УДК 351:004.8:351.746; JEL classification: H11, H56, O38
DOI: https://doi.org/10.36887/2415-8453-2026-3-59

Некряч Анастасія Іванівна, доктор політичних наук, професор, професор кафедри міжнародних відносин та політичного консалтингу, Інститут права та суспільних відносин, ЗВО «Відкритий міжнародний університет розвитку людини «Україна»

Nekriach Anastasiia, Doctor of Political Science, Professor, Professor of the Department of International Relations and Political Consulting, Institute of Law and Public Relations, Open International University of Human Development "Ukraine", Kyiv, https://orcid.org/0000-0001-5058-4145

ДЕРЖАВНЕ УПРАВЛІННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПІДВИЩЕННІ ОБОРОНОЗДАТНОСТІ УКРАЇНИ
STATE ADMINISTRATION FOR THE USE OF ARTIFICIAL INTELLIGENCE IN THE INFORMATION SECURITY SYSTEM AND IMPROVING THE DEFENSE CAPABILITY OF UKRAINE

Некряч А. І. Державне управління використання штучного інтелекту в системі забезпечення інформаційної безпеки та підвищенні обороноздатності України. *Український журнал прикладної економіки та техніки*. 2026. Том 11. № 3. С. 331 – 336.

Nekriach A. State administration for the use of artificial intelligence in the information security system and improving the defense capability of Ukraine. *Ukrainian Journal of Applied Economics and Technology*. 2026. Volume 11. № 3. pp. 331 – 336.

У статті досліджено теоретико-правові засади державного управління у сфері використання штучного інтелекту в системі забезпечення інформаційної безпеки та підвищення обороноздатності України. Узагальнено доктринальні та законодавчі підходи до визначення категорій «штучний інтелект», «державне управління» та «інформаційна безпека», сформовано авторське бачення їхнього змісту. Обґрунтовано зростання ролі технологій штучного інтелекту як інструменту підтримки управлінських рішень, аналізу інформаційних потоків, прогнозування ризиків і протидії сучасним кібернетичним та гібридним загрозам. Проаналізовано сучасний стан нормативно-правового забезпечення використання штучного інтелекту в Україні та визначено основні напрями його вдосконалення з урахуванням європейських підходів. Запропоновано авторську модель механізму державного управління у сфері використання штучного інтелекту, яка включає нормативно-правовий, інституційний, організаційно-управлінський, інформаційно-аналітичний, технологічний, кадровий та міжнародний компоненти. Доведено, що комплексна реалізація зазначених складових сприятиме підвищенню ефективності державного управління, зміцненню інформаційної безпеки та обороноздатності України.
Ключові слова: *штучний інтелект; державне управління; інформаційна безпека; національна безпека; обороноздатність; цифрова трансформація; публічне управління; кібербезпека; державна політика; цифрові технології.*

The article examines the theoretical and legal foundations of the public administration of artificial intelligence applications within Ukraine's information security and defense capability system. The doctrinal and legislative approaches to defining the key concepts of artificial intelligence, public administration, and information security are analyzed, and the author proposes a refined interpretation of these categories in the context of digital transformation. The growing role of artificial intelligence technologies as an essential tool for supporting managerial decision-making, processing Big Data, analyzing information flows, forecasting risks, detecting disinformation, and countering cyber and hybrid threats is substantiated. The paper analyzes the historical evolution of artificial intelligence and the current state of its legal regulation in Ukraine, identifying priority directions for its improvement. Particular emphasis is placed on adapting national legislation to European and international standards, specifically the EU Artificial Intelligence Act (AI Act), the Framework Convention of the Council of Europe, OECD AI Principles, and UNESCO Recommendations. The author proposes a comprehensive model of the public administration mechanism for the use of artificial intelligence, comprising seven interconnected components: legal, institutional, organizational-managerial, information-analytical, technological, personnel, and international. The practical application of this model is considered alongside strategic initiatives, including the AI Development Strategy until 2030, state security sector strategies, and specialized technological infrastructure such as the Defense AI Center "A1". It is concluded that the integrated implementation of these components will improve the efficiency of public administration, ensure algorithmic transparency and ethics, strengthen information security, enhance Ukraine's defense capabilities during martial law, and facilitate post-war recovery. Prospects for future research include evaluating the long-term impact of artificial intelligence on governance transparency, public trust, and alignment with global digital trends.
Keywords: *artificial intelligence, public administration, information security, national security, defense capability, digital transformation, public governance, cybersecurity, public policy, digital technologies.*

Вступ

Стрімкий розвиток технологій штучного інтелекту суттєво трансформує механізми державного управління, відкриваючи нові можливості для підвищення ефективності управлінської діяльності, водночас формуючи нові правові, організаційні та безпекові виклики. В умовах цифрової трансформації та триваючої збройної агресії проти України особливої актуальності набуває використання технологій штучного інтелекту для забезпечення інформаційної безпеки, своєчасного виявлення кіберзагроз, підтримки прийняття управлінських рішень і зміцнення обороноздатності держави. Разом із тим сучасне нормативно-правове забезпечення використання штучного інтелекту залишається фрагментарним, що зумовлює необхідність комплексного наукового дослідження механізмів державного управління в цій сфері.

Проблематика державного управління, інформаційної безпеки та використання технологій штучного інтелекту перебуває у центрі уваги багатьох вітчизняних і зарубіжних науковців. Теоретичні засади державного управління досліджував В. П. Рубцов, Н. І. Перинська та інші вчені. Правові аспекти розвитку цифрових технологій, інформаційної безпеки, цифрової трансформації та адаптації національного законодавства до європейських стандартів висвітлено у працях В. І. Теремецького, А. А. Петренка та інших дослідників.

Незважаючи на наявність значної кількості наукових досліджень, присвячених питанням державного управління, цифрової трансформації, інформаційної безпеки та розвитку технологій штучного інтелекту, комплексний підхід до державного управління використанням штучного інтелекту в системі забезпечення інформаційної безпеки та підвищення обороноздатності України залишається недостатньо сформованим. У науковій літературі переважно досліджуються окремі аспекти правового регулювання штучного інтелекту, цифровізації публічного управління або забезпечення кібербезпеки, тоді як питання інтеграції технологій штучного інтелекту в єдиний механізм державного управління сектором безпеки і оборони не отримало належного теоретичного та практичного обґрунтування.

This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

© Некряч Анастасія Іванівна, 2026

Потребують подальшого дослідження концептуальні засади державного управління використанням штучного інтелекту, визначення його місця в системі забезпечення інформаційної безпеки, формування цілісного механізму нормативно-правового, інституційного, організаційного та інформаційно-

аналітичного забезпечення, а також адаптація національної моделі правового регулювання до вимог законодавства Європейського Союзу, зокрема положень AI Act, міжнародних стандартів Ради Європи, ОЕСР та ЮНЕСКО. Недостатньо розробленими залишаються також питання використання технологій штучного інтелекту для підтримки управлінських рішень, прогнозування інформаційних і кібернетичних загроз, забезпечення кіберстійкості та зміцнення обороноздатності держави в умовах воєнного стану.

Формулювання цілей статті

Метою статті є обґрунтування концептуальних засад державного управління використанням технологій штучного інтелекту в системі забезпечення інформаційної безпеки та обороноздатності України, а також визначення напрямів удосконалення відповідних механізмів державного регулювання.

Виклад основного матеріалу дослідження

Феномен стрімкої трансформації світу під впливом штучного інтелекту (ШІ) зумовлений його здатністю прискорювати інновації, змінювати економічні процеси, впливати на способи взаємодії людей із технологіями та відкривати нові перспективи для розвитку людства. Останні роки відзначаються безпрецедентним темпом впровадження ШІ у ключові сфери життя, що суттєво змінює ринок праці, наукові дослідження, соціальні комунікації, глобальну безпеку та економіку. Проте ці зміни потребують усвідомленого підходу до регулювання, визначення етичних меж і адаптації суспільства до нових технологічних реалій. Важливо забезпечити, щоб ШІ залишався інструментом прогресу, що сприяє сталому розвитку, а не створював загрозу стабільності та добробуту людства [1].

Здійснюючи дослідження державного управління у сфері використання штучного інтелекту в системі забезпечення інформаційної безпеки та підвищення обороноздатності України в умовах воєнного стану, варто зупинитися на ключових категоріях і явищах, які «пронизують» цей процес.

Однією з таких категорій і є штучний інтелект. ШІ досліджують науковці, які представляють різні сфери, як за кордоном, так і в Україні. Якщо частково дослідити історію його виникнення (ґрунтовне вивчення не є метою нашого дослідження), то варто зазначити, що він виник відносно нещодавно.

Першим етапом в історії розвитку ШІ є Дартмутська конференція 1956 р., що об'єднала дослідників різних галузей, а саме інформатики, математики, фізики тощо, для визначення потенціалу синтетичного інтелекту (термін ШІ ще не існував). Учасники конференції обговорили напрями обробки природної мови, розв'язання задач і машинне навчання, а також розробили дорожню карту дослідження ШІ, зокрема розробку мов програмування та алгоритмів для створення інтелектуальних машин. На цій конференції було започатковано новий напрям у розвитку науки і технологій й саме поняття «штучний інтелект».

Другим етапом розвитку ШІ є прорив, який стався внаслідок практичної реалізації теоретичних концепцій, закладених на Дартмутській конференції.

Третім етапом в історії розвитку ШІ є стрімкий розвиток нових методів створення інтелектуальних машин, програмування для виконання завдань, пошук нових підходів до ШІ, окрім перцептрона, що відбувся у 1960-х рр. На цьому етапі було розроблено нові мови програмування, створено спеціальні інструменти для ШІ, а саме LISP і Prolog.

У наступний, четвертий етап (1980-ті та 1990-ті рр.) розвиток ШІ дещо сповільнився через обмежені обчислювальні можливості та високу вартість обробки даних. Відбулася так звана зима ШІ – період зменшення комерційного й наукового інтересу до галузі, розчарування через відсутність прогресу, скорочення фінансування, відмова дослідників від проєктів і бажання залишити цю сферу діяльності.

Історія розвитку штучного інтелекту в Україні бере свій початок у другій половині XX ст., коли Україна ще була частиною Радянського Союзу. У цей період дослідження штучного інтелекту проводили в академічних установах та науково-дослідних інститутах, зокрема, в Інституті кібернетики імені В. М. Глушкова НАН України [2, С. 358-360].

З огляду на стрімкий розвиток технологій штучного інтелекту, розширення сфер їх практичного застосування та зростання ролі у забезпеченні державного управління, інформаційної й національної безпеки, особливого значення набуває визначення сутності поняття «штучний інтелект». Аналіз наукових підходів до його трактування дає змогу окреслити ключові характеристики цієї категорії та визначити її місце в системі сучасного публічного управління.

Пропонується здійснити фрагментарний аналіз доктринальних джерел і законодавства.

Штучний інтелект (artificial intelligence, AI) – це галузь інформатики, що створює комп'ютерні системи, які здатні аналізувати, розуміти та вчиться на основі наданих даних, імітуючи при цьому поведінку людини в процесах прийняття рішень [3].

Штучний інтелект – міждисциплінарні наукові дослідження, у межах яких розробляють інтелектуальні машини, здатні виконувати завдання, що зазвичай потребують людського інтелекту: моделювання інтелектуальної діяльності, алгоритмів мислення, психічних процесів навчання, творчості [4].

Для отримання розуміння з етимологічної точки зору пропонується пристосувати тлумачення, сформульоване в Кембриджському словнику, а саме: штучний інтелект – використання або вивчення комп'ютерних систем чи машин, які мають деякі якості, властиві людському мозку, такі як здатність інтерпретувати та відтворювати мову у спосіб, що здається людським, розпізнавати або створювати зображення, вирішувати проблеми та навчатися на основі даних, що їм надаються [5].

На законодавчому рівні штучний інтелект визначено як: організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань [6].

Водночас формування національної політики у сфері штучного інтелекту здійснюється з урахуванням сучасних міжнародних підходів до його правового регулювання. Насамперед ідеться про Регламент Європейського Союзу Artificial Intelligence Act (Regulation (EU) 2024/1689), який запроваджує ризик-орієнтовану модель регулювання систем штучного інтелекту, визначає вимоги до високоризикових AI-систем, а також принципи прозорості, підзвітності та людського контролю. З огляду на євроінтеграційний курс України положення зазначеного акта мають стати одним із базових орієнтирів для подальшого розвитку національного законодавства [7].

Аналіз наукових підходів свідчить про відсутність єдиного універсальної дефініції категорії «штучний інтелект», і це пояснюється міждисциплінарним характером цього феномена. Незважаючи на існування значної кількості підходів, спільними для більшості є такі сутнісні характеристики: використання алгоритмів обробки даних,

здатність до навчання та самовдосконалення (machine learning), аналіз значних масивів інформації, підтримка або прийняття рішень, прогнозування, розпізнавання образів, обробка природної мови та адаптація до змін зовнішнього середовища.

З огляду на мету дослідження, під штучним інтелектом пропонується розуміти сукупність інтелектуальних інформаційних технологій, алгоритмів і моделей машинного навчання, здатних здійснювати автоматизований аналіз великих масивів даних, формувати прогнози, підтримувати або приймати управлінські рішення, адаптуватися до нових умов та виконувати складні когнітивні завдання, що традиційно потребують участі людини, з метою підвищення ефективності державного управління, забезпечення інформаційної, національної та оборонної безпеки.

Наступною категорією, яка становить наш науковий інтерес є «державне управління». На законодавчому рівні воно визначено як вид діяльності держави, що полягає у здійсненні нею управлінського, тобто організуючого впливу на ті сфери і галузі суспільного життя, які вимагають певного втручання держави шляхом використання повноважень виконавчої впади. Водночас державне управління здійснюється і за межами функціонування виконавчої влади, наприклад, на рівні державних підприємств, установ і організацій. Завдяки цьому поняття «державне управління» за змістом є ширшим, ніж поняття «виконавча влада». Для визначення змістовно поєднаних сфер або галузей суспільного життя, що потребують державного управління, використовується термін «сектор державного управління» [8].

Також «державне управління» – виконавчо-розпорядча діяльність державних органів, сутність якої полягає в організуючому впливі на суспільні відносини в економічній, соціо-культурній і адміністративно-політичній галузях шляхом застосування державно-владних повноважень [9].

Також влучною видається дефініція, запропонована В. П. Рубцовим та Н. І. Перинською: державне управління – це цілеспрямований організаційний і регулюючий вплив держави на стан і розвиток суспільних процесів, свідомість, поведінку та діяльність особи і громадянина з метою досягнення цілей та реалізації функцій держави, відображених у Конституції та законодавчих актах, шляхом запровадження державної політики, виробленої політичною системою та законодавчо закріпленої, через діяльність органів державної влади, наділених необхідною компетенцією [10, с. 113].

Таким чином, узагальнивши вищезазначені дефініції, під державним управлянням доцільно розуміти цілеспрямований (у жодному разі не стихійний) організаційно-регулюючий вплив держави, реалізація якого здійснюється через систему уповноважених органів та відповідних державно-владних повноважень з метою забезпечення належного функціонування та розвитку суспільних відносин, реалізації державної політики й виконання функцій держави.

Сучасні тенденції розвитку державного управління засвідчують поступовий перехід від традиційних адміністративних моделей до цифрового врядування, у межах якого технології штучного інтелекту розглядаються як інструмент підвищення ефективності управлінських рішень, прозорості діяльності органів влади та якості публічних послуг. Такий підхід відповідає Принципам ОЕСР щодо штучного інтелекту (OECD AI Principles), які визначають необхідність використання інноваційних технологій із дотриманням принципів верховенства права, відкритості, безпеки та підзвітності [11].

У сучасних умовах цифрової трансформації та зростання спектра кібернетичних і гібридних загроз одним із ключових напрямів реалізації державного управління є сфера інформаційної безпеки, ефективне забезпечення якої є необхідною передумовою захисту національних інтересів, стабільного функціонування державних інститутів і розвитку інформаційного суспільства.

У законодавстві України інформаційна безпека визначена у значній кількості нормативно-правових актів, і уточнення відбуваються, приймаючи до уваги ту чи іншу сферу. Одним із таких визначень є наступне: інформаційна безпека – це збереження конфіденційності, цілісності та доступності інформації [12].

Погоджуємося із думкою про те, якщо проаналізувати зміст та напрямки досліджень поняття інформаційної безпеки, то можна виокремити декілька підходів окреслення сутності цього феномену, а саме розуміння інформаційної безпеки в якості: стану захищеності інформаційного простору; процесу управління загрозами та небезпеками, що забезпечує інформаційний суверенітет України; стану захищеності національних інтересів України в інформаційному середовищі; захищеності встановлених законом правил, за якими відбуваються інформаційні процеси в державі; стану захищеності національних інтересів країни в інформаційній сфері; важливої функції держави; невід'ємної частини політичної, економічної, оборонної та інших складових національної безпеки [13, с. 15].

Водночас міжнародні стандарти дедалі більше акцентують увагу на необхідності забезпечення безпечного та людиноцентричного використання систем штучного інтелекту. Зокрема, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, ухвалена Радою Європи у 2024 році, визначає необхідність поєднання технологічного розвитку із захистом прав людини, демократичних цінностей і принципу верховенства права. Для України імплементація зазначених підходів має особливе значення в умовах цифрової трансформації сектору безпеки і оборони [14].

Отже, комплексний аналіз категорій «штучний інтелект», «державне управління» та «інформаційна безпека» свідчить, що їх взаємодія формує новий напрям розвитку державної політики, у межах якого сучасні технології штучного інтелекту виступають не лише об'єктом правового регулювання, а й інструментом реалізації функцій держави у сфері захисту національних інтересів. У зв'язку з цим особливої актуальності набуває дослідження державного управління у сфері використання штучного інтелекту в системі забезпечення інформаційної безпеки та підвищення обороноздатності України, що потребує визначення його правових, організаційних і інституційних засад.

Попри війну та економічну нестабільність, Україна зберігає потенціал для інтеграції в глобальну сферу штучного інтелекту (ШІ). Наприкінці грудня 2024 року Україна схвалила Стратегію цифрового розвитку інноваційної діяльності на період до 2030 року, спрямовану на стимулювання технологічного прогресу, залучення інвестицій і створення стійкої інноваційної екосистеми.

Незважаючи на виклики, країна демонструє прагнення до розвитку у сфері ШІ, цифрової трансформації та безпеки, що є запорукою її конкурентоспроможності в майбутньому. Війна спричинила відтік кадрів і руйнування інфраструктури, проте українські фахівці продовжують відігравати важливу роль у світовій індустрії [1].

У загальному вигляді, технології ШІ здатні суттєво підвищити якість публічних послуг через обробку даних у реальному часі, прогнозуванню суспільних потреб і оптимізації розподілу ресурсів у сферах охорони здоров'я, освіти та місцевого самоврядування. ШІ дедалі активніше інтегрується в сфери державного управління, місцевого самоврядування, забезпечення інформаційної безпеки та підвищенні обороноздатності.

Серед ключових переваг ШІ виділяється його роль в інклюзивному розвитку, де технології сприяють зменшенню цифрового розриву, покращенню доступу до послуг для вразливих груп населення та забезпеченню гендерної рівності, що вимагає адаптації публічного (державного) управління до реалій цифрового суспільства. Однак впровадження ШІ супроводжується значними ризиками, зокрема загрозами суверенному інформаційному простору, такими як кібербезпека, упередженість алгоритмів та залежність від іноземних технологій, що потребує правового регулювання та етичних рамок. Цілком підтримуємо думку про те, що для успішної інтеграції ШІ в Україні рекомендується розробка національної стратегії, яка включає освітні ініціативи для підвищення цифрових компетентностей, громадські консультації та фокус на поствоєнне відновлення, аби забезпечити баланс між інноваціями та демократичними цінностями. Перспективи подальших досліджень охоплюють оцінку довгострокового впливу ШІ на прозорість управління, довіру громадян, а також порівняльний аналіз міжнародного досвіду з акцентом на адаптацію до викликів глобальної цифрової трансформації [15, с. 312], забезпечення інформаційної безпеки та підвищення обороноздатності України.

Щодо можливостей використання штучного інтелекту у сфері інформаційної безпеки, пропонуємо виокремити такі сфери: виявлення дезінформації; аналіз інформаційних потоків; прогнозування інформаційних загроз та пропозиція способів їх усунення; кіберзахист; автоматизація управлінських процесів. Також штучний інтелект можна розглядати як новий фактор трансформації державного управління, що сприяє розвитку цифрової держави.

Приймаючи до уваги той факт, що відносини щодо використання штучного інтелекту не є врегульованими на національному рівні, українське суспільство потребує розробки спеціального Закону про штучний інтелект, який би встановлював комплексні нормативно-правові рамки застосування ШІ у державному секторі та визначав ключові положення, спрямовані на мінімізацію ризиків, забезпечення прозорості алгоритмічних процесів і підвищення ефективності публічного управління.

Штучний інтелект виступає стратегічним інструментом цифрової трансформації публічного управління, проте його впровадження має супроводжуватися створенням ефективного правового та нормативного середовища. На сьогоднішній день Україна лише розпочинає процес формування законодавства щодо штучного інтелекту, який має базуватися на міжнародних стандартах, зокрема на положеннях Акта Європейського Союзу про штучний інтелект. Основними завданнями у цьому контексті: розробка спеціального Закону про штучний інтелект, що визначатиме критерії відповідальності за алгоритмічні рішення та регламентуватиме використання ШІ у державному секторі; створення ефективних механізмів контролю, аудиту та сертифікації алгоритмів, які застосовуються у сфері публічного управління; забезпечення відповідності систем штучного інтелекту принципам прозорості, етичності та недискримінації; поступова адаптація українського законодавства до європейських норм, що сприятиме інтеграції України у єдиний цифровий та правовий простір Європейського Союзу [16, с. 19].

Позитивним моментом є те, що практичне втілення зазначених напрямів уже частково відображається у державних стратегічних документах, які визначають підходи до використання сучасних цифрових технологій у сфері безпеки та державного управління. Наразі Україною прийнято шість програмних довгострокових документів у безпековому напрямі, які стосуються (прямо або опосередковано) питань національної безпеки та обороноздатності держави й торкаються проблематики використання ШІ, Big Data та сучасних ІКТ у вказаних сферах: 1) Стратегія забезпечення державної безпеки; 2) Стратегія національної безпеки України; 3) Стратегія інформаційної безпеки; 4) Стратегія кібербезпеки України; 5) Стратегія воєнної безпеки України; 6) Стратегія розвитку оборонно-промислового комплексу України [17, С. 71].

Вартою уваги є думка, що для забезпечення національної безпеки та обороноздатності України у повоєнний період необхідно розробляти та впроваджувати у національне законодавство найкращі світові практики, що враховують потенційні можливості та загрози ШІ і забезпечують трансфер технологій ШІ через оборонну та безпекову сфери в інші галузі економіки. Необхідно забезпечити належний рівень кібербезпеки, захистити критичну інфраструктуру та розробити відповідні алгоритми й процедури для виявлення та запобігання загрозам. Штучний інтелект може стати важливим інструментом у сфері забезпечення національної безпеки та обороноздатності України в повоєнний період, допомагаючи підвищити ефективність і швидкість виконання військових завдань, знизити ризик втрат, підвищити захищеність військових систем і зменшити витрати на оборону. Однак під час розроблення та використання ШІ необхідно дотримуватися відповідних правових і етичних стандартів [17, с. 76].

Удосконалення державного управління з використанням штучного інтелекту (ШІ) спрямоване на підвищення ефективності, прозорості та якості прийняття рішень. Це досягається через оптимізацію публічних послуг, впровадження етичних стандартів і забезпечення безпеки даних [15, с. 307].

На сьогоднішній день вдосконалення державного управління штучним інтелектом (ШІ) в Україні базується на Стратегії розвитку ШІ до 2030 року [18] та включає створення єдиної екосистеми Defense AI Center «A1» [19] для аналізу даних на полі бою та протидії кіберзагрозам. Щодо основних напрямів державного управління та розвитку технологій використання штучного інтелекту в системі забезпечення інформаційної безпеки та підвищення обороноздатності України, то до них входять: підвищення обороноздатності; забезпечення інформаційної безпеки; оптимізація публічної адміністрації.

Крім нормативного забезпечення, міжнародні організації наголошують на необхідності дотримання етичних принципів під час застосування штучного інтелекту. Відповідно до Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021) держави повинні забезпечувати прозорість алгоритмів, недискримінацію, відповідальність розробників і користувачів, захист персональних даних та постійний людський контроль над критично важливими рішеннями. Зазначені принципи доцільно враховувати під час формування механізму державного управління використанням штучного інтелекту в Україні [20].

Ґрунтуючись на здійснене дослідження, пропонуємо авторську модель механізму державного управління використанням штучного інтелекту в системі забезпечення інформаційної та оборонної безпеки України. Доцільно структурувати її за такими компонентами (табл. 1).

Запропонована модель демонструє, що державне управління у сфері використання штучного інтелекту має базуватися на комплексному взаємодії нормативно-правових, інституційних, організаційних, інформаційно-аналітичних, технологічних, кадрових і міжнародних складових.

Таблиця 1. Модель механізму державного управління використанням штучного інтелекту в системі забезпечення інформаційної та оборонної безпеки України

Компонент	Зміст складової	Основні напрями реалізації
Нормативно-правовий	Формування правових засад функціонування та використання технологій штучного інтелекту	Розробка спеціального законодавства щодо ШІ; адаптація законодавства до стандартів ЄС; встановлення механізмів відповідальності за алгоритмічні рішення; нормативне регулювання захисту даних та кібербезпеки
Інституційний	Сукупність державних органів та інституцій, які забезпечують реалізацію політики у сфері ШІ	Координація діяльності органів державної влади; взаємодія сектору безпеки й оборони; створення міжвідомчих координаційних механізмів; розподіл повноважень
Організаційно-управлінський	Управлінські процеси та механізми прийняття рішень із використанням цифрових технологій	Впровадження цифрового врядування; автоматизація адміністративних процесів; використання ШІ для підтримки управлінських рішень; підвищення ефективності державного управління
Інформаційно-аналітичний	Формування та обробка інформаційних ресурсів для підтримки управлінської діяльності	Аналіз великих масивів даних; моніторинг суспільних процесів; прогнозування ризиків і загроз; створення систем аналітичної підтримки
Технологічний	Технологічна база функціонування систем штучного інтелекту	Розвиток цифрової інфраструктури; створення платформ ШІ; забезпечення кіберзахисту; інтеграція сучасних ІКТ
Кадровий	Формування людського потенціалу для забезпечення ефективного використання ШІ	Підготовка та перепідготовка державних службовців; розвиток цифрових компетентностей; підготовка фахівців у сфері ШІ; підвищення кваліфікації персоналу
Міжнародний	Інтеграція національної системи у міжнародний простір цифрового розвитку та безпеки	Імплементація стандартів ЄС і НАТО; міжнародне співробітництво; участь у міжнародних проєктах; адаптація найкращих світових практик

Джерело: сформовано автором.

Лише їх узгоджене функціонування забезпечує ефективне впровадження технологій штучного інтелекту у сфері інформаційної безпеки, сприяє підвищенню якості управлінських рішень, посиленню кіберстійкості та зміцненню обороноздатності України.

Висновки та перспективи подальших розвідок

Проведене дослідження підтвердило, що використання технологій штучного інтелекту стає одним із ключових напрямів модернізації державного управління у сфері інформаційної безпеки та оборони. Узагальнення доктринальних і законодавчих підходів дозволило уточнити зміст основних категорій та обґрунтувати необхідність комплексного нормативно-правового регулювання застосування штучного інтелекту в діяльності органів державної влади. Запропонована авторська модель механізму державного управління використанням штучного інтелекту визначає взаємопов'язані нормативно-правовий, інституційний, організаційно-управлінський, інформаційно-аналітичний, технологічний, кадровий та міжнародний компоненти. Її практична реалізація сприятиме підвищенню ефективності державного управління, зміцненню інформаційної безпеки та обороноздатності України, а також гармонізації національної політики із сучасними європейськими підходами. Подальший розвиток державної політики у цій сфері доцільно здійснювати з урахуванням положень AI Act Європейського Союзу, Конвенції Ради Європи щодо штучного інтелекту, Принципів ОЕСР та Рекомендацій ЮНЕСКО, що сприятиме гармонізації українського законодавства з міжнародними стандартами.

Література

1. Згуровський М. Штучний інтелект змінює світ: шанси і виклики для України. URL: https://svit.kpi.ua/2025/01/31/штучний-інтелект-змінює-світ-шанси-і-в/.
2. Гук О. В., Артеменко Л. П., Хитровська Ю. В. Історія штучного інтелекту в медіабізнесі: етапи розвитку, особливості застосування, виклики та перспективи. *Сторінки історії : збірник наукових праць*. 2024. Вип. 59. С. 253-278. DOI: https://doi.org/10.20535/2307-5244.59.2024.318894.
3. Штучний інтелект. Дія. ІТ-студії. URL: https://it-osvita.diia.gov.ua/task/item/3ba90df9-79a0-42c6-a793-b4eb5eebeb0e.
4. Штучний інтелект. Велика українська енциклопедія. URL: https://vue.gov.ua/Штучний_інтелект.
5. Artificial intelligence. Cambridge Dictionary. URL: https://dictionary.cambridge.org/dictionary/english/artificial-intelligence.
6. Концепція розвитку штучного інтелекту в Україні : схвалена розпорядженням Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р
7. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). – Official Journal of the European Union, 12.07.2024. URL: EUR-Lex – Regulation (EU) 2024/1689.
8. Про заходи щодо впровадження Концепції адміністративної реформи в Україні : Указ Президента України від 22.07.1998 № 810/98. URL: https://zakon.rada.gov.ua/laws/show/810/98.
9. Державне управління. Енциклопедія сучасної України. URL: https://esu.com.ua/article-26159.
10. Рубцов В. П., Перинська Н. І. Державне управління та державні установи : навч. посіб. Київ : Університет «Україна», 2008. 440 с.
11. OECD. Recommendation of the Council on Artificial Intelligence (OECD AI Principles). Paris: OECD Publishing, 2024. URL: https://oecd.ai/en/ai-principles
12. Про затвердження Положення про захист інформації та кіберзахист учасниками платіжного ринку : Постанова Національного банку України від 19.05.2021 № 43. URL: https://zakon.rada.gov.ua/laws/show/v0043500-21.
13. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Гельветика, 2017. 168 с.
14. Council of Europe. Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. Vilnius, 2024. URL: https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence.
15. Холод М., Костенюк Н., Воронов О. Перспективи використання штучного інтелекту в публічному управлінні: вплив на ефективність надання адміністративних послуг, процес ухвалення управлінських рішень та цифрову трансформацію. *Теоретичні та прикладні питання державотворення*. 2024. № 32. С. 307-314. DOI: https://doi.org/10.35432/tisb322024346575.
16. Дудко А. Г. Правове регулювання штучного інтелекту в публічному управлінні: виклики, міжнародний досвід та перспективи для України. *Актуальні проблеми політики*. 2025. Вип. 76. С. 16-21. DOI: https://doi.org/10.32782/app.v76.2025.2.
17. Пацурія Н. Упровадження технологій штучного інтелекту у забезпечення національної безпеки та обороноздатності України: правові проблеми та перспективи повоєнного періоду. *Теорія і практика інтелектуальної власності*. 2023. № 3. С. 68-78. DOI: https://doi.org/10.33731/32023.282185.
18. Стратегія розвитку штучного інтелекту України на період до 2030 року : схвалено розпорядженням Кабінету Міністрів України від 31.12.2024. № 1351-р URL: https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80/ed20241231#Text.
19. Defense AI Center «A1». URL: https://a1.mod.gov.ua/.

20. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO, 2021. URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137.

References

1. Zghurovskyi, M. (2025) *Shtuchnyi intelekt zminiue svit: shansy i vyklyky dlia Ukrainy* [Artificial intelligence is changing the world: Opportunities and challenges for Ukraine]. Available at: https://svit.kpi.ua/2025/01/31/штучний-інтелект-змінює-світ-шанси-і-в/.
2. Huk, O. V., Artemenko, L. P. & Khytrovska, Yu. V. (2024) Istoriia shtuchnoho intelektu v mediabisnesi: etapy rozvytku, osoblyvosti zastosuvannia, vyklyky ta perspektyvy [The history of artificial intelligence in the media business: Development stages, application features, challenges and prospects], *Storinky istorii*, issue 59, pp. 253–278. https://doi.org/10.20535/2307-5244.59.2024.318894.
3. Ministry of Digital Transformation of Ukraine (s.a.) *Shtuchnyi intelekt* [Artificial Intelligence]. Diia. Digital Education. Available at: https://it-osvita.diia.gov.ua/task/item/3ba90df9-79a0-42c6-a793-b4eb5eebeb0e.
4. Great Ukrainian Encyclopedia (s.a.) *Shtuchnyi intelekt* [Artificial Intelligence]. Available at: https://vue.gov.ua/Штучний_інтелект.
5. Cambridge Dictionary (s.a.) *Artificial intelligence*. Available at: https://dictionary.cambridge.org/dictionary/english/artificial-intelligence.
6. Cabinet of Ministers of Ukraine (2020) *Kontseptsiia rozvytku shtuchnoho intelektu v Ukraini* [Concept of artificial intelligence development in Ukraine]. Ordinance of December 2, 2020, No. 1556-r. Available at: https://zakon.rada.gov.ua/laws/show/1556-2020-р.
7. European Parliament & Council of the European Union (2024) *Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union, L 2024/1689. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.
8. President of Ukraine (1998) *Pro zakhody shchodo vprovadzhennia Kontseptsii administratyvnoi reformy v Ukraini* [On measures to implement the Concept of Administrative Reform in Ukraine]. Decree of July 22, 1998, No. 810/98. Available at: https://zakon.rada.gov.ua/laws/show/810/98.
9. Encyclopedia of Modern Ukraine (s.a.) *Derzhavne upravlinnia* [Public administration]. Available at: https://esu.com.ua/article-26159
10. Rubtsov, V. P. & Perynska, N. I. (2008) *Derzhavne upravlinnia ta derzhavni ustanovy* [Public administration and state institutions]. Educational manual. Kyiv: Open International University of Human Development "Ukraine".
11. OECD (2024) *Recommendation of the Council on Artificial Intelligence (OECD AI Principles)*. Paris: OECD Publishing. Available at: https://oecd.ai/en/ai-principles.
12. National Bank of Ukraine (2021) *Pro zatverdzhennia Polozhennia pro zakhyst informatsii ta kiberzakhyst uchasnykamy platizhnoho rynku* [On approval of the Regulation on information protection and cyber defense by payment market participants]. Resolution of May 19, 2021, No. 43. Available at: https://zakon.rada.gov.ua/laws/show/v0043500-21.
13. Nashynets-Naumova, A. Yu. (2017) *Informatsiina bezpeka: pytannia pravovoho rehuliuvannia* [Information security: Legal regulation issues]. Monograph. Kyiv: Helvetica.
14. Council of Europe (2024) *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. Council of Europe Treaty Series, No. 225. Vilnius. Available at: https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence.
15. Kholod, M., Kosteniuk, N. & Voronov, O. (2024) Perspektyvy vykorystannia shtuchnoho intelektu v publichnomu upravlinni: vplyv na efektyvnist nadannia administratyvnykh posluh, protses ukhvalennia upravlinskykh rishen ta tsyfrovu transformatsiiu [Prospects for the use of artificial intelligence in public administration: Impact on the efficiency of providing administrative services, the decision-making process and digital transformation], *Teoretychni ta prykladni pytannia derzhavotvorennia*, no. 32, pp. 307–314. https://doi.org/10.35432/tisb322024346575.
16. Dudko, A. H. (2025) Pravove rehuliuvannia shtuchnoho intelektu v publichnomu upravlinni: vyklyky, mizhnarodnyi dosvid ta perspektyvy dlia Ukrainy [Legal regulation of artificial intelligence in public administration: Challenges, international experience and prospects for Ukraine], *Aktualni problemy polityky*, issue 76, pp. 16–21. https://doi.org/10.32782/app.v76.2025.2.
17. Patsuriia, N. (2023) Uprovadzhennia tekhnolohii shtuchnoho intelektu u zabezpechennia natsionalnoi bezpeky ta oboronozdatnosti Ukrainy: pravovi problemy ta perspektyvy povoiennoho periodu [Implementation of artificial intelligence technologies in ensuring national security and defense capability of Ukraine: Legal problems and prospects of the post-war period], *Teoriia i praktyka intelektualnoi vlasnosti*, no. 3, pp. 68–78. https://doi.org/10.33731/32023.282185.
18. Cabinet of Ministers of Ukraine (2024) *Stratehiia rozvytku shtuchnoho intelektu Ukrainy na mezhuvannia do 2030 roku* [Strategy for the development of artificial intelligence in Ukraine for the period up to 2030]. Ordinance of December 31, 2024, No. 1351-r. Available at: https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80/ed20241231#Text.
19. Ministry of Defence of Ukraine (s.a.) *Defense AI Center "A1"*. Official portal. Available at: https://a1.mod.gov.ua/.
20. UNESCO (2021) *Recommendation on the Ethics of Artificial Intelligence*. Paris: UNESCO. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000381137.

Стаття надійшла до редакції / Received 02.08.2026 **Прийнята до друку / Accepted 14.08.2026**
Опубліковано/ Published 04.09.2026