

ЕТИЧНІ ВИКЛИКИ ТА РИЗИКИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПУБЛІЧНОМУ УПРАВЛІННІ

Арделян Іван Сергійович
аспірант

Кафедра журналістики та міжнародних відносин
Плецан Христина Василівна
доцент, к.н. з державного управління
професор кафедри готельно-ресторанного
і туристичного бізнесу
Київський університет культури, Україна

Штучний інтелект сьогодні розглядається як одна з ключових технологій, яка може змінити публічне управління, зробивши його орієнтованим на вирішення громадських потреб. Застосування технологій ШІ дозволяє автоматизувати рутинні процеси, підвищувати точність прийняття управлінських рішень, удосконалювати взаємодію з населенням та, що найголовніше, запобігати корупційним схемам. Зокрема, Мінцифра у березні 2025 р. оприлюднила рекомендації для публічних службовців щодо ефективного й безпечного використання ШІ в державному секторі та було відзначено, що станом на цей період у застосунку «Дія» понад 52 % звернень до служби підтримки вже обробляються із застосуванням ШІ-модулів [1]. Також, у квітні поточного року Міністерство провело навчальний захід, на якому були присутні понад 300 державних службовців та в процесі проведення якого отримали практичні знання про інтеграцію ШІ у держуправління [2]. Аналізуючи дану інформацію, слід відзначити, що в Україні технології ШІ досить ефективно інтегруються в сферу публічного управління, що власне впливає на етичність цієї технології в контексті захисту даних як самих службовців так і населення, яке користується послугами. Саме тому актуальності набуває більш глибоку дослідження основних етичних викликів та ризиків використання ШІ в сфері публічного управління в Україні.

Попри те, що ШІ є доволі перспективною технологією для вдосконалення публічного управління, присутні певні етичні виклики, які власне впливають на трансформаційні процеси в державному секторі. На рис. 1. сформовано основні етичні виклики, які виникають при використанні ШІ в публічному управлінні.

	Прозорість і підзвітність • Алгоритми приймають складні рішення, які громадяни часто не можуть зрозуміти чи перевірити, що створює ризик «чорних скриньок», коли люди не знають, чому система ухвалила саме таке рішення, а без чітких звітів та аудиту виникає недовіра до влади.
	Конфіденційність та захист даних • ІІІ працює з великими масивами персональної інформації (здоров'я, фінанси, соціальний статус), що створює небезпеку несанкціонованого доступу, витоків або використання даних без згоди громадян, та власне підриває їхнє право на приватність.
	Справедливість і недискримінація • Якщо алгоритми навчаються на історичних даних з упередженнями, вони можуть відтворювати або навіть посилювати дискримінацію окремих груп населення (за статтю, етнічністю, соціальним статусом тощо), що ставить під сумнів принцип рівності.
	Відповідальність за рішення • Нечітко визначено, хто відповідає за наслідки помилкових рішень ІІІ – розробники, державні органи чи окремі посадовці, що власне створює ризик уникнення відповідальності й відсутності механізмів відшкодування шкоди громадянам.
	Кібербезпека та стійкість систем • ІІІ-системи стають мішенню для хакерів, а атаки на дані чи моделі можуть призвести до викривлення рішень або витоків конфіденційної інформації, що ставить під загрозу як права громадян, так і національну безпеку.
	Правові рамки та управління ризиками • Законодавство часто відстає від розвитку технологій, що призводить до виникнення прогалин у регулюванні та ускладнює захист прав громадян і визначення меж допустимого використання ІІІ, а без чітких норм ризики етичних порушень зростають.

Рисунок 1. Характеристика етичних викликів при використанні ІІІ в сфері публічному управлінні. Джерело: [3]

Таким чином, слід відзначити, що етичні виклики у сфері ІІІ виходять за межі суто технічних характеристик систем, адже насамперед вони пов'язані з правами людини, справедливістю у доступі до послуг, прозорістю управлінських процесів та підзвітністю інституцій. Ідеться не лише про те, наскільки ефективно алгоритм виконує поставлене завдання, а й про те, чи не створює він прихованих загроз для суспільства. Іншими словами чи ІІІ не порушує право на приватність, чи не відтворює соціальні упередження та чи залишає можливість громадянам оскаржувати рішення, що власне є однією із головних причин етичного контексту технологій в сфері публічного управління [4].

Саме в контексті етичних викликів і виникають основні ризики впровадження ІІІ в публічному управлінні, оцінка яких більш детально наведена в табл. 1. Оцінювання ключових ризиків проводилось за шкалою від 1 до 10, де 1 означає, що ризик майже не впливає на впровадження ІІІ у сфері публічного управління, а 10 – має критичний вплив та може суттєво загальмувати процес цифровізації.

Таблиця 1 Оцінка ключових ризиків впровадження ІІІ в публічному управлінні в умовах цифровізації та етичних норм

Ризик	Оцінка	Характеристика
Кібератаки та злам ІІІ-систем	10	Може призвести до витоку державних даних, які можна використати для маніпуляції рішеннями та дисбалансу в країні
Порушення конфіденційності даних	9	Використання великих обсягів персональних даних створює ризики витоків та несанкціонованого доступу до особистих даних, які можуть бути використанні неправомірно
Недосконалість алгоритмів	8	Технічні помилки можуть спричиняти хибні управлінські рішення, які в свою чергу можуть призвести до загострювання відносин як в державі між управлінцями так і між громадянами і державою.
Алгоритмічне упередження	7	Викривлені дані ведуть до несправедливих рішень та можуть підривати довіру громадян, як от неправильне нарахування соціальних виплат через збій алгоритмічної формули
Відсутність чіткої правової бази	8	Законодавство не встигає за розвитком технологій через що можуть виникати «сірі зони», які призводять до маніпуляцій поточною ситуацією.
Високі фінансові витрати	6	Впровадження та обслуговування ІІІ-систем потребує значних ресурсів, що може обтяжувати бюджет країни, особливо тієї, яка розвивається
Соціальні наслідки (втрата робочих місць)	7	Автоматизація може витіснити державних службовців, викликаючи безробіття та напруження в органах державної влади
Залежність від технологічних постачальників	6	Залежність від постачальників може підривати сам процес інтеграції ІІІ та в певній мірі його уповільнювати
Опір змінам і низька цифрова грамотність	5	Частина державних службовців і громадян не готові користуватися новими технологіями, так як в них недостатньо знань та навичок для оволодіння технологіями

Джерело: [4-5]

Отже, проведена оцінка показала, що найбільший вплив на впровадження ІІІ у публічному управлінні мають кіберзагрози та порушення конфіденційності даних, адже вони здатні призвести до витоків інформації, маніпуляцій та підриву довіри громадян. Високими також залишаються ризики технічної недосконалості алгоритмів і відсутності чіткої правової бази, що може спричиняти помилкові рішення та створювати «сірі зони» для зловживань. Не менш важливий вплив здійснюють алгоритмічне упередження, соціальні наслідки у вигляді втрати робочих місць, а також фінансові витрати й залежність від зовнішніх постачальників, які в певній мірі і уповільнюють процеси технологічної трансформації. Найменший ризик становлять опір змінам та низька цифрова грамотність, які радше уповільнюють інтеграцію технологій, ніж блокують її. Для більш кращої візуалізації основних ризиків та їхнього впливу на процеси

цифровізації в державному управлінні пропонується навести багатокутних ризиків (рис. 2).



Рисунок 2. Багатокутних ризиків впровадження ІІІ в сферу публічного управління.
Джерело: зроблено автором

Як видно з рисунку, попри те, що цифрова трансформація державного управління піддається впливу різноманітних ризиків та етичних викликів, приклади успішного застосування штучного інтелекту в цій сфері доводять, що технологія може стати потужним інструментом на благо суспільства, яка працюватиме від прогнозування попиту на соціальні послуги до виявлення корупційних схем чи оптимізації використання бюджетних ресурсів.

Підсумовуючи все вищезазначене, підкреслимо, що кожен крок упровадження ІІІ повинен супроводжуватися оцінкою ризиків, етичних норм, впровадженням стандартів прозорості та механізмів захисту прав людини. Лише за умови забезпечення людиноцентричності технологій, поваги до приватності та справедливості рішень, сфера публічного управління зможе зберегти довіру суспільства і водночас використати потенціал штучного інтелекту для спрощення своєї роботи та суспільного розвитку.

Список використаних джерел

1. MediaSapiens. (2025). В Україні запрацювала перша держпослуга з підтримкою ІІІ. Detector Media. URL: <https://ms.detector.media/internet/post/38329/2025-08-19-v-ukraini-zapratsyuvava-persha-derzhposluga-z-pidtrymkoju-shi> (дата звернення 04.11.2025)
2. AI 360 Ukraine. (2025). Мінцифри презентувала посібник зі штучного інтелекту для публічних службовців. URL: <https://ai360.com.ua/mintsyfyry->

prezentovala-posibnyk-zi-shtuchoho-intelektu-dlia-publichnykh-sluzhbovtiv (дата звернення 04.11.2025)

3. Яровой Т. С. Возможности та риски использования штучного интеллекта в публичному управлінні. *Economic Synergy*, (2[8]), 36–46., 2023. URL: <https://doi.org/10.53920/ES-2023-2-3> (дата звернення 30.09.2025)

4. Кравчук О.Ю. Штучний інтелект у фокусі стратегічного планування публічного управління. *Суспільство і національні інтереси*. № 4(4), 2024.

5. Кравчук О. Ю. Забезпечення етичних стандартів та безпеки використання штучного інтелекту у публічному управлінні. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Публічне управління та адміністрування*, (4), стаття 13., 2024 URL: <https://doi.org/10.32782/TNU-2663-6468/2024.4/13> (дата звернення 30.09.2025)

ПЕРСОНАЛІЗОВАНА РЕКЛАМА В СОЦІАЛЬНИХ МЕРЕЖАХ: ВПЛИВ РЕЛЕВАНТНОСТІ ТА АЛГОРИТМІЧНИХ РЕКОМЕНДАЦІЙ НА ПОВЕДІНКУ СПОЖИВАЧІВ ПОКОЛІННЯ Z

Литвишко Лілія

к.е.н., доцент

Купрієнко Олексій

здобувач вищої освіти бакалаврського рівня

Кафедра менеджменту

Національний транспортний університет, Україна

Персоналізована реклама в соціальних мережах поступово перетворюється на ключовий інструмент комунікації між бізнесом та молодіжними сегментами споживачів, зокрема представниками покоління Z, для яких цифровий простір є основним середовищем соціальної взаємодії, навчання та споживання контенту [1; 9]. Активне впровадження алгоритмічних систем рекомендацій, заснованих на аналізі поведінки користувачів, дозволило компаніям істотно підвищити точність рекламних звернень, однак одночасно супроводжувалося зростанням вимог користувачів до якості, коректності та релевантності рекламних повідомлень [2; 3]. У цифровому середовищі, де рівень інформаційного навантаження є рекордно високим, релевантність рекламного контенту перетворюється на визначальний чинник конкуренції за увагу, а персоналізація - на механізм, що здатен не лише привернути увагу, але й сформував первинний інтерес до товару чи послуги [4].

Покоління Z характеризується високою обізнаністю щодо роботи цифрових платформ, швидкістю сприйняття інформації, схильністю до візуальних форматів і очікуванням моментальної реакції онлайн-сервісів [5; 6].