

УДК 351:004]:[004.056+004.8
DOI: 10.31673/2786-7412.2025.040710

Ліна СТОРОЖЕНКО

кандидат філологічних наук, доцент,
доцент кафедри публічного управління та адміністрування
Державного університету інформаційно-комунікаційних технологій, м. Київ
ORCID ID: 0000-0003-2766-3712
e-mail: st-leena@i.ua

Lina STOROZHENKO

Candidate of Philological Sciences, Associate Professor,
Associate Professor of Public Management and Administration,
State University of Information and Communication Technologies, Kyiv
ORCID ID: 0000-0003-2766-3712
e-mail: st-leena@i.ua

Каріна АНДРОСОВА

магістрант кафедри публічного управління та адміністрування
Державного університету інформаційно-комунікаційних технологій, м. Київ
e-mail: karin_ka@gmail.com

Karina ANDROSOVA

Master's student of the Department of Public Management and Administration
State University of Information and Communication Technologies, Kyiv
e-mail: karin_ka@gmail.com

Назарій ГАЛИЧ

магістрант кафедри публічного управління та адміністрування
Державного університету інформаційно-комунікаційних технологій, м. Київ
e-mail: halych_n@gmail.com

Nazariy HALYCH

Master's student, Department of Public Management and Administration
State University of Information and Communication Technologies, Kyiv
e-mail: halych_n@gmail.com

**ІНТЕЛЕКТУАЛЬНІ ТЕХНОЛОГІЇ ТА ІНФОРМАЦІЙНА БЕЗПЕКА:
СТРАТЕГІЧНІ ОРІЄНТИРИ РОЗВИТКУ
ЦИФРОВОГО ПУБЛІЧНОГО УПРАВЛІННЯ**

**INTELLECTUAL TECHNOLOGIES AND INFORMATION SECURITY:
STRATEGIC GUIDELINES FOR THE DEVELOPMENT
OF DIGITAL PUBLIC ADMINISTRATION**

Анотація. У статті досліджуються стратегічні орієнтири розвитку цифрового публічного управління в Україні через призму впровадження інтелектуальних технологій та забезпечення інформаційної безпеки.

Проаналізовано трансформацію владних відносин в умовах цифровізації, зокрема феномен нетократії як нової форми влади, що базується на контролі інформаційних потоків та мережевих ресурсів. Розглянуто виклики та можливості інтеграції штучного інтелекту, великих даних, блокчейн-технологій у систему публічного управління України.

Особливу увагу приділено проблемам кібербезпеки в контексті російської агресії та гібридних загроз. Досліджено досвід впровадження платформ електронного урядування, зокрема «Дія», як приклад успішної цифрової трансформації. На основі комбінованого підходу, що поєднує теоретичний аналіз і емпіричні дані, визначено ключові напрями удосконалення системи цифрового публічного управління: розбудова національної інфраструктури кібербезпеки, розвиток компетентностей цифрової нетократії, імплементація етичних принципів використання ШІ в державному секторі, створення стійких систем захисту критичної інфраструктури. Запропоновано модель розвитку цифрового публічного управління, що враховує специфіку воєнного стану та євроінтеграційні прагнення України.

Ключові слова: цифрове публічне управління, інтелектуальні технології, інформаційна безпека, нетократія, штучний інтелект, кібербезпека, цифрова трансформація, електронне урядування.

Abstract. The article examines strategic guidelines for the development of digital public administration in Ukraine through the prism of implementing intelligent technologies and ensuring information security. The transformation of power relations in the context of digitalization is analyzed, particularly the phenomenon of netocracy as a new form of power based on control of information flows and network resources. The challenges and opportunities of integrating artificial intelligence, big data, and blockchain technologies into Ukraine's public administration system are examined.

Special attention is paid to cybersecurity issues in the context of Russian aggression and hybrid threats. The experience of implementing e-government platforms, particularly «Diia», as an example of successful digital transformation is studied. Based on a combined approach that integrates theoretical analysis and empirical data, key areas for improving the digital public administration system are identified: development of national cybersecurity infrastructure, development of digital netocracy competencies, implementation of ethical principles for AI use in the public sector, creation of resilient critical infrastructure protection systems. A strategic model for the development of digital public administration is proposed, taking into account the specifics of martial law and Ukraine's European integration aspirations.

Keywords: digital public administration, intelligent technologies, information security, netocracy, artificial intelligence, cybersecurity, digital transformation, e-government.

Постановка проблеми. Сучасний етап розвитку публічного управління характеризується масштабною цифровою трансформацією, що радикально змінює механізми взаємодії держави, громадян та бізнесу. В умовах четвертої промислової революції інтелектуальні технології (штучний інтелект (ШІ), машинне навчання, обробка великих даних, блокчейн тощо) стають критичними факторами ефективності державного управління. Разом з тим, зростання цифровізації супроводжується новими викликами у сфері інформаційної безпеки, що особливо

актуально для України в контексті протидії російській агресії та гібридним загрозам.

Трансформація владних відносин у цифрову епоху призводить до формування нових еліт, так званої, нетократії, яка контролює інформаційні потоки та мережеві ресурси, витісняючи традиційну бюрократію. Цей «нетократичний» феномен суттєво впливає на архітектуру публічного управління, створюючи як нові можливості для демократизації та прозорості, так і ризики монополізації цифрової влади. Україна демонструє амбітні кроки у цифровій трансформації державного сектору. Створення платформи «Дія», впровадження електронних сервісів, розвиток відкритих даних свідчать про готовність держави до інноваційних змін. Однак повномасштабне вторгнення Росії у 2022 році актуалізувало питання стійкості цифрової інфраструктури, захисту критичних інформаційних систем та кібербезпеки як компоненту національної безпеки.

Актуальність дослідження зумовлена необхідністю формування стратегічного бачення розвитку цифрового публічного управління в Україні, що забезпечить баланс між технологічними інноваціями, ефективністю державних послуг та надійним захистом інформаційного простору в умовах воєнного стану та євроінтеграційних процесів.

Аналіз останніх досліджень і публікацій. Проблематика цифрової трансформації публічного управління активно досліджується вітчизняними та зарубіжними науковцями.

Українські дослідники С. Квітка, В. Корсун, Ю. Магиляс аналізували перспективні напрямки досліджень цифрової трансформації публічного управління, наголошуючи на необхідності системного підходу до цифрового розвитку [5]; О. Карпенко досліджував специфіку публічного управління в умовах цифрової трансформації [6]; Н. Грицяк та Ю. Соломко вивчали цифрову трансформацію публічного управління та перспективи для України [7]; В. Куйбіда, О. Карпенко, В. Наместнік розробляли базові дефініції понятійно-категоріального апарату цифрового врядування в Україні [8]; К. Линьов досліджував відкриті дані як інструмент публічного управління [9]; Л. Стороженко аналізувала нетократичне публічне управління в контексті електронної демократії та глобалізаційних орієнтирів інформаційного суспільства [21; 22]; теоретичні засади електронного урядування розглядали О. Баранов [1], А. Семенченко [2], наголошуючи на необхідності системного підходу до впровадження цифрових технологій у державному секторі. Свого часу питання інформаційної безпеки в контексті публічного управління студіювали В. Горбулін, О. Додонов, Д. Ланде, підкреслюючи критичну важливість захисту державних інформаційних ресурсів [10]; Д. Дубов, М. Ожеван, С. Гнатюк досліджували інформаційну безпеку в умовах критичної інформаційної інфраструктури держави [11].

Застосування штучного інтелекту в державному управлінні досліджували низка закордонних авторів, які аналізували потенціал ШІ для трансформації публічних послуг [12], та розглядали алгоритмічне управління та його етичні виміри [13], питання підзвітності автоматизованих рішень у публічному секторі [14]. М. Кастельс у фундаментальній праці «Інформаційна епоха: економіка, суспільство і культура» розвинув ідею мережевого суспільства, в якому влада концентрується навколо вузлів глобальних інформаційних мереж [4]. Концепція нетократії була запропонована шведськими футурологами А. Бардом та

Я. Зодерквістом, які прогнозували заміну індустріальної бюрократії мережевою елітою, яка контролює інформаційні потоки [3].

Попри значний науковий доробок, у науковій літературі, на нашу думку, недостатньо представлені комплексні дослідження, що інтегрують проблематику інтелектуальних технологій, інформаційної безпеки та феномену нетократії в контексті стратегічного розвитку цифрового публічного управління України, особливо з урахуванням воєнних реалій та євроінтеграційних процесів.

Мета статті – визначити стратегічні орієнтири розвитку цифрового публічного управління в Україні на основі аналізу взаємозв'язку інтелектуальних технологій, інформаційної безпеки та трансформації владних відносин у напрямку нетократії.

Виклад основного матеріалу. Трансформація суспільних відносин в умовах інформаційної революції призводить до формування нової владної еліти – нетократії. На відміну від традиційної бюрократії, що базувалася на ієрархічному контролі та монополії на інформацію, нетократія отримує владу через контроль мережових потоків інформації, даних та цифрових платформ. А. Бард та Я. Зодерквіст стверджують, що в постіндустріальному суспільстві найціннішим ресурсом стає не капітал, а увага та доступ до інформаційних мереж [3]. Нетократи – це не лише ІТ-спеціалісти, але й усі, хто володіє компетенціями управління інформаційними потоками, створення та модерації цифрових платформ, аналізу великих даних. М. Кастельс в унісон цій ідеї, показує, як у мережевому суспільстві влада набуває нових форм, базуючись на контролі інформаційних потоків та комунікаційних мереж [4].

У контексті публічного управління нетократія проявляється у кількох вимірах:

- ❧ відбувається зміщення центру прийняття рішень від традиційних бюрократичних структур до цифрових платформ та систем на основі даних. Відтак алгоритми ШІ, системи аналітики великих даних фактично стають новими «чиновниками», які приймають або готують рішення у різних сферах [12];
- ❧ формується нова технократична еліта, яка володіє цифровими компетенціями та має привілейований доступ до управління критичною інфраструктурою. Наприклад, в Україні це проявляється у зростанні впливу Міністерства цифрової трансформації, ІТ-спеціалістів державних органів, розробників цифрових платформ [16; 21];
- ❧ відбувається поступова трансформація механізмів легітимації влади – якщо бюрократія легітимізувалася через формальні процедури та ієрархію, то нетократія отримує легітимність через «цифрову ефективність» – швидкість, зручність, персоналізацію послуг тощо [5];
- ❧ виникають нові форми нерівності – збільшується цифровий розрив між тими, хто володіє цифровими компетенціями та доступом до мережових ресурсів, і тими, хто залишається поза цифровими процесами, що створює ризики цифрової ексклюзії вразливих груп населення.

Для України феномен нетократії має особливе значення. З одного боку, молоде покоління державних службовців із цифровими компетенціями може стати драйвером модернізації архаїчної бюрократичної системи [17], з іншого – існують ризики формування закритої технократичної еліти, яка контролюватиме цифрову інфраструктуру без достатньої демократичної підзвітності. Відтак критично

важливим є створення механізмів «демократичної нетократії» – моделі, де цифрова влада поєднується з принципами прозорості, підзвітності, інклюзивності та захисту прав громадян [8; 22], що вимагає розробки нормативно-правової бази, яка регулює використання алгоритмічних систем прийняття рішень, захищає персональні дані та забезпечує право на пояснення автоматизованих рішень.

Впровадження інтелектуальних технологій у публічне управління радикально змінює його можливості, створюючи необхідні передумови для переходу від реактивного до проактивного урядування. Штучний інтелект у публічному управлінні застосовується у кількох напрямках. Так, автоматизація адміністративних процесів передбачає використання чат-ботів та віртуальних асистентів, які обробляють звернення громадян 24/7, систем розпізнавання образів для прискорення перевірки документів, алгоритмів машинного навчання для оптимізації розподілу ресурсів [12], крім цього, в Україні запроваджено AI-помічника у додатку «Дія», який консультує громадян з питань отримання послуг [16].

Аналітика та прогнозування за допомогою систем на основі ШІ дозволяє аналізувати великі масиви даних для виявлення трендів, прогнозування соціально-економічних процесів, раннього попередження кризових ситуацій, що дозволяє переходити від реагування на проблеми до їх превентивного вирішення [13]; персоналізація послуг через ШІ дає можливість адаптувати державні послуги до індивідуальних потреб громадян, пропонуючи релевантні сервіси на основі життєвих подій та контексту користувача. Підтримка прийняття рішень через інтелектуальні системи полягає в аналізі складних багатофакторних ситуацій, моделюванні наслідків альтернативних рішень, наданні рекомендацій особам, які приймають рішення.

Великі дані трансформують доказову базу державної політики – замість спорадичних опитувань та звітності, уряд отримує можливість аналізувати реальну поведінку громадян та бізнесу в реальному часі [9]. Наприклад, аналіз транзакційних даних платформи «Дія» дозволяє виявляти проблемні місця у наданні послуг, оптимізувати процеси, персоналізувати комунікацію; блокчейн-технології забезпечують прозорість, незмінність та безпеку державних реєстрів. Україна є одним із «піонерів» застосування блокчейну в публічному секторі (електронні аукціони Prozorro працюють на блокчейні, розробляються проєкти блокчейн-реєстрів земельних ділянок та освітніх документів). Блокчейн стала прогресивною технологією завдяки якій реалізується можливість зниження корупційних ризиків.

Однак впровадження інтелектуальних технологій породжує і низку викликів. Так, етичні проблеми пов'язані з тим, що алгоритмічна упередженість може відтворювати та посилювати існуючу дискримінацію; непрозорість «чорних скриньок» ШІ ускладнює підзвітність рішень; масове збирання даних загрожує приватності та ін. [14]; технологічні ризики включають залежність від IT-систем, що створює різнотипові вразливості; помилки в алгоритмах можуть мати масштабні наслідки; недостатня кібербезпека відкриває шлях для зловмисників тощо [11]; організаційні бар'єри проявляються у дефіциті цифрових компетенцій у державних службовців; інституційній інерції та опорі змінам; фрагментарності впровадження без системної інтеграції [17]; правові прогалини стосуються відсутності регулювання використання ШІ в публічному секторі; неузгодженості із

європейськими стандартами захисту даних; правової невизначеності статусу автоматизованих рішень [20].

Для України критично важливим є розробка Національної стратегії штучного інтелекту, яка б визначила принципи етичного та безпечного використання ШІ в державному секторі, механізми аудиту алгоритмів, вимоги до прозорості та пояснюваності автоматизованих рішень.

Повномасштабна російська агресія проти України продемонструвала критичну важливість кібербезпеки для стійкості держави. Кібератаки стали невід'ємним компонентом гібридної війни, цілями якої є критична інфраструктура, державні інформаційні системи, фінансовий сектор [11]. Водночас Україна продемонструвала високий рівень кіберстійкості: критичні системи продовжували функціонувати, платформа «Дія» забезпечувала надання послуг навіть під час масованих атак, швидко відновлювалися скомпрометовані ресурси, що стало можливим завдяки проактивній політиці кібербезпеки [18]. Ще до повномасштабного вторгнення Україна інвестувала в розбудову національної системи кібербезпеки, створювала команди реагування (CERT-UA), проводила навчання та тренінги.

Міжнародна співпраця з НАТО, ЄС, провідними технологічними компаніями (Microsoft, Google, Amazon) забезпечила технічну підтримку, обмін розвідданими про загрози, доступ до хмарних ресурсів. Децентралізація та резервування критичних державних систем на серверах за кордоном, застосування розподіленої архітектури ускладнили їх виведення з ладу. Залучення приватного сектору, зокрема волонтерської «ІТ-армії» України, проведення контрнаступальних кібероперацій, надання технічної експертизи та ресурсів ІТ-компаніями також сприяло кіберстійкості держави.

Попри все, виклики залишаються значними. Інфраструктурна вразливість полягає в тому, що значна частина державних органів використовує застаріле програмне забезпечення та обладнання; недостатньо розвинена культура кібергігієни серед державних службовців. Кадровий дефіцит проявляється у браку спеціалістів з кібербезпеки у державному секторі; конкуренції з приватним сектором за талановитих фахівців. Правові обмеження стосуються недосконалості законодавства про кіберзлочини; складності міжнародного переслідування кіберзловмисників. Загрози критичній інфраструктурі зростають, оскільки енергетика, транспорт, фінанси дедалі більше залежать від цифрових систем, що робить їх привабливими цілями.

Відтак стратегічними пріоритетами розвитку кібербезпеки в Україні мають стати: розбудова національної інфраструктури кібербезпеки через створення Національного центру кібербезпеки з потужними аналітичними можливостями; розвиток державно-приватного партнерства у сфері кіберзахисту [18]; підготовка кадрів, яка передбачає розширення освітніх програм з кібербезпеки; стажування державних службовців у провідних центрах кіберзахисту; створення привабливих умов для роботи спеціалістів у державному секторі [17]; міжнародна інтеграція, що вимагає гармонізації вітчизняного законодавства з європейськими стандартами; участь у міжнародних системах обміну інформацією про кіберзагрози [15]; захист критичної інфраструктури, який передбачає проведення обов'язкових аудитів кібербезпеки об'єктів критичної інфраструктури; впровадження принципів «безпеки за дизайном» тощо.

Наразі платформа «Дія» є флагманським проектом цифрової трансформації держави в Україні, що демонструє можливості інтелектуальних технологій для модернізації публічних послуг [16]. Запущена у 2020 році, «Дія» швидко стала найпопулярнішим державним додатком у Східній Європі. Ключові досягнення платформи включають масштаб впровадження: станом на 2024 рік додатком користується понад 20 мільйонів українців, доступно понад 120 електронних послуг. Цифрові документи – електронні паспорти, водійські посвідчення, студентські квитки, COVID-сертифікати мають юридичну силу, що робить Україну піонером у цифровій ідентифікації.

Спрощення процедур через «Дію» (реєстрація ФОП за 15 хвилин, зміна місця реєстрації онлайн, отримання довідок без відвідування установ та ін.) радикально знизило бюрократичне навантаження. Інтеграція життєвих подій реалізує концепцію «держава у смартфоні», де громадянин автоматично отримує релевантні послуги на основі життєвих подій (народження дитини, придбання авто тощо). Зауважимо, що «Дія» продовжувала працювати навіть під масованими російськими кібератаками завдяки розподіленій архітектурі та хмарним технологіям; через «Дію» здійснювалися виплати внутрішньо переміщеним особам, підтримка постраждалих від війни, що забезпечило швидкість та прозорість соціальної допомоги.

Досвід «Дії» доводить, що успішна цифрова трансформація вимагає не лише технологічних інновацій, але й організаційних змін, політичної волі, підтримки громадян [5]. Важливим фактором успіху стало створення окремого Міністерства цифрової трансформації України з мандатом на проведення реформ та необхідними ресурсами. Перспективи розвитку платформи передбачають впровадження повноцінної цифрової ідентичності, що дозволить використовувати «Дію» для доступу до приватних сервісів; розширення міжнародної інтероперабельності для визнання українських цифрових документів в ЄС [20]; інтеграцію з системами електронної демократії для участі громадян у прийнятті рішень; розвиток предиктивних сервісів на основі ШІ тощо.

На основі проведеного аналізу пропонується стратегічна модель розвитку цифрового публічного управління в Україні, що інтегрує інтелектуальні технології, інформаційну безпеку та принципи демократичної нетократії. Ключові принципи моделі передусім мають враховувати аспект громадянорічності, коли цифрова трансформація орієнтується на потреби громадян, а не на інтереси технократичної еліти [8], що, у свою чергу, передбачає залучення користувачів до проектування сервісів, забезпечення доступності для всіх категорій населення, захист прав та свобод. Безпека за дизайном означає, що кібербезпека повинна бути інтегрована на всіх етапах розробки цифрових систем, а не додаватися постфактум [18].

Відкритість та прозорість передбачають використання відкритих стандартів, API, відкритого програмного коду (у випадку, якщо це не суперечить безпеці), що забезпечує прозорість, інтероперабельність, залучення інновацій від спільноти [9]. Етичне використання ШІ вимагає, щоб алгоритми, які використовуються для прийняття рішень, були зрозумілими, справедливими, аудитовані на предмет упередженості [14]. Адже громадяни мають право знати, коли рішення приймається автоматизованою системою, та оскаржити його. Державно-приватне партнерство визнає, що держава не може самостійно забезпечити всі технологічні інновації – партнерство з ІТ-сектором, стартапами, науковими установами є критичним для успіху цифрової трансформації, а міжнародна інтеграція через

гармонізацію з європейськими стандартами забезпечить визнання українських цифрових рішень та створить основу для інтеграції в єдиний цифровий ринок ЄС [15; 20].

Стратегічні напрями моделі, на нашу думку, повинні враховувати шість ключових векторів розвитку:

- ❧ розбудова цифрової інфраструктури та кібербезпеки (створення національної суверенної хмарної інфраструктури для критичних державних систем; розвиток Національного центру кібербезпеки з функціями моніторингу, реагування та координації; обов'язкова сертифікацію кібербезпеки для систем критичної інфраструктури; інвестиції у технології кіберзахисту);
- ❧ розвиток компетентностей та людського капіталу (впровадження обов'язкових програм розвитку цифрових компетенцій для державних службовців [17]; створення спеціалізованих освітніх програм з цифрового врядування та кібербезпеки; програми залучення ІТ-талантів до державного сектору через гранти та конкурентну оплату; програми цифрової грамотності для громадян, особливо вразливих груп);
- ❧ нормативно-правове забезпечення (прийняття Закону про штучний інтелект з визначенням етичних принципів та механізмів підзвітності; гармонізація законодавства про захист персональних даних; розробка стандартів цифрової доступності державних сервісів; створення правових механізмів відповідальності за помилки автоматизованих систем [20]);
- ❧ інституційний розвиток (зміцнення координуючої ролі Мінцифри у цифровій трансформації; створення органу з етики штучного інтелекту при Кабінеті Міністрів; формування міжвідомчих команд для реалізації наскрізних цифрових проєктів; розвиток механізмів громадського контролю за цифровою трансформацією);
- ❧ технологічні інновації (пілотні проєкти застосування ШІ в державному управлінні (предиктивна аналітика, автоматизація) [12]; розширення використання блокчейну для державних реєстрів та забезпечення прозорості; розвиток платформ відкритих даних та аналітики великих даних [9]; впровадження технологій Інтернету речей для «розумних міст»);
- ❧ міжнародна співпраця (участь у європейських ініціативах цифрової трансформації; обмін досвідом з країнами-лідерами електронного урядування (наприклад, Естонія, Данія, Фінляндія) [15]; інтеграція українських цифрових ідентифікаторів у європейські системи; співпраця з міжнародними організаціями у протидії кіберзагрозам).

Індикатори успішності реалізації стратегії визначають позицію України в індексі розвитку електронного урядування ООН [19]; частку населення, що користується державними електронними послугами; рівень довіри громадян до цифрових державних сервісів; кількість успішно відбитих кібератак на критичну інфраструктуру; частку державних послуг, доступних онлайн без необхідності особистої присутності; економію бюджетних коштів завдяки цифровізації адміністративних процесів.

Проведене дослідження підтверджує, що цифрова трансформація публічного управління є неминучим та незворотним процесом, який кардинально змінює характер державно-громадянських відносин, а феномен нетократії не є негативним явищенням, він відкриває можливості для модернізації архаїчних

бюрократичних структур, підвищення ефективності та прозорості влади. Однак критично важливим є формування «демократичної нетократії», де технологічна влада поєднується з підзвітністю, інклюзивністю та захистом прав громадян [8; 22]. Досвід України у впровадженні платформи «Дія» демонструє, що навіть в умовах обмежених ресурсів та воєнного стану можливо досягти значних успіхів у цифровізації [16] – ключовими факторами успіху є політична воля, створення спеціалізованого органу з мандатом на реформи (Мінцифри), залучення ІТ-сектору, орієнтація на потреби користувачів. Водночас, виявлені виклики (цифровий розрив, ризики конфіденційності, залежність від іноземних технологій та ін.) вимагають системної уваги.

Запропонована стратегічна модель розвитку цифрового публічного управління інтегрує технологічні, організаційні, правові та соціальні аспекти трансформації. Її реалізація вимагатиме значних інвестицій, міжвідомчої координації, залучення громадянського суспільства та приватного сектору. Однак це є необхідною умовою для модернізації держави, підвищення її конкурентоспроможності та інтеграції до європейського цифрового простору. Порівняння з досвідом країн-лідерів показує, що Україна має унікальну можливість «стрибка через етап» – впровадження найсучасніших технологій без тягара застарілої спадщини. Молоде населення з високими цифровими компетенціями, потужний ІТ-сектор, готовність до інновацій створюють сприятливе середовище для трансформації.

Водночас слід уникнути спокуси «технологічного солюціонізму» – віри в те, що технології самі по собі вирішать усі проблеми. Цифрова трансформація має супроводжуватися реформою державної служби, боротьбою з корупцією, зміцненням верховенства права. Технології є інструментом, а не метою реформ. Особлива увага має приділятися питанням цифрової інклюзії та подолання цифрового розриву. Нетократична модель влади не повинна призводити до маргіналізації тих груп населення, які з різних причин не можуть повною мірою користуватися цифровими сервісами. Держава має забезпечити альтернативні канали доступу до публічних послуг та програми підвищення цифрової грамотності для всіх категорій громадян.

Висновки. Дослідження стратегічних орієнтирів розвитку цифрового публічного управління в Україні через призму інтелектуальних технологій, інформаційної безпеки та феномену нетократії дозволяє сформулювати такі висновки:

- ❧ нетократія як нова парадигма влади трансформує публічне управління, зміщуючи центр прийняття рішень від традиційних бюрократичних структур до цифрових платформ та мережевих еліт; для України критично важливим є формування «демократичної нетократії», що поєднує технологічну ефективність з підзвітністю, прозорістю та інклюзивністю;
- ❧ інтелектуальні технології (ШІ, великі дані, блокчейн, IoT) є драйверами трансформації, що відкривають можливості для автоматизації, персоналізації послуг, предиктивного управління, однак їх впровадження вимагає розробки етичних принципів, механізмів аудиту алгоритмів, захисту приватності та забезпечення цифрової інклюзії;
- ❧ інформаційна безпека є стратегічним пріоритетом цифрової трансформації, особливо в умовах гібридних загроз; досвід України демонструє високий рівень кіберстійкості, але потребує подальшого посилення через розбудову

національної інфраструктури кібербезпеки, підготовку спеціалізованих кадрів, міжнародну співпрацю;

- ❧ платформа «Дія» є успішним прикладом цифрової трансформації, що поєднує технологічні інновації, громадянорічний підхід та організаційні реформи; досвід «Дії» може бути масштабований на інші сфери державного управління та став моделлю для інших країн;
- ❧ стратегічна модель розвитку цифрового публічного управління має базуватися на принципах громадянорічності, безпеки за дизайном, відкритості, етичного використання ІІІ, державно-приватного партнерства та міжнародної інтеграції; реалізація моделі вимагає скоординованих дій у таких напрямках: інфраструктура та кібербезпека, людський капітал, нормативно-правове забезпечення, інституційний розвиток, технологічні інновації, міжнародна співпраця;
- ❧ євроінтеграційні процеси створюють сприятливий контекст для цифрової трансформації через гармонізацію стандартів, доступ до європейських програм підтримки, обмін досвідом; інтеграція до цифрового ринку ЄС має стати стратегічним пріоритетом;
- ❧ воєнний контекст актуалізує питання стійкості цифрової інфраструктури, але водночас стимулює інновації та мобілізує ресурси для цифровізації; післявоєнна відбудова повинна передбачати масштабну цифрову трансформацію як основу модернізації держави.

Цифрова трансформація публічного управління – це не одноразовий проєкт, а тривалий процес постійної адаптації до технологічних змін, успіх якого залежить від здатності держави балансувати між інноваціями та безпекою, ефективністю та справедливістю, технологічним прогресом та людиноцентричністю. Україна має унікальну можливість стати регіональним лідером цифрової трансформації, але це вимагає стратегічного бачення, рішучих дій та консолідації зусиль держави, бізнесу та громадянського суспільства.

ДЖЕРЕЛА ТА ЛІТЕРАТУРА

1. Баранов О. А. Інтернет речей і штучний інтелект: витоки проблеми правового регулювання. *Інформація і право*. 2018. № 2(25). С. 46–59.
2. Семенченко А. І. Концептуальні засади електронного урядування та електронної демократії : монографія. Київ : ФОП Москаленко О. М., 2017. 264 с.
3. Bard A., Söderqvist J. Netocracy: The New Power Elite and Life After Capitalism. London : Pearson FT Press, 2002. 288 p.
4. Castells M. The Information Age: Economy, Society and Culture. Vol. 1: The Rise of the Network Society. 2nd ed. Oxford : Wiley-Blackwell, 2010. 624 p.
5. Квітка С. А., Корсун В. І., Магиляс Ю. Б. Перспективні напрямки досліджень цифрової трансформації публічного управління. *Аспекти публічного управління*. 2020. Т. 8, № 6. С. 90–101.
6. Карпенко О. В. Публічне управління в умовах цифрової трансформації. *Теорія та практика державного управління і місцевого самоврядування*. 2020. № 2. URL: http://nbuv.gov.ua/UJRN/Ttpdu_2020_2_7
7. Грицяк Н. В., Соломко Ю. С. Цифрова трансформація публічного управління та перспективи для України. *Аспекти публічного управління*. 2020. Т. 8, № 4. С. 77–86.

8. Куйбіда В. С., Карпенко О. В., Наместнік В. В. Цифрове врядування в Україні: базові дефініції понятійно-категоріального апарату. *Вісник Національної академії державного управління при Президентові України*. Серія: Державне управління. 2018. № 1. С. 5–10.
9. Линьов К. О. Відкриті дані як інструмент публічного управління : монографія. Дніпро : ГРАНІ, 2018. 196 с.
10. Горбулін В. П., Додонов О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. Київ : Інтертехнологія, 2009. 164 с.
11. Дубов Д. В., Ожеван М. А., Гнатюк С. Л. Інформаційна безпека в умовах критичної інформаційної інфраструктури держави : монографія. Київ : НІСД, 2020. 224 с.
12. 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, № 7. P. 596–615. DOI: 10.1080/01900692.2018.1498103.
13. Engin Z., Treleaven P. Algorithmic Government: Automating Public Services and Supporting Civil Servants in Using Data Science Technologies. *The Computer Journal*. 2019. Vol. 62, № 3. P. 448–460. DOI: 10.1093/comjnl/bxy082.
14. Yeung K. Algorithmic regulation: A critical interrogation. *Regulation & Governance*. 2018. Vol. 12, № 4. P. 505–523. DOI: 10.1111/rego.12158.
15. OECD Digital Government Index: 2019 Results. Paris : OECD Publishing, 2020. 260 p. DOI: 10.1787/4de9f5bb-en.
16. Дія. Цифрова держава : офіційний вебсайт. URL: <https://diia.gov.ua>.
17. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації : розпорядження Кабінету Міністрів України від 3 берез. 2021 р. № 167-р. URL: <https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80>.
18. Про Стратегію кібербезпеки України : Указ Президента України від 14 верес. 2023 р. № 573/2023. URL: <https://www.president.gov.ua/documents/5732023-47577>.
19. United Nations E-Government Survey 2024: Digital Government in the Decade of Action for Sustainable Development. New York : United Nations, 2024. 340 p.
20. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*. 2016. L 119. P. 1–88.
21. Стороженко Л. Г. «Recommendation of the Committee of Ministers to Member States on Electronic Democracy» як глобалізаційний орієнтир нетократичного публічного управління. *Наукові праці Міжрегіональної Академії управління персоналом*. Політичні науки та публічне управління. 2023. № 5(71). С. 93–99. DOI: 10.32689/2523-4625-2023-5(71)-12.
22. Стороженко Л. Г. Електронна демократія в умовах трансформації сучасних комунікаційних процесів: особливості формування. *Дніпровський науковий часопис публічного управління, психології, права*. 2022. № 5. URL: <https://chasopys-ppp.dp.ua/index.php/chasopys/article/view/295>.

REFERENCES

1. Baranov, O. A. (2018). Internet rechei i shtuchnyi intelekt: vytoky problemy pravovoho rehuliuвання [Internet of Things and artificial intelligence: Origins of the legal regulation problem]. *Informatsiia i pravo – Information and Law*, 2(25), 46–59 [in Ukrainian].
2. Semenchenko, A. I. (2017). *Kontseptualni zasady elektronnoho uriaduvannia ta elektronnoi demokratii* [Conceptual foundations of e-government and e-democracy]. Kyiv: FOP Moskalenko O. M. [in Ukrainian].
3. Bard, A., & Söderqvist, J. (2002). *Netocracy: The new power elite and life after capitalism*. London: Pearson FT Press.
4. Castells, M. (2010). *The information age: Economy, society and culture. Vol. 1. The rise of the network society* (2nd ed.). Oxford: Wiley-Blackwell.
5. Kvitka, S. A., Korsun, V. I., & Mahylias, Yu. B. (2020). Perspektyvni napriamky doslidzhen tsyfrovoi transformatsii publichnoho upravlinnia [Promising research areas of digital transformation of public administration]. *Aspekty publichnoho upravlinnia – Aspects of Public Administration*, 8(6), 90–101 [in Ukrainian].
6. Karpenko, O. V. (2020). Publichne upravlinnia v umovakh tsyfrovoi transformatsii [Public administration in the context of digital transformation]. *Teoriia ta praktyka derzhavnoho upravlinnia i mistsevoho samovriaduvannia – Theory and Practice of Public Administration and Local Self-Government*, 2. Retrieved from http://nbuv.gov.ua/UJRN/Ttpdu_2020_2_7 [in Ukrainian].
7. Hrytsiak, N. V., & Solomko, Yu. S. (2020). Tsyfrova transformatsiia publichnoho upravlinnia ta perspektyvy dlia Ukrainy [Digital transformation of public administration and prospects for Ukraine]. *Aspekty publichnoho upravlinnia – Aspects of Public Administration*, 8(4), 77–86 [in Ukrainian].
8. Kuibida, V. S., Karpenko, O. V., & Namestnik, V. V. (2018). Tsyfrove vriaduvannia v Ukraini: bazovi definitsii poniatiino-katehorialnoho aparatu [Digital governance in Ukraine: Basic definitions of the conceptual and categorical apparatus]. *Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy. Serii: Derzhavne upravlinnia – Bulletin of the National Academy for Public Administration under the President of Ukraine. Public Administration Series*, 1, 5–10 [in Ukrainian].
9. Lynov, K. O. (2018). *Vidkryti dani yak instrument publichnoho upravlinnia* [Open data as a tool of public administration]. Dnipro: Hrani [in Ukrainian].
10. Horbulin, V. P., Dodonov, O. H., & Lande, D. V. (2009). *Informatsiini operatsii ta bezpeka suspilstva: zahrozy, protydiia, modeliuвання* [Information operations and security of society: Threats, counteraction, modeling]. Kyiv: Intertekhnolohiia [in Ukrainian].
11. Dubov, D. V., Ozhevan, M. A., & Hnatiuk, S. L. (2020). *Informatsiina bezpeka v umovakh krytychnoi informatsiinoi infrastruktury derzhavy* [Information security in the context of critical information infrastructure of the state]. Kyiv: NISD [in Ukrainian].
12. Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial intelligence and the public sector – Applications and challenges. *International Journal of Public Administration*, 42(7), 596–615. <https://doi.org/10.1080/01900692.2018.1498103>

13. Engin, Z., & Treleaven, P. (2019). Algorithmic government: Automating public services and supporting civil servants in using data science technologies. *The Computer Journal*, 62(3), 448–460. <https://doi.org/10.1093/comjnl/bxy082>
14. Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12(4), 505–523. <https://doi.org/10.1111/rego.12158>
15. OECD. (2020). *OECD digital government index: 2019 results*. Paris: OECD Publishing. <https://doi.org/10.1787/4de9f5bb-en>
16. Diia. Tsyfrova derzhava [Diia. Digital state]. (n.d.). <https://diia.gov.ua> [in Ukrainian].
17. Cabinet of Ministers of Ukraine. (2021). Pro skhvalennia Kontseptsii rozvytku tsyfrovykh kompetentnostei ta zatverdzhennia planu zakhodiv z yii realizatsii [On approval of the concept for the development of digital competences and the action plan for its implementation]. Resolution № 167-r (March 3, 2021). <https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80> [in Ukrainian].
18. President of Ukraine. (2023). Pro Stratehiiu kiberbezpeky Ukrainy [On the Cybersecurity Strategy of Ukraine]. Decree № 573/2023 (September 14, 2023). <https://www.president.gov.ua/documents/5732023-47577> [in Ukrainian].
19. United Nations. (2024). *United Nations e-government survey 2024: Digital government in the decade of action for sustainable development*. New York: United Nations.
20. European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, L119, 1–88.
21. Storozhenko, L. H. (2023). “Recommendation of the Committee of Ministers to Member States on Electronic Democracy” yak hlobalizatsiinyi oriientyr netokratychnoho publichnoho upravlinnia [“Recommendation of the Committee of Ministers to Member States on Electronic Democracy” as a globalization guideline for netocratic public administration]. *Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Politychni nauky ta publichne upravlinnia – Scientific Works of the Interregional Academy of Personnel Management. Political Sciences and Public Administration*, 5(71), 93–99. [https://doi.org/10.32689/2523-4625-2023-5\(71\)-12](https://doi.org/10.32689/2523-4625-2023-5(71)-12) [in Ukrainian].
22. Storozhenko, L. H. (2022). Elektronna demokratiia v umovakh transformatsii suchasnykh komunikatsiinykh protsesiv: osoblyvosti formuvannia [Electronic democracy in the context of transformation of modern communication processes: Formation features]. *Dniprovskyi naukovyi chasopys publichnoho upravlinnia, psykholohii, prava – Dnipro Scientific Journal of Public Administration, Psychology and Law*, 5. Retrieved from <https://chasopys-ppp.dp.ua/index.php/chasopys/article/view/295> [in Ukrainian].