МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ МЕНЕДЖМЕНТУ ТА ПІДПРИЄМНИЦТВА
КАФЕДРА ПУБЛІЧНОГО УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ

КВАЛІФІКАЦІЙНА РОБОТА

на тему

«Штучний інтелект у системі публічного управління: перспективи впровадження в Україні»

на здобуття освітнього ступеня магістра
зі спеціальності 281 «Публічне управління та адміністрування»
освітньо-професійної програми «Публічне управління та адміністрування»

Кваліфікаційна робота містить результати власних досліджень.
Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Назарій ГАЛИЧ
(підпис)

Виконав: здобувач вищої освіти,
гр. ПУДМ-61
Назарій ГАЛИЧ

Керівник: к.філол.н., доцент
Ліна СТОРОЖЕНКО

Рецензент: к.е.н., доцент
Людмила ПАРІЙ

Київ, 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут менеджменту та підприємництва

Кафедра публічного управління та адміністрування
Ступінь вищої освіти «Магістр»
Спеціальність 281 «Публічне управління та адміністрування»
Освітньо-професійна програма «Публічне управління та адміністрування»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Ірина АНТИПЕНКО
«31» жовтня 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Галича Назарія Сергійовича

1. Тема роботи **«Штучний інтелект у системі публічного управління: перспективи впровадження в Україні»**;
керівник кваліфікаційної роботи – Стороженко Ліна Григорівна, к.філол.н., доцент, затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467.
2. Термін подання кваліфікаційної роботи – «22» грудня 2025 р.
3. Вихідні дані до кваліфікаційної роботи: спеціальна теоретична і методична наукова література; наукові публікації (статті, монографії, дисертаційні дослідження) провідних вітчизняних та закордонних дослідників за темою кваліфікаційної роботи; результати науково-дослідної роботи кафедри публічного управління та адміністрування «Теоретико-прикладні аспекти розвитку цифрової держави в Україні»; нормативно-правові документи; матеріали переддипломної практики.
4. Перелік ілюстративного матеріалу: *презентація*
5. Дата видачі завдання: «27» червня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Структура роботи, вступ	27.06.2025 – 29.08.2025	Виконано
2.	Розділ І	01.09.2025 – 26.09.2025	Виконано
3.	Розділ ІІ	29.09.2025 – 24.10.2025	Виконано
4.	Розділ ІІІ	27.10.2025 – 28.11.2025	Виконано
5.	Висновки, додатки	01.12.2025 – 12.12.2025	Виконано
6.	Презентація	15.12.2025 – 19.12.2025	Виконано

Здобувач вищої освіти _____ Назарій ГАЛИЧ

Керівник
кваліфікаційної роботи _____ Ліна СТОРОЖЕНКО

РЕФЕРАТ

Галич Н.С. Штучний інтелект у системі публічного управління: перспективи впровадження в Україні: кваліф. робота на здобуття освіт. ступеня магістра; спец. 281 «Публічне управління та адміністрування»; Держ. у-т інформац.-комунікац. технолог.; каф. публічного управління та адміністрування; наук. керівник Л.Г. Стороженко, к. філол. н., доц. Київ, 2025. 82 с.

Метою дослідження є комплексний аналіз теоретичних засад, сучасного стану та перспектив впровадження технологій штучного інтелекту у систему публічного управління України з розробкою науково обґрунтованих рекомендацій щодо оптимізації цього процесу.

Об'єкт дослідження – процеси цифровізації системи публічного управління в Україні.

Предмет дослідження – теоретичні засади, сучасний стан, проблеми та перспективи впровадження технологій штучного інтелекту у систему публічного управління України.

Короткий зміст роботи. Розкрито теоретико-методологічні засади штучного інтелекту в державному управлінні, зокрема, з'ясувано сутність, ключові концепції та підходи до інтеграції інтелектуальних технологій у публічний сектор; проаналізовано еволюцію цифрових технологій у публічному управлінні (від електронного урядування до інтелектуального управління, визначивши тенденції диджиталізації та їх вплив на управлінські процеси); досліджено принципи, механізми та інституційно-правові засади впровадження штучного інтелекту у діяльність органів публічної влади, включаючи нормативно-правове забезпечення, регуляторні рамки та моделі прийняття рішень на основі даних; оцінено сучасний стан цифрової трансформації публічної влади в Україні та визначено готовність органів державного управління і державних службовців до використання інтелектуальних систем; ідентифіковано бар'єри, ризики та виклики впровадження штучного інтелекту в державному секторі, а також напрями зміцнення інформаційної безпеки та захисту даних; узагальнено міжнародний досвід та розроблено стратегічні напрями державної політики розвитку штучного інтелекту в публічному секторі України, окресливши вимоги до компетентностей цифрового державного службовця.

Ключові слова: штучний інтелект; інтелектуальне державне управління; цифрова трансформація; публічний сектор; великі дані; цифрові компетентності; електронне урядування; інформаційна безпека; кіберстійкість; державна політика; інституційно-правове забезпечення; ризики та бар'єри впровадження ШІ; етичні стандарти; цифрові платформи; державні електронні сервіси; міжнародний досвід.

ABSTRACT

Halych N. Artificial Intelligence in the Public Administration System: Prospects for Implementation in Ukraine: Master's qualification work; specialty 281 «Public Administration and Management»; State University of Information and Communication Technologies; Department of Public Administration and Management; academic supervisor L. Storozhenko, PhD in Philology, Associate Professor. Kyiv, 2025. 82 p.

The aim of the research is to conduct a comprehensive analysis of the theoretical foundations, current state, and prospects for implementing artificial intelligence technologies in the public administration system of Ukraine, as well as to develop scientifically grounded recommendations for optimizing this process.

Object of the research – the processes of digitalization of the public administration system in Ukraine.

Subject of the research – theoretical foundations, current state, challenges, and prospects for implementing artificial intelligence technologies in the public administration system of Ukraine.

Summary. The work reveals the theoretical and methodological foundations of artificial intelligence in public administration, including the essence, key concepts, and approaches to integrating intelligent technologies into the public sector. It analyzes the evolution of digital technologies in public administration (from e-government to intelligent governance, identifying digitalization trends and their impact on management processes); examines the principles, mechanisms, and institutional-legal frameworks for implementing artificial intelligence in the activities of public authorities, including regulatory provisions, governance frameworks, and data-driven decision-making models. The study evaluates the current state of digital transformation of public authorities in Ukraine and assesses the readiness of public administration bodies and civil servants to use intelligent systems; identifies barriers, risks, and challenges associated with the implementation of artificial intelligence in the public sector, as well as directions for strengthening information security and data protection. It also summarizes international experience and develops strategic directions of state policy for the development of artificial intelligence in Ukraine's public sector, outlining the competencies required of a digital civil servant.

Keywords: artificial intelligence; intelligent public governance; digital transformation; public sector; big data; digital competencies; e-government; information security; cyber resilience; public policy; institutional and legal framework; risks and barriers to AI implementation; ethical standards; digital platforms; state electronic services; international experience.

ЗМІСТ

ВСТУП 6

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СИСТЕМУ ПУБЛІЧНОГО УПРАВЛІННЯ 11

1.1. Сутність і концептуальні підходи до розуміння штучного інтелекту в контексті державного управління 11

1.2. Еволюція цифрових технологій у публічному секторі: від електронного уряду до інтелектуального управління 16

1.3. Принципи інтеграції ШІ у механізми прийняття управлінських рішень 21

РОЗДІЛ 2. СУЧАСНИЙ СТАН ТА ПРОБЛЕМИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ УКРАЇНИ 30

2.1. Сучасний стан цифрової трансформації органів публічної влади в Україні 30

2.2. Зарубіжний досвід використання штучного інтелекту у вітчизняному публічному управлінні (США, ЄС, Південна Корея, Естонія) 36

2.3. Інституційно-правові засади розвитку штучного інтелекту в державному секторі 41

2.4. Основні бар’єри та ризики впровадження ШІ у публічному управлінні (правові, етичні, безпекові) 47

РОЗДІЛ 3. ПЕРСПЕКТИВИ ТА НАПРЯМИ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПУБЛІЧНЕ УПРАВЛІННЯ УКРАЇНИ 53

3.1. Розвиток інформаційної безпеки та захисту даних в умовах використання ШІ 53

3.2. Формування компетентностей цифрового державного службовця як умова ефективного впровадження інтелектуальних технологій 57

3.3. Стратегічні напрями державної політики щодо розвитку ШІ у публічному секторі України 62

ВИСНОВКИ 71

ДОДАТКИ 75

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 76

ВСТУП

Актуальність теми дослідження. Сучасний етап розвитку глобального суспільства характеризується стрімким поширенням цифрових технологій, які докорінно трансформують усі сфери людської діяльності, включаючи систему публічного управління. Штучний інтелект, який ще декілька десятиліть тому сприймався як футуристична концепція, сьогодні стає невід'ємною складовою державного апарату провідних країн світу. Технології машинного навчання, обробки великих даних, комп'ютерного зору та природної мови відкривають принципово нові можливості для підвищення ефективності, прозорості та якості надання публічних послуг.

Четверта промислова революція, концептуалізована К. Швабом, передбачає конвергенцію фізичних, цифрових та біологічних технологій, що створює фундаментально нову парадигму суспільного розвитку. У цьому контексті впровадження штучного інтелекту у систему публічного управління виступає не лише технологічним викликом, а й стратегічним завданням, від успішності виконання якого залежить конкурентоспроможність держави у глобальному просторі. Провідні міжнародні організації, зокрема ОЕСР, Європейська комісія, ЮНЕСКО, визнають штучний інтелект ключовим драйвером цифрової трансформації публічного сектору та розробляють відповідні рекомендації щодо етичного та відповідального його використання.

Для України питання впровадження технологій штучного інтелекту у систему публічного управління набуває особливої актуальності в контексті кількох взаємопов'язаних чинників. По-перше, євроінтеграційний курс держави передбачає гармонізацію вітчизняних стандартів цифрового врядування з європейськими нормами, що зафіксовано у низці стратегічних документів, зокрема Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки. По-друге, масштабна цифрова трансформація, яка реалізується Міністерством цифрової трансформації України через ініціативи «Держава у смартфоні» та екосистему «Дія», створила технологічну основу

для інтеграції інтелектуальних систем у процеси державного управління. По-третє, воєнний стан, спричинений російською агресією, продемонстрував критичну важливість цифрової інфраструктури для забезпечення безперервності функціонування державних органів та надання послуг громадянам в умовах надзвичайних ситуацій.

Прийняття у 2020 році Концепції розвитку штучного інтелекту в Україні засвідчило усвідомлення державою стратегічного значення цієї технології та необхідності формування комплексної політики щодо її розвитку. Однак реалізація амбітних цілей, визначених у Концепції, стикається з численними викликами інституційного, правового, технологічного, кадрового та етичного характеру. Відсутність чіткої нормативно-правової бази, яка б регулювала використання систем штучного інтелекту у прийнятті управлінських рішень, обмеженість фінансових ресурсів, дефіцит фахівців з необхідними компетентностями, проблеми забезпечення кібербезпеки та захисту персональних даних створюють суттєві бар'єри на шляху цифровізації публічного сектору.

Водночас зарубіжний досвід демонструє значний потенціал використання штучного інтелекту для оптимізації державного управління. Естонія, яка визнана світовим лідером у сфері електронного урядування, успішно інтегрувала інтелектуальні системи у платформу X-Road, що забезпечує безпечний обмін даними між різними державними реєстрами. Сінгапур реалізує стратегію «Smart Nation», спрямовану на створення інтелектуального міста-держави з використанням штучного інтелекту та Інтернету речей. Сполучені Штати Америки розробили федеральну стратегію штучного інтелекту, яка визначає пріоритетні напрями використання цієї технології для посилення національної безпеки та конкурентоспроможності. Європейський Союз прийняв Акт про штучний інтелект, який встановлює гармонізовані правила регулювання систем ШІ з урахуванням ризиків, що вони створюють.

Стан розроблення теми. Аналіз наукового дискурсу свідчить про зростання інтересу вітчизняних та зарубіжних дослідників до проблематики впровадження штучного інтелекту у публічне управління. Теоретичні аспекти цифровізації державного сектору розглядаються у працях Дрешпака В. М., Клименка І. В., Грицяк Н. В., Семенченка А. І. [26; 27; 28; 69]. Технологічні можливості та виклики застосування штучного інтелекту досліджують Чукут С. А., Карчевський М. В., Баранов О. А. [5; 6; 24; 23]. Міжнародний досвід цифрової трансформації аналізують Wirtz B. W., Zuiderwijk A., Dawes S. S., Gil-Garcia J. R. [48; 49; 50; 51]. Питання інформаційної безпеки та захисту даних висвітлюють Золотар О. О., Швець М. Я. [55; 56]. Водночас комплексні дослідження, які б системно охоплювали теоретико-методологічні засади, практичні аспекти та перспективи впровадження штучного інтелекту саме у систему публічного управління України з урахуванням сучасних реалій, залишаються обмеженими.

Недостатня розробленість теоретичних засад інтеграції штучного інтелекту у механізми державного управління, фрагментарність емпіричних досліджень готовності вітчизняного публічного сектору до використання інтелектуальних систем, необхідність узагальнення міжнародного досвіду та розробки практичних рекомендацій щодо адаптації кращих практик до українських реалій зумовлюють актуальність обраної теми дослідження.

Мета і завдання дослідження. Метою дослідження є комплексний аналіз теоретичних засад, сучасного стану та перспектив впровадження технологій штучного інтелекту у систему публічного управління України з розробкою науково обґрунтованих рекомендацій щодо оптимізації цього процесу.

Для досягнення поставленої мети визначено наступні завдання:

- розкрити теоретико-методологічні засади штучного інтелекту в державному управлінні, зокрема з’ясувати сутність, ключові концепції та підходи до інтеграції інтелектуальних технологій у публічний сектор;

- проаналізувати еволюцію цифрових технологій у публічному управлінні – від електронного урядування до інтелектуального управління, визначивши тенденції діджиталізації та їх вплив на управлінські процеси;
- дослідити принципи, механізми та інституційно-правові засади впровадження штучного інтелекту у діяльність органів публічної влади, включаючи нормативно-правове забезпечення, регуляторні рамки та моделі прийняття рішень на основі даних;
- оцінити сучасний стан цифрової трансформації публічної влади в Україні та визначити готовність органів державного управління і державних службовців до використання інтелектуальних систем;
- ідентифікувати бар'єри, ризики та виклики впровадження штучного інтелекту в державному секторі, а також напрями зміцнення інформаційної безпеки та захисту даних;
- узагальнити міжнародний досвід та розробити стратегічні напрями державної політики розвитку штучного інтелекту в публічному секторі України, окресливши вимоги до компетентностей цифрового державного службовця.

Об'єкт дослідження – процеси цифровізації системи публічного управління в Україні.

Предмет дослідження – теоретичні засади, сучасний стан, проблеми та перспективи впровадження технологій штучного інтелекту у систему публічного управління України.

Методи дослідження. Для досягнення мети дослідження та вирішення поставлених завдань використано комплекс загальнонаукових та спеціальних методів пізнання. Системний підхід застосовано для комплексного аналізу штучного інтелекту як елемента системи публічного управління та визначення взаємозв'язків між технологічними, інституційними, правовими та соціальними аспектами його впровадження. Структурно-функціональний аналіз використано для дослідження еволюції цифрових технологій у

публічному секторі та визначення функціональних можливостей штучного інтелекту у різних сферах державного управління. Порівняльний метод застосовано для зіставлення досвіду впровадження штучного інтелекту у публічне управління різних країн світу та виявлення кращих практик, придатних для адаптації в українських умовах. Нормативно-правовий аналіз використано для дослідження інституційно-правових засад розвитку штучного інтелекту в державному секторі України та виявлення прогалин у законодавчому регулюванні. Метод експертних оцінок застосовано для аналізу готовності державних службовців до використання інтелектуальних систем. SWOT-аналіз використано для визначення сильних і слабких сторін, можливостей та загроз впровадження штучного інтелекту у вітчизняне публічне управління.

Структура роботи. Дослідження складається зі вступу, трьох розділів, висновків, додатку та списку використаних джерел. Загальний обсяг роботи складає 82 сторінок. Список використаних джерел нараховує 70 позицій.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СИСТЕМУ ПУБЛІЧНОГО УПРАВЛІННЯ

1.1. Сутність і концептуальні підходи до розуміння штучного інтелекту в контексті державного управління

Штучний інтелект як феномен сучасної науки і технології має багатогранну природу, що зумовлює множинність підходів до визначення його сутності. У найширшому розумінні штучний інтелект являє собою галузь інформатики, яка займається створенням комп'ютерних систем, здатних виконувати завдання, що традиційно вимагають людського інтелекту. Класичне визначення, запропоноване у фундаментальній праці Рассела та Норвіга, характеризує штучний інтелект як вивчення і конструювання раціональних агентів, які сприймають своє середовище і здійснюють дії, що максимізують шанси на успішне досягнення їхніх цілей [62].

Концептуалізація штучного інтелекту в академічному дискурсі відбувається через призму кількох взаємодоповнюючих підходів. Перший підхід фокусується на когнітивних здібностях систем і визначає штучний інтелект як здатність машин імітувати розумову діяльність людини, зокрема навчання, міркування, розв'язання проблем, сприйняття та розуміння природної мови. Другий підхід наголошує на функціональних можливостях і розглядає штучний інтелект як сукупність технологій, що дозволяють комп'ютерним системам аналізувати складні дані, розпізнавати закономірності, робити прогнози та приймати рішення з мінімальним втручанням людини [10].

У контексті публічного управління штучний інтелект набуває специфічного значення як інструмент підвищення ефективності, прозорості та якості державних послуг. Вітчизняна дослідниця С. А. Чукут визначає штучний інтелект у публічному управлінні як комплекс інтелектуальних технологій, що дозволяють автоматизувати процеси збору, обробки та аналізу

великих обсягів даних, оптимізувати прийняття управлінських рішень та персоналізувати взаємодію держави з громадянами [5].

Сучасні системи штучного інтелекту базуються на декількох ключових технологіях, кожна з яких має специфічне застосування у сфері державного управління. Машинне навчання (machine learning) являє собою підгалузь штучного інтелекту, що дозволяє комп'ютерним системам автоматично вдосконалюватися через досвід без явного програмування [67]. Ця технологія знаходить застосування у прогнозній аналітиці, виявленні аномалій у фінансових операціях державних установ, оптимізації розподілу бюджетних ресурсів.

Глибоке навчання (deep learning) як підмножина машинного навчання використовує багатошарові нейронні мережі для обробки складних структурованих і неструктурованих даних. Організація економічного співробітництва та розвитку у своєму звіті підкреслює, що системи глибокого навчання здатні аналізувати текстові документи, зображення, відео та аудіоматеріали, що відкриває можливості для автоматизації адміністративних процедур, моніторингу дотримання законодавства, аналізу громадської думки через соціальні мережі.

Обробка природної мови (natural language processing) дозволяє комп'ютерним системам розуміти, інтерпретувати та генерувати людську мову. У публічному секторі ця технологія використовується для створення чат-ботів, що надають консультації громадянам, автоматичного аналізу звернень до державних органів, перекладу документів, підготовки узагальнених звітів на основі великих текстових масивів.

Комп'ютерний зір (computer vision) надає системам здатність інтерпретувати візуальну інформацію з цифрових зображень та відео. Ця технологія застосовується для розпізнавання осіб у системах контролю доступу, аналізу супутникових знімків для моніторингу землекористування, автоматичної обробки документів, контролю дотримання правил дорожнього руху.

Експертні системи як один з ранніх напрямів розвитку штучного інтелекту продовжують відігравати важливу роль у державному управлінні. Вони використовують базу знань експертів певної предметної області та механізм логічного висновку для розв'язання складних задач, що потребують спеціалізованих знань. У публічному секторі експертні системи застосовуються для податкового консультування, оцінки ризиків у регуляторній діяльності, прийняття рішень про надання соціальних виплат.

Концептуальне розуміння штучного інтелекту в контексті державного управління передбачає усвідомлення його двоїстої природи. З одного боку, штучний інтелект є технологічним інструментом, що розширює можливості державних службовців у виконанні їхніх функцій. З іншого боку, він виступає як агент трансформації, що змінює саму логіку функціонування публічного сектору, переосмислює взаємовідносини між державою та громадянами, створює нові форми політичної участі та громадського контролю.

Важливим аспектом концептуалізації штучного інтелекту у публічному управлінні є розрізнення між слабким (вузьким) та сильним (загальним) штучним інтелектом. Слабкий штучний інтелект спеціалізується на виконанні конкретних завдань у чітко визначених межах і саме цей тип систем знаходить сьогодні практичне застосування в державному секторі. Сильний штучний інтелект, який би володів загальними когнітивними здібностями, порівнянними з людськими, залишається теоретичною концепцією і не має безпосереднього відношення до поточної практики публічного управління [62].

У контексті публічного управління доцільно виділити три рівні застосування штучного інтелекту. Перший рівень – операційний – передбачає використання інтелектуальних систем для автоматизації рутинних адміністративних процедур, обробки документів, обслуговування громадян. Другий рівень – аналітичний – охоплює застосування штучного інтелекту для аналізу даних, виявлення закономірностей, прогнозування соціально-економічних процесів, підготовки рекомендацій для прийняття управлінських

рішень. Третій рівень, стратегічний, стосується використання потенціалу штучного інтелекту для моделювання складних сценаріїв розвитку, оцінки впливу політичних рішень, формування довгострокових стратегій розвитку [49].

Український дослідник М. В. Карчевський наголошує, що штучний інтелект у публічному управлінні слід розглядати не як самоціль, а як засіб досягнення фундаментальних цілей державного управління – забезпечення добробуту громадян, захисту їхніх прав і свобод, ефективного використання публічних ресурсів, підвищення якості та доступності державних послуг [24].

Концептуальне осмислення штучного інтелекту в публічному секторі передбачає також врахування етичного виміру його використання. ЮНЕСКО у своїх рекомендаціях з етики штучного інтелекту підкреслює необхідність дотримання принципів поваги до прав людини, справедливості, недискримінації, прозорості, підзвітності, безпеки та конфіденційності при розробці та впровадженні інтелектуальних систем [46].

Особливу увагу в академічному дискурсі приділяють феномену алгоритмічного управління (algorithmic governance), коли рішення, що впливають на права та інтереси громадян, повністю або частково приймаються автоматизованими системами на основі алгоритмів штучного інтелекту. Це породжує питання легітимності, підзвітності та можливості оскарження таких рішень, що потребує перегляду традиційних правових концепцій адміністративного права.

Штучний інтелект у державному управлінні також слід розглядати через призму концепції інформаційного суспільства та цифрової економіки. Дослідниця С. В. Коляденко зазначає, що штучний інтелект є ключовим елементом цифрової трансформації економіки та суспільства, що створює нову парадигму взаємодії між технологіями, економічними процесами та соціальними інститутами [8].

Важливим аспектом концептуального розуміння штучного інтелекту в публічному управлінні є усвідомлення його впливу на трансформацію адміністративних процесів. Традиційна бюрократична модель, заснована на ієрархії, формалізації процедур та людському прийнятті рішень, поступається місцем більш гнучким, мережевим формам організації, де штучний інтелект виступає як координуючий та оптимізуючий механізм.

Концептуалізація штучного інтелекту у контексті державного управління також передбачає розуміння його ролі у реалізації принципів належного врядування (good governance). Інтелектуальні системи можуть сприяти підвищенню прозорості через автоматичне оприлюднення інформації, посиленню підзвітності через моніторинг діяльності державних органів, забезпеченню участі громадян через цифрові платформи громадського обговорення, підвищенню ефективності через оптимізацію використання ресурсів.

Водночас необхідно усвідомлювати обмеження штучного інтелекту у сфері публічного управління. Інтелектуальні системи функціонують на основі даних, алгоритмів та обчислювальної потужності, але позбавлені здатності до етичних суджень, розуміння соціального контексту, врахування унікальних індивідуальних обставин, що робить неможливим повну заміну людського фактору у прийнятті управлінських рішень, особливо тих, що стосуються фундаментальних прав людини [65].

Таким чином, сутність штучного інтелекту в контексті державного управління полягає у його здатності розширювати когнітивні можливості державних інституцій через обробку великих обсягів даних, виявлення складних закономірностей, автоматизацію рутинних операцій та підтримку прийняття обґрунтованих рішень, при цьому залишаючись інструментом, який доповнює, а не замінює людський інтелект і відповідальність у сфері публічного управління.

1.2. Еволюція цифрових технологій у публічному секторі: від електронного уряду до інтелектуального управління

Трансформація публічного сектору під впливом інформаційно-комунікаційних технологій є еволюційним процесом, який пройшов кілька якісно відмінних етапів розвитку. Розуміння цієї еволюції є необхідною передумовою для осмислення місця та ролі штучного інтелекту в сучасній системі державного управління.

Початковий етап цифровізації публічного сектору, який розпочався наприкінці XX століття, характеризувався простою автоматизацією окремих адміністративних процесів та створенням базових інформаційних систем для внутрішнього використання державними органами. Цей період можна охарактеризувати як етап інформатизації, коли основною метою було перенесення паперових документів у цифровий формат та впровадження техніки у діяльність державних установ.

Наступним етапом стало формування концепції електронного уряду (e-government), яка набула широкого розповсюдження на початку 2000-х років. Дослідники С. Доус визначає електронний уряд як використання інформаційних технологій, зокрема Інтернету, для надання державних послуг громадянам та бізнесу більш ефективним, зручним та прозорим способом [50].

Концепція електронного уряду базувалася на кількох ключових принципах. По-перше, це орієнтація на користувача, що передбачала проектування електронних послуг з урахуванням потреб та можливостей громадян. По-друге, принцип «єдиного вікна», згідно з яким громадянин має отримувати послугу без необхідності звертатися до різних відомств. По-третє, принцип інтероперабельності, що означає здатність різних інформаційних систем обмінюватися даними та ефективно взаємодіяти [51].

Еволюція електронного уряду відбувалася через послідовне проходження кількох стадій зрілості. Перша стадія (інформаційна присутність) передбачала створення веб-сайтів державних органів з базовою

інформацією для громадян. Друга стадія (односторонню взаємодію) характеризувалася можливістю завантажити форми та документи з веб-сайту. Третя стадія (двостороння взаємодія) дозволяла громадянам не лише отримувати інформацію, але й надсилати заповнені форми в електронному вигляді. Четверта стадія (транзакції) означала можливість повного виконання послуги онлайн, включаючи оплату. П'ята стадія (безшовна інтеграція) передбачала повну інтеграцію всіх державних послуг через єдиний портал [52].

В Україні розвиток електронного урядування набув інституційного оформлення з прийняттям у 2018 році Концепції розвитку цифрової економіки та суспільства, яка визначила стратегічні напрями цифровізації державного сектору [1]. Важливою віхою стало створення Міністерства цифрової трансформації України у 2019 році, що засвідчило політичну волю до системної цифровізації публічного управління [22].

Паралельно з концепцією електронного уряду розвивалася ідея електронної демократії (e-democracy), яка передбачала використання цифрових технологій для розширення політичної участі громадян, підвищення прозорості та підзвітності влади. Вітчизняні дослідники Н. В. Грицяк та С. Г. Соловйов визначають електронну демократію як форму організації суспільно-політичної діяльності громадян, яка забезпечує їхню широку участь у державних та громадських справах на основі використання інформаційно-комунікаційних технологій [69].

Наступним етапом еволюції став перехід до концепції електронного врядування (e-governance), яка є ширшою за обсягом порівняно з електронним урядом. Якщо електронний уряд фокусується переважно на наданні послуг та взаємодії з громадянами, то електронне врядування охоплює всі аспекти використання інформаційних технологій для вдосконалення процесів управління, включаючи формування політики, прийняття рішень, залучення стейкхолдерів, міжвідомчу координацію.

Важливою характеристикою сучасного етапу розвитку є перехід від електронного уряду до цифрового уряду (digital government). Дослідник Т. Яновські визначає цифровий уряд як використання цифрових технологій як інтегральної частини стратегій модернізації уряду для створення публічної цінності, з акцентом на даних, цифрових послугах та цифрових навичках [52].

Ключовою відмінністю цифрового уряду від електронного є зміщення фокусу з простої автоматизації існуючих процесів на їх фундаментальне переосмислення та трансформацію з урахуванням можливостей цифрових технологій. Цифровий уряд характеризується наступними ознаками: орієнтація на дані як стратегічний актив, проактивне надання послуг на основі аналізу потреб громадян, персоналізація взаємодії, використання мобільних технологій, застосування хмарних обчислень, впровадження штучного інтелекту та аналітики великих даних.

Практичним втіленням концепції цифрового уряду в Україні стала державна програма «Держава у смартфоні» та створення екосистеми «Дія», яка об’єднує мобільний застосунок, веб-портал та освітню платформу [33]. Мобільний застосунок «Дія» дозволяє громадянам використовувати цифрові документи, отримувати понад 50 державних послуг онлайн, взаємодіяти з державними органами без необхідності фізичної присутності [35].

Еволюція цифрових технологій у публічному секторі тісно пов’язана з технологічними інноваціями. Впровадження технології блокчейн відкриває можливості для створення розподілених реєстрів, що підвищують прозорість та захищеність даних, забезпечують незмінність записів, дозволяють здійснювати транзакції без посередників [68]. Інтернет речей створює інфраструктуру для «розумних міст», де датчики та пристрої збирають дані про стан навколишнього середовища, транспортні потоки, споживання ресурсів, що дозволяє оптимізувати міське управління.

Особливе місце в еволюції цифрових технологій посідає концепція відкритих даних (open data), згідно з якою державні органи оприлюднюють масиви даних у машиночитному форматі для вільного використання

громадянами, бізнесом, дослідниками. Відкриті дані сприяють підвищенню прозорості влади, стимулюють інновації, дозволяють громадському сектору здійснювати моніторинг діяльності державних органів [70].

Четверта промислова революція, концептуалізована К. Швабом, характеризується конвергенцією технологій, що розмиває межі між фізичною, цифровою та біологічною сферами [64]. У контексті публічного управління це означає інтеграцію штучного інтелекту, робототехніки, Інтернету речей, блокчейну, хмарних обчислень у єдину екосистему, що створює якісно нову парадигму державного управління.

Сучасний етап еволюції можна охарактеризувати як перехід до інтелектуального управління (intelligent governance), де штучний інтелект та аналітика великих даних стають центральними елементами системи прийняття рішень. Інтелектуальне управління передбачає не просто реагування на запити громадян, а проактивне передбачення їхніх потреб, автоматичне виявлення проблем, що потребують втручання держави, оптимізацію розподілу ресурсів на основі прогнозних моделей.

Приклади інтелектуального управління можна побачити у провідних країнах світу. Естонія використовує штучний інтелект для автоматичного виявлення шахрайства у податковій системі, прогнозування потреби у соціальних послугах, оптимізації роботи системи охорони здоров’я. Сінгапур реалізує концепцію «Smart Nation», де штучний інтелект застосовується для управління транспортними потоками, моніторингу стану інфраструктури, персоналізації державних послуг [45].

Важливою характеристикою інтелектуального управління є перехід від дискретних електронних послуг до безшовних життєвих подій (life events). Замість того, щоб громадянин звертався за окремими послугами при настанні певної життєвої події (народження дитини, зміна місця проживання, відкриття бізнесу), держава автоматично надає комплекс необхідних послуг, використовуючи дані з різних реєстрів та аналітику на основі штучного інтелекту [49].

Еволюція цифрових технологій у публічному секторі також супроводжується трансформацією організаційних моделей державного управління. Традиційна ієрархічна бюрократична модель поступається місцем мережевим структурам, де різні державні органи, приватний сектор, громадянське суспільство взаємодіють через цифрові платформи для спільного вирішення суспільних проблем.

Однак еволюція до інтелектуального управління не є лінійним процесом і супроводжується численними викликами. Дослідниця А. Зейдервейк зазначає, що впровадження штучного інтелекту у публічному секторі вимагає не лише технологічних інвестицій, але й організаційних змін, розвитку нових компетентностей, переосмислення нормативно-правової бази, забезпечення етичності та підзвітності алгоритмічних рішень [49].

Український контекст еволюції цифрових технологій характеризується певною специфікою. З одного боку, Україна демонструє високий рівень цифрової грамотності населення, наявність потужного ІТ-сектору, політичну волю до цифровізації. З іншого боку, обмеженість фінансових ресурсів, фрагментарність інформаційних систем державних органів, недосконаліть нормативно-правової бази створюють перешкоди для системної цифрової трансформації.

Важливим елементом сучасного етапу є розуміння даних як стратегічного активу держави. Доповідь Світового банку підкреслює, що дані є ключовим ресурсом для економічного розвитку, соціального прогресу, інновацій, але їх потенціал може бути реалізований лише за умови належного регулювання, захисту прав на приватність, забезпечення якості та доступності [47].

Еволюція від електронного уряду до інтелектуального управління супроводжується також зміною парадигми взаємовідносин між державою та громадянами. Громадянин перестає бути пасивним отримувачем послуг і стає активним учасником процесу державного управління через цифрові

платформи участі, краудсорсингові ініціативи, спільне створення публічних сервісів.

Таким чином, еволюція цифрових технологій у публічному секторі від інформатизації через електронний уряд до інтелектуального управління є послідовним процесом якісних трансформацій, кожний етап якого характеризується специфічними технологіями, організаційними моделями та цілями, при цьому сучасний етап впровадження штучного інтелекту знаменує перехід до принципово нової парадигми проактивного, персоналізованого та ефективного публічного управління, заснованого на даних та інтелектуальних технологіях.

1.3. Принципи інтеграції ШІ у механізми прийняття управлінських рішень

Інтеграція штучного інтелекту у механізми прийняття управлінських рішень у публічному секторі потребує дотримання комплексу принципів, які забезпечують ефективність, легітимність, етичність та підзвітність використання інтелектуальних систем. Ці принципи формуються на перетині технологічних можливостей, правових норм, етичних цінностей та управлінських практик.

Фундаментальним принципом є антропоцентричність, згідно з яким системи штучного інтелекту мають служити людині та суспільству, а не замінювати людський розсуд у прийнятті рішень, що впливають на фундаментальні права і свободи [39]. Рекомендації Організації економічного співробітництва та розвитку наголошують, що штучний інтелект повинен приносити користь людям та планеті, сприяючи інклюзивному зростанню, сталому розвитку та добробуту [37].

Принцип прозорості передбачає, що процес прийняття рішень за допомогою систем штучного інтелекту має бути зрозумілим для тих, кого ці рішення стосуються. Це означає необхідність пояснюваності алгоритмів,

розкриття інформації про дані, які використовуються для навчання моделей, критерії прийняття рішень, обмеження системи. Однак принцип прозорості стикається з технологічними обмеженнями, оскільки деякі типи моделей машинного навчання, зокрема глибокі нейронні мережі, є «чорними скриньками», логіка роботи яких важко піддається інтерпретації.

Принцип підзвітності вимагає чіткого визначення відповідальності за рішення, прийняті за допомогою систем штучного інтелекту. Навіть якщо рішення генерується автоматично, має існувати людина або організація, які несуть юридичну та моральну відповідальність за це рішення та його наслідки [65]. У контексті публічного управління це означає, що державний службовець не може перекладати відповідальність на алгоритм, а повинен мати можливість та обов'язок перевірити, зрозуміти та, за необхідності, скоригувати автоматично згенероване рішення.

Принцип справедливості та недискримінації є критично важливим для публічного сектору. Системи штучного інтелекту не повинні дискримінувати людей на основі раси, статі, віку, інвалідності, соціального статусу чи інших ознак. Проблема полягає у тому, що алгоритми можуть відтворювати та навіть посилювати існуючі у суспільстві упередження, якщо навчальні дані містять історичні дисбаланси або якщо модель спроектована без урахування потенційних джерел упередженості. Дослідження показують, що алгоритми, які використовуються для прогнозування рецидивів злочинів, оцінки кредитоспроможності, відбору кандидатів на посади, можуть систематично дискримінувати певні групи населення [48].

Принцип безпеки та стійкості вимагає, щоб системи штучного інтелекту функціонували надійно протягом усього життєвого циклу, були захищені від кібератак, випадкових збоїв, маніпуляцій. У публічному секторі, де рішення можуть стосуватися життя та здоров'я людей, національної безпеки, критичної інфраструктури, вимоги до безпеки систем є особливо високими. Це передбачає необхідність ретельного тестування систем перед впровадженням,

постійного моніторингу їх роботи, наявності механізмів швидкого реагування на виявлення проблем.

Принцип конфіденційності та захисту персональних даних набуває особливого значення в умовах, коли системи штучного інтелекту потребують великих обсягів даних для навчання та функціонування. Європейський Союз встановив жорсткі вимоги до обробки персональних даних через Загальний регламент про захист даних (GDPR), який надає громадянам право знати, які дані про них збираються, як вони використовуються, право на видалення даних, право заперечувати проти автоматизованого прийняття рішень [56]. Україна рухається шляхом гармонізації свого законодавства з європейськими стандартами, що зафіксовано у Законі «Про захист персональних даних».

Принцип пропорційності передбачає, що використання систем штучного інтелекту має бути адекватним цілям, які переслідуються, і не повинно створювати надмірних ризиків або обмежень прав людини. Європейський Акт про штучний інтелект запроваджує ризик-орієнтований підхід, класифікуючи системи ШІ за рівнями ризику від неприйнятного (заборонено), високого (суворе регулювання), обмеженого (певні вимоги) до мінімального (без спеціального регулювання).

Принцип людського нагляду означає, що критично важливі рішення не можуть прийматися виключно автоматизованими системами без можливості втручання людини [65]. Це передбачає проектування систем з урахуванням механізмів «human-in-the-loop» (людина в циклі), «human-on-the-loop» (людина контролює цикл) або «human-in-command» (людина командує), залежно від рівня критичності рішень. У публічному управлінні це особливо актуально для рішень, що стосуються надання чи відмови у соціальній допомозі, притягнення до відповідальності, обмеження прав.

Принцип технологічної нейтральності означає, що регулювання має фокусуватися на цілях та результатах, а не на конкретних технологіях [27]. Це дозволяє уникнути ситуації, коли нормативно-правова база швидко застаріває

через технологічний прогрес, та забезпечує гнучкість у виборі технологічних рішень залежно від конкретних потреб та можливостей.

Принцип інтероперабельності передбачає, що системи штучного інтелекту різних державних органів мають бути здатними обмінюватися даними та ефективно взаємодіяти. Естонський досвід створення платформи X-Road демонструє важливість забезпечення технічної, семантичної та організаційної інтероперабельності для реалізації принципу «один раз» (once-only principle), згідно з яким громадянин надає інформацію державі лише один раз, а далі вона автоматично використовується різними відомствами.

Принцип доступності означає, що переваги використання штучного інтелекту у публічному управлінні мають бути доступні для всіх громадян, незалежно від їх технологічних можливостей, цифрової грамотності, соціально-економічного статусу, що вимагає забезпечення альтернативних (не цифрових) каналів доступу до послуг для тих, хто не має можливості або не бажає користуватися цифровими сервісами, а також проектування інтерфейсів з урахуванням потреб людей з інвалідністю.

Принцип ефективності використання ресурсів передбачає, що впровадження систем штучного інтелекту має приносити вимірні переваги, які виправдовують інвестиції [36]. Це вимагає проведення аналізу вигод та витрат, визначення ключових показників ефективності, регулярної оцінки результативності впровадження. У публічному секторі, де ресурси обмежені і підлягають суспільному контролю, обґрунтування економічної доцільності інвестицій у штучний інтелект є особливо важливим.

Принцип участі та консультацій означає, що розробка та впровадження систем штучного інтелекту у публічному секторі мають здійснюватися з залученням широкого кола стейкхолдерів – громадян, експертів, громадських організацій, бізнесу. Це забезпечує легітимність рішень, дозволяє врахувати різноманітні перспективи та потреби, сприяє формуванню суспільної довіри до інтелектуальних систем.

Принцип поетапності впровадження передбачає, що інтеграція штучного інтелекту має здійснюватися поступово, починаючи з пілотних проектів у контрольованих умовах, з ретельною оцінкою результатів перед масштабуванням. Це дозволяє мінімізувати ризики, виявити та усунути проблеми на ранніх етапах, адаптувати систему до специфіки українського контексту.

Принцип неперервного навчання та вдосконалення визнає, що системи штучного інтелекту не є статичними продуктами, а потребують постійного моніторингу, оновлення, перенавчання на нових даних [67]. У публічному управлінні це означає необхідність створення процесів та виділення ресурсів для підтримки та розвитку систем протягом їх життєвого циклу.

Принцип збалансованості автоматизації та експертизи передбачає розумне поєднання можливостей штучного інтелекту та людської експертизи [62]. Системи ШІ мають використовуватися там, де вони демонструють переваги – обробка великих обсягів даних, виявлення складних закономірностей, виконання рутинних операцій, але остаточні рішення у складних випадках, що потребують врахування унікального контексту, етичних міркувань, соціальних наслідків, мають прийматися людьми.

Принцип відкритості та повторного використання передбачає, що розроблені державним сектором алгоритми, дані, системи штучного інтелекту за можливості мають бути відкритими для громадськості. Це сприяє прозорості, дозволяє незалежним дослідникам перевіряти системи на наявність упередженості чи помилок, стимулює інновації через повторне використання публічних наробок приватним сектором.

Принцип етичної рефлексії вимагає, щоб на всіх етапах розробки та впровадження систем штучного інтелекту здійснювалася оцінка етичних наслідків, зокрема впливу на права людини, справедливість, приватність, автономію особистості. ЮНЕСКО рекомендує створення етичних комітетів або призначення відповідальних осіб для проведення такої оцінки.

Принцип сталого розвитку означає, що використання штучного інтелекту має враховувати не лише економічні та соціальні цілі, але й екологічні наслідки [64]. Навчання великих моделей машинного навчання потребує значних обчислювальних ресурсів та енергії, що створює екологічний слід. Тому при виборі технологічних рішень необхідно враховувати їх енергоефективність та внесок у досягнення цілей сталого розвитку.

Принцип правової визначеності передбачає, що використання штучного інтелекту у публічному управлінні має здійснюватися на основі чіткої нормативно-правової бази, яка визначає повноваження, обов'язки, відповідальність, процедури оскарження. Дослідниця І. Є. Тімошенко наголошує на необхідності розробки спеціального законодавства, яке б регулювало використання систем штучного інтелекту у публічному секторі з урахуванням специфіки цієї сфери [4].

Принцип адаптивності та гнучкості визнає, що технології штучного інтелекту швидко розвиваються, тому системи регулювання та управління мають бути здатними адаптуватися до змін. Це може передбачати використання регуляторних пісочниць (regulatory sandboxes), де нові технології можуть тестуватися в контрольованому середовищі з тимчасовим послабленням деяких регуляторних вимог.

Практична реалізація цих принципів вимагає їх операціоналізації через конкретні процедури, стандарти, інструменти [39]. Європейська комісія розробила рамкові настанови з етики штучного інтелекту, які включають вимоги щодо оцінки впливу на права людини, технічної стійкості, якості даних, прозорості, різноманітності команд розробників, механізмів підзвітності.

Важливим аспектом інтеграції штучного інтелекту є створення системи управління ризиками, яка б дозволяла ідентифікувати, оцінювати та мітигувати ризики, пов'язані з використанням інтелектуальних систем. Це включає технічні ризики (помилки алгоритмів, збої системи), соціальні ризики

(дискримінація, маргіналізація певних груп), етичні ризики (порушення приватності, автономії), правові ризики (невизначеність відповідальності), політичні ризики (зловживання технологіями для контролю за населенням).

Інтеграція штучного інтелекту у механізми прийняття рішень також вимагає перегляду організаційних процесів та культури державних органів. Традиційна бюрократична культура, що характеризується ієрархією, формалізмом, схильністю до уникнення ризиків, може виявитися несумісною з гнучким, ітеративним, експериментальним підходом, необхідним для успішного впровадження інтелектуальних технологій.

Важливою передумовою успішної інтеграції є розвиток компетентностей державних службовців, які мають працювати з системами штучного інтелекту [60]. Це включає не лише технічні навички роботи з конкретними системами, але й розуміння принципів роботи алгоритмів машинного навчання, усвідомлення їх можливостей та обмежень, здатність критично оцінювати автоматично згенеровані рекомендації, навички роботи з даними.

Принципи інтеграції штучного інтелекту мають також враховувати специфічний контекст України. Воєнний стан створює додаткові виклики щодо забезпечення кібербезпеки критичних систем, захисту від зовнішніх втручань, забезпечення безперервності функціонування державних сервісів в умовах атак на інфраструктуру [54]. Водночас він демонструє можливості швидкої цифровізації та інновацій в умовах кризи.

Міжнародний досвід показує, що країни використовують різні моделі регулювання штучного інтелекту – від м’якого саморегулювання до жорсткого законодавчого регулювання. Вибір моделі залежить від правової традиції, рівня розвитку технологій, культурних цінностей, готовності суспільства до сприйняття інновацій. Для України доцільним є орієнтування на європейську модель, яка поєднує стимулювання інновацій з надійним захистом прав людини.

Таким чином, інтеграція штучного інтелекту у механізми прийняття управлінських рішень має базуватися на комплексі взаємопов'язаних принципів, які забезпечують баланс між технологічними можливостями та етичними, правовими, соціальними вимогами, при цьому ключовим є принцип антропоцентричності, згідно з яким технології мають служити людині та суспільству, а не навпаки, і остаточна відповідальність за рішення завжди залишається за людиною.

Отже, теоретичний аналіз засад впровадження штучного інтелекту у систему публічного управління дозволяє зробити наступні висновки.

По-перше, штучний інтелект у контексті державного управління являє собою не просто технологічний інструмент, а комплексний феномен, що охоплює технічні, організаційні, етичні та соціальні виміри. Його сутність полягає у здатності розширювати когнітивні можливості державних інституцій через обробку великих обсягів даних, виявлення складних закономірностей, автоматизацію рутинних операцій та підтримку прийняття обґрунтованих рішень. Водночас штучний інтелект залишається інструментом, який доповнює, а не замінює людський інтелект і відповідальність у сфері публічного управління.

По-друге, еволюція цифрових технологій у публічному секторі від початкової інформатизації через електронний уряд до сучасного інтелектуального управління є закономірним процесом послідовних якісних трансформацій. Кожний етап характеризується специфічними технологіями, організаційними моделями та цілями. Сучасний етап впровадження штучного інтелекту знаменує перехід до принципово нової парадигми проактивного, персоналізованого та ефективного публічного управління, заснованого на даних та інтелектуальних технологіях.

По-третє, успішна інтеграція штучного інтелекту у механізми прийняття управлінських рішень потребує дотримання комплексу принципів, серед яких ключовими є антропоцентричність, прозорість, підзвітність, справедливість, безпека, конфіденційність, пропорційність та людський нагляд. Ці принципи

мають бути операціоналізовані через конкретні процедури, стандарти та механізми управління ризиками, а їх реалізація вимагає не лише технологічних інвестицій, але й організаційних змін, розвитку компетентностей, створення відповідної нормативно-правової бази.

Теоретичні засади, розглянуті у першому розділі, створюють фундамент для аналізу сучасного стану та проблем впровадження технологій штучного інтелекту в системі публічного управління України, що буде здійснено у наступному розділі дослідження.

РОЗДІЛ 2. СУЧАСНИЙ СТАН ТА ПРОБЛЕМИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ УКРАЇНИ

2.1. Сучасний стан цифрової трансформації органів публічної влади в Україні

Цифрова трансформація публічного сектору України є одним з ключових пріоритетів державної політики останніх років. Системний підхід до цифровізації розпочався з прийняттям у 2018 році Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки, яка визначила стратегічні напрями та механізми цифрового розвитку держави.

Створення у січні 2019 року Міністерства цифрової трансформації України стало знаковою подією, що засвідчила політичну волю до системної модернізації державного управління через впровадження цифрових технологій [22]. Міністерство отримало широкі повноваження щодо формування та реалізації державної політики у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій, електронного урядування та електронної демократії, розвитку інформаційного суспільства.

Флагманською ініціативою цифрової трансформації в Україні стала державна програма «Держава у смартфоні», яка передбачає перенесення всіх публічних послуг у цифровий формат та забезпечення їх доступності через мобільні пристрої [33]. Центральним елементом цієї програми є мобільний застосунок «Дія», запущений у лютому 2020 року. Станом на 2024 рік застосунком користується понад 19 мільйонів українців, що становить близько половини дорослого населення країни [32].

Функціональність застосунку «Дія» постійно розширюється і на сьогодні включає понад 50 державних послуг. Громадяни можуть використовувати цифрові документи (паспорт, водійське посвідчення, студентський квиток, свідоцтво про народження дитини), отримувати

різноманітні довідки без відвідування державних установ, реєструвати бізнес онлайн, подавати декларації, оформляти соціальні виплати [35]. Важливим досягненням є те, що цифрові документи у застосунку мають повну юридичну силу, що є унікальним випадком на пострадянському просторі.

Портал «Дія» (diia.gov.ua) функціонує як єдиний державний вебпортал електронних послуг, забезпечуючи доступ до понад 120 онлайн-послуг для громадян та бізнесу [34]. Портал інтегрований з численними державними реєстрами та інформаційними системами, що дозволяє автоматично отримувати необхідні дані без потреби громадян збирати довідки з різних установ.

Освітня платформа «Дія.Цифрова освіта» пропонує безкоштовні онлайн-курси з цифрової грамотності для різних категорій населення, включаючи державних службовців, підприємців, школярів, що сприяє підвищенню загального рівня цифрових компетентностей населення, що є необхідною передумовою успішної цифровізації.

У сфері електронних адміністративних послуг Україна демонструє значний прогрес. Відповідно до Закону України «Про адміністративні послуги», всі базові адміністративні послуги мають бути доступні в електронній формі. Запроваджено систему електронної ідентифікації та автентифікації користувачів через кваліфіковані електронні підписи, що регулюється Законом України «Про електронні довірчі послуги» [21].

Важливим елементом цифрової інфраструктури є система електронної взаємодії державних електронних інформаційних ресурсів «Трембіта», яка забезпечує безпечний обмін даними між державними реєстрами та інформаційними системами різних відомств. Система побудована на основі естонського рішення X-Road і дозволяє реалізувати принцип «один раз» – громадянин надає дані державі один раз, після чого вони автоматично використовуються різними органами влади без потреби повторного звернення.

Розвиток відкритих даних є важливим напрямом цифровізації публічного сектору. Єдиний державний веб-портал відкритих даних

data.gov.ua містить тисячі наборів даних від різних державних органів у машиночитному форматі. Це сприяє прозорості влади, дозволяє громадськості здійснювати моніторинг діяльності державних органів, стимулює розробку інноваційних додатків та сервісів на основі публічних даних.

У сфері електронних закупівель Україна є визнаним світовим лідером. Система ProZorro забезпечує прозорість та конкурентність у сфері публічних закупівель через використання технології блокчейн та відкритих даних [68]. Впровадження цієї системи дозволило зекономити мільярди гривень бюджетних коштів та суттєво знизити рівень корупції у сфері державних закупівель.

Однак, незважаючи на значні досягнення, цифрова трансформація публічного сектору України стикається з численними викликами. Дослідниця А. І. Семенченко відзначає, що основними проблемами є фрагментарність інформаційних систем різних відомств, недостатня інтероперабельність, дублювання функціональності, обмеженість фінансових ресурсів для модернізації застарілої ІТ-інфраструктури [25].

Воєнний стан, спричинений російською агресією, створив додаткові виклики для цифровізації, зокрема загрози кібербезпеці критичної інфраструктури, необхідність забезпечення безперервності надання послуг в умовах руйнування фізичної інфраструктури, масові кібератаки на державні інформаційні системи. Водночас війна стала каталізатором прискореної цифровізації у багатьох сферах, продемонструвала критичну важливість цифрової інфраструктури для функціонування держави в екстремальних умовах.

Що стосується безпосереднього використання технологій штучного інтелекту у вітчизняному публічному управлінні, то цей процес перебуває на початковій стадії. Прийнята у 2020 році Концепція розвитку штучного інтелекту в Україні визначила стратегічне бачення та пріоритетні напрями, але її реалізація стикається з численними перешкодами організаційного, фінансового та кадрового характеру.

Окремі приклади використання елементів штучного інтелекту можна побачити у різних сферах публічного управління. У податковій службі використовуються системи автоматичного аналізу податкових декларацій для виявлення потенційних порушень. У митній службі застосовуються технології комп'ютерного зору для автоматичної ідентифікації товарів. У сфері надання адміністративних послуг використовуються чат-боти для консультування громадян. У системі охорони здоров'я пілотуються проекти з використання штучного інтелекту для діагностики захворювань на основі медичних зображень [15].

Портал «Дія» інтегрує окремі елементи штучного інтелекту для персоналізації послуг, автоматичної обробки документів, виявлення шахрайства. Однак системне використання передових технологій машинного навчання, глибоких нейронних мереж, обробки природної мови залишається обмеженим [33].

Український IT-сектор має значний потенціал для розвитку рішень у сфері штучного інтелекту. В Україні працюють тисячі IT-компаній, значна частина яких спеціалізується на розробці програмного забезпечення, включаючи рішення на базі машинного навчання та штучного інтелекту [30]. Однак взаємодія між IT-сектором та публічним управлінням залишається недостатньою, державні замовлення на розробку інтелектуальних систем є обмеженими.

Важливим аспектом є наявність даних як необхідної передумови для функціонування систем штучного інтелекту. Україна має численні державні реєстри та інформаційні системи, що накопичують великі обсяги даних. Однак якість цих даних часто є недостатньою – вони можуть бути неповними, застарілими, містити помилки, не бути стандартизованими [57]. Це створює серйозні перешкоди для ефективного використання технологій машинного навчання, які потребують якісних навчальних даних.

Цифрова грамотність населення є важливим чинником успішності цифровізації. Україна демонструє відносно високий рівень проникнення

Інтернету та користування цифровими технологіями серед молодого та середнього віку населення. Однак існує значний цифровий розрив між містом та селом, молодими та літніми людьми, що створює ризики соціальної ексклюзії у процесі цифровізації державних послуг.

Нормативно-правова база цифровізації в Україні розвивається, але містить численні прогалини, особливо щодо регулювання використання штучного інтелекту. Закон України «Про електронні довірчі послуги» створив правові основи для електронної ідентифікації та електронних підписів [21]. Закон України «Про захист персональних даних» регулює питання обробки персональних даних, хоча потребує гармонізації з європейським GDPR. Однак спеціальне законодавство, яке б комплексно регулювало використання систем штучного інтелекту у публічному секторі, відсутнє.

Організаційна структура державного управління цифровізацією потребує вдосконалення. Хоча Міністерство цифрової трансформації відіграє координуючу роль, кожне відомство самостійно відповідає за цифровізацію своєї сфери, що призводить до дублювання зусиль, несумісності систем, неефективного використання ресурсів. Відсутня єдина стратегія розвитку штучного інтелекту у публічному секторі з чіткими цілями, індикаторами, фінансуванням.

Фінансування цифровізації публічного сектору є обмеженим, особливо в умовах воєнного стану, коли бюджетні ресурси спрямовуються переважно на оборону та соціальний захист [11]. Це створює труднощі для реалізації масштабних проектів з впровадження інтелектуальних систем, які потребують значних інвестицій у технології, інфраструктуру, навчання персоналу.

Таким чином, сучасний стан цифрової трансформації органів публічної влади в Україні характеризується значними досягненнями у створенні базової цифрової інфраструктури, запровадженні електронних послуг, розвитку відкритих даних, при цьому використання передових технологій штучного інтелекту перебуває на початковій стадії і потребує системних зусиль щодо

створення сприятливого організаційного, правового, технологічного та кадрового середовища.

Подальший розвиток цифрової держави передбачає не лише розширення доступності сервісів, а й їх інтелектуалізацію – перехід від простого автоматизованого надання послуг до формування адаптивних, прогнозних та аналітичних систем управління. Це вимагає інтеграції AI-технологій у ключові функції держави: ухвалення рішень, управління ресурсами, моделювання ризиків, персоналізацію комунікацій з громадянами. Водночас нагальною залишається потреба формування надійної системи кіберзахисту, що забезпечуватиме безпечну взаємодію державних інформаційних систем, захист персональних даних та запобігання технологічним зловживанням.

Важливим чинником стає здатність державних службовців працювати з великими масивами даних, алгоритмами, аналітичними платформами та інтелектуальними сервісами. Це визначає необхідність нової моделі цифрових компетентностей та перегляду підходів до професійного навчання державного апарату. Окрім того, інтеграція штучного інтелекту у публічне управління потребує підвищення інституційної спроможності органів влади, удосконалення нормативно-правової бази та узгодження з європейськими стандартами регулювання.

Загалом, цифрова трансформація України перебуває на етапі переходу від діджиталізації до інтелектуалізації управління, де ключовим орієнтиром виступає побудова ефективної, стійкої та проактивної моделі державного управління, заснованої на даних, алгоритмах та високому рівні цифрової культури. Від того, наскільки швидко та системно буде забезпечено розвиток інтелектуальних технологій, залежить конкурентоспроможність держави, її здатність адаптуватися до глобальних викликів і забезпечити якісно новий рівень взаємодії між владою та суспільством.

2.2. Зарубіжний досвід використання штучного інтелекту у вітчизняному публічному управлінні (США, ЄС, Південна Корея, Естонія)

Аналіз міжнародного досвіду впровадження штучного інтелекту у публічне управління дозволяє виявити кращі практики, уникнути помилок та адаптувати успішні рішення до українського контексту. Різні країни обрали відмінні стратегії та підходи до інтеграції інтелектуальних технологій у державний сектор, що відображає специфіку їх політичних систем, економічного розвитку, правових традицій.

Сполучені Штати Америки є світовим лідером у розробці технологій штучного інтелекту та активно впроваджують їх у публічному секторі. У 2019 році президент Д. Трамп підписав виконавчий указ «Про підтримання американського лідерства у штучному інтелекті», який визначив п’ять ключових принципів: стимулювання інновацій, розвиток довіри, навчання робочої сили, захист американських переваг, міжнародне співробітництво [40].

Федеральний уряд США використовує штучний інтелект у широкому спектрі застосувань. Агентство національної безпеки застосовує алгоритми машинного навчання для виявлення загроз тероризму через аналіз великих обсягів даних [41]. Служба громадянства та імміграції використовує системи розпізнавання осіб для ідентифікації заявників. Податкова служба застосовує штучний інтелект для виявлення податкового шахрайства та оптимізації аудиторських перевірок.

У сфері охорони здоров’я Національні інститути здоров’я фінансують дослідження з використання штучного інтелекту для діагностики захворювань, розробки ліків, персоналізованої медицини. Адміністрація ветеранів впровадила систему штучного інтелекту для прогнозування ризику самогубства серед ветеранів на основі аналізу їх медичних записів.

Національна стратегія досліджень та розвитку штучного інтелекту, оновлена у 2023 році, визначає довгострокові інвестиції у фундаментальні дослідження, розвиток людського капіталу, створення етичних та правових рамок, забезпечення безпеки систем штучного інтелекту. Стратегія наголошує на необхідності підтримання технологічного лідерства США у глобальній конкуренції, особливо з Китаєм.

Однак американський підхід також стикається з критикою щодо недостатнього регулювання використання штучного інтелекту правоохоронними органами, зокрема систем розпізнавання осіб, які можуть порушувати права на приватність та дискримінувати певні расові групи. Міста Сан-Франциско, Бостон, Портленд заборонили використання технології розпізнавання осіб правоохоронними органами через етичні занепокоєння [48].

Європейський Союз обрав відмінний від США підхід, орієнтований на регулювання та захист прав людини. У квітні 2021 року Європейська комісія представила проект Акту про штучний інтелект (AI Act), який став першою у світі комплексною правовою рамкою регулювання систем штучного інтелекту [38].

AI Act запроваджує ризик-орієнтований підхід, класифікуючи системи штучного інтелекту за чотирма категоріями ризику. Системи неприйнятного ризику заборонені – це включає соціальне кредитування урядами, маніпулятивні технології, біометричну ідентифікацію у реальному часі у громадських місцях правоохоронними органами (з обмеженими винятками). Системи високого ризику підлягають суворим вимогам щодо якості даних, документації, прозорості, людського нагляду, кібербезпеки – це включає системи, що використовуються для оцінки кредитоспроможності, прийняття рішень у правосудді, управління критичною інфраструктурою, доступу до освіти та зайнятості [38].

Європейська комісія розробила Етичні настанови для надійного штучного інтелекту, які визначають сім ключових вимог: людський нагляд,

технічна стійкість та безпека, конфіденційність та управління даними, прозорість, різноманітність та недискримінація, соціальне та екологічне благополуччя, підзвітність [39].

Країни-члени ЄС впроваджують штучний інтелект у публічному секторі з урахуванням цих загальноєвропейських принципів. Франція створила Національну координаційну програму зі штучного інтелекту з бюджетом 1,5 мільярда євро для стимулювання досліджень та впровадження ШІ. Німеччина інвестує 5 мільярдів євро до 2025 року у розвиток штучного інтелекту, включаючи використання у публічному секторі [42].

Естонія є визнаним світовим лідером у сфері цифрового урядування та одним з піонерів використання штучного інтелекту у публічному секторі. Цифрова трансформація Естонії розпочалася ще у 1990-х роках і сьогодні 99% державних послуг доступні онлайн 24/7 [43].

Ключовим елементом естонської цифрової інфраструктури є платформа X-Road, яка забезпечує безпечний обмін даними між різними державними реєстрами, базами даних та інформаційними системами [44]. X-Road використовує технологію блокчейн для забезпечення цілісності та незмінності даних. Понад 900 організацій та 2800 сервісів підключені до цієї платформи, що дозволяє реалізувати принцип «один раз» – громадяни надають дані державі лише один раз.

Естонія активно впроваджує штучний інтелект у різні сфери публічного управління. Податкова служба використовує алгоритми машинного навчання для автоматичного попереднього заповнення податкових декларацій на основі даних з різних джерел – роботодавців, банків, страхових компаній. Система також автоматично виявляє потенційні помилки чи шахрайство [43].

У судовій системі Естонії розробляється система штучного інтелекту для вирішення дрібних спорів (до 7000 євро) без участі судді. Алгоритм аналізує подані документи, застосовує відповідні правові норми та генерує рішення, яке може бути оскаржене в суді з участю людини-судді. У сфері охорони здоров’я використовується штучний інтелект для аналізу медичних

зображень, прогнозування епідемій, оптимізації розподілу ресурсів системи охорони здоров'я [43].

Естонія розробила Національну стратегію зі штучного інтелекту, яка визначає три пріоритетні напрями: підвищення ефективності публічного сектору через ШІ, розвиток освіти у сфері ШІ, створення правових та етичних рамок. Важливим принципом естонського підходу є прозорість – громадяни можуть побачити через систему eesti.ee, які державні органи та коли отримували доступ до їхніх даних [43].

Південна Корея є азіатським лідером у впровадженні штучного інтелекту у публічне управління. У 2019 році уряд оприлюднив Національну стратегію зі штучного інтелекту, яка передбачає інвестиції у розмірі 2,2 трильйона вон (близько 2 мільярдів доларів США) до 2030 року [42].

Південна Корея має амбітну мету стати однією з трьох провідних країн у сфері штучного інтелекту та створити «AI-готову» державу. Стратегія визначає шість ключових напрямів: підготовка світового рівня талантів, створення екосистеми для стартапів, розвиток обчислювальної інфраструктури, забезпечення доступу до даних, встановлення норм та стандартів, інтеграція ШІ у суспільство.

Уряд Південної Кореї впроваджує штучний інтелект у широкий спектр публічних послуг. У сфері соціального забезпечення використовуються алгоритми для виявлення громадян, які потребують соціальної допомоги, але не звернулися за нею. Система аналізує дані з різних джерел (доходи, майно, медичні записи, споживання комунальних послуг) і проактивно пропонує допомогу тим, хто відповідає критеріям [42].

У сфері громадської безпеки Сеул використовує систему штучного інтелекту для прогнозування злочинів на основі аналізу історичних даних, погодних умов, часу доби, локації. Це дозволяє оптимізувати патрулювання поліції та превентивно посилювати безпеку у зонах підвищеного ризику. У транспортній сфері штучний інтелект використовується для оптимізації

світлофорів, управління автобусними маршрутами, прогнозування завантаженості транспорту.

Південна Корея також розробила Етичні принципи штучного інтелекту, які включають повагу до прав людини, справедливість, прозорість, підзвітність, безпеку. Створено Національний комітет з етики штучного інтелекту для моніторингу дотримання цих принципів.

Порівняльний аналіз досвіду цих країн дозволяє виявити спільні риси та відмінності. Всі країни визнають стратегічне значення штучного інтелекту та розробили національні стратегії з значними державними інвестиціями. Всі наголошують на необхідності етичного використання ШІ, захисту прав людини, прозорості, підзвітності. Однак підходи до регулювання відрізняються – від м'якого саморегулювання у США до жорсткого законодавчого регулювання в ЄС [41].

Естонський досвід є особливо релевантним для України через подібність історичного контексту (обидві країни є пострадянськими, здобули незалежність у 1990-х роках), відносно невеликий розмір території та населення, амбітні цілі щодо цифровізації. Естонська модель базується на кількох ключових принципах, які можуть бути адаптовані в Україні: децентралізована архітектура з центральною платформою обміну даними, цифрова ідентифікація як основа всіх сервісів, відкритість коду та стандартів, орієнтація на користувача, постійні інновації [44].

Міжнародні організації також відіграють важливу роль у формуванні глобальних стандартів використання штучного інтелекту у публічному секторі. ОЕСР розробила Рекомендації зі штучного інтелекту, які стали першими міжнародними стандартами, прийнятими урядами [37]. ЮНЕСКО прийняла Рекомендації з етики штучного інтелекту, які підкреслюють необхідність орієнтації на людину, недискримінації, справедливості [46]. Світовий банк досліджує можливості використання штучного інтелекту для досягнення Цілей сталого розвитку у країнах, що розвиваються [47].

Для України корисним є вивчення не лише технологічних рішень, але й організаційних моделей, нормативно-правових рамок, стратегій залучення громадськості, механізмів фінансування, підходів до розвитку компетентностей. Важливо адаптувати кращі практики до специфіки українського контексту, враховуючи обмежені ресурси, особливості політичної системи, рівень цифрової грамотності населення, воєнний стан.

Таким чином, зарубіжний досвід демонструє різноманітність підходів до впровадження штучного інтелекту у публічне управління, при цьому спільними є визнання стратегічного значення цих технологій, необхідність значних державних інвестицій, важливість етичних принципів та захисту прав людини, потреба у розвитку людського капіталу, а Естонія завдяки своєму успішному досвіду цифровізації публічного сектору та схожості історичного контексту може слугувати особливо цінним орієнтиром для України.

2.3. Інституційно-правові засади розвитку штучного інтелекту в державному секторі

Формування адекватної інституційно-правової бази є критично важливою передумовою успішного впровадження штучного інтелекту у систему публічного управління. В Україні цей процес перебуває на початковій стадії, характеризується фрагментарністю нормативного регулювання та відсутністю комплексного законодавчого акту, який би системно врегульовував використання інтелектуальних технологій у державному секторі.

Ключовим стратегічним документом є Концепція розвитку штучного інтелекту в Україні, схвалена розпорядженням Кабінету Міністрів України від 2 грудня 2020 року № 1556-р [2]. Концепція визначає мету, завдання, принципи та напрями розвитку штучного інтелекту в Україні на період до 2030 року. Документ наголошує на необхідності створення сприятливих умов для розвитку ШІ, стимулювання досліджень та інновацій, підготовки

кваліфікованих фахівців, забезпечення етичного та відповідального використання технологій [16].

Концепція визначає п’ять стратегічних цілей: створення національної екосистеми штучного інтелекту, використання ШІ для економічного зростання, забезпечення застосування ШІ для вирішення соціальних викликів, інтеграція України у глобальну екосистему ШІ, розвиток етичного та відповідального ШІ [2]. Документ передбачає розробку плану заходів з реалізації Концепції, проте станом на 2024 рік повноцінна імплементація стратегічних цілей залишається обмеженою через брак фінансування, відсутність спеціального законодавства, недостатню міжвідомчу координацію [6].

Базовим документом у сфері цифровізації є Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки, схвалена розпорядженням Кабінету Міністрів України від 17 січня 2018 року № 67-р. Хоча Концепція не фокусується виключно на штучному інтелекті, вона визначає загальні рамки цифрової трансформації, включаючи розвиток цифрової інфраструктури, електронне урядування, цифрові компетентності, кібербезпеку. Документ передбачав реалізацію до 2020 року, однак багато завдань залишаються актуальними і потребують продовження.

Постанова Кабінету Міністрів України від 30 січня 2019 року № 56 «Деякі питання цифрового розвитку» визначила повноваження Міністерства цифрової трансформації як центрального органу виконавчої влади, відповідального за формування та реалізацію державної політики у сферах цифровізації [3]. Це створило інституційну основу для координації процесів цифрової трансформації публічного сектору, включаючи впровадження технологій штучного інтелекту.

Положення про Міністерство цифрової трансформації України, затверджене постановою Кабінету Міністрів України від 18 вересня 2019 року № 856, визначає широкі повноваження Міністерства, включаючи розробку та реалізацію державної політики у сфері штучного інтелекту, цифрового

розвитку, електронного урядування, розвиток цифрових навичок громадян, забезпечення доступу до публічної інформації у формі відкритих даних [22].

У сфері електронних довірчих послуг ключовим є Закон України «Про електронні довірчі послуги» від 5 жовтня 2017 року № 2155-VIII [21]. Закон регулює питання електронної ідентифікації, електронних підписів, електронних печаток, електронних позначок часу, що є необхідною інфраструктурою для функціонування електронних державних послуг та інтеграції систем штучного інтелекту. Закон гармонізований з європейським регламентом eIDAS, що забезпечує сумісність української системи електронних довірчих послуг з європейською.

Захист персональних даних регулюється Законом України «Про захист персональних даних», який визначає правові засади обробки персональних даних, права суб'єктів даних, обов'язки власників та розпорядників баз даних [56]. У контексті штучного інтелекту цей закон набуває особливого значення, оскільки системи ШІ потребують великих обсягів даних для навчання та функціонування. Однак закон потребує вдосконалення для повної гармонізації з європейським GDPR, зокрема щодо права на пояснення автоматизованих рішень, права на видалення даних, принципу мінімізації даних.

Важливим елементом правової бази є Закон України «Про відкриті дані» від 1 липня 2015 року, який зобов'язує розпорядників інформації оприлюднювати публічну інформацію у формі відкритих даних [58]. Відкриті дані є критично важливими для розвитку штучного інтелекту, оскільки надають доступ до навчальних даних для дослідників, стартапів, громадських організацій. Закон визначає вимоги до формату, структури, актуальності відкритих даних, процедуру їх оприлюднення.

У сфері кібербезпеки діє Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року, який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору [54]. У контексті штучного інтелекту це включає захист систем

ШІ від кібератак, маніпуляцій, несанкціонованого доступу, забезпечення цілісності та конфіденційності даних.

Однак українське законодавство має суттєві прогалини щодо регулювання штучного інтелекту. Відсутній спеціальний закон про штучний інтелект, який би визначав правовий статус систем ШІ, вимоги до їх розробки та використання, відповідальність за рішення, прийняті за допомогою ШІ, механізми захисту прав громадян [4]. Дослідниця І. Є. Тімошенко у своїй дисертації детально аналізує прогалини правового регулювання та пропонує концептуальні засади спеціального законодавства про штучний інтелект.

Не врегульовано питання алгоритмічної підзвітності – хто несе відповідальність, якщо система штучного інтелекту приймає помилкове або дискримінаційне рішення, яке порушує права громадянина. Традиційні концепції юридичної відповідальності, що передбачають вину, причинно-наслідковий зв'язок, дієздатність, важко застосовувати до автоматизованих систем [23].

Відсутні нормативні вимоги щодо прозорості та пояснюваності алгоритмів, які використовуються в публічному секторі. Громадяни не мають права знати, що рішення, яке впливає на їхні права, було прийнято за допомогою штучного інтелекту, які критерії використовувалися, які дані аналізувалися, як можна оскаржити таке рішення [6].

Не врегульовано питання якості та упередженості даних, які використовуються для навчання систем штучного інтелекту у публічному секторі. Якщо навчальні дані містять історичні дисбаланси або дискримінацію, алгоритм може відтворювати та посилювати ці упередження, що призводить до систематичної дискримінації певних груп населення [49].

Відсутні стандарти тестування та сертифікації систем штучного інтелекту перед їх впровадженням у публічному секторі. Немає вимог щодо незалежного аудиту алгоритмів, оцінки ризиків, моніторингу функціонування систем після впровадження [38].

Не визначено організаційно-інституційну структуру управління розвитком штучного інтелекту у публічному секторі. Відсутній спеціалізований регуляторний орган, який би відповідав за нагляд за використанням систем ШІ державними органами, розробку стандартів, сертифікацію, розгляд скарг громадян.

Професійний стандарт фахівця з цифрового розвитку, затверджений наказом Міністерства цифрової трансформації від 7 грудня 2021 року № 171, визначає вимоги до компетентностей фахівців, які працюють у сфері цифровізації. Однак стандарт має загальний характер і не містить специфічних вимог щодо компетентностей у сфері штучного інтелекту.

У контексті євроінтеграції України важливим є гармонізація вітчизняного законодавства з європейськими нормами, зокрема з Актом про штучний інтелект ЄС [38]. Це вимагає імплементації ризик-орієнтованого підходу, створення системи класифікації систем ШІ за рівнями ризику, встановлення відповідних регуляторних вимог, розробки механізмів нагляду та контролю.

Національне агентство України з питань державної служби відповідає за розробку та впровадження програм підвищення кваліфікації державних службовців, включаючи навчання цифровим компетентностям. Однак системні програми з підготовки державних службовців до роботи з системами штучного інтелекту відсутні, навчальні матеріали обмежені, викладачі часто не мають практичного досвіду роботи з інтелектуальними технологіями.

Інституційна структура координації впровадження штучного інтелекту у публічному секторі є фрагментованою. Міністерство цифрової трансформації відповідає за загальну політику цифровізації, але кожне відомство самостійно приймає рішення щодо впровадження систем ШІ у своїй сфері [34]. Це призводить до дублювання зусиль, несумісності систем, неефективного використання ресурсів, відсутності єдиних стандартів та кращих практик.

Відсутня національна дорожня карта впровадження штучного інтелекту у публічному секторі з конкретними цілями, завданнями, індикаторами, термінами, бюджетом, відповідальними виконавцями. Концепція розвитку штучного інтелекту визначає загальні напрями, але не містить детального плану імплементації з механізмами моніторингу та оцінки результатів.

Механізми громадської участі у формуванні політики щодо штучного інтелекту є обмеженими. Відсутня платформа для широкого громадського обговорення етичних, правових, соціальних наслідків впровадження інтелектуальних технологій у державне управління. Громадські організації, експерти, науковці мають обмежені можливості впливати на процес прийняття рішень щодо використання ШІ у публічному секторі.

Позитивним прикладом є діяльність Лабораторії цифрової безпеки, яка надала пропозиції до Концепції розвитку штучного інтелекту, що були враховані урядом [16]. Однак такі випадки залишаються поодинокими, а не системною практикою.

Міжнародне співробітництво у сфері штучного інтелекту розвивається, але має потенціал для розширення. Україна є членом Глобального партнерства зі штучного інтелекту (GPAI), що дозволяє обмінюватися досвідом з провідними країнами світу [20]. Співробітництво з Естонією у сфері цифрового урядування включає можливості для вивчення та адаптації естонського досвіду використання штучного інтелекту.

Фінансування розвитку штучного інтелекту у публічному секторі не виділено окремою бюджетною програмою, що ускладнює оцінку обсягів інвестицій та ефективності їх використання [11]. Державні замовлення на розробку систем ШІ для публічного сектору є обмеженими, що не стимулює вітчизняний ІТ-сектор до інвестицій у дослідження та розробки у цій сфері.

Таким чином, інституційно-правові засади розвитку штучного інтелекту в державному секторі України перебувають на стадії формування, характеризуються наявністю окремих стратегічних документів та загального законодавства про цифровізацію, але відсутністю комплексного спеціального

регулювання використання систем ШІ, що створює правову невизначеність, перешкоджає масштабному впровадженню інтелектуальних технологій та потребує розробки відповідного законодавства з урахуванням європейських стандартів та кращих міжнародних практик.

2.4. Основні бар'єри та ризики впровадження ШІ у публічному управлінні (правові, етичні, безпекові)

Впровадження штучного інтелекту у систему публічного управління супроводжується численними бар'єрами та ризиками, які можна класифікувати за кількома категоріями: правові, етичні, технологічні, організаційні, фінансові, кадрові, безпекові. Розуміння цих бар'єрів та ризиків є необхідною передумовою для розробки ефективних стратегій їх подолання.

Правові бар'єри та ризики пов'язані з відсутністю адекватної нормативно-правової бази регулювання використання штучного інтелекту у публічному секторі. Як було проаналізовано у попередньому підрозділі, українське законодавство не визначає правовий статус систем ШІ, вимоги до їх розробки та використання, відповідальність за помилкові або дискримінаційні рішення, що створює правову невизначеність, яка стримує державні органи від масштабного впровадження інтелектуальних технологій через побоювання потенційних правових наслідків.

Особливо проблемним є питання відповідальності за рішення, прийняті за допомогою систем штучного інтелекту. Традиційні правові конструкції передбачають, що юридична відповідальність настає за наявності вини, яка може бути приписана дієздатному суб'єкту [23]. Однак у випадку автоматизованих систем складно визначити, хто несе відповідальність – розробник алгоритму, постачальник системи, державний орган, який використовує систему, конкретний державний службовець, який прийняв рішення на основі рекомендацій ШІ.

Відсутність механізмів оскарження автоматизованих рішень створює ризики порушення прав громадян на справедливий розгляд їхніх справ. Якщо рішення про відмову у соціальній допомозі, притягнення до відповідальності, відхилення заяви приймається автоматично алгоритмом, громадянин має право знати про це, отримати пояснення, оскаржити рішення [6]. Однак процедури такого оскарження в українському законодавстві не визначені.

Етичні бар'єри та ризики пов'язані з потенційною дискримінацією, упередженістю, порушенням приватності, автономії особистості при використанні систем штучного інтелекту. Дослідження показують, що алгоритми машинного навчання можуть відтворювати та посилювати упередження, які присутні у навчальних даних. Якщо історичні дані містять дискримінацію певних груп (за ознакою статі, віку, етнічності, соціального статусу), алгоритм, навчений на цих даних, буде систематично дискримінувати ці групи у майбутніх рішеннях.

Приклади з інших країн демонструють серйозність цих ризиків. У США система COMPAS, яка використовувалася судами для оцінки ризику рецидиву при прийнятті рішень про умовно-дострокове звільнення, систематично переоцінювала ризики для афроамериканців та недооцінювала для білих [48]. У Нідерландах система автоматичного виявлення шахрайства у соціальних виплатах несправедливо позначала як потенційних шахраїв людей з низькими доходами, мігрантів, що призвело до скандалу та відставки уряду.

Ризик порушення приватності виникає через те, що системи штучного інтелекту потребують великих обсягів персональних даних для навчання та функціонування. Навіть якщо дані номінально знеособлені, сучасні техніки машинного навчання можуть реідентифікувати осіб через комбінацію різних атрибутів. Крім того, агрегування даних з різних джерел (медичні записи, фінансові дані, соціальні мережі, геолокація) створює детальні профілі громадян, що може використовуватися для масового спостереження.

Автономія особистості може бути порушена, коли рішення, що впливають на життя людини, приймаються автоматизованими системами без

можливості людського втручання. Навіть якщо система технічно працює коректно, громадяни можуть відчувати втрату контролю над власним життям, коли важливі рішення приймаються «чорною скринькою», логіка роботи якої їм незрозуміла.

Технологічні бар'єри та ризики включають обмеження самих технологій штучного інтелекту, проблеми якості даних, інтероперабельності систем. Системи машинного навчання потребують великих обсягів якісних навчальних даних. В українському публічному секторі дані часто є неповними, застарілими, містять помилки, не стандартизовані [57]. Це знижує точність та надійність моделей, створює ризики помилкових рішень.

Проблема «чорної скриньки» полягає у тому, що складні моделі глибокого навчання важко інтерпретувати – навіть їхні розробники не завжди можуть пояснити, чому система прийняла конкретне рішення [67]. Це створює проблеми для дотримання принципу прозорості у публічному управлінні, де рішення мають бути обґрунтованими та зрозумілими.

Ризик технологічної залежності виникає, коли держава покладається на системи штучного інтелекту, розроблені приватними компаніями, часто іноземними. Це створює ризики щодо суверенітету даних, можливості аудиту алгоритмів, гнучкості у модифікації систем відповідно до специфічних потреб.

Інтероперабельність залишається проблемою, коли різні відомства розробляють власні системи, які не можуть ефективно обмінюватися даними та взаємодіяти, що знижує потенційні переваги інтеграції даних з різних джерел, призводить до дублювання зусиль та неефективного використання ресурсів.

Безпекові бар'єри та ризики набувають критичного значення в умовах воєнного стану. Системи штучного інтелекту у публічному секторі можуть стати об'єктами кібератак, спрямованих на маніпуляцію даними, отримання несанкціонованого доступу, виведення систем з ладу [54]. Дослідники виділяють кілька типів атак на системи ШІ: отруєння даних (data poisoning), коли зловмисники вносять спотворені дані у навчальну вибірку, щоб алгоритм

навчився неправильним закономірностям; змагальні приклади (adversarial examples), коли спеціально сконструйовані входи обманюють систему; викрадення моделі (model stealing), коли зловмисники відтворюють модель через багаторазові запити.

Воєнний стан створює додаткові виклики. Російські кібератаки на українську цифрову інфраструктуру є постійною загрозою [54], що суттєво ускладнює процес цифрової трансформації та вимагає від держави посилення захисних механізмів на всіх рівнях публічного управління. Під ударом опиняються інформаційні системи органів влади, державні реєстри, електронні послуги, комунікаційні платформи, об’єкти енергетичної, транспортної та логістичної інфраструктури, інтегровані у цифрові мережі. У таких умовах державні інституції повинні одночасно забезпечувати безперебійність

функціонування сервісів та підвищувати стійкість цифрової екосистеми до складних і високотехнологічних атак. Це включає розбудову багаторівневих систем кіберзахисту, посилення моніторингу кіберінцидентів у режимі реального часу, інвестування у захищені канали зв’язку й резервні інфраструктурні рішення, модернізацію державних реєстрів за принципами нульової довіри (Zero Trust) та активізацію міжнародної співпраці з ЄС, НАТО, США й іншими партнерами. Водночас ключовим напрямом є протидія інформаційним операціям, спрямованим на підрив довіри громадян до державних інституцій, оскільки кіберзагрози дедалі частіше поєднуються з дезінформаційними кампаніями та маніпулятивним впливом у цифровому середовищі.

У контексті впровадження штучного інтелекту воєнні ризики стають ще більш значущими, адже інтелектуальні системи, що працюють із великими обсягами даних, мають бути максимально стійкими до зовнішніх втручань, спроб підміни інформації чи змін алгоритмів. Безпека має охоплювати не лише технічні компоненти, але й логіку прийняття управлінських рішень, яка може бути спотворена у разі компрометації систем. Таким чином, війна стала

потужним каталізатором переосмислення підходів до кіберзахисту, інформаційної безпеки та цифрової стійкості держави. Україна поступово формує модель «цифрової обороноздатності», що інтегрує захист критичної інфраструктури, забезпечення безпеки даних та підвищення стійкості цифрових платформ як необхідну умову подальшої цифрової трансформації та розвитку інтелектуальних державних сервісів.

Узагальнюючи результати дослідження у Розділі 2, можна стверджувати, що впровадження технологій штучного інтелекту в систему публічного управління України перебуває на етапі формування і характеризується поєднанням значного потенціалу та суттєвих структурних обмежень. Україна демонструє прогрес у цифровізації базових управлінських процесів, розбудові електронних сервісів, розвитку відкритих даних та створенні інституційних засад цифрової модернізації. Проте впровадження інтелектуальних технологій, зокрема систем підтримки прийняття рішень, автоматизованої аналітики, машинного навчання та алгоритмічних моделей управління, все ще залишається фрагментарним і недостатньо інтегрованим у практику органів влади.

До ключових викликів, що уповільнюють інтелектуалізацію державного управління, належать: нерівномірність цифрової готовності органів влади, обмеженість фінансових та технічних ресурсів, недостатній рівень кадрових цифрових компетентностей, а також неузгодженість та фрагментарність нормативно-правового регулювання у сфері штучного інтелекту. Додатковими ускладненнями стали умови воєнного стану, що посилили кіберзагрози, підвищили вимоги до цифрової стійкості та актуалізували необхідність зміцнення систем захисту державних інформаційних ресурсів.

Водночас аналіз міжнародного досвіду засвідчує, що ефективне використання штучного інтелекту може суттєво підвищити спроможність публічного сектору шляхом оптимізації процедур, зменшення бюрократичного навантаження, покращення прогнозування, автоматизації рутини та підтримки стратегічних рішень. Це визначає для України

необхідність поглиблення цифрової трансформації, створення цілісної регуляторної рамки, формування компетентнісної моделі цифрового державного службовця, розвитку інституційної спроможності та модернізації цифрової інфраструктури.

Отже, сучасний стан упровадження технологій штучного інтелекту у публічному управлінні України можна охарактеризувати як перехідний: від діджиталізації базових процесів – до формування передумов інтелектуалізації державного сектору. Для подальшого прогресу потрібна системна політика, стратегічне бачення та комплексні організаційно-правові рішення, здатні забезпечити ефективне, безпечне та відповідальне використання інтелектуальних технологій в інтересах держави та громадян.

РОЗДІЛ 3. ПЕРСПЕКТИВИ ТА НАПРЯМИ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПУБЛІЧНЕ УПРАВЛІННЯ УКРАЇНИ

3.1. Розвиток інформаційної безпеки та захисту даних в умовах використання ШІ

Забезпечення інформаційної безпеки та захисту даних є критично важливою передумовою успішного впровадження штучного інтелекту у систему публічного управління. В умовах воєнного стану та постійних кіберзагроз з боку російської федерації ця проблематика набуває особливої актуальності для України.

Системи штучного інтелекту створюють специфічні виклики для кібербезпеки, які відрізняються від традиційних загроз інформаційним технологіям. По-перше, моделі машинного навчання можуть бути об’єктом спеціалізованих атак, таких як отруєння даних, змагальні приклади, викрадення моделі [54]. По-друге, системи ШІ потребують доступу до великих обсягів даних, часто чутливих та персональних, що створює додаткові ризики для конфіденційності. По-третє, складність алгоритмів глибокого навчання ускладнює виявлення вразливостей та забезпечення прозорості функціонування систем.

Розробка комплексної Стратегії кібербезпеки систем штучного інтелекту у публічному секторі України має стати першочерговим пріоритетом. Ця стратегія повинна базуватися на принципах «безпеки за дизайном» (security by design), коли питання безпеки враховуються на всіх етапах життєвого циклу системи – від проектування до виведення з експлуатації [55]. Стратегія має включати оцінку ризиків, визначення вимог до безпеки залежно від категорії системи та чутливості даних, процедури тестування та сертифікації, механізми моніторингу та реагування на інциденти.

Технічні заходи захисту мають охоплювати кілька рівнів. На рівні інфраструктури необхідно забезпечити захист обчислювальних ресурсів, сховищ даних, мережевих з'єднань через використання міжмережевих екранів, систем виявлення вторгнень, шифрування каналів передачі даних. Державні дата-центри, які обробляють чутливі дані, мають відповідати найвищим стандартам фізичної та технічної безпеки.

На рівні даних критично важливим є забезпечення їх цілісності, конфіденційності та доступності. Методи шифрування мають застосовуватися як для даних у спокої (зберігання), так і для даних у русі (передача).

Особливої уваги потребує захист навчальних даних від отруєння – зловмисники можуть намагатися внести спотворені дані, щоб модель навчилася неправильним закономірностям. Технології блокчейн можуть використовуватися для забезпечення незмінності критичних даних та аудиту їх використання [68].

На рівні моделей необхідно захищати алгоритми від атак змагальних прикладів, коли спеціально сконструйовані входи обманюють систему. Методи захисту включають адверсаріальне навчання, коли модель тренується на прикладах атак, верифікацію входів, ансамблеві методи. Інтелектуальна власність на алгоритми та навчені моделі також потребує захисту від викрадення та несанкціонованого копіювання.

Управління доступом до систем штучного інтелекту має базуватися на принципі мінімальних привілеїв – користувачі та програми отримують лише ті права доступу, які необхідні для виконання їхніх функцій. Багаторівнева автентифікація, включаючи біометричні методи, має використовуватися для доступу до критичних систем [21]. Детальне логування всіх операцій з даними та моделями дозволяє здійснювати аудит та розслідування інцидентів.

Захист персональних даних у контексті використання штучного інтелекту потребує особливої уваги. Гармонізація українського законодавства з європейським GDPR має включати імплементацію специфічних вимог щодо автоматизованого прийняття рішень. Громадяни повинні мати право знати, що

рішення, яке впливає на їхні права, було прийнято автоматично, право отримати пояснення логіки рішення, право заперечувати проти автоматизованої обробки у певних випадках, право на втручання людини.

Технології підвищення конфіденційності (privacy-enhancing technologies) дозволяють використовувати дані для навчання моделей без розкриття чутливої інформації. Диференційна приватність додає контрольований шум до даних, щоб унеможливити реідентифікацію окремих осіб, зберігаючи при цьому статистичні властивості, необхідні для навчання [47]. Федеративне навчання дозволяє тренувати моделі на розподілених даних без їх централізованого збору. Гомоморфне шифрування дозволяє обробляти зашифровані дані без їх розшифрування.

Оцінка впливу на захист даних (Data Protection Impact Assessment) має проводитися для всіх проектів впровадження штучного інтелекту у публічному секторі, які передбачають обробку персональних даних. Оцінка включає визначення типів даних, які обробляються, мети обробки, правових підстав, ризиків для прав та свобод людей, заходів мітигації ризиків. Результати оцінки мають бути задокументовані та доступні для перевірки регуляторними органами.

Роль Уповноваженого Верховної Ради України з прав людини має бути посилена у частині нагляду за дотриманням прав громадян при використанні систем штучного інтелекту у публічному управлінні. Створення спеціалізованого підрозділу або призначення експерта з питань алгоритмічної підзвітності дозволить професійно розглядати скарги громадян на автоматизовані рішення.

Міжнародне співробітництво у сфері кібербезпеки має розвиватися через участь України у глобальних ініціативах обміну інформацією про загрози, спільних навчаннях, програмах розбудови спроможностей. Співробітництво з НАТО у рамках програми посиленого партнерства, з ЄС у рамках угоди про асоціацію, з провідними країнами-партнерами дозволяє доступ до передових технологій захисту та кращих практик.

Створення Національного центру кібербезпеки систем штучного інтелекту може стати інституційною основою для координації зусиль різних відомств, розробки стандартів, проведення досліджень вразливостей, реагування на інциденти, навчання фахівців. Центр може функціонувати як центр компетенцій, який надає консультації державним органам щодо безпечного впровадження систем ШІ.

Стандарти кібербезпеки для систем штучного інтелекту мають розроблятися з урахуванням міжнародних кращих практик, зокрема стандартів ISO/IEC 27001 щодо управління інформаційною безпекою, ISO/IEC 42001 щодо систем управління штучним інтелектом, рекомендацій NIST щодо надійного штучного інтелекту [41]. Обов'язкова сертифікація критичних систем ШІ перед їх впровадженням у публічному секторі має забезпечити дотримання мінімальних вимог безпеки.

Освіта та підвищення обізнаності державних службовців щодо кіберзагроз, пов'язаних зі штучним інтелектом, є важливою складовою стратегії безпеки. Працівники мають розуміти, що системи ШІ можуть бути об'єктом атак, уміти виявляти ознаки компрометації, дотримуватися процедур безпечної роботи з даними та моделями.

Регулярний аудит безпеки систем штучного інтелекту має проводитися незалежними експертами для виявлення вразливостей, оцінки ефективності заходів захисту, перевірки дотримання стандартів. Результати аудиту мають використовуватися для постійного вдосконалення систем безпеки.

Планування безперервності діяльності має включати сценарії компрометації або виведення з ладу систем штучного інтелекту. Резервні копії даних та моделей, альтернативні режими функціонування без автоматизації, процедури швидкого відновлення мають забезпечити мінімальне порушення надання критичних публічних послуг у випадку інцидентів безпеки [54].

Етичні аспекти використання даних для навчання систем штучного інтелекту потребують уваги. Дані, зібрані для одних цілей, не повинні використовуватися для інших без згоди суб'єктів даних. Принцип мінімізації

даних означає, що збираються лише ті дані, які необхідні для конкретної мети. Обмеження строків зберігання забезпечує, що дані не зберігаються довше, ніж це необхідно.

Таким чином, розвиток інформаційної безпеки та захисту даних в умовах використання штучного інтелекту вимагає комплексного підходу, що включає розробку спеціалізованої стратегії кібербезпеки, впровадження багаторівневих технічних заходів захисту, гармонізацію законодавства з європейськими стандартами, посилення інституційного нагляду, міжнародне співробітництво, підвищення обізнаності персоналу, при цьому особлива увага має приділятися специфічним загрозам для систем ШІ та забезпеченню балансу між інноваціями та захистом прав громадян.

3.2. Формування компетентностей цифрового державного службовця як умова ефективного впровадження інтелектуальних технологій

Людський капітал є критичним фактором успішності впровадження штучного інтелекту у систему публічного управління. Формування нового типу державного службовця – цифрово компетентного, технологічно обізнаного, здатного ефективно працювати з інтелектуальними системами – вимагає системної трансформації підходів до підбору, навчання та розвитку кадрів у публічному секторі.

Концепція цифрового державного службовця передбачає володіння комплексом компетентностей, що виходять за межі традиційних знань з адміністративного права, державного управління, економіки. Ці компетентності можна структурувати за кількома рівнями. Базовий рівень включає цифрову грамотність – здатність використовувати комп’ютери, Інтернет, офісне програмне забезпечення, електронну пошту, онлайн-сервіси [32]. Середній рівень охоплює розуміння принципів роботи інформаційних систем, баз даних, основ кібербезпеки, роботи з даними.

Просунутий рівень включає знання з аналітики даних, машинного навчання, штучного інтелекту, здатність працювати зі спеціалізованим програмним забезпеченням.

Професійний стандарт «Фахівець з цифрового розвитку», затверджений Міністерством цифрової трансформації, визначає базові вимоги до компетентностей, але потребує деталізації та розширення у частині штучного інтелекту [60]. Необхідна розробка спеціалізованих професійних стандартів для різних категорій працівників – аналітиків даних у державних органах, менеджерів проектів цифрової трансформації, фахівців з інтеграції систем ШІ, етичних аудиторів алгоритмів.

Реформування системи підготовки державних службовців має розпочатися на етапі вищої освіти. Спеціальності з публічного управління та адміністрування у закладах вищої освіти мають включати обов'язкові дисципліни з цифрових технологій, аналітики даних, основ штучного інтелекту [53]. Практичні завдання, кейси, проектна робота з використанням реальних даних державних органів мають готувати студентів до роботи у цифровому середовищі.

Національна академія державного управління при Президентові України як провідний заклад підготовки та підвищення кваліфікації державних службовців має модернізувати навчальні програми з урахуванням потреб цифрової трансформації. Створення Центру цифрових компетентностей при НАДУ може стати інституційною основою для розробки спеціалізованих курсів, проведення тренінгів, сертифікації компетентностей [59].

Модульна система навчання дозволяє гнучко комбінувати різні компоненти відповідно до потреб та вихідного рівня підготовки слухачів. Обов'язковий модуль «Основи штучного інтелекту для державних службовців» має включати розуміння того, що таке ШІ, як працюють основні типи алгоритмів, які можливості та обмеження технологій, етичні та правові аспекти використання. Спеціалізовані модулі можуть фокусуватися на

конкретних застосуваннях ШІ у різних сферах – охороні здоров’я, освіті, соціальному захисті, правоохоронній діяльності, транспорті [32].

Практико-орієнтований підхід до навчання передбачає не лише теоретичні лекції, але й практичні воркшопи, де учасники працюють з реальними інструментами аналітики даних, експериментують з моделями машинного навчання, аналізують кейси використання ШІ у публічному управлінні інших країн. Симуляційні вправи, де учасники приймають рішення на основі рекомендацій штучного інтелекту в змодельованих сценаріях, розвивають здатність критично оцінювати автоматизовані рекомендації [62].

Онлайн-платформа безперервного навчання «Дія.Освіта» має бути розширена спеціалізованими курсами для державних службовців. Мікронавчання через короткі відео, інтерактивні вправи, геймифіковані завдання дозволяє державним службовцям навчатися у зручний час без відриву від роботи. Сертифікація компетентностей через онлайн-тестування та практичні завдання забезпечує об’єктивну оцінку досягнутого рівня.

Програми стажування у технологічних компаніях дозволяють державним службовцям вивчати кращі практики розробки та впровадження систем штучного інтелекту, розуміти культуру інновацій, будувати професійні мережі. Зворотні стажування, коли фахівці з ІТ-сектору тимчасово працюють у державних органах, привносять свіжий погляд, технологічну експертизу, менторять державних службовців.

Міжнародні програми обміну та навчання дозволяють українським державним службовцям вивчати досвід провідних країн у впровадженні штучного інтелекту у публічне управління. Естонія, Сінгапур, країни Скандинавії активно ділять ься своїм досвідом через програми для іноземних делегацій. Участь у міжнародних конференціях, воркшопах, онлайн-курсах провідних університетів світу розширює горизонти та забезпечує доступ до новітніх знань.

Створення спільнот практиків (communities of practice) всередині публічного сектору дозволяє державним службовцям, які працюють з

цифровими технологіями, обмінюватися досвідом, обговорювати виклики, спільно шукати рішення. Регулярні зустрічі, онлайн-форуми, спільні проекти сприяють поширенню знань та формуванню культури інновацій.

Залучення молодих фахівців з технологічними компетентностями до державної служби вимагає подолання кількох бар'єрів. Конкурентні зарплати для спеціалізованих позицій (дата-сайентисти, інженери машинного навчання, кібербезпека) є необхідною умовою залучення талантів [60]. Гнучкі форми зайнятості, можливість віддаленої роботи, проектна зайнятість можуть бути привабливими для молодих професіоналів, які цінують баланс між роботою та особистим життям.

Престиж державної служби як місця, де можна працювати над інноваційними проектами зі суспільним впливом, має активно формуватися через комунікаційні кампанії, висвітлення успішних кейсів, визнання та нагородження інноваторів. Програма «Дія.Сіті», яка створює спеціальний правовий режим для ІТ-галузі, може бути розширена на державні ІТ-проекти, що зробить роботу у публічному секторі привабливішою для технологічних фахівців.

Менторство та наставництво, коли досвідчені державні службовці передають знання новачкам, а технологічні експерти менторять працівників публічного сектору в освоєнні нових інструментів, прискорює процес адаптації та розвитку компетентностей. Формалізовані програми менторства з чіткими цілями, структурою, підтримкою забезпечують системність цього процесу.

Оцінка компетентностей має проводитися регулярно через сертифікаційні іспити, портфоліо виконаних проектів, оцінку 360 градусів, що включає зворотний зв'язок від колег, керівників, партнерів [60]. Результати оцінки мають використовуватися для планування індивідуальних траєкторій розвитку, прийняття рішень про кар'єрне зростання, формування команд для інноваційних проектів.

Мотиваційні механізми мають поєднувати матеріальні та нематеріальні стимули. Підвищення заробітної плати за наявність сертифікованих цифрових компетентностей стимулює інвестиції державних службовців у власний розвиток [60]. Прискорене кар'єрне зростання для інноваторів, які успішно впроваджують цифрові рішення, демонструє цінність цих компетентностей для організації. Нематеріальні стимули – визнання, нагороди, публічне висвітлення досягнень, можливість працювати над цікавими проектами – також є важливими мотиваторами.

Культура безперервного навчання має стати нормою у публічному секторі. Виділення робочого часу для навчання, підтримка участі у конференціях та тренінгах, заохочення експериментування та права на помилку створюють середовище, сприятливе для постійного вдосконалення [28]. Керівники державних органів мають подавати приклад, демонструючи власну відкритість до навчання нових технологій.

Етична освіта державних службовців у контексті штучного інтелекту є критично важливою. Працівники мають розуміти ризики дискримінації, упередженості, порушення приватності, уміти виявляти етичні проблеми, застосовувати етичні фреймворки у прийнятті рішень. Включення модуля з етики штучного інтелекту у всі навчальні програми для державних службовців має стати обов'язковою вимогою.

Міждисциплінарні команди, які поєднують державних службовців з глибоким розумінням предметної області та технологічних фахівців, є найбільш ефективними для проектів впровадження штучного інтелекту [48]. Розвиток навичок командної роботи, комунікації між різними професійними групами, розуміння мов один одного є важливою компетентністю для цифрового державного службовця.

Таким чином, формування компетентностей цифрового державного службовця вимагає системної трансформації, що включає модернізацію освітніх програм, створення інституційної інфраструктури для безперервного навчання, розвиток практико-орієнтованих форм підготовки, залучення

молодих талантів, створення мотиваційних механізмів, формування культури інновацій та безперервного навчання, при цьому особлива увага має приділятися етичним аспектам використання штучного інтелекту та розвитку здатності критично оцінювати автоматизовані рекомендації.

3.3. Стратегічні напрями державної політики щодо розвитку ШІ у публічному секторі України

Формування ефективної державної політики щодо розвитку штучного інтелекту у публічному секторі України вимагає стратегічного бачення, чіткої координації, адекватного фінансування та постійного моніторингу результатів. На основі аналізу теоретичних засад, сучасного стану, проблем та міжнародного досвіду можна визначити ключові стратегічні напрями.

Перший стратегічний напрям – розробка комплексної нормативно-правової бази регулювання штучного інтелекту у публічному секторі. Необхідне прийняття спеціального Закону України «Про штучний інтелект», який би визначав правовий статус систем ШІ, вимоги до їх розробки та використання, відповідальність за рішення, прийняті за допомогою ШІ, механізми захисту прав громадян, процедури оскарження автоматизованих рішень [4]. Закон має базуватися на принципах антропоцентричності, прозорості, підзвітності, справедливості та гармонізуватися з європейським AI Act [38].

Підзаконні нормативні акти мають деталізувати вимоги до різних категорій систем штучного інтелекту залежно від рівня ризику. Системи високого ризику, які використовуються для прийняття рішень, що впливають на фундаментальні права громадян (соціальна допомога, правосуддя, правоохоронна діяльність, освіта), мають підлягати суворим вимогам щодо якості даних, прозорості алгоритмів, людського нагляду, обов’язкової сертифікації перед впровадженням.

Гармонізація законодавства про захист персональних даних з європейським GDPR має включити специфічні положення щодо автоматизованого прийняття рішень, права на пояснення, права заперечувати проти автоматизованої обробки [56]. Створення ефективного регуляторного органу з повноваженнями нагляду, сертифікації, розгляду скарг є необхідною передумовою забезпечення дотримання законодавства.

Другий стратегічний напрям – створення інституційної інфраструктури для координації розвитку штучного інтелекту у публічному секторі. Доцільним є створення Національного координаційного центру розвитку штучного інтелекту при Кабінеті Міністрів України або Міністерстві цифрової трансформації [2]. Центр має виконувати функції розробки стратегій та програм, координації діяльності різних відомств, моніторингу впровадження, аналізу кращих практик, міжнародного співробітництва.

Міжвідомча рада з питань штучного інтелекту, яка включає представників ключових міністерств, регуляторних органів, експертної спільноти, бізнесу, громадянського суспільства, має забезпечувати узгодження позицій, обмін досвідом, спільне вирішення проблем [34]. Регулярні засідання ради, робочі групи з конкретних питань, публічні консультації забезпечують прозорість та інклюзивність процесу формування політики.

Створення мережі Центрів компетенцій зі штучного інтелекту у ключових сферах (охорона здоров'я, освіта, соціальний захист, правоохоронна діяльність, транспорт) дозволить накопичувати спеціалізовану експертизу, розробляти галузеві стандарти, надавати консультації відповідним органам влади.

Третій стратегічний напрям – розробка та реалізація Національної програми впровадження штучного інтелекту у публічне управління на 2025-2030 роки. Програма має включати чіткі цілі, завдання, індикатори, бюджет, відповідальних виконавців, терміни реалізації [20]. Пріоритетними напрямами впровадження можуть бути: автоматизація адміністративних процедур для

підвищення швидкості та зниження вартості послуг; аналітика даних для evidence-based policy making; персоналізація послуг на основі аналізу потреб громадян; проактивне надання послуг без необхідності звернення; виявлення шахрайства та корупції через аномалії у даних; прогнозування соціально-економічних трендів для превентивних втручань.

Програма має передбачати поетапний підхід – від пілотних проектів у контрольованих умовах до масштабування успішних рішень. Кожен проект має супроводжуватися ретельною оцінкою результатів, включаючи технічну ефективність, економічну доцільність, вплив на права людини, соціальні наслідки [49]. Механізм швидкого припинення проектів, які не демонструють очікуваних результатів або створюють неприйнятні ризики, має бути частиною гнучкого управління програмою.

Четвертий стратегічний напрям – забезпечення адекватного фінансування розвитку штучного інтелекту у публічному секторі. Необхідне виділення окремої бюджетної програми «Розвиток штучного інтелекту у публічному управлінні» з чітко визначеними статтями витрат, цілями, індикаторами результативності [11]. Фінансування має покривати не лише придбання технологій, але й розвиток інфраструктури, навчання персоналу, проведення досліджень, міжнародне співробітництво.

Диверсифікація джерел фінансування через залучення міжнародної технічної допомоги (ЄС, Світовий банк, двосторонні донори), грантів міжнародних організацій, державно-приватного партнерства дозволить масштабувати проекти за обмежених бюджетних ресурсів. Створення Фонду інновацій у публічному управлінні, який би підтримував інноваційні проекти впровадження штучного інтелекту через конкурсні гранти, може стимулювати креативність та експериментування.

П’ятий стратегічний напрям – розвиток національної екосистеми штучного інтелекту через партнерство публічного сектору, бізнесу, науки, громадянського суспільства. Державні замовлення на розробку систем штучного інтелекту для публічного сектору мають стимулювати вітчизняний

ІТ-бізнес до інвестицій у дослідження та розробки. Прозорі конкурсні процедури, справедлива оплата інтелектуальної праці, можливість масштабування рішень на інші органи влади роблять публічний сектор привабливим ринком для інноваційних компаній.

Науково-дослідні інститути та університети мають залучатися до розробки алгоритмів, проведення незалежних оцінок систем, етичних аудитів [53]. Програми спільних досліджень, коли держава фінансує наукові проекти з практичним застосуванням у публічному управлінні, створюють цінність для обох сторін. Стипендіальні програми для молодих дослідників, які працюють над проблемами використання ШІ у публічному секторі, формують кадровий резерв.

Громадянське суспільство має відігравати роль незалежного моніторингу впровадження штучного інтелекту, захисту прав громадян, формування суспільного діалогу про етичні наслідки [69]. Фінансування організацій громадянського суспільства для проведення досліджень, адвокації, громадського контролю забезпечує баланс між державними та суспільними інтересами.

Шостий стратегічний напрям – інтеграція України у глобальну екосистему штучного інтелекту через міжнародне співробітництво. Активна участь у міжнародних ініціативах, таких як Глобальне партнерство зі штучного інтелекту (GPAI), дозволяє обмінюватися досвідом, впливати на формування глобальних стандартів, отримувати доступ до кращих практик [20]. Двостороннє співробітництво з країнами-лідерами (Естонія, Сінгапур, Фінляндія) через меморандуми про взаєморозуміння, програми обміну експертами, спільні проекти прискорює навчання.

Гармонізація українських стандартів з європейськими у контексті підготовки до членства в ЄС має охоплювати не лише правове регулювання, але й технічні стандарти, процедури сертифікації, підходи до етичної оцінки. Це забезпечить сумісність українських систем з європейськими, полегшить транскордонне надання послуг, підвищить довіру європейських партнерів.

Сьомий стратегічний напрям – формування суспільної довіри до використання штучного інтелекту у публічному управлінні через прозорість та залучення громадян. Публічні консультації щодо впровадження систем ШІ у критичних сферах мають проводитися на ранніх етапах планування проектів [69]. Громадяни, експерти, зацікавлені групи мають можливість висловити занепокоєння, надати пропозиції, вплинути на дизайн систем.

Прозорість алгоритмів, які використовуються для прийняття рішень у публічному секторі, має забезпечуватися через публікацію інформації про логіку роботи, дані, які використовуються, критерії прийняття рішень, обмеження систем [70]. Портал відкритих даних має включати розділ «Алгоритмічна прозорість», де оприлюднюється інформація про системи ШІ, що використовуються державними органами.

Комунікаційна стратегія має роз'яснювати громадянам переваги використання штучного інтелекту для покращення якості послуг, заощадження бюджетних коштів, боротьби з корупцією, але також чесно визнавати обмеження та ризики [19]. Інформаційні кампанії через медіа, соціальні мережі, публічні заходи формують реалістичні очікування та розвіюють міфи про штучний інтелект.

Восьмий стратегічний напрям – створення системи моніторингу та оцінки впровадження штучного інтелекту у публічному секторі. Ключові індикатори ефективності (KPI) мають відстежувати технічну продуктивність систем (точність, швидкість, надійність), економічну ефективність (співвідношення витрат та вигод, економія бюджетних коштів), соціальний вплив (задоволеність громадян, доступність послуг, справедливість), впровадження етичних принципів (відсутність дискримінації, забезпечення прозорості, підзвітності).

Регулярні звіти про стан впровадження Національної програми, які включають досягнення, виклики, коригувальні дії, мають публікуватися та обговорюватися з широким колом стейкхолдерів. Незалежні оцінки, проведені

науковими інститутами або міжнародними організаціями, забезпечують об’єктивний погляд на результати.

Дев’ятий стратегічний напрям – розвиток етичної культури використання штучного інтелекту у публічному секторі. Прийняття Етичного кодексу використання штучного інтелекту у державному управлінні, який би визначав цінності, принципи, процедури етичного аналізу, механізми розв’язання етичних дилем, має стати орієнтиром для всіх учасників процесу. Створення етичних комітетів або призначення етичних радників у державних органах, які впроваджують системи ШІ, забезпечує інституційну підтримку етичної рефлексії.

Навчання державних службовців етичним аспектам штучного інтелекту, проведення етичних аудитів систем перед впровадженням, публічні обговорення етичних кейсів формують культуру відповідального використання технологій [59]. Механізми whistleblowing, коли працівники можуть конфіденційно повідомляти про етичні проблеми без страху репресій, забезпечують внутрішній контроль.

Десятий стратегічний напрям – побудова цифрової інфраструктури, необхідної для функціонування систем штучного інтелекту. Інвестиції у обчислювальні потужності (хмарні сервіси, дата-центри з GPU для навчання моделей), сховища даних, високошвидкісні мережі є передумовою для роботи з великими обсягами даних та складними алгоритмами [57]. Розвиток національної хмарної платформи для державного сектору, яка забезпечує масштабовані обчислювальні ресурси на вимогу, дозволяє уникнути необхідності кожному відомству будувати власну інфраструктуру.

Удосконалення якості даних у державних реєстрах та інформаційних системах через стандартизацію форматів, очищення від помилок, заповнення прогалин, регулярне оновлення підвищує цінність даних для аналітики та машинного навчання. Інтероперабельність систем через загальні стандарти API, єдині довідники, платформу «Трембіта» дозволяє інтегрувати дані з різних джерел для комплексного аналізу.

Впровадження принципів data governance – чітке визначення власників даних, правил доступу, процедур забезпечення якості, життєвого циклу даних – створює порядок у роботі з даними як стратегічним активом держави. Призначення Chief Data Officer у ключових відомствах забезпечує лідерство у управлінні даними.

Одинадцятий стратегічний напрям – стимулювання досліджень та інновацій у сфері штучного інтелекту для публічного управління. Програми грантової підтримки науково-дослідних проектів, які працюють над практичними задачами впровадження ШІ у державному секторі, створюють інтелектуальну базу для інновацій. Державні замовлення на дослідження конкретних проблем (виявлення шахрайства, прогнозування соціальних ризиків, оптимізація розподілу ресурсів) через конкурсні процедури залучають кращі наукові колективи.

Створення регуляторних пісочниць (regulatory sandboxes), де інноваційні рішення можуть тестуватися у контрольованому середовищі з тимчасовим послабленням деяких регуляторних вимог, заохочує експериментування [52]. Після успішного тестування та доведення безпечності рішення може масштабуватися на весь публічний сектор.

Хакатони, конкурси інновацій, виклики (challenges), де пропонуються реальні проблеми публічного управління, а учасники розробляють рішення на основі штучного інтелекту, залучають креативний потенціал широкого кола учасників – від студентів до досвідчених професіоналів. Переможці отримують призи, можливість впровадження рішення, контракти з державними органами.

Дванадцятий стратегічний напрям – забезпечення інклюзивності цифровізації та недопущення поглиблення цифрового розриву. Програми цифрової освіти для вразливих груп (літні люди, мешканці сільської місцевості, люди з інвалідністю) забезпечують, що переваги цифровізації доступні всім [12]. Розвиток цифрової інфраструктури у сільській місцевості, забезпечення доступності послуг через мобільні центри у віддалених регіонах,

альтернативні (не цифрові) канали для тих, хто не може користуватися технологіями, запобігають соціальній ексклюзії.

Проектування систем штучного інтелекту з урахуванням потреб різних груп користувачів, включаючи людей з обмеженими можливостями, дотримання стандартів веб-доступності, підтримка різних мов інтерфейсу забезпечують інклюзивність. Тестування систем на репрезентативних вибірках користувачів, включаючи вразливі групи, виявляє потенційні бар'єри доступності.

Таким чином, стратегічні напрями державної політики щодо розвитку штучного інтелекту у публічному секторі України охоплюють комплекс взаємопов'язаних заходів у сферах правового регулювання, інституційного розвитку, програмного планування, фінансування, партнерства, міжнародного співробітництва, формування довіри, моніторингу, етичної культури, інфраструктури, досліджень та інклюзивності, реалізація яких вимагає політичної волі, ресурсів, координації та послідовності протягом тривалого періоду.

Отже, аналіз перспектив та напрямів впровадження штучного інтелекту в публічне управління України дозволяє сформулювати наступні висновки.

По-перше, забезпечення інформаційної безпеки та захисту даних в умовах використання штучного інтелекту вимагає комплексного підходу, що включає розробку спеціалізованої стратегії кібербезпеки, впровадження багаторівневих технічних заходів захисту, гармонізацію законодавства з європейськими стандартами, посилення інституційного нагляду, при цьому особлива увага має приділятися специфічним загрозам для систем ШІ в умовах воєнного стану.

По-друге, формування компетентностей цифрового державного службовця є критичним фактором успішності впровадження інтелектуальних технологій і вимагає системної трансформації підходів до підбору, навчання та розвитку кадрів, включаючи модернізацію освітніх програм, створення

інфраструктури безперервного навчання, залучення молодих талантів, формування культури інновацій та особливої уваги до етичних аспектів.

По-третє, ефективна державна політика щодо розвитку штучного інтелекту у публічному секторі має базуватися на дванадцяти стратегічних напрямах, що охоплюють правове регулювання, інституційний розвиток, програмне планування, фінансування, партнерство, міжнародне співробітництво, формування довіри, моніторинг, етичну культуру, розвиток інфраструктури, стимулювання досліджень та забезпечення інклюзивності, при цьому успішна реалізація цих напрямів вимагає політичної волі, координації зусиль та послідовності дій протягом тривалого періоду.

ВИСНОВКИ

Узагальнюючи результати проведеного дослідження, можна констатувати, що формування інтелектуального публічного управління на основі технологій штучного інтелекту є ключовим стратегічним напрямом модернізації державного сектору України. Комплексний аналіз теоретичних засад, етапів цифрової еволюції, сучасного стану цифровізації, інституційно-правового забезпечення, бар'єрів та ризиків, міжнародних практик і потенційних моделей розвитку дозволив виявити систему чинників, які визначають можливості та обмеження впровадження інтелектуальних технологій у діяльність органів публічної влади. У цьому контексті сформульовані висновки відображають логіку проведеного дослідження та слугують методологічним підґрунтям для розроблення практичних рекомендацій і стратегічних рішень щодо подальшого розвитку штучного інтелекту в публічному секторі України.

1. Проведений аналіз засвідчив, що штучний інтелект у сфері публічного управління виступає якісно новим типом управлінського інструментарію, який поєднує технологічні алгоритми, соціально-управлінські механізми та етичні норми. Інтелектуальні системи в державному секторі не обмежуються автоматизацією рутинних операцій – вони формують підґрунтя для появи інтелектуального управління, орієнтованого на обробку великих масивів даних, створення прогнозних моделей і реалізацію проактивної логіки взаємодії держави з громадянами. Встановлено, що головною методологічною особливістю ШІ є його доповнювальна, а не замінювальна природа: технологія підсилює людський інтелект, але не може повністю перебрати на себе відповідальність за критичні рішення. Це вимагає поєднання алгоритмічних можливостей із людським контролем, а також формування етичних рамок, що запобігатимуть упередженості, дискримінації та непрозорості алгоритмів.

2. Здійснений аналіз етапів цифрової трансформації показав, що розвиток електронного урядування відбувався поступово: від інформатизації

окремих процесів до розбудови інтегрованих цифрових платформ і початку переходу до інтелектуального управління. Україна, попри складні політичні та економічні умови, змогла сформувати потужні цифрові активи – екосистему «Дія», електронні послуги, електронні реєстри, «Трембіту». Наступний етап трансформації передбачає не лише доступність сервісів, а й здатність держави проактивно реагувати на потреби громадян і прогнозувати управлінські рішення на основі даних. Еволюція цифрових технологій засвідчує, що інтелектуалізація держави є закономірним результатом розвитку цифрових платформ, однак потребує зміни управлінської культури, відмови від надмірної бюрократичності та переходу до мережевих моделей управління.

3. Дослідження показало, що впровадження штучного інтелекту потребує системного нормативно-правового забезпечення, яке охоплює питання етики, відповідальності, управління ризиками, захисту даних та безпеки. Наразі українське законодавство включає лише загальні цифрові акти та окремі концептуальні документи, а комплексне регулювання систем ШІ відсутнє. Це створює правовий вакуум, що стримує масштабування інтелектуальних рішень у публічному секторі. Для формування зрілої екосистеми необхідні: ухвалення спеціального Закону «Про штучний інтелект», створення національного регулятора або координаційного центру, впровадження стандартів етичного використання алгоритмів, розробка процедур оцінки ризиків та визначення відповідальності за використання автоматизованих рішень. Також потребує вдосконалення нормативна база щодо доступності, інтероперабельності та якості даних, що становлять основу роботи інтелектуальних систем.

4. Оцінка цифрової трансформації в Україні засвідчила, що країна має суттєві напрацювання в модернізації цифрової інфраструктури, однак рівень готовності органів влади до широкого використання ШІ залишається недостатнім. Інтелектуальні системи впроваджуються точково – як пілотні проєкти, а не як частина системної політики. Водночас цифрові компетентності державних службовців потребують значного підсилення:

більшість управлінців не володіють інструментами аналізу даних, не розуміють принципи роботи алгоритмів та їх обмеження, мають низький рівень готовності до змін і інновацій. Таким чином, розвиток інтелектуального управління вимагає комплексної реформи навчання та підвищення кваліфікації – через Національну програму з розвитку цифрових і AI-компетентностей, створення Центру цифрових компетентностей, модернізацію освітніх стандартів НАДУ, стимулювання безперервного професійного розвитку та формування культури інновацій у державному секторі.

5. Виявлено широкий спектр бар'єрів – технологічних (низька якість даних, відсутність інтероперабельності), організаційних (опір змінам, бюрократичність структур), правових (відсутність регулювання відповідальності), етичних (ризики дискримінації, упередженості), кадрових (нестача фахівців), фінансових (обмежені ресурси) та безпекових. Особливої складності додає воєнний контекст, адже українська цифрова інфраструктура постійно зазнає російських кібератак. Це робить питання кіберзахисту систем ШІ надзвичайно актуальним. Зміцнення інформаційної безпеки потребує створення багаторівневих систем захисту, гармонізації законодавства з GDPR, створення Національного центру кібербезпеки систем ШІ, розробки спеціальної стратегії з кіберзахисту алгоритмічних моделей та впровадження систем моніторингу аномалій у реальному часі. Також важливо формувати етичні практики, що мінімізуватимуть дискримінаційні ризики та забезпечуватимуть захист прав людини.

6. Аналіз міжнародного досвіду показав, що провідні країни успішно впроваджують ШІ завдяки стратегічному підходу, державним інвестиціям, наявності спеціального законодавства, розвитку дослідницьких центрів, співпраці між державою та бізнесом та увазі до етичності й безпеки систем. Особливу цінність для України становлять естонська модель X-Road, канадські стандарти етичного використання алгоритмів, європейські регуляції AI Act, корейські моделі державних AI-сервісів. На основі цього визначено

стратегічні напрями державної політики України: прийняття спеціального закону про ШІ; створення координаційної інституції; розробка Національної програми впровадження ШІ у публічне управління до 2030 року; розвиток цифрової інфраструктури; формування вимог до компетентностей державних службовців; активна участь у міжнародних альянсах; стимулювання досліджень і бізнес-інновацій; розвиток етичних стандартів; забезпечення інклюзивності цифровізації.

Україна знаходиться на стратегічному рубежі переходу від цифровізації базових процесів до системного впровадження інтелектуальних технологій у державне управління. Від здатності інтегрувати штучний інтелект відповідально, безпечно та ефективно залежить якість управління, рівень довіри громадян до влади, стійкість держави до глобальних і воєнних загроз та темпи європейської інтеграції. Реалізація потенціалу ШІ потребує комплексної політики, системної координації, інституційної спроможності, високих компетентностей управлінців та збалансування технологічних інновацій з цінностями демократичного врядування.

Додаток

АПРОБАЦІЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ

Результати кваліфікаційної магістерської роботи були апробовані у ході науково-дослідної практики. Основні положення та висновки представлені на науковій конференції Результати кваліфікаційної магістерської роботи були апробовані у ході науково-дослідної практики. Основні положення та висновки представлені на XVI Міжнародній науково-практичній конференції «Концептуальні шляхи розвитку науки та освіти» (15-16 листопада 2025 року). Матеріали дослідження опубліковано у збірнику конференції: Галич Н. Стратегічні напрями державної політики щодо розвитку штучного інтелекту у публічному секторі України. *Концептуальні шляхи розвитку науки та освіти*: матеріали XVI Міжнародної науково-практичної конференції м. Львів, 15-16 листопада 2025 року. Львів : Львівський науковий форум, 2025. С. 24-24. Окремі результати дослідження опубліковано у фаховому науковому журналі у статті: Стороженко Л., Андросова К., Галич Н. Інтелектуальні технології та інформаційна безпека: стратегічні орієнтири розвитку цифрового публічного управління. *Публічно-управлінські та цифрові практики.* 2025. Вип. 4(7). URL: https://journals.duikt.edu.ua/index.php/public/about.

Апробація засвідчує коректність застосованих методів, наукову обґрунтованість та практичну релевантність отриманих результатів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації : розпорядження Кабінету Міністрів України від 17 січ. 2018 р. № 67-р. URL: https://zakon.rada.gov.ua/go/67-2018-р.

2. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 2 груд. 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/go/1556-2020-р.

3. Деякі питання цифрового розвитку : постанова Кабінету Міністрів України від 30 січ. 2019 р. № 56. URL: https://zakon.rada.gov.ua/laws/show/56-2019-п.

4. Тімошенко І. Є. Правове регулювання використання систем штучного інтелекту : дис.... канд. юрид. наук : 12.00.07. Київ, 2021. 253 с.

5. Чукут С. А. Штучний інтелект у публічному управлінні: переваги цифрових технологій та загрози суверенному інформаційному простору. Публічне управління та регіональний розвиток. 2024. № 2. С. 145–162. URL: https://www.researchgate.net/publication/378525811.

6. Чукут С. А. Виклики застосування штучного інтелекту у сфері публічного управління, врядування та послуг. Державне управління: удосконалення та розвиток. 2024. № 2. URL: https://www.researchgate.net/publication/378526159.

7. Бурак А. В. Штучний інтелект у сфері публічного управління: можливості та виклики. Актуальні проблеми підвищення кваліфікації та перепідготовки державних службовців : матеріали наук.-практ. конф. Полтава: ПДАУ, 2023. С. 18–22.

8. Коляденко С. В. Цифрова економіка: передумови та етапи становлення в Україні та світі. Економіка. Фінанси. Менеджмент: актуальні питання науки і практики. 2016. № 6. С. 105–112.

9. Красноносова О. М., Грицишен Д. О., Ревуцька Н. В. Застосування штучного інтелекту в бізнес-діяльності підприємств. Економіка та суспільство. 2023. Вип. 58. URL: https://economyandsociety.in.ua/index.php/journal/article/view/3348.

10. Дубина О. В., Плотніков О. В. Штучний інтелект: сутність, аналіз застосування, перспективи розвитку. Науковий вісник Херсонського державного університету. Серія Економічні науки. 2018. Вип. 30. С. 183–187. URL: https://ej.journal.kspu.edu/index.php/ej/article/view/405.

11. Безус А. М. Стан та перспективи розвитку законодавства України у сфері цифрової економіки та цифрового суспільства. Київський часопис права. 2021. № 2. С. 68–73. URL: https://kyivchasprava.kneu.in.ua/index.php/kyivchasprava/article/view/26.

12. Гринчук Ю. С., Ковальчук В. Б. Аспекти розвитку цифрової економіки в Україні. Економічний простір. 2018. № 139. С. 79–90. URL: https://prostir.pdaba.dp.ua/index.php/journal/article/view/372.

13. Апалькова В. В. Концепція розвитку цифрової економіки в Євросоюзі та перспективи України. Вісник Дніпропетровського університету. Серія: Менеджмент інновацій. 2015. № 4. С. 9–18.

14. Стан розвитку штучного інтелекту у світі. Сідкон. URL: https://sidcon.com.ua/tpost/tztfujgpk1-stan-rozvitku-shtuchnogo-ntelektu-u-svt.

15. Штучний інтелект в Україні: як розвивається галузь і яку користь для країни приносить. Cases Media. 2023. 26 жовт. URL: https://cases.media/en/article/shtuchnii-intelekt-v-ukrayini-yak-rozvivayetsya-galuz-i-yaku-korist-dlya-krayini-prinosit.

16. Уряд затвердив Концепцію розвитку штучного інтелекту в Україні з урахуванням пропозицій Цифролаби. Лабораторія цифрової безпеки. URL: https://dslua.org/publications/uriad-zatverdyv-kontseptsiiu-rozvytku-shtuchnoho-intelektu-v-ukraini-z-urakhuvanniam-propozytsiy-tsyfrolaby/.

17. Концепція розвитку цифрової економіки та суспільства. Український інститут майбутнього. URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html.

18. Кабмін затвердив концепцію розвитку штучного інтелекту в Україні. Економічна правда. 2020. 2 груд. URL: https://epravda.com.ua/news/2020/12/2/668750/.

19. Штучний інтелект у державному управлінні викликає недовіру громадян. Наука 314. 2025. 13 лип. URL: https://sci314.com/news/shtuchnyi-intelekt-u-derzhavnomu-upravlinni-vyklykaie-nedoviru-hromadian/.

20. Ukraine National Strategy for Development of Artificial Intelligence 2021-2030. OECD.AI. 2021. URL: https://wp.oecd.ai/app/uploads/2021/12/Ukraine_National_Strategy_for_Development_of_Artificial_Intelligence_in_Ukraine_2021-2030.pdf.

21. Закон України «Про електронні довірчі послуги» : Закон України від 5 жовт. 2017 р. № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19.

22. Про затвердження Положення про Міністерство цифрової трансформації України : постанова Кабінету Міністрів України від 18 верес. 2019 р. № 856. URL: https://zakon.rada.gov.ua/laws/show/856-2019-п.

23. Баранов О. А. Інтернет речей і штучний інтелект: витоки проблеми правового регулювання. Інформація і право. 2018. № 3(26). С. 61–70.

24. Карчевський М. В. Штучний інтелект як інструмент публічного управління: переваги та загрози. Державне управління: удосконалення та розвиток. 2020. № 11. URL: http://www.dy.nayka.com.ua/?op=1&z=1960.

25. Семенченко А. І. Цифрова трансформація публічного управління в Україні: виклики та перспективи. Теорія та практика державного управління. 2019. № 4(67). С. 1–8.

26. Дрешпак В. М. Електронне урядування та електронна демократія : навч. посіб. : у 15 ч. Київ : ФОП Москаленко О. М., 2017. Ч. 1: Основи. 88 с.

27. Клименко І. В. Технології електронного урядування. Київ : ДП «Видавничий дім «Персонал», 2018. 236 с.

28. Соломко Ю. Цифрова трансформація як драйвер розвитку та інструмент забезпечення стратегічних інтересів держави на міжнародній арені. Стратегічні пріоритети. 2019. № 1-2. С. 78–89.

29. Машлій Г., Яцина В. Розвиток електронного урядування в Україні в контексті європейської інтеграції. Ефективність державного управління. 2020. Вип. 1(62). С. 123–133.

30. Гудзь О. Є., Федулова Л. І., Кожушко О. А. Штучний інтелект та інклюзивне зростання економіки. Проблеми економіки. 2020. № 2(44). С. 219–227.

31. Ляшенко В. І., Вишневський О. С. Цифрова модернізація економіки України як можливість проривного розвитку : монографія. Київ : Інститут економіки промисловості НАН України, 2018. 252 с.

32. Дія. Цифрова освіта : веб-сайт. URL: https://osvita.diia.gov.ua/.

33. Портал Дія : веб-сайт. URL: https://diia.gov.ua/.

34. Міністерство цифрової трансформації України : офіційний веб-сайт. URL: https://thedigital.gov.ua/.

35. Єдиний державний вебпортал електронних послуг : веб-сайт. URL: https://portal.diia.gov.ua/.

36. OECD Artificial Intelligence in Society. Paris : OECD Publishing, 2019. 150 p. URL: https://doi.org/10.1787/eedfee77-en.

37. OECD Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449. Paris : OECD, 2019. URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

38. 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. 2024. 2024/1689. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

39. European Commission. Ethics Guidelines for Trustworthy AI. Brussels: European Commission, 2019. 39 p. URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

40. White House. Executive Order on Maintaining American Leadership in Artificial Intelligence. Washington, D.C., 2019. URL: https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

41. National Artificial Intelligence Research and Development Strategic Plan 2023 Update. Washington, D.C. : National Science and Technology Council, 2023. 80 p.

42. South Korea. National Strategy for Artificial Intelligence. Seoul : Ministry of Science and ICT, 2019. URL: https://www.msit.go.kr/english/.

43. e-Estonia : веб-сайт. URL: https://e-estonia.com/.

44. X-Road : веб-сайт. URL: https://x-road.global/.

45. Smart Nation Singapore : веб-сайт. URL: https://www.smartnation.gov.sg/.

46. UNESCO Recommendation on the Ethics of Artificial Intelligence. Paris : UNESCO, 2021. 38 p. URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137.

47. World Bank. World Development Report 2021: Data for Better Lives. Washington, D.C. : World Bank, 2021. 352 p. URL: https://www.worldbank.org/en/publication/wdr2021.

48. Wirtz B. W., Weyerer J. C., Geyer C. Artificial Intelligence and the Public Sector–Applications and Challenges. International Journal of Public Administration. 2019. Vol. 42, No. 7. P. 596–615. DOI: 10.1080/01900692.2018.1498103.

49. Zuiderwijk A., Chen Y.-C., Salem F. Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. Government Information Quarterly. 2021. Vol. 38, Iss. 3. Article 101577. DOI: 10.1016/j.giq.2021.101577.

50. Dawes S. S. The Evolution and Continuing Challenges of E-Governance. Public Administration Review. 2008. Vol. 68, Suppl. 1. P. S86–S102. DOI: 10.1111/j.1540-6210.2008.00981.x.

51. Gil-Garcia J. R., Pardo T. A. E-government success factors: Mapping practical tools to theoretical foundations. Government Information Quarterly. 2005. Vol. 22, Iss. 2. P. 187–216. DOI: 10.1016/j.giq.2005.02.001.

52. Janowski T. Digital government evolution: From transformation to contextualization. Government Information Quarterly. 2015. Vol. 32, Iss. 3. P. 221–236. DOI: 10.1016/j.giq.2015.07.001.

53. Осадча Н. В., Осадча К. П. Аналіз досвіду використання технологій штучного інтелекту у закладах освіти різних країн світу. Науковий вісник Ужгородського університету. Серія: Педагогіка. Соціальна робота. 2019. Вип. 2(45). С. 233–236.

54. Кібербезпека в Україні: виклики та загрози : аналітична доповідь / за ред. Горбуліна В. П. Київ : НІСД, 2016. 96 с.

55. Золотар О. О. Інформаційна безпека людини: теорія і практика : монографія. Київ, 2018. 446 с.

56. Швець М. Я. Захист персональних даних в умовах цифровізації: виклики та перспективи для України. Інформація і право. 2020. № 2(33). С. 87–95.

57. Корнієнко Д. М., Опир М. А. Big Data у публічному управлінні: можливості та виклики. Інвестиції: практика та досвід. 2019. № 20. С. 120–125.

58. Відкриті дані : портал відкритих даних. URL: https://data.gov.ua/.

59. Національне агентство України з питань державної служби : офіційний веб-сайт. URL: https://nads.gov.ua/.

60. Про затвердження Професійних стандартів за професіями «Фахівець з цифрового розвитку», «Менеджер цифрового розвитку» : наказ Мінцифри від 7 груд. 2021 р. № 171. URL: https://zakon.rada.gov.ua/rada/show/v0171881-21.

61. Нижник Н. Р., Машков О. А. Системний підхід в організації державного управління : навч. посіб. Київ : УАДУ, 1998. 160 с.

62. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 4th ed. Hoboken : Pearson, 2020. 1136 p.

63. Brynjolfsson E., McAfee A. The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. New York : W. W. Norton & Company, 2014. 336 p.

64. Schwab K. The Fourth Industrial Revolution. Geneva : World Economic Forum, 2016. 192 p.

65. Floridi L. The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities. Oxford : Oxford University Press, 2023. 272 p.

66. Їжак О. І. Цифрова трансформація державного управління: проблеми та перспективи. Інвестиції: практика та досвід. 2020. № 15-16. С. 133–137.

67. Машинне навчання та глибоке навчання: основи та застосування / за ред. Бідюк П. І. Київ : НТУУ «КПІ», 2019. 312 с.

68. Петренко С. А. Блокчейн у державному управлінні: можливості та перспективи впровадження. Публічне управління та митне адміністрування. 2019. № 3(22). С. 89–94.

69. Грицяк Н. В., Соловйов С. Г. Електронна демократія : навч. посіб. Київ : НАДУ, 2015. 66 с.

70. Коліушко І. Б., Тимощук В. П. Інформаційна відкритість органів виконавчої влади. Київ : Факт, 2015. 78 с.