УДК 351.72:004.8:004.056

А. В. Кузьменко,
аспірант, ДЗВО "Університет менеджменту освіти" НАПН України
ORCID ID: https://orcid.org/0009-0000-4159-355X

DOI: 10.32702/2306-6814.2025.22.344

СТРАТЕГІЯ ІНТЕГРАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРУ ПУБЛІЧНИХ ВІДНОСИН ЯК УМОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

A. Kuzmenko,
Postgraduate Student, State Educational Institution "University
of Educational Management" of the National Academy of Sciences of Ukraine

STRATEGY FOR INTEGRATION OF ARTIFICIAL INTELLIGENCE INTO THE SPHERE OF PUBLIC RELATIONS AS A CONDITION FOR INFORMATION SECURITY IN UKRAINE

Перехід до цифрового уряду та ухвалення Європейським Парламентом Акта про штучний інтелект (EU AI Act) актуалізує необхідність формування національної стратегії інтеграції Штучного Інтелекту (ШІ) в Україні. Наявна "Концепція розвитку штучного інтелекту в Україні" закладає основи, але не містить чіткої "дорожньої карти" та механізмів, які б безпосередньо пов'язували впровадження ШІ з посиленням інформаційної безпеки (ІБ). Існують значні прогалини у сфері комплексної стратегії, міжвідомчої координації та управління ризиками ШІ у критичній інфраструктурі, а також у правовому визначенні відповідальності за дії автономних систем. Метою статті є обгрунтування стратегії інтеграції ШІ у сферу публічних відносин як ключової умови інформаційної безпеки України.

У роботі застосовано порівняльно-правовий аналіз європейського та національного регулювання, а також метод моделювання для розробки структури допуску ШІ до даних.

Досліджено необхідність імплементації положень EU AI Act в українське законодавство, як це передбачено "дорожньою картою" Міністерства цифрової трансформації. Встановлено, що чинне законодавство, зокрема Постанова КМУ № 1137 щодо порталу "Дія", не передбачає правосуб'єктності або правового режиму для ШІ, що ускладнює його адаптацію.

Розроблено авторську ієрархію трьох рівнів допуску ШІ до інформації при здійсненні контрольно-наглядової діяльності, залежно від потенційних правових наслідків для суспільства:

— Базовий рівень (камеральні перевірки, відкриті джерела).

— Просунутий рівень (виїзні перевірки, інформація на запит з верифікацією людини).

— Предиктивний рівень (аналіз тяжких злочинів, автоматичний запит до закритих баз без участі людини). Ця модель пропонує алгоритм передачі справ людині-ініціатору перевірки у разі виявлення суттєвого впливу на суспільство, забезпечуючи конфіденційність, неупередженість та прозорість діяльності ШІ.

Запропоновано низку регуляторних заходів для посилення ІБ та запобігання "зливу персональних даних":

— Введення оборотних штрафів (6-10% від виручки) та механізму дискваліфікації для посадових осіб за правопорушення у сфері обробки даних.

— Створення "другого контуру безпеки" в особі ШІ, який виявлятиме помилки в алгоритмах, закладених органами публічного управління.

— Введення спеціального реєстру рівня готовності технології ШІ для оперативного перегляду законодавства.

На середньостроковому етапі обгрунтовано необхідність надання особам, що використовують ШІ, відповідного правового статусу (наприклад, "електронна особа"). Пропонується диференційований підхід до визначення розміру статутного капіталу для розробників ШІ залежно від їхньої афілійованості (великий бізнес, наукові установи, стартапи), що дозволить збалансовано захистити інтереси всіх учасників.

Стаття формує стійку конструкцію функціонування ОПУ з урахуванням ШІ на короткостроковий період. Обгрунтовано, що інтеграція ШІ в ПУ потребує не просто технологічного впровадження, а цілісної стратегії з адаптацією правового поля, введенням механізмів відповідальності, контролю доступу до даних та прозорості алгоритмів. Внесені пропозиції спрямовані на створення сприятливих правових умов для розвитку технології ШІ в Україні, одночасно підвищуючи рівень її кіберстійкості та інформаційної безпеки.

The transition to digital government and the adoption of the EU AI Act by the European Parliament have highlighted the need to develop a national strategy for integrating Artificial Intelligence (AI) in Ukraine. The existing "Concept for the Development of Artificial Intelligence in Ukraine" lays the foundations, but does not contain a clear "roadmap" and mechanisms that would directly link the implementation of AI with the strengthening of information security (IS). There are significant gaps in the area of a comprehensive strategy, interagency coordination and risk management of AI in critical infrastructure, as well as in the legal definition of responsibility for the actions of autonomous systems. The aim of the article is to substantiate the strategy for integrating AI into the sphere of public relations as a key condition for the information security of Ukraine.

The paper uses a comparative legal analysis of European and national regulation, as well as a modeling method to develop a structure for AI access to data.

The need to implement the provisions of the EU AI Act into Ukrainian legislation was studied, as provided for in the "roadmap" of the Ministry of Digital Transformation. It was found that the current legislation, in particular the Resolution of the Cabinet of Ministers No. 1137 on the "Diya" portal, does not provide for legal personality or a legal regime for AI, which complicates its adaptation.

An author's hierarchy of three levels of AI access to information when carrying out control and supervisory activities was developed, depending on the potential legal consequences for society:

— Basic level (cameral inspections, open sources).

— Advanced level (field inspections, information upon request with human verification).

— Predictive level (analysis of serious crimes, automatic query to closed databases without human participation). This model offers an algorithm for transferring cases to a human initiator of the inspection in case of a significant impact on society, ensuring confidentiality, impartiality and transparency of AI activities.

A number of regulatory measures are proposed to strengthen IS and prevent the "drain of personal data":

— Introduction of revolving fines (6—10% of revenue) and a disqualification mechanism for officials for data processing offenses.

— Creation of a "second security loop" in the person of AI, which will detect errors in algorithms established by public administration bodies.

— Introduction of a special register of the level of readiness of AI technology for prompt revision of legislation.

At the medium-term stage, the need to provide persons using AI with an appropriate legal status (for example, an "electronic person") is substantiated. A differentiated approach is proposed to determine the size of the authorized capital for AI developers depending on their affiliation (big business, scientific institutions, startups), which will allow for balanced protection of the interests of all participants.

The article forms a sustainable design of the functioning of the OPU taking into account AI for the short-term period. It is substantiated that the integration of AI in the PU requires not just technological implementation, but a holistic strategy with the adaptation of the legal framework, the introduction of liability mechanisms, control of data access and transparency of algorithms. The proposals are aimed at creating favorable legal conditions for the development of AI technology in Ukraine, while simultaneously increasing the level of its cyber resilience and information security.

Ключові слова: Штучний інтелект (ШІ), інформаційна безпека, публічні відносини, кібербезпека, стратегія інтеграції, Україна, EU AI Act, цифрова трансформація, кіберстійкість, державні дані, алгоритмічна упередженість, управління ризиками, допуск до даних, контрольно-наглядова діяльність, електронний уряд, європейське регулювання, відповідальність ШІ, кадрова політика, Big Data, нормативно-правове регулювання.

Key words: Artificial Intelligence (AI), information security, public relations, cybersecurity, integration strategy, Ukraine, EU AI Act, digital transformation, cyber resilience, state data, algorithmic bias, risk management, data access, control and supervision, e-government, European regulation, AI responsibility, personnel policy, Big Data, regulatory and legal regulation.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Європейським парламентом 13 березня 2024 року ухвалений Акт про штучний інтелект, який забезпечує інформаційну безпеку при застосуванні штучного інтелекту (ШІ) [1].

В Україні затверджено Концепцію розвитку штучного інтелекту в Україні [2]. Необхідно реалізувати базову ініціатива про необхідність розвитку технології ШІ щодо розробки стратегії розвитку технологій у галузі ШІ. Зазначена концепція визначає основні підходи до стимулювання розвитку технології ШІ в Україні, необхідні принципи, показники для подальшого опрацювання Урядом України (створення робочих місць, створення умов для залучення фахівців, розвиток корпоративної науки тощо). При цьому у якості основних показників пропонується закріпити збільшення кількості організацій, що розробляють ШІ, а також збільшення кількості зареєстрованих результатів інтелектуальної діяльності в галузі ШІ. Також концепція містить завдання, принципи, загальногалузеві завдання регулювання ШІ тощо.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Значна частина публікацій (Дж. Мічелл, Д. Веллер, І. С. Сливка) підкреслює, що ШІ може суттєво підвищити ефективність надання публічних послуг, прозорість рішень та швидкість обробки великих масивів даних (Big Data), що є критичним для сучасного "електронного уряду". Інші науковці (О. В. Кушнір, С. М. Євдокимова) наголошують на соціально-етичних та правових проблемах. Йдеться про алгоритмічну упередженість (bias), що може призводити до дискримінації, прозорість процесу прийняття рішень (концепція "пояснюваного ШІ" — Explainable AI, XAI) та відповідальність за помилки, допущені автономними системами.

В Україні (праці О. М. Спіріна, В. М. Мадзигона) активно вивчається питання готовності інституцій ПУ до інтеграції ШІ, яка поки що перебуває на початковій стадії порівняно з країнами-лідерами (США, ЄС, Китай).

Існує недостатність досліджень, які комплексно оцінюють вплив інтеграції ШІ у ПУ на загальний периметр кіберзахисту держави. Це створює нові вектори атак через системи ШІ, які керують критичними державними процесами.

Таким чином, нормативно-правові та технологічні аспекти ШІ та ІБ є глибоко розробленими, але дослідження демонструють істотну прогалину у сфері комплексної стратегії. Недостатньо вивченим залишається питання стратегічної інтеграції ШІ саме як гаранта інформаційної безпеки України, а не просто як технологічного інструменту чи нової загрози. Це стосується механізмів міжвідомчої координації, управління ризиками ШІ у критичній інфраструктурі та формування кадрового потенціалу. Ці нерозв'я-

зані проблеми та відсутність цілісної стратегії визначають актуальність подальшого дослідження.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є обгрунтування стратегії інтеграції штучного інтелекту у сферу публічних відносин як умова інформаційної безпеки україни.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Міністерство цифрової трансформації презентувало дорожню карту з регулювання ШІ [3]. Розвиваючи питання, присвячене регулюванню ШІ в Україні та формуванню базових підходів до подальшого впровадження у сферу публічних правовідносин, необхідно відзначити дорожню карту з регулювання ШІ [3]. У межах зазначеного документа має відбутися імплементація (повна або поступова) Закону ЄС про ШІ (EU AI Act) [1].

Ми розглянемо правові конструкції застосування ШІ при рівні низького рівня готовності технології ШІ у розрізі функціональних сегментів застосування. Слід розуміти, що зазначений механізм оцінки рівня готовності в України законодавчо не закріплений і, ймовірно, вимагатиме додаткових інструментів фіксації в правовому полі для можливості оперативного визначення необхідності перегляду законодавства з урахуванням рівня готовності технології та його впливу на суспільні відносини.

Поточні підходи до нормативно-правового регулювання ШІ спираються на досвід зарубіжних країн, а також на чинні правові інструменти, які закріплені законодавчо для суміжних ринків технології ШІ. Ключовим джерелом даних у рамках функціонування ШІ є допуск до інформаційних послуг держави. Одним із центральних сервісів для виконання публічних завдань, закладених у парадигмі електронного уряду, є сайт "Дія" [4]. Оператором даної системи виступає Міністерство цифрової трансформації України, яке здійснює публікацію відомостей про державні послуги, розробляє методичні вимоги до порталу, надає доступ функціонування, дотримання вимог законодавства в галузі захисту інформації тощо, а органи влади в рамках своєї компетенції повинні визначити коло послуг, можливих до розміщення на даному порталі, та забезпечити належне їх виконання в рамках процесуальних термінів (з урахуванням призначення відповідальних осіб, їх підключення до системи та одержання електронно-цифрових послуг).

Але виникає питання про адаптивність поточного регулювання до впровадження штучного інтелекту, як у оператора послуги, так і органів влади, що надають послуги. Постанова Кабінету Міністрів України "Питання Єдиного державного вебпорталу електронних послуг та Реєстру адміністративних послуг" від 4 грудня 2019 р. № 1137 [5] не передбачає окремої правосуб'єктності чи правового режиму щодо ШІ у сфері публічних правовідносин. В рамках діяльності контрольно-наглядових органів дії щодо підконтрольного суб'єкта вимагають дотримання як регламентуючих процедур, так і внутрішньовідомчих регламентів та положень, що проходять відповідну процедуру узгодження та подальшого затвердження в Мін'юсті України.

Однак, якщо ми говоримо про ШІ, то він у своїй діяльності може використовувати як доказову базу відомості, які можуть бути інтерпретовані як порушуючі базові принципи та цінності, затверджені в Конституції України. Якщо ми говоримо про регламентацію процедури проведення будь-яких перевірочних заходів, ми розуміємо, що чим прозоріше та простіше описана процедура, тим нижчим є ризик двоякого тлумачення дій представників органів публічного управління. Однак якщо ми говоримо про ШІ, дана алгоритмізація вимагає встановлення рівнів допуску до баз даних для аналізу в залежності від предмета потенційного правопорушення.

Пропонується наступна ієрархія допустимих рівнів допуску для ШІ при здійсненні контрольно-наглядової діяльності та подання доказової бази для визначення відповідальних при скоєнні того чи іншого адміністративного правопорушення:

1. Базовий рівень (проведення камеральних перевірок із незначним рівнем правових наслідків для суспільства):

— інформація, отримана за відкритими джерелами даних, які не викликають сумніву в їх достовірності, та надана у спільне користування самим громадянином (наприклад, біографія керівника органу влади, опублікована на сторінці органу влади);

— внутрішні бази даних органу влади, який представляє ШІ. Цей підхід націлений на мінімізацію ризиків переслідування людини чи юридичної особи поза компетенцією органу влади.

2. Просунутий рівень (проведення камеральних та виїзних перевірок зі значним рівнем правових наслідків для суспільства (потенційне поєднання адміністративної та кримінальної відповідальності малої та середньої тяжкості):

— інформація, отримана на запит ШІ в органу влади або оператора даних; цей пункт вимагає обов'язкової верифікації у представника органу влади — людини;

— аналіз інформації, яка надана учасниками адміністративного процесу, та приймається технологією ШІ за підписаною угодою про передачу цієї інформації на адресу ШІ або за сформованим описом, який підписав представник органу влади, який здійснює контрольно-наглядові функції.

3. Предиктивний рівень (проведення аналізу щодо потенційних правопорушень, що тягне за собою гарантоване притягнення до адміністративної та кримінальної відповідальності з тяжких та особливо тяжких злочинів):

— робиться автоматичний запит до систем держпослуги, закритих баз даних без участі людини, представника органу влади;

— проводиться збір інформації з усіх можливих відкритих джерел інформації.

У рамках першого пункту допуску ШІ ми розуміємо, що дана робота має бути спрямована на виконання рутинної частини роботи з мінімальними правовими наслідками для органу влади та суб'єкта нагляду.

У рамках другого пункту допуску ШІ ми потенційно маємо або звернення громадянина (юридичної особи), чиї законні права та інтереси були порушені та потребують предметного розгляду органу влади, або ініційовано відповідну процедуру перевірки іншими органами влади (за винятком внутрішньої ініціації держорганом).

У рамках третього пункту допуску ШІ ми потенційно маємо транскордонне питання, яке тягне задіяність кількох органів влади або принципову небезпеку дії, що впливає на інтереси країни.

Слід зазначити, що як тільки ШІ профільного відомства виявляє, що зазначена справа має більш суттєвий характер впливу на суспільство, то зазначена справа передається за підвідомчістю до профільного відомства з напрацюваннями, зробленими раніше, з погодженням профільної посадової особи — ініціатора процедури перевірки.

Базовими принципами для всіх трьох рівнів допуску до інформації є конфіденційність, неупередженість, об'єктивність та прозорість ШІ.

У контексті конфіденційності слід зазначити, що ризик "зливу персональних даних" носить систематичний характер і потребує відповідних ініціатив та заходів з боку органів влади. Рекомендується розглянути внесення поправок у Кодекс України про адміністративні правопорушення, розширивши санкційну частину статей, на запровадження оборотних штрафів. При цьому, враховуючи досвід ЄС, як прийнятний діапазон рекомендується визначити 6—10% від сукупної виручки юридичної особи. Крім того, стосовно посадової особи, яка допустила зазначене правопорушення, рекомендується передбачити запровадження механізму дискваліфікації, розширивши її застосування на діяльність, пов'язану збиранням обробкою даних ШІ.

У частині неупередженості та об'єктивності винесення рішення рекомендується розробка на рівні Уряду України Постанови, яка зобов'яже органи публічного управління впровадити "другий" контур безпеки в особі ШІ; обов'язків, або виявляти помилки під час здійснення алгоритмів виконання закону, закладених у регламентуючих органах публічного управління. В рамках забезпечення прозорості діяльності ШІ необхідно враховувати ступінь готовності розкриття відповідної інформації перед заявником та (або) піднаглядовим суб'єктом. фіксацією обов'язки про нерозголошення шляхом підписання ЕЦП.

Крім того, сама процедура розробки ШІ для публічних цілей повинна перебувати в полі наукових організацій або державних організацій (якщо ми говоримо про сервіси для публічних потреб). Даний механізм убезпечить ШІ від зовнішнього впливу. Слід також відзначити необхідність введення спеціального реєстру рівня готовності технології ШІ в публічній та непублічній сфері. зафіксувати лише на рівні Постанови Уряду України, сформулювавши базові правові визначення рівня готовності технології та умов їх застосування всіма відомствами, на відміну локальних ініціатив у виконанні державних цільових програм.

В рамках описаного алгоритму нами потенційно сформовано стійку конструкцію функціонування органів публічного управління та громадськості з урахуванням розвитку та впровадження технології ШІ на короткостроковий період до 2030 року.

Варто врахувати, що потребує подальше регулювання на середньо та довгостроковий період.

Потребує адаптації нормативне регулювання в частині, що стосується взаємодії людини зі штучним інтелектом, та вироблення відповідних етичних норм. У контексті правових підходів нами розроблено авторську модель та порядок її адаптації під діючу правову конструкцію в Україні з урахуванням світового досвіду, представленого раніше, а в частині етичних норм запропоновані підходи будуть розглянуті надалі. При цьому нам важливим відзначити відсутність необхідності надмірного регулювання, яке потенційно може уповільнити розвиток технології.

У результаті формування правового середовища передбачається розвиток сприятливих правових умов для доступу до даних (з урахуванням можливості їх знеособлення), створення єдиних систем стандартизації тощо.

На середньостроковому етапі особи, які використовують технології ШІ, набули відповідного правового статусу та збалансованого підходу до визначення як електронної особи. Дане визначення закріплено в європейському законодавстві [7], а базові контури регулювання самого ринку ШІ формуються вже на рівні окремої законодавчої бази, як це робиться для фінансового ринку, ринку аудиторських послуг, нотаріальних послуг тощо.

На даному етапі для різних учасників ринку потенційно встановлюються різні параметри за розміром статутного капіталу з урахуванням самого ринку, а також кінцевої афілійованості технології ШІ (до великого бізнесу, фундаментальної науки або стартап ініціативи). Цей збалансований підхід, визначений у перспективному законі, дає можливість оперативно захищати як інтереси всіх учасників суспільних відносин.

Нами пропонується, щоб статутний капітал для великих учасників ринку, які виступають розробниками, користувачами, продавцями та іншими особами, які беруть участь у функціонуванні та застосуванні ШІ, становив до 10% виручки компанії за звітний період у розрізі профільного ринку та рекомендацій, представлених профільними органами публічного управління.

У контексті формування організацій, що займаються розробками ШІ в рамках фундаментальної науки, а також для потреб публічної сфери статутний капітал компаній, що займаються цим при наукових установах (державних), повинен керуватися розміром гранту, державних цільових програм або іншої форми надання коштів, що виділяються науковою організацією для потреб розробки та подальшого розвитку ШІ. Залежно від сегмента застосування ШІ можливо визначити рівень відповідальності наукової організації за результат у розмірі 50% від виділеного фінансування.

ВИСНОВКИ

У контексті стартап-підприємств, які ініціативно розробляють технології ШІ, рекомендується:

— при створенні або перереєстрації зазначеного типу осіб обов'язково надавати бізнес-план особи, з визначенням потенційної частки ринку, яку планує зайняти особу;

— виходячи з прогнозованої частки ринку, визначити потенційний розмір виручки на горизонт 3—5 років та з неї виділити незнижуваний розмір статутного та додаткового капіталу, який щорічно переглядатиметься виходячи з виконання бізнес-плану;

— сам моніторинг виконання цього бізнес-плану покласти на створену організацію.

Література:

1. The EU Artificial Intelligence Act adopted on 13 March 2024 by the European Parliament. URL: https://artificialintelligenceact.eu/ (Дата звернення: 05.11.2025).

2. Розпорядження Кабінету Міністрів України "Про схвалення Концепції розвитку штучного інтелекту в Україні" від 2 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (Дата звернення: 05.11.2025).

3. Міністерство цифрової трансформації України. Дорожня карта з регулювання штучного інтелекту в Україні. Bottom-Up Підхід. URL: https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs_compressed.pdf (Дата звернення: 05.11.2025).

4. Дія (сайт) 2025. Державні послуги онлайн. URL: https://diia.gov.ua/ (Дата звернення: 05.11.2025).

5. Постанова Кабінету Міністрів України "Питання Єдиного державного вебпорталу електронних послуг та Реєстру адміністративних послуг" від 4 грудня 2019 р. № 1137. URL: https://zakon.rada.gov.ua/laws/show/1137-2019-%D0%BF#Text (Дата звернення: 05.11.2025).

6. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (Дата звернення: 05.11.2025).

7. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103 (INL). URL: https://www.europarl.europa.eu/doceo/ document/TA-8-2017-0051_EN.html (Дата звернення: 05.11.2025).

References:

1. European Parliament (2024), "The EU Artificial Intelligence Act", available at: https://artificialintelligenceact.eu/ (Accessed 05 November 2025).

8. Cabinet of Ministers of Ukraine (2020), Order "On the approval of the Concept for the Development of Artificial Intelligence in Ukraine", available at: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (Accessed 05 November 2025).

9. Ministry of Digital Transformation of Ukraine (2025), "Roadmap for AI Regulation in Ukraine: Bottom-Up Approach", available at: https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs_compressed.pdf (Accessed 05 November 2025).

10. Diia (2025), "Official website of the online government services portal", available at: https://diia.gov.ua/ (Accessed 05 November 2025).

11. Cabinet of Ministers of Ukraine (2019), Resolution "Issues of the Unified State Web Portal of Electronic Services and the Register of Administrative Services", available at: https://zakon.rada.gov.ua/laws/show/1137-2019-%D0%BF#Text (Accessed 05 November 2025).

12. Verkhovna Rada of Ukraine (1984), "Code of Ukraine on Administrative Offences", available at: https://zakon.rada.gov.ua/laws/show/80731-10#Text (Accessed 05 November 2025).

13. European Parliament (2017), "Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))", available at: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (Accessed 05 November 2025).

Стаття надійшла до редакції 05.11.2025 р.