Проблеми правового регулювання безпеки використання штучного інтелекту у системі публічного управління

Ярема Оксана Григорівна[1]
Шопіна Ірина Миколаївна [2]

Опубліковано	Секція	УДК
30.01.2026	Право	342.9

DOI: https://doi.org/10.5281/zenodo.20714978

Анотація. Мета статті полягала у тому, щоб охарактеризувати проблеми правового регулювання безпеки використання штучного інтелекту у системі публічного управління. Завдання статті полягають у тому, щоб проаналізувати сучасні підходи до правового регулювання використання штучного інтелекту в діяльності органів публічної влади; визначити основні ризики та загрози інформаційній безпеці, що виникають у процесі застосування технологій штучного інтелекту в управлінській діяльності; окреслити проблемні аспекти забезпечення інформаційної безпеки при використанні таких технологій.

У процесі дослідження використано комплекс загальнонаукових і спеціально-юридичних методів. Зокрема, застосовано діалектичний, системний, формально-юридичний, структурно-функціональний та інші методи наукового пізнання, що дозволило проаналізувати чинне законодавство України, акти Європейського Союзу, а також виявити прогалини та суперечності у правовому забезпеченні досліджуваної сфери.

У статті встановлено, що швидкий розвиток технологій штучного інтелекту випереджає формування належного нормативно-правового забезпечення, що ускладнює ефективне регулювання їх використання у сфері публічного управління. Проаналізовано сучасні підходи до правового регулювання штучного інтелекту, зокрема положення актів Європейського Союзу та стратегічних документів України у сфері цифрової трансформації та інформаційної безпеки. З'ясовано, що існуючі механізми державного контролю за використанням систем штучного інтелекту в системі публічного управління мають фрагментарний характер і потребують подальшого розвитку. Визначено, що безконтрольне та не обмежене відповідно до існуючих ризиків використання ШІ у системі публічної влади може утворювати загрози національній, інформаційній та воєнній безпеці. Такі загрози обумовлені трьома основними факторами: 1) можливістю прийняття помилкового управлінського рішення, базованого на помилкових результатах застосування інструментів ШІ (т. зв. галюцинацій або марення ШІ); 2) несанкціонованим витоком відомостей та даних, які

[1] кандидат юридичних наук, доцент, в.о. завідувача кафедри адміністративно-правових дисциплін навчально-наукового інституту права та правоохоронної діяльності Львівського державного університету внутрішніх справ, https://orcid.org/ 0000-0003-3550-0454
[2] доктор юридичних наук, професор, професор кафедри адміністративно-правових дисциплін навчально-наукового інституту права та правоохоронної діяльності Львівського державного університету внутрішніх справ, https://orcid.org/0000-0003-3334-7548

можуть бути використані державою-агресором; 3) поступовою депрофесіоналізацією публічних службовців внаслідок систематичного застосування інструментів ШІ для збору даних, аналітичної діяльності, створення прогнозів, планування тощо.

Ключові слова: штучний інтелект, інформаційні технології, інформаційна безпека, кібербезпека, органи публічної влади, публічне управління, органи виконавчої влади.

Legal Challenges of Regulating the Secure Use of Artificial Intelligence in Public Administration

Annotation. The article aims to characterize the legal challenges surrounding the secure integration of artificial intelligence (AI) within the public administration system. To achieve this, the study seeks to analyze contemporary legal frameworks for the use of AI within public authorities, identify the primary information security risks and threats emerging from its application in governance, and outline the critical challenges of ensuring information security when implementing such technologies.

The study employs a comprehensive suite of general scientific and specialized legal methodologies. Specifically, the use of dialectical, systemic, formal-legal, and structural-functional methods enabled a rigorous analysis of current Ukrainian legislation and European Union frameworks. This approach facilitated the identification of critical gaps and inconsistencies within the existing legal safeguards of the field under study.

The findings indicate that the rapid evolution of AI technologies consistently outpaces the development of robust regulatory frameworks, thereby hindering effective oversight within public governance. The paper analyzes contemporary legal approaches to AI regulation, with a particular focus on EU legislative acts and Ukraine's strategic documents regarding digital transformation and information security. The study reveals that current state control mechanisms for AI systems in public administration remain fragmented and require further development. It is argued that the unregulated use of AI within public authorities, lacking risk-based constraints, poses significant threats to national, informational, and military security. These threats are attributed to three primary factors: 1) the risk of flawed administrative decision-making based on inaccurate AI outputs (so-called "AI hallucinations"); 2) the potential for unauthorized data leaks that could be exploited by an aggressor state; and 3) the gradual deprofessionalization of public servants resulting from over-reliance on AI tools for data collection, analytics, forecasting, and strategic planning.

Keywords: artificial intelligence, information technology, information security, cybersecurity, public authorities, public administration, executive bodies.

Вступ

Широке впровадження технологій штучного інтелекту (далі – ШІ) у всі сфери людської діяльності поставило на порядок денний питання про необхідність регламентації суспільних відносин, що виникають під час використання вказаних технологій. При цьому, як відомо, суспільні відносини можуть регулюватися різними соціальними нормами – моральними, релігійними, сімейними, правовими, корпоративними тощо. Належність того чи іншого об'єкта соціального регулювання до певної галузі завжди викликає потребу у дискусіях і тлумаченнях. Не є винятком і технології ШІ – останнім часом у суспільстві та серед експертів розгорнулися активні дискусії щодо меж його регулювання.

Так, Е. Д. Мітчелл, Д. Лет та Л. Тан з'ясували, що ШІ стрімко розвивається з середини 20-го століття. Сьогодні ШІ впроваджується в багато аспектів нашого повсякденного життя та стає все більш повсюдним. Водночас, занепокоєння щодо ШІ, включаючи дискримінацію, конфіденційність та безпеку, спонукали до закликів до посилення регулювання. З цією метою регуляторні органи можуть звертатися за доступом до вихідного коду ШІ (програми, яку може читати людина). Однак багато торговельних угод містять положення, що забороняють розкриття вихідного коду як умову доступу до ринку у відповідних країнах.

Автори детально розглядають суперечність між регулюванням ШІ та цими положеннями [1]. А. Тейхакх обґрунтовує, що швидкий розвиток ШІ та посилення його впровадження в таких сферах, як автономні транспортні засоби, системи летальної зброї, робототехніка тощо, створюють серйозні виклики для урядів, оскільки вони повинні керувати масштабами та швидкістю соціально-технічних переходів, що відбуваються. Хоча з'являється значна кількість літератури про різні аспекти ШІ, управління ШІ є значною мірою недостатньо розвиненою галуззю. Нові застосування ШІ пропонують можливості для підвищення економічної ефективності та якості життя, але вони також породжують неочікувані та непередбачувані наслідки та створюють нові форми ризиків, які необхідно вирішити. Щоб збільшити переваги ШІ, мінімізуючи водночас негативні ризики, урядам у всьому світі необхідно краще розуміти масштаби та глибину ризиків, що виникають, та розробляти регуляторні та управлінські процеси та структури для вирішення цих викликів [2]. Т. Давтян всебічно аналізує підхід США до управління ШІ і робить висновок, що, на відміну від Акту Європейського Союзу про ШІ, який забезпечує юридично обов'язкову базу, США застосовують децентралізовану, галузеву стратегію регулювання, яка в основному ґрунтується на добровільних зобов'язаннях приватних компаній та керується федеральними агентствами. Крім того, ініціативи на рівні штатів, часто під впливом конкретних місцевих проблем, сприяють різноманітному регуляторному середовищу. Автор розглядає федеральні законодавчі та виконавчі ініціативи, нормативні акти агентств та участь галузі, висвітлюючи проблеми, які цей фрагментований підхід створює для досягнення єдності та вирішення критичних питань, таких як конфіденційність, безпека та підзвітність [3]. Ці та інші роботи науковців свідчать, що визначення меж та критеріїв регулювання ШІ потребує виваженого підходу, що базується на аналізі національних законодавств, міжнародного правового регулювання та правозастосовної практики. Вказане обумовлює актуальність цієї статті.

Мета статті – охарактеризувати проблеми правового регулювання безпеки використання штучного інтелекту у системі публічного управління.

Завдання статті: Завдання статті полягають у тому, щоб проаналізувати сучасні підходи до правового регулювання використання штучного інтелекту в діяльності органів публічної влади; визначити основні ризики та загрози інформаційній безпеці, що виникають у процесі застосування технологій штучного інтелекту в управлінській діяльності; окреслити проблемні аспекти забезпечення інформаційної безпеки при використанні таких технологій.

Методологічну основу статті становить поєднання загальнонаукових та спеціально-юридичних методів пізнання, що дозволяють комплексно дослідити проблеми правового регулювання використання технологій ШІ у системі публічного управління. Застосовано діалектичний метод для аналізу сучасних тенденцій розвитку правового регулювання ШІ та виявлення суперечностей між технологічним розвитком і нормативним забезпеченням діяльності органів публічної влади. За допомогою системного методу досліджено взаємозв’язок правових, організаційних та інформаційно-безпекових аспектів використання ШІ у діяльності державних інституцій. Формально-юридичний метод використано для аналізу положень національного законодавства України, стратегічних документів державної політики у сфері ШІ, а також міжнародних актів і рекомендаційних документів, зокрема підходів Європейського Союзу. Логіко-юридичний і структурно-функціональний методи використано для уточнення понятійно-категоріального апарату дослідження, визначення ролі ШІ у процесах прийняття управлінських рішень та обґрунтування напрямів удосконалення нормативно-правового регулювання у відповідній сфері.

Результати

Особливістю інформаційного права є його комплексний характер, що обумовлює поєднання в ньому норм публічного та приватного права. Слід також згадати про тісний

зв'язок цієї галузі права зі сферою інформаційних технологій, з якої інформаційне право активно запозичує термінологію та деякі алгоритми. Сукупність цих факторів обумовлює складнощі у розвитку інформаційного законодавства, оскільки відмінності цієї галузі потребують розгляду будь-яких новацій як з правової, так і з технічної та технологічної позицій.

Феномен ШІ стрімко увійшов у соціальні відносини багатьох держав світу. Як і в багатьох інших сферах правового регулювання, безпосередній розвиток інформаційних технологій та їх освоєння користувачами значно випередили розвиток відповідного правового регулювання. Проривом у цій сфері став Artificial Intelligence Act – Регламент (ЄС) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року, що встановлює гармонізовані правила щодо штучного інтелекту [4]. У цьому правовому документі, зокрема, було визначено, що деякі держави-члени вже вивчили можливість прийняття національних правил, щоб забезпечити надійність та безпеку ШІ, а також його розробку та використання відповідно до зобов'язань щодо основних прав. Розбіжності в національних правилах можуть призвести до фрагментації внутрішнього ринку та знизити правову визначеність для операторів, які розробляють, імпортують або використовують системи ШІ. Тому слід забезпечити послідовний та високий рівень захисту по всьому Союзу, щоб досягти надійності ШІ, тоді як розбіжності, що перешкоджають вільному обігу, інноваціям, розгортанню та впровадженню систем ШІ та пов'язаних з ними продуктів і послуг на внутрішньому ринку, слід запобігати шляхом встановлення єдиних зобов'язань для операторів та гарантування єдиного захисту переважаючих міркувань суспільного інтересу та прав осіб на всьому внутрішньому ринку на основі статті 114 Договору про функціонування Європейського Союзу [4]. Як можна побачити, на рівні ЄС було проголошено необхідність унормування стандартів, алгоритмів та правил безпеки під час застосування ШІ. Було, зокрема, визначено системи штучного інтелекту високого ризику, до яких віднесено біометричні дані, якщо їх використання дозволено відповідним законодавством Союзу або національним законодавством (системи дистанційної біометричної ідентифікації; системи штучного інтелекту, призначені для використання в біометричній категоризації відповідно до конфіденційних або захищених атрибутів чи характеристик на основі виведення цих атрибутів чи характеристик; системи штучного інтелекту, призначені для розпізнавання емоцій). Для різних рівнів ризику було встановлено окремі запобіжники, метою впровадження яких стало запобігання шкідливим наслідкам використання ШІ [4].

Для України, як для держави, яка вже п’ятий рік потерпає від повномасштабної збройної російської агресії, забезпечення інформаційної безпеки є одним із важливих чинників збереження державного суверенітету. Інформаційний суверенітет України, на нашу думку, є здатністю держави обмежувати деструктивні інформаційні впливи на публічне управління, економіку, громадянське суспільство та інші сфери суспільних відносин, а також не допускати витоку національних відомостей та даних, які можуть бути використані противником для досягнення його політичних та військових цілей. Забезпечення інформаційного суверенітету в контексті використання технологій ШІ потребує комплексного та багаторівневого підходу. Насамперед варто врахувати, що правове регулювання використання технологій штучного інтелекту в Україні має спиратися на три взаємопов’язані складові: правову – створення гармонійної системи правового регулювання, яка визначатиме допустимі межі застосування ШІ, особливо у сферах безпеки, оборони, публічного управління та захисту персональних даних; технічну – розробку стандартів і протоколів, що забезпечуватимуть прозорість алгоритмів, їхню перевірюваність та відповідність міжнародним вимогам; організаційну – формування інституційної спроможності держави контролювати використання ШІ, включно з незалежними органами моніторингу та аудитами систем високого ризику.

У цьому контексті особливого значення набуває гармонізація українського законодавства у сфері використання ШІ. Однак ситуація у сфері правового регулювання

використання технологій ШІ в нашій державі характеризується нерівномірністю. З одного боку, Україна однією з перших держав Центрально-Східної Європи сформувала стратегічне бачення розвитку ШІ. Ключові чинники, загрози та ризики, пов'язані з технологіями ШІ знайшли своє правове закріплення у Концепції розвитку штучного інтелекту в Україні, схваленої розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. У вказаному правовому документі було проголошено, що реалізація державної політики у галузі штучного інтелекту впливатиме на ключові інтереси таких заінтересованих сторін, як громадяни, заклади освіти, суб'єкти господарської діяльності, органи виконавчої влади та місцевого самоврядування. У Концепції знайшли відображення і питання інформаційної безпеки. Так, відзначалося, що застосування технологій штучного інтелекту в забезпеченні інформаційної безпеки є одним із факторів, що сприятиме забезпеченню національних інтересів. Зокрема, моніторинг соціальних мереж та інтернет-ресурсів електронних медіа з використанням технологій штучного інтелекту дає можливість виявляти системні тренди і проблематику, діяти на випередження, аналізувати цільову аудиторію [5]. На виконання вказаного правового документа було затверджено План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021-2024 роки, відповідно до якого мали бути розроблені Концепція законопроекту про розвиток штучного інтелекту, система показників для оцінки стану інформаційної безпеки з використанням технологій штучного інтелекту, забезпечено використання технологій штучного інтелекту для проведення аналізу та оцінки, прогнозування та моделювання показників ефективності системи державного управління [6]. Однак, як і багато інших планів в сфері інформаційного забезпечення публічного управління, цей план залишився не повною мірою реалізованим. Почасти цьому сприяв початок повномасштабної російської збройної агресії, почасти – певна нереалістичність його положень та недостатність коштів для виконання його заходів. Від центральних органів виконавчої влади щодо виконання Плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021-2024 роки мала щорічно надходити інформація до Міністерства цифрової трансформації про стан виконання зазначеного плану. У свою чергу, цей орган після узагальнення вказаних заходів мав подавати її Кабінетові Міністрів України. На жаль, на офіційному вебсайті Міністерства цифрової трансформації станом на 3 березня 2026 року нам не вдалося знайти звітних документів з цього приводу. Так само не вдалося знайти звітну інформація про виконання зазначеного Плану на офіційному вебсайті Кабінету Міністрів України.

Розпорядженням від 9 травня 2025 р. № 457-р Кабінет Міністрів України затверджує новий План у досліджуваній сфері – на 2025-2026 роки. Він менший за обсягом запланованих заходів, ніж попередній, деякі його пункти дублюють положення Плану на 2021-2024 роки, але в іншій редакції. Зокрема, це стосується розроблення та подання Кабінетові Міністрів України законопроекту щодо правового врегулювання у сфері розвитку штучного інтелекту, що Міністерство цифрової трансформації має здійснити у IV кварталі 2026 року. Разом з тим, із нового Плану [7] зникли будь-які згадування про інформаційну безпеку, присутні у п.7 Плану на 2021-2024 роки [6].

Розбудова і зміцнення систем інформаційної безпеки на рівні виконавчої влади має носити цілеспрямований характер, що повинно знаходити своє відображення у програмних і планових документах, затверджених Урядом. Інакше така діяльність стає хаотичною, неефективною, утруднюється контроль та інтерпретація його результатів. На жаль, аналіз правових та організаційних передумов зміцнення інформаційної безпеки за досліджуваним напрямом не дозволяє зробити висновок про системність, цілеспрямованість та послідовність у здійсненні вказаних заходів. Проте слід позитивно відзначити деякі досягнення у галузі кібербезпеки як складової інформаційної безпеки, зокрема, виконання п. 2 Плану на 2025-2026 роки, яким передбачалося розроблення, затвердження і оприлюднення на офіційному вебсайті Адміністрації Держспецзв'язку Рекомендацій з кіберзахисту інформаційно-комунікаційних систем, які використовують технології штучного інтелекту,

затверджених наказом Адміністрації Держспецзв'язку від 23.02.2026 року № 154 [8]. Рекомендації можуть використовуватися власниками та/або розпорядниками інформаційних, електронних комунікаційних, інформаційно-комунікаційних і технологічних систем, які використовують технології штучного інтелекту, під час розробки плану кіберзахисту. Рекомендації стосуються специфічної сфери правового регулювання (кіберзахисту) і наповнені технічними термінами, розуміння яких державними службовцями органів виконавчої влади без спеціальної освіти, скоріше за все, буде викликати труднощі (перехресна валідація, федеративне навчання, комплексна видимість тощо). Однак багато положень вказаних Рекомендацій є надзвичайно корисними для побудови систем інформаційної безпеки органів виконавчої влади. Зокрема, це стосується п. 7, відповідно до якого у процесі забезпечення якості та релевантності даних власник та/або розпорядник ІКС із ШІ враховує ризики виникнення упередженості у даних та моделях ШІ включно з упередженістю, що може: бути наслідком навмисного або ненавмисного «отруєння» даних; спричиняти некоректні рішення моделей та технологій ШІ, які впливають на безпеку ІКС із ШІ; знижувати стійкість моделі ШІ та ІКС із ШІ відповідно до деструктивного впливу та загроз; створювати передумови для компрометації ІКС із ШІ через спрямовані маніпуляції набором даних; бути наслідком використання іноземних продуктів, які не є адаптованими до українських реалій [8].

Слід також відзначити наявність низки документів, підготовлених Міністерством цифрової трансформації України. Перш за все слід сказати, що вказаним центральним органом виконавчої влади підготовлено і розміщено на своєму офіційному вебсайті Дорожню карту з регулювання штучного інтелекту в Україні [9]. На жаль, у тексті цього документа відсутні відомості про його офіційне затвердження. Поряд з безумовно позитивною оцінкою намагань авторів Дорожньої карти створити модель дій для безпечного використання технологій ШІ у всіх сферах життєдіяльності держави, слід відзначити недостатньо професійний рівень підготовки цього тексту. По-перше, викликає питання назва документа, оскільки регулювати ШІ можуть його розробники, розпорядники або власники технології. На сьогоднішній день в Україні розробляються деякі інструменти ШІ, але така розробка здійснюється переважно приватними ІТ-компаніями і орієнтована здебільшого на міжнародний ринок. Головні офіси розробників найбільш відомих українських продуктів ШІ – Grammarly і People.ai знаходяться у м. Сан-Франциско (США) і здійснюють свою діяльність відповідно до норм американського законодавства. Безумовно, в Україні існують деякі власні розробки ШІ, у тому числі у військовій сфері, однак масштаб їх застосування в нашій державі є значно меншим, ніж інструментів іноземних розробників. За результатами соціологічних досліджень, найбільш часто використовуваними в Україні моделями ШІ станом на жовтень 2025 року є наступні: ChatGPT – 85%; Google Gemini – 64%; Microsoft Copilot – 20%; Midjourney – 11%; Claude – 8%; інше – 8%; DALL-E – 7%; Perplexity AI – 5%; жодна – 3% [10]. Як відомо, розробниками і власниками вказаних моделей є компанії, розташовані на території США. Отже, Україна позбавлена можливості впливати на архітектуру та алгоритми цих моделей, однак може регулювати порядок їх використання на національному рівні саме у сфері інформаційної безпеки: зокрема, регулювати поведінку користувачів технологій ШІ (наприклад, державних службовців органів виконавчої влади) або заходи інформаційної безпеки, які мають вживати розробники продуктів, які використовують можливості ШІ, тощо.

Недостатня увага до правової складової використання ШІ у Дорожній карті з регулювання штучного інтелекту в Україні притаманна й деяким положенням цього документа. Так, наприклад, простежується відхилення від усталеної юридичної лексики у формулюванні «Впровадження (на кінцевому етапі) регуляції, яка пропонує найвищий у світі рівень захисту прав людини від ризиків та злонаміреного використання ШІ» [8]. Можливо, під регуляцією мався на увазі Закон України «Про штучний інтелект», під його впровадженням на кінцевому етапі – прийняття такого закону Верховною Радою України, а

під пропонуванням найвищого в світі захисту – включення до цього правового документа норм про інформаційну безпеку, однак це скоріше припущення, і таких неконкретизованих положень у цьому документі ще багато.

Окремо слід зупинити увагу на підготовлених Міністерством цифрової трансформації України Порадах з відповідального використання штучного інтелекту публічними службовцями (розробники та особливості затвердження цього документа також не знайшли в ньому відображення). Не зважаючи на те, що термін «Поради» є дещо незвичним для українських правових документів рекомендаційного характеру, сумнівів в існуванні нагальної потреби для його розробки і широкого впровадження не виникає. Водночас, в аспекті інформаційної безпеки спостерігається наявність численних прогалин. Так, публічному службовцю, який взаємодіє із системами ШІ, рекомендується звертати увагу на політику конфіденційності сервісу до використання у взаємодії з ним персональних даних. Це пояснюється тим, що в умовах війни росії проти України особливу увагу варто приділяти країнам походження ШІ інструмента, зокрема тим, які підтримують агресію, та враховувати безпекову репутацію розробника [11]. Але, як відомо, моделі ШІ, які проголосили політику прозорості для користувача, не приховують, що їх безкоштовні версії збирають надану користувачами інформацію, у тому числі персональні дані, і використовують її для фільтрації шкідливого контенту, навчання нових моделей ШІ, а також, з використанням певного ступеня анонімізації, ця інформація може бути доступною для рецензентів. Вказане викликає питання: а чи може взагалі публічний службовець органу виконавчої влади надавати інструментам ШІ доступ до публічної інформації або персональних даних, що стали йому відомі у зв'язку з його професійною діяльністю? Щодо країни-лідера у розробці ШІ і її позиції щодо повномасштабної російської збройної агресії проти України також виникають певні питання, пов'язані із забезпеченням національної, інформаційної та воєнної безпеки.

Слід також звернути увагу на неконкретність багатьох положень Порад, що не дає змоги публічному службовцю органу виконавчої влади побудувати власну модель правомірної поведінки при використанні ШІ. З одного боку, з огляду на надання в аналізованому документі достатньої інформації щодо помилок (т.зв. галюцинацій) ШІ, певна частина користувачів, здатних до самонавчання і мотивованих до постійного професійного самовдосконалення, зможе побудувати власні стратегії поводження з ШІ (зокрема, шляхом самостійного розроблення і коректного використання промтів). Однак слід пам'ятати, що, за даними досліджень, більша частина дорослого населення світу не має мотивації до постійного самонавчання. Так, за даними звіту Організації економічного співробітництва та розвитку 2025 року, прагнення до самонавчання залежить від розвитку навичок особи: 70 % людей з добре розвиненими навичками активно беруть участь у навчанні; тоді як серед людей з низько розвиненими навичками таких лише 26 % [12]. Вказане свідчить про необхідність більш високого рівня регламентації та стандартизації дій персоналу – комплаєнс у сфері інформаційної безпеки під час збройного конфлікту високої інтенсивності, на нашу думку, є недоречним.

Однак слід звернути увагу на той факт, що у Білій книзі з регулювання ШІ в Україні, датованій червнем 2024 року, представлена офіційна позиція Міністерства цифрової трансформації України, яка полягає у намірі вивести питання інформаційної безпеки під час використання ШІ за межі правового регулювання. Зокрема, у цьому документі зазначається, що, впроваджуючи підхід під час повномасштабного вторгнення російської федерації, цей орган усвідомлює важливість розробки інноваційних рішень для відсічі агресії та жодним чином не має наміру пропонувати регулювання систем ШІ у сфері оборони. Це, на думку розробників цього документа, обумовлено як національними інтересами держави, так і реальним станом речей у безпековому секторі – одностороннє регулювання (обмеження) використання ШІ у сфері оборони на рівні норм національного законодавства лише поставить нашу країну у менш вигідне становище порівняно з агресором, який аналогічного регулювання не впровадить [13].

Ми високо оцінюємо внесок Міністерства цифрової трансформації України у розвиток передумов правового регулювання використання штучного інтелекту органами публічного управління та іншими суб'єктами. За кілька років зроблено масштабну роботу, спрямовану на убезпечення публічних службовців та інших осіб від ризиків, які супроводжують використання ШІ. Але стратегічна лінія на саморегулювання не забезпечує належного рівня правової визначеності діяльності органів виконавчої влади (хоча для суб'єктів підприємницької діяльності такий підхід є більш виправданим). Відповідно до ч. 2 ст. 6 Конституції України органи законодавчої, виконавчої та судової влади здійснюють свої повноваження у встановлених цією Конституцією межах і відповідно до законів України [14]. Це обумовлює високий ступінь правової регламентації дій публічних службовців, зменшення частки їх дискреційних повноважень. У сфері інформаційної безпеки, як одного із видів національної безпеки, необхідність правової регламентації правил користування інструментами ШІ для персоналу органів виконавчої влади є особливо важливою.

Безумовно, у багатьох сферах суспільних відносин України все більш поширеними стають ситуації, коли важливі відносини в організаціях, корпораціях, професійних середовищах регулюються на локальному рівні. Протягом останніх 10 років було розроблено і затверджено кілька десятків правил поведінки, кодексів професійної етики та інших комплаєнс-документів, у яких визначалися вимоги до поведінки і результатів діяльності працівників. Разом з тим хотілося б звернути увагу на той факт, що норми, пов'язані з безпекою вищих посадових осіб України, органів державної влади та місцевого самоврядування, правоохоронних органів, інших складових сектора безпеки і оборони ніколи не регулювалися на рівні правил поведінки, добровільно схвалених колективами працівників.

У цьому є своя логіка, оскільки питання безпеки є комплексними, багатогранними, впливають на функціонування всієї системи публічного управління, тому не можуть віддаватися на вільний суб'єктивний розсуд групи осіб. Сфера безпеки не може базуватися на комплаєнсі: вона потребує централізованого управління і єдиноначальності у системі прийняття рішень. Тому уявляється небезпечною тенденція врегулювати відносини у сфері використання ШІ нормами, які мають добровільний характер і можуть лише рекомендуватися для застосування у певних структурах, у тому числі в центральних органах виконавчої влади тощо.

Для того, щоб система безпеки ефективно працювала, потрібна, по-перше, жорстка правова регламентація її вимог; по-друге, зрозумілий порядок виконання найбільш типових дій, які систематично повторюються у службовій діяльності; і, по-третє, мають існувати адекватні заходи юридичної відповідальності за недодержання встановлених вимог.

В умовах ведення бойових дій і постійних атак держави-агресора на об'єкти критичної інфраструктури надзвичайно широке коло відомостей та даних може бути корисним для противника, щоб більш ефективно вражати об'єкти української цивільної інфраструктури, спричинюючи максимальні страждання цивільного населення. За таких умов уявляється необхідним розмежування між тими аспектами використання ШІ, які можуть бути врегульовані на рівні етичних кодексів і виконуватися добровільно, та тими аспектами, які пов'язані із забезпеченням національної, інформаційної, воєнної та інших видів безпеки і мають супроводжуватися, у разі неправомірної поведінки працівників, заходами юридичної відповідальності. Особливо важливими ці положення, на нашу думку, слід розуміти в контексті правовідносин у секторі безпеки і оборони (розробники Білої книги з регулювання ШІ в Україні вживають термін «сфера оборони», який не має достатнього рівня правової визначеності і є скоріше публіцистичним). Як відомо, сектор безпеки і оборони, відповідно до положень Закону України «Про національну безпеку України», включає до свого складу оборонно-промисловий комплекс України - сукупність органів державного управління, підприємств, установ і організацій промисловості та науки, що розробляють, виробляють, модернізують і утилізують продукцію військового призначення, надають послуги в інтересах

оборони для оснащення та матеріального забезпечення сил безпеки і сил оборони, а також здійснюють постачання товарів військового призначення та подвійного використання, надання послуг військового призначення під час виконання заходів військово-технічного співробітництва України з іншими державами [15]. Станом на жовтень 2025 року, за даними Міністерства оборони України, в нашій державі функціонувало близько 900 підприємств оборонно-промислового комплексу, лише 100 з яких мали статус державних, а їх загальний потенціал оцінювався у 35 млрд доларів [16]. Таким чином, здійснений нами аналіз свідчить, що у Білій книзі з регулювання ШІ в Україні мова йде у тому числі про відсутність правового регулювання використання ШІ для 800 суб'єктів підприємницької діяльності, які мають величезний потенціал для розвитку цих технологій.

Загальновідомо, що головною метою будь-якого суб'єкта підприємницької діяльності є отримання прибутку. Отже, виникає питання: чи не створить Україна, виводячи за межі правового регулювання використання технологій ШІ потужними суб'єктами підприємницької діяльності, монстра, який, у погоні за прибутком, створить численні ризики порушення прав людини та загрози національній і воєнній безпеці? Ситуація ускладнюється відсутністю правових механізмів контролю за використанням ШІ в секторі безпеки і оборони та у сфері публічного управління в цілому.

Вказане вище свідчить, що вихід за межі правового регулювання з метою посилення обороноспроможності держави у сфері використання ШІ може мати прямо протилежні наслідки: зниження мобілізаційного потенціалу України за рахунок посилення імміграційних тенденцій серед громадян України, незадоволених порушенням їх прав і свобод, а також зниження оборонного потенціалу за рахунок численних вразливостей інструментів ШІ, які періодично спричиняють виток у вільний доступ чутливої інформації. Виходом з такої ситуації є, на наш погляд, імплементація принципів та процедур, закріплених в Artificial Intelligence Act, який передбачає чотири рівні ризиків: неприйнятний (технологія ШІ забороняється), високий ризик (використання технології ШІ суворо обмежено), обмежений ризик (використання відповідно до правил), мінімальний ризик (вільне використання). [4].

Сектор безпеки і оборони є надзвичайно важливим, але не єдиним елементом публічного управління. Слід також звернути увагу на той факт, що безконтрольне та не обмежене відповідно до наведених вище рівнів ризиків використання ШІ у системі публічної влади також може утворювати загрози національній, інформаційній та воєнній безпеці. Такі загрози обумовлені трьома основними факторами: 1) можливістю прийняття помилкового управлінського рішення, базованого на помилкових результатах застосування інструментів ШІ (т. зв. галюцинацій або марення ШІ); 2) несанкціонованим витоком відомостей та даних, які можуть бути використані державою-агресором; 3) поступовою депрофесіоналізацією публічних службовців внаслідок систематичного застосування інструментів ШІ для збору даних, аналітичної діяльності, створення прогнозів, планування тощо. Безумовно, запровадження для сфери публічного управління деяких заборон та контролю за використанням інструментів ШІ певною мірою обмежить можливості персоналу системи публічної влади підвищувати продуктивність своєї рутинної діяльності. Разом з тим у воюючій державі вимоги безпеки, на нашу думку, мають бути пріоритетними порівняно з вимогами зручності.

Висновки

У результаті проведеного дослідження встановлено, що використання технологій ШІ у системі публічного управління потребує системного правового регулювання, яке повинно враховувати як потенційні переваги таких технологій, так і ризики, пов'язані з їх застосуванням у діяльності державних органів та інших суб'єктів інформаційної діяльності. Виявлено, що чинна нормативна база України лише частково охоплює питання використання штучного інтелекту, а більшість наявних документів мають стратегічний або рекомендаційний характер. Водночас наукові та практичні дискусії

свідчать про наявність низки концептуальних суперечностей щодо співвідношення державного регулювання та механізмів саморегулювання у сфері застосування штучного інтелекту. Окремою проблемою є відсутність чіткого визначення меж використання технологій штучного інтелекту під час підготовки та прийняття управлінських рішень органами публічної влади. Крім того, потребують подальшого опрацювання питання інформаційної безпеки, захисту персональних даних та відповідальності за наслідки використання алгоритмічних систем у діяльності державних інституцій.

Встановлено, що особливу складність становить правове регулювання використання штучного інтелекту у сфері національної безпеки та оборони, де виникає необхідність поєднання вимог безпеки, режиму секретності та принципів демократичного цивільного контролю. У зв'язку з цим доцільним є формування багаторівневої моделі регулювання, яка поєднуватиме загальні норми законодавства, спеціальні правила використання штучного інтелекту у діяльності органів публічної влади та окремі механізми правового регулювання для сектору безпеки і оборони. Перспективним напрямом розвитку національного законодавства є адаптація підходів, сформованих у праві Європейського Союзу, з урахуванням особливостей функціонування української системи публічного управління. Водночас імплементація міжнародних стандартів повинна супроводжуватися уточненням компетенції органів державної влади у сфері контролю за використанням алгоритмічних систем. Реалізація зазначених підходів сприятиме підвищенню прозорості застосування технологій ШІ у діяльності органів публічної влади та забезпеченню належного рівня інформаційної безпеки у процесі прийняття управлінських рішень.

Список використаних джерел

1. Mitchell A. D., Let D., Tang L. AI Regulation and the Protection of Source Code. International Journal of Law and Information Technology. 2023. Vol. 31, No. 4. P. 297–322. DOI: 10.1093/ijlit/eaad026.
2. Taeihagh A. Governance of Artificial Intelligence. Policy and Society. 2021. DOI: 10.1080/14494035.2021.1928377
3. Davtyan T. The U.S. Approach to AI Regulation: Federal Laws, Policies, and Strategies Explained. Case Western Reserve Journal of Law, Technology & the Internet. 2025. Vol. 16, No. 2. P. 223–251. https://scholarlycommons.law.case.edu/jolti/vol16/iss2/2 (дата звернення 27.02.2026).
4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 (дата звернення 27.02.2026).
5. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення 27.02.2026).
6. План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021-2024 роки: затверджено розпорядженням Кабінету Міністрів України від 12 травня 2021 р. № 438-р. URL: https://zakon.rada.gov.ua/laws/show/438-2021-%D1%80#Text (дата звернення 27.02.2026).
7. План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025-2026 роки: затверджено розпорядженням Кабінету Міністрів України від 9 травня

2025 р. № 457-р. URL: https://zakon.rada.gov.ua/laws/show/457-2025-%D1%80#Text (дата звернення 27.02.2026).
8. Рекомендації з кіберзахисту інформаційно-комунікаційних систем, які використовують технології штучного інтелекту: затверджені наказом Адміністрації Держспецзв'язку від 23.02.2026 року № 154. URL: https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-23-02-2026-154-pro-zatverdzhennya-rekomendacii-z-kiberzakhistu-informaciino-komunikaciinikh-sistem-yaki-vikoristovuyut-tekhnologiyi-shtuchnogo-intelektu (дата звернення 27.02.2026).
9. Дорожня карта з регулювання штучного інтелекту в Україні. URL: https://storage.thedigital.gov.ua/files/2/22/363bbcaec30bf9d4e598375fecac3227.pdf (дата звернення 27.02.2026).
10. Пилипенко Н. Вже 60% українців використовують ШІ: які моделі і застосунки. URL: https://thepage.ua/ua/news/skilki-ukrayinciv-koristuyutsya-shi-ta-yaki-instrumenti-obirayut (дата звернення 27.02.2026).
11. Поради з відповідального використання штучного інтелекту публічними службовцями. URL: https://storage.thedigital.gov.ua/files/f/bf/a9595e0dcd238ab2b3602909107aabf9.pdf
12. Education at a Glance 2025 OECD Indicators. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/09/education-at-a-glance-2025_c58fc9ae/1c0d9c79-en.pdf (дата звернення 27.02.2026).
13. Біла книга з регулювання ШІ в Україні: бачення Мінцифри. Версія для консультацій / відповідальний за розробку матеріалу Г. Румянцев. Київ, 2024. URL: https://storage.thedigital.gov.ua/files/d/9d/0bbc3a705c821a197bedfcdfe00899d9.pdf (дата звернення 27.02.2026).
14. Конституція України. Закон України 28.06.1996. Відомості Верховної Ради України. 1996. №30. Ст.141.
15. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. Відомості Верховної Ради України. 2018. № 31. Ст. 241.
16. Україна є найперспективнішим ринком для інвестицій в ОПК – Денис Шмигаль. URL: https://mod.gov.ua/news/ukrayina-ye-najperspektivnishim-rinkom-dlya-investiczij-v-opk-denis-shmigal (дата звернення 27.02.2026).