЧНОМУ УПРАВЛІННІ В УМОВАХ ЄВРОІНТЕГРАЦІЇ

Сімонцева Л. О. *– кандидат юридичних наук, доцент, завідувач кафедри публічного управління, права та гуманітарних наук Херсонського державного аграрно-економічного університету*
ORCID: 0000-0003-2722-4402

У статті проаналізовано використання технологій штучного інтелекту (ШІ) у процесах автоматизованого та напівавтоматизованого прийняття рішень у публічному управлінні України. Наголошено, що у процесі цифрової трансформації державного сектору та розбудови е-врядування інтеграція ШІ розглядається як інструмент підвищення ефективності, прозорості та підзвітності органів влади, однак одночасно створює підвищені ризики для прав людини, зокрема у сфері захисту персональних даних, недискримінації та доступу до правосуддя. На основі узагальнення міжнародних досліджень моделей застосування ШІ в публічному секторі окреслено типові сценарії автоматизованого прийняття рішень.

Особливу увагу приділено європейським та міжнародним стандартам регулювання автоматизованих рішень у публічному секторі: Загальному регламенту про захист даних (GDPR), Регламенту про штучний інтелект (AI Act), Принципам ОЕСР щодо ШІ, Рекомендації ЮНЕСКО з етики ШІ та Рамковій конвенції Ради Європи про ШІ, права людини, демократію та верховенство права. Розкрито ключові вимоги цих актів щодо правових підстав обробки даних, заборони суто алгоритмічних рішень без належного людського контролю, права на пояснення, оцінки впливу високоризикових систем, прозорості, підзвітності та інституційного нагляду. Також проаналізовано національне законодавство – насамперед Закон України «Про захист персональних даних» інші нормативно-правові акти у сфері публічних електронних послуг та стратегічних документів щодо розвитку ШІ – з точки зору їхньої готовності до регулювання автоматизованого прийняття рішень.

Обґрунтовано, що національне правове поле рухається у напрямі європейських стандартів фрагментарно: відсутні спеціальні норми щодо автоматизованих рішень і профілювання, процедури оцінки впливу систем ШІ на права людини, інституціоналізований алгоритмічний аудит, прозорі механізми участі стейкхолдерів. Показано ризики алгоритмічної упередженості та цифрової дискримінації у відносинах між державою та вразливими групами населення в умовах воєнних і повоєнних трансформацій. Запропоновано основні напрями адаптації української політики та законодавства до європейських і міжнародних стандартів: оновлення Концепції розвитку сфери ШІ до 2030 року з урахуванням risk-based підходу, гармонізація Закону «Про захист персональних даних» із положеннями GDPR щодо автоматизованих рішень, модернізація законодавства про публічні електронні послуги відповідно до вимог AI Act щодо високоризикових систем, а також формування цілісної системи врядування ШІ, орієнтованої на захист прав людини, стійкість демократії та зміцнення довіри до публічної влади.

Ключові слова: *штучний інтелект, автоматизоване прийняття рішень, публічне управління, захист персональних даних, алгоритмічна упередженість, цифрова дискримінація,європейські стандарти, GDPR, AI Act.*

Simontseva L. O. Artificial intelligence and automated decision-making in public administration in the context of European integration

The article analyzes the use of artificial intelligence (AI) technologies in automated and semi-automated decision-making processes in the public administration of Ukraine. It emphasizes that, in the context of the digital transformation of the public sector and the development of e-governance, AI integration is viewed as a tool for increasing the efficiency, transparency, and accountability of public authorities; however, at the same time, it generates heightened risks to human rights, particularly in the areas of personal data protection, non-discrimination, and access to justice. Based on a synthesis of international research on AI application models in the public sector, the study outlines typical scenarios of automated decision-making.

Special attention is paid to European and international regulatory standards governing automated decisions in the public sector: the General Data Protection Regulation (GDPR), the Artificial Intelligence Act (AI Act), the OECD Principles on AI, the UNESCO Recommendation on the Ethics of AI, and the Council of Europe Framework Convention on AI, Human Rights, Democracy and the Rule of Law. The article identifies the key requirements of these instruments regarding the lawful basis for data processing, the prohibition of purely algorithmic decisions without adequate human oversight, the right to explanation, impact assessments for high-risk systems, transparency, accountability, and institutional supervision. The paper also examines national legislation–primarily the Law of Ukraine «On Personal Data Protection», as well as other legal acts regulating public electronic services and strategic documents on AI development–from the perspective of their readiness to govern automated decision-making.

It is substantiated that the national legal framework is moving toward European standards in a fragmented manner: there are no specific rules on automated decisions and profiling, no procedures for assessing the human-rights impact of AI systems, no institutionalized algorithmic audit, and no transparent mechanisms for stakeholder participation. The study highlights the risks of algorithmic bias and digital discrimination in relations between the state and vulnerable population groups under conditions of wartime and post-war transformations. The article proposes key directions for adapting Ukrainian policy and legislation to European and international standards, including updating the Concept for AI Development until 2030 with a risk-based approach, harmonizing the Law «On Personal Data Protection» with the GDPR provisions on automated decision-making, modernizing legislation on public electronic services in line with the AI Act requirements for high-risk systems, and building a comprehensive AI governance system focused on human rights protection, democratic resilience, and strengthening public trust in government.

Key words: *artificial intelligence, automated decision-making, public administration, personal data protection, algorithmic bias, digital discrimination, European standards, GDPR, AI Act.*

Постановка проблеми. Стрімкий розвиток технологій штучного інтелекту (ШІ) радикально змінює конфігурацію публічного управління. Якщо перший етап цифровізації переважно зводився до переведення існуючих процедур у електронну форму, то зараз все більше органів влади переходять до автоматизованого та напівавтоматизованого прийняття рішень на основі алгоритмічної обробки даних. Такі системи використовуються для попереднього відбору заяв, оцінювання ризиків, виявлення шахрайства, визначення пріоритетності звернень, а в перспективі – для формування персоналізованих траєкторій доступу до публічних послуг.

У контексті України ця тенденція відбувається на тлі масштабної цифрової трансформації публічного сектору, розвитку інфраструктури е-врядування, впровадження екосистеми «Дія», а також курсом держави на відбудову та європейську інтеграцію. Відповідно, інтеграція ШІ в процеси публічного управління розглядається як потенційно потужний інструмент підвищення ефективності, прозорості та підзвітності органів влади, оптимізації витрат і поліпшення якості публічних послуг [1–9].

Водночас автоматизоване прийняття рішень у публічному управлінні є сферою підвищеного ризику з точки зору захисту прав людини. Ідеться не лише про технічні вразливості, а й про системні загрози: непрозорість алгоритмів, алгоритмічну упередженість, цифрову дискримінацію, невизначеність меж відповідальності за «рішення, прийняті ШІ» [7–9]. Особливо небезпечним є поєднання широких масивів персональних даних із високою дискретійністю алгоритмів і недостатньо розвиненими механізмами правового та інституційного контролю.

Європейський Союз у відповідь на ці виклики сформував комплексну регуляторну рамку, яка поєднує вимоги Загального регламенту із захисту даних (GDPR), ризик-орієнтований підхід Регламенту про штучний інтелект (AI Act), етичні засади Принципів ОЕСР щодо ШІ, Рекомендації ЮНЕСКО щодо етики ШІ та Рамкової конвенції Ради Європи про ШІ, права людини, демократію та верховенство права [10–14]. У центрі цих міжнародних актів – захист

персональних даних, забезпечення права особи на неприпустимість ухвалення щодо неї юридично значущих рішень, базованих виключно на автоматизованій обробці даних без належного людського втручання, вимоги прозорості та пояснюваності, оцінка впливу високоризикових систем, а також створення ефективних механізмів нагляду.

Національне законодавство наразі лише частково відображає ці підходи. Закон «Про захист персональних даних» не містить чітко закріплених норм щодо автоматизованого прийняття рішень, профілювання та права на людський перегляд; законодавство про публічні електронні послуги не розрізняє стандарти для систем із різним рівнем ризику; відсутня інституціоналізована практика оцінки впливу систем ШІ на права людини, персональні дані та демократичні процеси [15–16]. У поєднанні з воєнним і повоєнним контекстом це створює високі ризики як для громадян, так і для самої легітимності публічної влади.

Метою статті є проаналізувати автоматизоване прийняття рішень у публічному управлінні з використанням технологій ШІ крізь призму захисту персональних даних та європейських стандартів (GDPR, AI Act, етичні документи), оцінити відповідність українського правового поля цим підходам та запропонувати напрями його адаптації.

Виклад основного матеріалу. У сучасній науковій літературі ШІ розглядається не лише як сукупність технологій обробки даних, а як організаційний ресурс, що змінює способи прийняття рішень в організації [1; 2]. S. J. Alotaibi, узагальнюючи моделі використання ШІ в організаціях, показує, що алгоритмічні системи можуть виконувати роль:

– інструмента підтримки рішень (decision support), коли остаточне рішення залишається за людиною;

– співавтора рішень (decision augmentation), коли ШІ формує варіанти рішень і пропонує їх для оцінки;

– автономного агента (automated decision maker), коли система ухвалює рішення без безпосереднього втручання людини [1].

У публічному управлінні ці моделі набувають особливої ваги, оскільки рішення органів влади безпосередньо впливають на права, свободи та обов'язки людини. Як підкреслюють Kh. Farooq і B. Solowiej, інтеграція ШІ в публічний сектор відкриває можливості для підвищення ефективності, прогнозування та таргетування політик, але водночас посилює асиметрію влади між державою та громадянами, якщо відсутні прозорі й підзвітні механізми governance таких систем [2].

M. Babšek та співавтори, аналізуючи найцитованіші дослідження у сфері «AI & public administration», виокремлюють кілька типових сценаріїв застосування ШІ:

– аналітика політики (policy analytics) – моделювання сценаріїв, оцінка регуляторного впливу, прогнозування;

– інтелектуалізовані публічні послуги – персоналізація, скорочення часу обробки, автоматизоване сортування звернень;

– управління ресурсами та операціями – оптимізація логістики, інфраструктурних рішень, розподілу навантаження;

– наглядово-контрольна аналітика – виявлення шахрайства, порушень, аномальних патернів поведінки [3].

У всіх цих випадках ШІ так чи інакше вбудовується у процес прийняття рішень: або як фільтр і «голкіпер», який вирішує, які справи розглядати в першу чергу; або як механізм рекомендованих рішень; або як повністю автоматизований модуль, результат якого орган влади фактично сприймає без критичної перевірки.

A. V. Rakšnys, D. Gudelis та A. Guogis наголошують, що в публічному секторі використання ШІ не може розглядатися лише як технічна модернізація: воно переформатовує саму роль держави, зокрема соціальної [4]. Алгоритмічні системи посилюють спроможність держави збирати й аналізувати дані про громадян, прогнозувати їх поведінку, забезпечувати вибірковий контроль та проводити диференційований моніторинг, що створює як потенціал для більш адресної підтримки, так і ризики надмірного контролю та втручання в приватність.

Вітчизняні автори доповнюють цей міжнародний дискурс національним виміром. Т. С. Яровий показує, що в Україні технології ШІ насамперед інтегруються у функції збирання, обробки та аналізу інформації, підготовки та ухвалення управлінських рішень, а також у комунікацію з громадськістю [7]. О. Оболенський, В. Косицька та А. Рвач акцентують, що використання ШІ змінює вимоги до інституційної спроможності органів влади: від уміння «управляти процесами» до здатності «управляти даними» і ризиками, пов'язаними з алгоритмічними рішеннями [8].

У цьому контексті автоматизоване прийняття рішень у публічному управлінні можна розглядати як перетин трьох площин: технологічної (алгоритмічні можливості та якість даних), правової (захист прав людини та нормативне регулювання) та етичної (прозорість, справедливість і суспільна довіра).

Подальший аналіз у статті фокусується саме на третій площині, демонструючи, якою мірою європейські стандарти захисту персональних даних та регулювання автоматизованих рішень (GDPR, AI Act, етичні документи) можуть і повинні бути імплементовані в українське правове поле.

Європейський підхід до автоматизованого прийняття рішень у публічному секторі вибудовується навколо кількох основних документів, які задають правові та етико-ціннісні рамки. Загальний регламент про захист даних (GDPR) фіксує базову логіку: використання персональних даних для автоматизованої обробки, профілювання чи ухвалення рішень щодо фізичної особи є допустимим лише за умови наявності чіткої правової підстави, пропорційності й наявності ефективних гарантій [10]. Особливе значення для публічного управління має положення про право особи на захист від суто алгоритмічних рішень, що ґрунтуються виключно на автоматизованій обробці, включно з профілюванням, якщо таке рішення має для неї юридичні наслідки або подібним чином істотно впливає на її становище. У цьому положенні сконцентровано кілька ключових вимог одночасно: поінформованість суб'єкта даних, можливість оскарження, право на «людський перегляд» алгоритмічного висновку, обмеження сфери застосування повністю автоматизованих рішень.

Регламент про штучний інтелект (AI Act) розвиває цю логіку, переводячи її в ризик-орієнтовану модель регулювання [11]. Системи ШІ, що застосовуються у сфері публічного управління, у багатьох випадках відносяться до категорії високоризикових: ідеться про рішення, пов'язані з доступом до соціальних послуг, оцінкою благонадійності, адмініструванням публічних ресурсів, наглядом та правозастосуванням. Для таких систем AI Act встановлює підвищені вимоги до якості даних, документації, прозорості, простежуваності й підзвітності, а також передбачає необхідність проведення ex ante оцінки ризиків і впливу, реєстрації високоризикових систем, створення ефективних механізмів нагляду. Для публічного сектора це означає, що інтеграція ШІ в управлінські процеси не може бути «технічним рішенням ІТ-відділу»; вона повинна бути вписана в чітко окреслену систему регуляторних вимог і контролю.

Принципи ОЕСР щодо штучного інтелекту та Рекомендація ЮНЕСКО щодо етики ШІ задають ширшу ціннісну рамку, у якій правові механізми набувають свого змісту [12–13]. У фокусі цих документів – людиноцентричність, повага до прав людини, інклюзивність, недискримінація, прозорість і підзвітність. Для публічного управління це має подвійний ефект. З одного боку, закріплюється вимога, щоби системи ШІ у діяльності органів влади були орієнтовані на суспільне благо, зменшення нерівностей і розширення можливостей громадян, а не лише на оптимізацію витрат чи підвищення контролю. З іншого – підкреслюється обов'язок держави створити процедури етичної оцінки, незалежного моніторингу, участі різних груп стейкхолдерів у виробленні правил використання ШІ.

Рамкова конвенція Ради Європи про штучний інтелект, права людини, демократію і верховенство права поглиблює цей підхід, прямо пов'язуючи використання ШІ в публічному секторі з вимогами доступу до правосуддя, справедливого провадження, ефективних засобів правового захисту [14]. У центрі уваги є не лише захист персональних даних, а й ширший набір прав і свобод, що можуть бути обмежені внаслідок алгоритмічних рішень: право на недискримінацію, свободу вираження поглядів, участь у виборчих процесах, соціальні права. Для держав – учасниць Конвенції це означає обов'язок забезпечити такі механізми врядування ШІ, які б не лише мінімізували ризики, а й гарантували змістовний контроль за алгоритмічними системами з боку судів, наглядових органів та громадянського суспільства.

У сукупності ці акти формують багаторівневу модель: правові норми щодо даних і ШІ, етичні стандарти, механізми інституційного нагляду та участі суспільства. Саме до цієї моделі доводиться «прикладати» українське законодавство, оцінюючи його готовність до автоматизованого прийняття рішень у публічному управлінні.

Національне правове поле, що опосередковано регулює використання ШІ в публічному управлінні, сьогодні складається з кількох блоків: законодавства про захист персональних даних, нормативних актів у сфері е-врядування та публічних електронних послуг, а також стратегічних документів, присвячених розвитку цифрової економіки та сфери ШІ [15–19]. Попри значний прогрес у цифровізації, ці блоки залишаються слабо інтегрованими між собою саме в контексті автоматизованого прийняття рішень.

Закон України «Про захист персональних даних» формально закріплює основні принципи обробки даних, права суб'єктів і обов'язки володільців та розпорядників інформації [15]. Однак у ньому відсутнє чітке регулювання автоматизованих рішень і профілювання за аналогією до ст. 22 GDPR [10]: не розмежовано ситуації, коли рішення органу влади ґрунтується виключно на алгоритмічній обробці; не передбачено спеціальних гарантій, пов'язаних із правом на пояснення логіки такого рішення, перегляд його людиною, оскарження з урахуванням особливостей алгоритмічної обробки. У результаті автоматизовані модулі, які фактично впливають на доступ до послуг чи надання пільг, опиняються в «сірої зоні» права, де забезпечення прав суб'єктів даних залежить більше від доброї волі адміністратора системи, ніж від чітко прописаних процедур.

Акти, що регулюють надання публічних електронних послуг та функціонування цифрової інфраструктури, значною мірою орієнтовані на забезпечення доступності сервісів, їхню сумісність, інтеграцію реєстрів, але не на управління ризиками ШІ. У законодавстві про е-послуги не розрізняються інформаційні системи загального призначення та потенційно високоризикові рішення, у яких

алгоритмічна логіка може прямо впливати на юридичний статус особи. Відсутні норми, які б зобов'язували органи влади повідомляти громадян про використання ШІ, фіксувати факти застосування автоматизованих рішень у конкретній справі, забезпечувати доступ до зрозумілої інформації про критерії й дані, що враховуються при такій обробці [16–18].

Стратегічні документи, зокрема Концепція розвитку сфери штучного інтелекту до 2030 року, фіксують важливі орієнтири – розвиток досліджень, освіти, інфраструктури, підтримку інноваційного бізнесу, формування етичних підходів до використання ШІ [19]. Водночас питання автоматизованого прийняття рішень у публічному управлінні, оцінки впливу таких систем на права людини, прозорості та підзвітності алгоритмів, ролі незалежних наглядових інституцій залишаються радше задекларованими намірами, ніж конкретними зобов'язаннями. Це посилює розрив між швидкістю технічних змін і повільністю нормативного реагування.

Українська доктрина демонструє чітке усвідомлення цих прогалин. Дослідники, які аналізують вплив ШІ на права і свободи людини, персональні дані, правосуб'єктність, наголошують на необхідності не просто «дописати окремі норми», а переосмислити підхід до регулювання алгоритмічних систем, перейшовши від технологічно нейтральних формулювань до risk-based logics, співзвучної AI Act]. У поле зору потрапляють не лише питання приватності, а й проблематика цифрової дискримінації, алгоритмічної упередженості, небезпеки перенесення прихованих соціальних нерівностей у структуру рішень, що ухвалюються органами влади.

Один із найбільш чутливих аспектів автоматизованого прийняття рішень у публічному секторі пов'язаний з алгоритмічною упередженістю та цифровою дискримінацією. Йдеться про ситуації, коли системи ШІ, що працюють із великими масивами даних, відтворюють або посилюють уже наявні соціальні нерівності, закріплюючи їх в автоматизованих рішеннях. Джерелом такої упередженості стають не лише технічні особливості алгоритмів, а й «упереджені» дані, на основі яких ці алгоритми навчаються, нерепрезентативність вибірок, некоректний вибір індикаторів, а також приховані ціннісні припущення розробників.

У публічному управлінні наслідки алгоритмічної упередженості особливо небезпечні, оскільки вони можуть впливати на доступ до соціальних послуг, розподіл ресурсів, визначення пріоритетів нагляду, оцінювання благонадійності, взаємодію з «групами ризику». Українські та зарубіжні дослідники підкреслюють, що у сфері прийняття рішень державою навіть незначна похибка або асиметрія в алгоритмі може призвести до систематичного неблагополуччя для певних категорій громадян [7–9]. У такий спосіб ШІ ризикує перетворитися на інструмент легітимації вже наявних упереджень, надаючи їм видимість «об'єктивності» й «науковості».

Особливу увагу привертає проблема непрозорості алгоритмів. Для багатьох сучасних моделей, передусім тих, що базуються на машинному навчанні, характерна складність пояснення логіки прийнятого рішення не лише для користувачів, а інколи й для самих розробників. У публічному секторі така непрозорість конфліктує з вимогами підзвітності та обов'язком органів влади обґрунтовувати свої рішення. Якщо громадянин отримує відмову у наданні послуги або зміну свого правового статусу на основі алгоритмічного висновку, але не може зрозуміти, з яких причин і на основі яких даних це сталося, підривається довіра до інституцій, а також реальність права на ефективний засіб юридичного захисту.

Для України, де публічне управління одночасно переживає процеси децентралізації, цифровізації, воєнних трансформацій і відбудови, виклик цифрової дискримінації набуває додаткових вимірів. Ідеться про вразливість внутрішньо переміщених осіб, ветеранів, мешканців територій, що постраждали від бойових дій, соціально незахищених груп. Якщо системи ШІ, які підтримують прийняття рішень щодо соціальної допомоги, відновлення інфраструктури, доступу до житлових програм, працюватимуть із неповними або упередженими даними, ризик відтворення структурної нерівності лише посилюватиметься. Тим важливішими стають інституціоналізовані механізми виявлення, моніторингу та корекції алгоритмічної упередженості, включно з участю незалежних експертів і представників громадянського суспільства.

Питання адаптації української політики й законодавства до європейських та міжнародних стандартів у сфері ШІ не можна звести до механічного запозичення окремих положень GDPR чи AI Act. Йдеться про формування цілісної системи врядування ШІ, у якій правові, етичні та організаційні компоненти взаємопов'язані.

Ключовим напрямом виглядає переосмислення та оновлення Концепції розвитку сфери ШІ до 2030 року з урахуванням вже ухваленого AI Act, Рекомендації ЮНЕСКО, Принципів ОЕСР та Рамкової конвенції Ради Європи [11–13; 19]. У такому оновленні акцент має бути зміщений від загальних декларацій про «етичність» і «безпеку» до конкретних механізмів: запровадження обов'язкової оцінки впливу високоризикових систем ШІ на права людини та персональні дані; встановлення вимог прозорості та explainability для алгоритмічних рішень у публічному управлінні; визначення ролі незалежних наглядових інституцій і процедур участі стейкхолдерів при розробленні та впровадженні таких систем.

Не менш важливим є перегляд законодавства про захист персональних даних. Його гармонізація з GDPR передбачає не лише уточнення термінології чи процедур реєстрації володільців, а й змістовне закріплення норм про автоматизоване прийняття рішень, профілювання, право особи на заперечення проти таких рішень, право вимагати людського перегляду й отримувати зрозуміле пояснення логіки обробки [10]. Для публічного управління доцільно прямо встановити, що рішення органів влади, які мають істотний вплив на права й обов'язки громадян, не можуть ґрунтуватися виключно на автоматизованій обробці даних без наявності спеціальних гарантій і процедур перегляду.

Законодавство про публічні електронні послуги [16]. також потребує перегляду крізь призму risk-based підходу AI Act. Йдеться про запровадження диференційованих вимог до систем, які лише інформують або надають доступ до сервісів, і систем, що ухвалюють чи підтримують юридично значущі рішення. Для останніх має бути закріплено обов'язкове документування використання алгоритмічних модулів у кожній конкретній справі, можливість фіксації й подальшого аналізу помилок, спеціальні процедури аудиту та зовнішнього нагляду. Паралельно необхідно формувати практику публічної звітності органів влади щодо застосування ШІ – із зазначенням сфер використання, типів даних, базових принципів роботи алгоритмів, виявлених ризиків і заходів реагування.

Адаптація до європейських стандартів не обмежується змінами законодавчих актів. Вона передбачає також розбудову інституційної спроможності: підготовку кадрів, розвиток компетентностей з етичного та правового оцінювання систем ШІ, створення міждисциплінарних команд, які поєднуватимуть фахівців у галузі права, публічного управління, ІТ, кібербезпеки, соціальних наук. Без такої спроможності

навіть формально коректні норма права ризикують залишитися деклараціями.

Нарешті, важливо, щоби процес адаптації не перетворився на суто технічну «гармонізацію» під європейські акти. Український контекст – воєнний і повоєнний, із великими масивами вразливих груп, із завданнями відбудови та зміцнення довіри до інституцій – потребує осмисленого, людиноцентричного підходу. ШІ в публічному управлінні має розглядатися не як чергова «модна технологія», а як інструмент, який може як посилити здатність держави захищати права й забезпечувати стійкість, так і створити нові форми нерівностей і контролю. Саме тому адаптація до європейських стандартів має сприйматися не як зовнішній обов'язок, а як внутрішня потреба публічної влади залишатися легітимною, підзвітною та орієнтованою на громадянина в умовах алгоритмічної епохи.

Висновки. Аналіз європейських та міжнародних підходів до регулювання штучного інтелекту, насамперед у контексті автоматизованого прийняття рішень у публічному управлінні, дозволяє зробити кілька узагальнюючих висновків. У центрі цих підходів перебуває не технологія як така, а захист прав людини, підзвітність публічної влади та збереження демократичних процедур у ситуації, коли дедалі більше рішень ухвалюється за участю алгоритмів. GDPR, AI Act, Принципи ОЕСР щодо ШІ, Рекомендація ЮНЕСКО та Рамкова конвенція Ради Європи [10–14] формують багаторівневу модель, у якій поєднано норми щодо обробки даних, вимоги до ризик-орієнтованого регулювання, етичні стандарти, механізми інституційного нагляду й участі стейкхолдерів.

Українське законодавство поки що рухається в цьому напрямі фрагментарно. Закон «Про захист персональних даних» закріплює базові принципи приватності, але не містить розгорнутого регулювання автоматизованих рішень, профілювання, права на пояснення та людський перегляд алгоритмічних висновків за аналогією до ст. 22 GDPR . Норми, що регулюють публічні електронні послуги та цифрову інфраструктуру, зосереджені передусім на технічній та організаційній доступності сервісів, а не на управлінні ризиками високоризикових систем ШІ та гарантіях недискримінації користувачів. Стратегічні документи у сфері цифрової трансформації та розвитку ШІ, включно з Концепцією розвитку сфери штучного інтелекту до 2030 року , фіксують важливі орієнтири, але натепер не містять достатньо конкретних інструментів оцінки впливу алгоритмічних систем на права людини, прозорості та підзвітності рішень, ухвалених із використанням ШІ [10; 15–19].

Окремого акценту потребує проблема алгоритмічної упередженості та цифрової дискримінації. Як показує і міжнародна, і українська доктрина, системи ШІ, які працюють із великими масивами даних, здатні не лише підвищувати ефективність аналітики та прогнозування, а й відтворювати й посилювати вже наявні соціальні нерівності [7–9]. У публічному управлінні це має прямі наслідки для доступу до соціальних послуг, розподілу бюджетних ресурсів, визначення «ризикових» категорій громадян, пріоритетів нагляду та контролю. В умовах воєнного й повоєнного розвитку України, масового переміщення населення, зростання кількості вразливих груп ризик цифрової дискримінації набуває особливої гостроти. Інституційно не врегульована, алгоритмічна упередженість загрожує підважити довіру до держави й відтворити структурні нерівності вже в «цифровому вимірі».

У цьому контексті адаптація української політики та законодавства до європейських і міжнародних стандартів у сфері ШІ має розглядатися не як формальна «гармонізація» окремих норм, а як побудова цілісної системи врядування штучним інтелектом у публічному секторі. Йдеться про необхідність переосмислення Концепції розвитку сфери ШІ до 2030 року з урахуванням risk-based підходу AI Act,

етичних орієнтирів Рекомендації ЮНЕСКО та людиноцентричної логіки Рамкової конвенції Ради Європи; модернізації Закону «Про захист персональних даних» через імплементацію положень, що стосуються автоматизованих рішень, профілювання, пояснюваності алгоритмів, права на заперечення та людський перегляд; оновлення законодавства про публічні електронні послуги з урахуванням вимог до високоризикових систем ШІ, у тому числі щодо реєстрів, аудиту, прозорості та захисту прав користувачів.

Водночас одних лише законодавчих змін недостатньо. Необхідним є послідовне нарощування інституційної спроможності органів публічної влади до етичного та правового управління ШІ. Це передбачає формування спеціалізованих компетентностей у сфері data governance, алгоритмічного аудиту, оцінки впливу на права людини; створення механізмів незалежного нагляду (у тому числі у формі уповноважених органів та етичних комітетів), розвиток практик публічної звітності щодо використання ШІ; забезпечення реальної, а не декларативної участі стейкхолдерів – наукової спільноти, бізнесу, громадянського суспільства – у виробленні політики щодо ШІ. Без таких елементів будь-які формальні посилання на «європейські стандарти» ризикують залишитися лише риторикою.

На нашу думку, ключовим критерієм успішності адаптації української політики та законодавства у сфері ШІ має стати не швидкість «перенесення» положень GDPR чи AI Act у національне право, а здатність побудувати таку модель автоматизованого прийняття рішень у публічному управлінні, яка одночасно підвищуватиме ефективність держави та посилюватиме захист прав людини, довіру до інституцій і стійкість демократії в умовах воєнних і повоєнних трансформацій. ШІ у публічному секторі має розглядатися як інструмент, що може працювати як на посилення людиноцентричного, прозорого та справедливого врядування, так і на відтворення контролю та нерівностей. Від того, наскільки послідовно Україна інтегрує європейські та міжнародні стандарти в поєднанні з власним унікальним контекстом, залежатиме, до якого з цих сценаріїв ми наближатимемося.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Alotaibi S. J. Theories, Frameworks, and Models of Using Artificial Intelligence in Organizations. Journal of the Korea Convergence Society. 2022. Vol. 13, No. 4. P. 1–10. URL: https://www.koreascience.kr/article/JAKO202232764037011.pdf (дата звернення: 10.11.2025).

2. Farooq Kh., Solowiej B. J. Artificial Intelligence in the Public Sector: Maximizing Opportunities, Managing Risks. Washington, D.C. : World Bank Group, 2020. 108 p. URL: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/809611616042736565/artificial-intelligence-in-the-public-sector-maximizing-opportunities-managing-risks (дата звернення: 05.09.2025).

3. Babšek M., Rakar T., Kovač P., Seme T. Artificial Intelligence Adoption in Public Administration: An Overview of Top-Cited Articles and Practical Applications. AI. 2025. Vol. 6, No. 3. P. 44. URL: https://www.mdpi.com/2673-2688/6/3/44 (дата звернення: 08.09.2025).

4. Rakšnys A. V., Gudelis D., Guogis A. The Uses of Artificial Intelligence in the Public Sector: Challenges and Prospects. Public Policy and Administration. 2025. Vol. 24, No. 3. URL: https://vpa.ktu.lt/index.php/PPA/article/view/39489 (дата звернення: 10.09.2025).

5. Rekunenko I., Kobushko I., Dzydzyguri O., Balahurovska I., Yurynets O., Zhuk O. The use of artificial intelligence in public administration: Bibliometric analysis. Problems and Perspectives in Management. 2025. Vol. 23, Issue 1. P. 209–224. URL: https://www.businessperspectives.org/index.php/journals/

problems-and-perspectives-in-management/issue-473/the-use-of-artificial-intelligence-in-public-administration-bibliometric-analysis (дата звернення: 10.19.2025).

6. Vatamanu A. F., Tofan M. Integrating Artificial Intelligence into Public Administration: Challenges and Vulnerabilities. Administrative Sciences. 2025. Vol. 15, No. 4. P. 149. URL: https://www.mdpi.com/2076-3387/15/4/149 (дата звернення: 10.19.2025).

7. Яровий Т. С. Можливості та ризики використання штучного інтелекту в публічному управлінні. Economic Synergy. 2023. № 2(8). С. 36–47. URL: https://es.istu.edu.ua/index.php/EconomicSynergy/article/download/113/84/251 (дата звернення: 10.19.2025).

8. Оболенський О. Ю., Косицька В., Рвач А. Штучний інтелект у публічному управлінні: вимоги, проблеми та ризики. Вчені записки. 2023. № 33(4). С. 121–137. URL: https://vz.kneu.ua/archive/2023/33%284%29.10 (дата звернення: 10.19.2025).

9. Ніколюк О. В., Савченко Т. В., Родіна О. В. Проблеми та переваги штучного інтелекту як ефективного інституту для розбудови управлінських рішень в публічному управлінні. Вчені записки ТНУ імені В. І. Вернадського. Серія: Публічне управління та адміністрування. 2023. Т. 34(73), № 3. С. 124–131. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2023/3_2023/19.pdf (дата звернення: 10.19.2025).

10. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation – GDPR). EUR-Lex. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 06.11.2025).

11. Regulation (EU) 2024/1689 of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (AI Act). Official Journal of the European Union. 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (дата звернення: 07.10.2025).

12. OECD Principles on Artificial Intelligence. OECD. 2019. URL: https://archive.epic.org/algorithmic-transparency/OECD-AI-Principles-flyer.pdf (дата звернення: 01.10.2025).

13. Recommendation on the Ethics of Artificial Intelligence. UNESCO. 2021. URL: https://www.naavi.org/uploads_wp/2023/Recommendation%20on%20the%20Ethics%20of%20Artificial%20Intelligence%20-%20UNESCO%20Digital%20Library.pdf (дата звернення: 07.11.2025).

14. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. Strasbourg : Council of Europe, 2024. URL: https://rm.coe.int/1680afae3c (дата звернення: 10.11.2025).

15. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 05.11.2025).

16. 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#Text (дата звернення: 20.10.2025).

17. Про електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 22.10.2025).

18. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 23.10.2025).

19. Про схвалення Концепції розвитку штучного інтелекту в Україні до 2030 р.: Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/go/1556-2020-%D1%80 (дата звернення: 10.10.2025).

REFERENCES:

1. Alotaibi, S. J. (2022). Theories, frameworks, and models of using artificial intelligence in organizations. Journal of the Korea Convergence Society, 13(4), 1–10. URL:

https://www.koreascience.kr/article/JAKO202232764037011.pdf (дата звернення: 10.11.2025).

2. Farooq, Kh., & Solowiej, B. J. (2020). Artificial intelligence in the public sector: Maximizing opportunities, managing risks. World Bank Group. URL: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/809611616042736565/artificial-intelligence-in-the-public-sector-maximizing-opportunities-managing-risks (дата звернення: 05.09.2025).

3. Babšek, M., Rakar, T., Kovač, P., & Seme, T. (2025). Artificial intelligence adoption in public administration: An overview of top-cited articles and practical applications. AI, 6(3), Article 44. URL: https://www.mdpi.com/2673-2688/6/3/44 (дата звернення: 08.09.2025).

4. Rakšnys, A. V., Gudelis, D., & Guogis, A. (2025). The uses of artificial intelligence in the public sector: Challenges and prospects. Public Policy and Administration, 24(3). URL: https://vpa.ktu.lt/index.php/PPA/article/view/39489 (дата звернення: 10.09.2025).

5. Rekunenko, I., Kobushko, I., Dzydzyguri, O., Balahurovska, I., Yurynets, O., & Zhuk, O. (2025). The use of artificial intelligence in public administration: Bibliometric analysis. Problems and Perspectives in Management, 23(1), 209–224. URL: https://www.businessperspectives.org/index.php/journals/problems-and-perspectives-in-management/issue-473/the-use-of-artificial-intelligence-in-public-administration-bibliometric-analysis (дата звернення: 19.10.2025).

6. Vatamanu, A. F., & Tofan, M. (2025). Integrating artificial intelligence into public administration: Challenges and vulnerabilities. Administrative Sciences, 15(4), Article 149. URL: https://www.mdpi.com/2076-3387/15/4/149 (дата звернення: 19.10.2025).

7. Yarovyi, T. S. (2023). Mozhlyvosti ta ryzyky vykorystannia shtuchnoho intelektu v publichnomu upravlinni [Opportunities and risks of using artificial intelligence in public administration]. Economic Synergy, 2(8), 36–47. URL: https://es.istu.edu.ua/index.php/EconomicSynergy/article/download/113/84/251 (дата звернення: 19.10.2025).

8. Obolenskyi, O. Yu., Kosytska, V., & Rvach, A. (2023). Shtuchnyi intelekt u publichnomu upravlinni: vymohy, problemy ta ryzyky [Artificial intelligence in public administration: Requirements, problems, and risks]. Vcheni zapysky, 33(4), 121–137. URL: https://vz.kneu.ua/archive/2023/33%284%29.10 (дата звернення: 19.10.2025).

9. Nikoliuk, O. V., Savchenko, T. V., & Rodina, O. V. (2023). Problemy ta perevahy shtuchnoho intelektu yak efektyvnoho instytutu dlia rozbudovy upravlinskykh rishen v publichnomu upravlinni [Problems and advantages of artificial intelligence as an effective institution for developing managerial decisions in public administration]. Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: Publichne upravlinnia ta administruvannia, 34(73)(3), 124–131. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2023/3_2023/19.pdf (дата звернення: 19.10.2025).

10. European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation—GDPR). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 06.11.2025).

11. European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (AI Act). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (дата звернення: 07.10.2025).

12. Organisation for Economic Co-operation and Development. (2019). OECD principles on artificial intelligence. URL: https://archive.epic.org/algorithmic-transparency/OECD-AI-Principles-flyer.pdf (дата звернення: 01.10.2025).

13. UNESCO. (2021). Recommendation on the ethics of artificial intelligence. URL: https://www.naavi.org/uploads_wp/2023/Recommendation%20on%20the%20Ethics%20

of%20Artificial%20Intelligence%20-%20UNESCO%20Digital%20Library.pdf (дата звернення: 07.11.2025).

14. Council of Europe. (2024). Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. URL: https://rm.coe.int/1680afae3c (дата звернення: 10.11.2025).

15. Verkhovna Rada of Ukraine. (2010). Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 01.06.2010 No. 2297-VI [On personal data protection: Law of Ukraine dated 01.06.2010 No. 2297-VI]. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 05.11.2025).

16. Verkhovna Rada of Ukraine. (2021). Pro osoblyvosti nadannia publichnykh (elektronnykh publichnykh) posluh: Zakon Ukrainy vid 15.07.2021 No. 1689-IX [On the specifics of providing public (electronic public) services: Law of Ukraine dated 15.07.2021 No. 1689-IX]. URL: https://zakon.rada.gov.ua/laws/show/1689-20#Text (дата звернення: 20.10.2025).

17. Verkhovna Rada of Ukraine. (2017). Pro elektronni dovirchi posluhy: Zakon Ukrainy vid 05.10.2017 No. 2155-VIII [On electronic trust services: Law of Ukraine dated 05.10.2017 No. 2155-VIII]. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 22.10.2025).

18. Verkhovna Rada of Ukraine. (2011). Pro dostup do publichnoi informatsii: Zakon Ukrainy vid 13.01.2011 No. 2939-VI [On access to public information: Law of Ukraine dated 13.01.2011 No. 2939-VI]. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 23.10.2025).

19. Cabinet of Ministers of Ukraine. (2020). Pro skhvalennia Kontseptsii rozvytku shtuchnoho intelektu v Ukraini do 2030 r.: Rozporiadzhennia vid 02.12.2020 No. 1556-r [On approval of the Concept of artificial intelligence development in Ukraine until 2030: Order dated 02.12.2020 No. 1556-r]. URL: https://zakon.rada.gov.ua/go/1556-2020-%D1%80 (дата звернення: 10.10.2025).

Дата першого надходження рукопису до видання: 25.11.2025
Дата прийнятого до друку рукопису після рецензування: 12.12.2025
Дата публікації: 30.12.2025