

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА МОИ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

ГЕРМАН ДЕНИС ВАДИМОВИЧ

УДК 35.078.3:004(477)

ДИСЕРТАЦІЯ

**МЕХАНІЗМИ ФОРМУВАННЯ ТА РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ
ПОЛІТИКИ ЦИФРОВОГО РОЗВИТКУ В УКРАЇНІ**

Спеціальність 281 «Публічне управління та адміністрування»

Подається на здобуття ступеня доктора філософії

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

_____ Д. В. Герман

Науковий керівник – Карпенко Олександр Валентинович,
доктор наук з державного управління, професор

Київ – 2025

АНОТАЦІЯ

Герман Д.В. Механізми формування та реалізації державної політики цифрового розвитку в Україні. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування». – Київський національний економічний університет імені Вадима Гетьмана, Київ, 2025.

У дисертаційній роботі вирішено нове наукове завдання, яке полягає у науково-теоретичному обґрунтуванні механізмів вироблення державної політики цифрового розвитку та розробленні перспективних рекомендацій щодо їх практичного використання в умовах збройної агресії проти України.

Уперше розроблено прогностично-сценарну модель цифрового розвитку України на основі поєднання технологічного, інституційного та користувацького векторів-чинників, що оперує кількома перспективними підходами (еволюційним поступом; адаптивним проривом; ризик-орієнтованою трансформацією; кооперативною інновацією) та представляє собою аналітично-ситуативну конструкцію з п'яти альтернативних сценаріїв («Незалежність та цифрове лідерство»; «Інтеграція та цифрова імплементація»; «Фрагментація та конвенціональна цифровізація»; «Автократія та цифрова ізоляція»; «Дезорганізація та цифрова деградація»), за якими здійснюється проектування політичних, правових, інституціональних, організаційних, економічних, соціальних, технологічних, інформаційних, ресурсних та інших механізмів вироблення (формування та реалізації) державної політики у зазначеній сфері.

Також уперше визначено основні траєкторії цифрового розвитку інформаційної безпеки у публічному управлінні («цифрова пропаганда», «цифрові альянси», «цифрова радикалізація», «цифровий контроль»), розкрито їх зміст та обґрунтовано механізми їх реалізації з урахуванням

інноваційних та еволюційних змін.

Удосконалено регуляторно-правові механізми вироблення державної політики цифрового розвитку у сфері протидії дезінформації через надання практичних рекомендацій щодо моніторингу національних цифрових платформ, контролю використання штучного інтелекту в медіа, обмеження віральності фейкового контенту, протидії бот-мережам, забезпечення прозорості політичної реклами та посилення адміністративного контролю з боку державних регуляторів.

Окрім того, удосконалено інструментально-функціональні підходи щодо виявлення сумісності застосування концепцій цифрократії і трансгуманізму у публічному управлінні через наукове обґрунтування спільних цілей, завдань, методів й інструментів застосування технологій цифрового розвитку для підвищення ефективності функціонування різних сфер життєдіяльності суспільства та покращення фізичної, розумової природи людських можливостей (підвищення рівня інтелекту, подовження життя, удосконалення тіла та ін.).

У роботі набула подальшого розвитку періодизація нормативно-правового забезпечення державної політики цифрового розвитку України, що дало змогу виокремити три її основні етапи: *усталення* (інформатизація, 1998-2009 рр.) – унормовано використання ІКТ при здійсненні управлінських функцій, становленні електронної інфраструктури публічного управління, автоматизації частини адміністративної діяльності органів державної влади, врегульовано запровадження електронного документообігу та засобів обчислювальної техніки на робочих місцях публічних службовців; *впровадження* (електронне урядування, 2010-2017 рр.) – здійснено оптимізацію процесу надання адміністративних послуг за допомогою унормування процедур використання технічних засобів, врегульовано запровадження єдиної автоматизованої платформи інформаційної взаємодії органів публічної влади з громадянами та суб'єктами господарювання; *просування* (цифрова трансформація, з 2018 р. по т.ч.) – характеризується

всебічним та повсюдним застосуванням цифрових технологій у процесі здійснення управлінської діяльності та при прийнятті суспільно-важливих рішень.

Також набув подальшого розвитку понятійно-категорійний апарат дослідження шляхом введення у науковий обіг сфери державного управління нових дефініцій: «гібридний інтелект у публічному управлінні – інноваційна форма цифрового розвитку, яка уособлює симбіоз людського і машинного (штучного) мислення, їх інтегрованих можливостей, потенціалу, партисипації та етичних орієнтирів для вироблення обґрунтованих, неупереджених та оптимальних державно-управлінських рішень»; «алгоритмічне лобіювання – це цифрова форма політичного впливу на публічне управління, яка реалізується за допомогою технологій штучного інтелекту, аналітики великих даних та комунікативних інструментів, здатних модифікувати інформаційні потоки, формувати суспільну думку і зумовлювати процеси ухвалення необхідних рішень».

Розкрито існуючі наукові розробки українських та зарубіжних вчених щодо визначення сутності механізмів формування та реалізації державної політики цифрового розвитку, що дало змогу визначити наступну проблематику: недостатність опанування цифрових компетенцій публічними службовцями; неналежність забезпечення кібербезпеки критичної інфраструктури та захисту цифрових прав і свобод громадян. Визначено, що, подальших досліджень потребують: розробка механізмів адаптації кращих зарубіжних практик цифровізації до українських реалій; реалізація належної державної політики у сфері інтеграції України до єдиного цифрового ринку ЄС; визначення ключових інструментів здійснення цифрової та кібердипломатії; здійснення моніторингу соціально-економічних наслідків цифрової трансформації у розрізі регіонів України; дослідження етичних, правових та соціальних викликів, пов'язаних із впровадженням штучного інтелекту, в тому числі і як інструменту зниження корупційних ризиків у сфері публічних закупівель; перспективи застосування концепцій цифрократії та

трансгуманізму в галузі публічного управління; виокремлення ключових напрямів та механізмів реалізації захисту державних інституцій від дезінформації; вироблення стратегічних напрямів державної політики цифрового розвитку України в умовах інтенсифікації ведення інформаційних воєн.

Окрім того, у дисертаційному дослідженні набула подальшого розвитку парадигма державної політики цифрового розвитку в Україні, структурний конструкт фундаментальної рамки якої визначається концепцією (умовами, метою, завданнями та прогнозами), операційно-процедурною складовою – механізмами формування та реалізації (політичними, правовими, інституціональними, економічними, соціальними, організаційними, технологічними, інформаційними, ресурсними), а також змістовним ядром – чинниками, принципами, складовими, факторами, інноваціями, трансформаціями, а головне – очікуваними результатами (продуктами), що досягаються під впливом об’єктивних та суб’єктивних перешкод (ризиків, загроз, проблем).

Обґрунтовано, що цифровий розвиток України повинен здійснюватися з урахуванням створення дієвої та ефективної нормативно-правової бази у цифровій сфері, насамперед для забезпечення: інформаційної прозорості діяльності органів публічної влади, законності та легітимності дій держави у віртуальному просторі, захисту основних інформаційних прав та свобод людини; зниження адміністративних бар’єрів і обмежень; відстоювання національних інтересів України у кіберпросторі. Запропоновано розвивати нормативно-правове забезпечення у таких сегментах цифрового розвитку як: захист конфіденційності даних через впровадження систем та алгоритмів штучного інтелекту; державно-приватне партнерство на основі людино-центричного підходу; перелік доступних державних онлайн-послуг; цифрові компетентності.

Встановлено роль штучного інтелекту як суб’єкту державного управління завдяки аналізу можливостей алгоритмічного лобіювання

впливати на прийняття рішень та змінювати механізми політичної взаємодії. На основі практичних прикладів застосування алгоритмічного впливу доведено його ефективність у формуванні громадської думки, а також небезпечність завдяки відсутності підзвітності, застосуванню алгоритмічного спотворення реальності та поступовому перетворенню держави на «цифрового заручника» маніпулятивних технологій. Надано рекомендації щодо формування багаторівневої системи регуляції алгоритмічного лобіювання та пропозиції щодо демократичного контролю за алгоритмами.

Визначено основні переваги застосування штучного інтелекту для зниження корупційних ризиків у сфері публічних закупівель на основі дослідження нормативних, організаційних та технологічних особливостей здійснення публічних закупівель у період дії правового режиму воєнного стану в Україні. Доведено, що для послідовного впровадження штучного інтелекту слід враховувати передусім переваги його технологій й алгоритмів, які будуть використовуватися для зниження корупційних ризиків, підвищення ефективності та результативності публічних закупівель. Визначено основні переваги алгоритмів та технологій штучного інтелекту за умови їх впровадження у сферу публічних закупівель, що сприятиме заощадженню бюджету для замовників та/або отримання прибутку для постачальників (своєчасне та належне інформування потенційних учасників закупівельного процесу; моніторинг великих масивів даних відкритих тендерів; планування, здійснення аналітичної та прогностичної діяльності; роботизація трудомістких, рутинних, стандартних, типових та повторюваних операцій; оптимізація та/або узгодження внутрішніх операцій закупівельного процесу; розробка стратегій з управління закупівельним процесом). Доведено, необхідність використання чат-ботів, побудованих на основі спеціальних програмних рішень штучного інтелекту, які завдяки використанню технології «machine learning» зможуть аналізувати типові помилки та існуючі проблеми закупівельних процесів, допомагати учасникам відкритих торгів правильно заповнити та своєчасно подати свої пропозиції. Надано практичні

рекомендації для максимізації рівня розробки оптимальних алгоритмів закупівельних процедур (вдосконалити механізм підготовки процедур відкритих торгів та укладання контрактів через впровадження системи оцінювання та аналізу даних попередніх торгів та контрактів; обирати роботи, товари і послуги, які краще підходять для проведення відкритих торгів, їх необхідний обсяг та оптимальну вартість за допомогою оптимізаційних алгоритмів та машинного навчання).

Запропоновано перспективні форми (гібридний інтелект та алгоритмічне врядування) та комплексні технологічні рішення (технології збереження приватності без розкриття ідентифікаційних характеристик особи; технології зондування та комунікацій; інтегровані технології нового покоління зв'язку, цифрові твіни та інші імерсивні технології візуалізації та моделювання різних інфраструктурних об'єктів) цифрового розвитку галузі публічного управління, що розширює технічні можливості комунікаційного середовища органів публічної влади, формує нову інтелектуальну, адаптивну та стійку архітектуру цифрового врядування – чутливу до змін, захищену від загроз зовнішнього втручання, побудовану на емпіричних даних, орієнтовану на довіру та швидке реагування.

Визначено пріоритетні сфери використання перспективних технологічних рішень цифрового розвитку галузі публічного управління (генерування аналітики без застосування персональних даних; реалізація концепції самокерованої ідентичності; створення конфіденційних цифрових сервісів; захист анонімності онлайн-голосування для виборців; забезпечення балансу між відкритістю операцій та захистом економічних інтересів учасників публічних закупівель; впровадження у національну систему ідентифікації (Дія.ID); взаємодія складових елементів інфраструктурних об'єктів; підвищення енергоефективності територій; удосконалення транспортного, енергетичного та телекомунікаційного секторів критичної інфраструктури; модернізація смарт-інфраструктури; стратегічне планування; моделювання ситуацій для прийняття управлінських рішень, візуалізації їх

наслідків та оптимізації використання ресурсів; просторове планування; підтримка соціально-чутливих державних послуг; розгортання платформ цифрової партисипації населення з підтримкою доповненої реальності; формування нових каналів доступу до адміністративних послуг для вразливих або ізольованих груп населення).

Практичне значення отриманих результатів дисертаційного дослідження полягає у виробленні пропозицій щодо вдосконалення механізмів формування та реалізації державної політики цифрового розвитку в Україні.

Ключові слова: державна політика, цифровий розвиток, цифровізація, цифрова трансформація, цифрове врядування, цифрократія, трансгуманізм, гібридний інтелект, штучний інтелект, алгоритмічне врядування, алгоритмічне лобіювання, органи публічної влади.

ABSTRACT

Herman D.V. Mechanisms for the Formation and Implementation of Public Policy on Digital Development in Ukraine. – Qualification research paper, manuscript.

Dissertation for the Academic Degree of Doctor of Philosophy in Specialty 281 «Public Management and Administration». – Kyiv National Economic University named after Vadym Hetman, Kyiv, 2025.

The dissertation addresses a novel scientific problem, namely the theoretical substantiation of mechanisms for the formulation of public policy on digital development and the development of practical recommendations for their application under conditions of armed aggression against Ukraine.

For the first time, a foresight-based scenario model of Ukraine's digital development has been developed, combining technological, institutional, and user-driven vectors. This model incorporates several forward-looking approaches

(evolutionary progression; adaptive breakthrough; risk-oriented transformation; cooperative innovation) and represents the analytical-situational framework comprising five alternative scenarios ('Independence and Digital Leadership', 'Integration and Digital Implementation', 'Fragmentation and Conventional Digitalization', 'Autocracy and Digital Isolation', 'Disorganization and Digital Degradation'). These scenarios serve as the basis for designing political, legal, institutional, organizational, economic, social, technological, informational, resource-based, and other mechanisms for the formulation and implementation of public policy in the relevant domain.

For the first time, the main trajectories of digital development in information security within public administration have been identified (digital propaganda, digital alliances, digital radicalization, digital control). Their content has been clarified, and mechanisms for their implementation have been substantiated, taking into account both innovative and evolutionary changes.

Regulatory and legal mechanisms for the formulation of public policy on digital development in the field of combating disinformation have been improved through the introduction of practical recommendations for monitoring national digital platforms, controlling the use of artificial intelligence in the media, limiting the virality of fake content, countering bot networks, ensuring transparency of political advertising, and strengthening administrative oversight by state regulators.

In addition, instrumental and functional approaches have been improved to identify the compatibility of applying the concepts of digitocracy and transhumanism in public administration. This has been achieved through scientific substantiation of their shared goals, objectives, methods and tools for employing digital development technologies to enhance the effectiveness of various spheres of societal life and to improve the physical and cognitive capacities of human potential (such as increasing intelligence, prolonging life, enhancing the body, etc).

The periodization of the regulatory and legal framework for Ukraine's public policy on digital development has been further developed in this work, making it possible to distinguish three main stages: *consolidation (informatization, 1998 -*

2009): the use of ICT in performing administrative functions was standardized, as well as the establishment of electronic infrastructure in public administration, the automation of certain administrative functions within government authorities, and the regulation of electronic document flow and computing equipment at the workplaces of public servants); *implementation (E-Governance, 2010 - 2017)*: the process of delivering administrative services was optimized through the standardization of procedures involving technical tools, and the introduction of a unified automated platform for information exchange between public authorities, citizens, and economic entities was regulate; *advancement (digital transformation, from 2018 to the present)*: is characterized by the comprehensive and widespread application of digital technologies in the performance of administrative activities and in the making of socially significant decisions.

The conceptual and categorical framework of the study has also been further developed by introducing new definitions into the academic discourse of public administration: '*hybrid intelligence in public administration*' is defined as 'an innovative form of digital development that embodies the symbiosis of human and machine (artificial) cognition - their integrated capabilities, potential, participation, and ethical orientations - for the formulation of well-reasoned, unbiased, and optimal public governance decisions'. '*Algorithmic lobbying*' is defined as 'a digital form of political influence on public administration, implemented through artificial intelligence technologies, big data analytics, and communication tools capable of modifying information flows, shaping public opinion, and conditioning the decision-making processes'.

The existing academic contributions of Ukrainian and international scholars on defining the essence of mechanisms for formulating and implementing public digital development policy have been explored. This has made it possible to identify the following research issues: insufficient mastery of digital competencies by public servants, inadequate cybersecurity protection of critical infrastructure and insufficient safeguarding of citizens' digital rights and freedoms. It has been determined that further research is needed in the following areas: the development

of mechanisms for adapting best international digitalization practices to the Ukrainian context; the implementation of an appropriate public policy for Ukraine's integration into the EU Digital Single Market; identification of key instruments for conducting digital and cyber diplomacy; monitoring the socio-economic impacts of digital transformation across the regions of Ukraine; research into the ethical, legal, and social challenges associated with the implementation of artificial intelligence, including its use as a tool for reducing corruption risks in the field of public procurement; prospects for the application of the concepts of digitocracy and transhumanism in the field of public administration; identification of key areas and mechanisms for protecting government institutions against disinformation; formulation of strategic directions for Ukraine's policy on digital development under conditions of intensified information warfare.

In addition, the dissertation further advances the paradigm of Ukraine's public policy on digital development. Its structural framework is defined by *a foundational concept* (including conditions, objectives, tasks, and forecasts), *an operational-procedural component* comprising mechanisms for formulation and implementation (political, legal, institutional, economic, social, organizational, technological, informational, and resource-based), as well as *a substantive core* encompassing factors, principles, elements, innovations, transformations, and - most importantly - anticipated outcomes (products) that are achieved under the influence of both objective and subjective obstacles (risks, threats, challenges).

It has been substantiated that Ukraine's digital development must be carried out with the establishment of an effective and functional regulatory and legal framework in the digital sphere - primarily to ensure informational transparency of public authorities' activities, legality and legitimacy of state actions in virtual space, protection of fundamental information rights and human freedoms; reduction of administrative barriers and restrictions; and the defense of Ukraine's national interests in cyberspace.

It is proposed to develop regulatory and legal support in the following segments of digital development: protection of data privacy through the

implementation of artificial intelligence systems and algorithms; public-private partnerships based on a human-centered approach; expansion of the range of available state online services; and development of digital competencies.

The role of artificial intelligence as a subject of public administration has been established through the analysis of the potential of algorithmic lobbying to influence decision-making and transform mechanisms of political interaction. Based on practical cases of algorithmic influence, its effectiveness in shaping public opinion has been demonstrated, alongside with the dangers it poses due to a lack of accountability, the use of algorithmic distortion of reality, and the gradual transformation of the state into a “digital hostage” of manipulative technologies. Recommendations for the development of a multi-level system for regulating algorithmic lobbying and proposals for establishing democratic oversight of algorithms have been provided.

The main advantages of using artificial intelligence to reduce corruption risks in the field of public procurement have been identified, based on the analysis of the regulatory, organizational, and technological specifics of public procurement during the legal regime of martial law in Ukraine. It has been demonstrated that, for the consistent implementation of artificial intelligence, emphasis should be placed on the advantages of its technologies and algorithms to reduce corruption risks, and to enhance the efficiency and effectiveness of public procurement. The main advantages of artificial intelligence algorithms and technologies, when implemented in the public procurement sector, have been identified. These include their potential to generate budget savings for contracting authorities and/or profit for suppliers (through timely and appropriate notification of potential procurement participants; monitoring of large datasets from open tenders; planning and conducting analytical and predictive activities; automation of labor-intensive, routine, standard, typical, and repetitive operations; optimization and/or coordination of internal procurement processes; and the development of procurement management strategies). The necessity of using chatbots based on specialized artificial intelligence solutions has been substantiated. By leveraging machine learning technology, these chatbots will

be able to analyze common errors and existing problems in procurement processes, assist participants of open tenders in correctly completing and timely submitting their proposals. Practical recommendations have been provided to maximize the development of optimal procurement procedure algorithms. These include improving the mechanism for preparing open tender procedures and concluding contracts through the implementation of a system for evaluating and analyzing data from previous tenders and contracts; and selecting works, goods, and services that are best suited for open tenders, along with determining their required volumes and optimal pricing, using optimization algorithms and machine learning.

Prospective forms (hybrid intelligence and algorithmic governance) and integrated technological solutions have been proposed for the digital development of the public administration sector. These include privacy-preserving technologies that do not reveal personal identifiers; probing and communication technologies; integrated next-generation communication technologies; digital twins; and other immersive technologies for visualizing and modeling various infrastructure objects. These solutions expand the technical capacities of the communication environment within public authorities and contribute to the formation of a new digital governance architecture - intelligent, adaptive, and resilient – that is responsive to change, protected from external interference, grounded in empirical data, and oriented toward trust and rapid responsiveness.

The priority areas for applying advanced technological solutions in the digital development of the public administration sector have been identified. These include: generating analytics without the use of personal data; implementing the concept of self-sovereign identity; creating confidential digital services; protecting the anonymity of online voting for citizens; ensuring a balance between operational transparency and the protection of economic interests in public procurement; integrating with the national identification system (Diia.ID); enabling interaction among components of infrastructure objects; enhancing the energy efficiency of territories; modernizing the transportation, energy, and telecommunications sectors of critical infrastructure; upgrading smart infrastructure; strategic planning;

modeling scenarios for decision-making, visualizing their outcomes, and optimizing resource utilization; spatial planning; supporting socially sensitive public services; deploying digital citizen participation platforms with augmented reality support; and establishing new channels for access to administrative services for vulnerable or isolated population groups).

The practical significance of the dissertation's findings lies in the development of proposals aimed at improving the mechanisms for formulating and implementing Ukraine's public policy on digital development.

Key words: public policy, digital development, digitalization, digital transformation, digital governance, digitocracy, transhumanism, hybrid intelligence, artificial intelligence, algorithmic governance, algorithmic lobbying, public authorities.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Статті у наукових фахових виданнях України

1. Герман, Д., & Карпенко, Ю. (2022). Перспективи застосування концепцій цифрократії та трансгуманізму в галузі публічного управління. *Аспекти публічного управління*, 10(6), 19-23. <https://doi.org/10.15421/152239>
2. Карпенко, О., Карпенко, Ю., & Герман, Д. (2023). Штучний інтелект як інструмент зниження корупційних ризиків у сфері публічних закупівель. *Аспекти публічного управління*, 11(2), 129-135. <https://doi.org/10.15421/152328>
3. Герман, Д., & Пузько, М. (2024). Особливості використання штучного інтелекту у сфері культури та креативних індустрій: державно-управлінський аспект. *Університетські наукові записки*, 3(99), 23-36. <https://doi.org/10.37491/UNZ.99.3>
4. Герман, Д. (2025). Особливості нормативно-правового забезпечення державної політики цифрового розвитку України. *Аспекти публічного управління*, 13(1), 82-92. <https://doi.org/10.15421/152510>

В інших виданнях

5. Карпенко О.В., & Герман Д.В. (2021). Цифрова грамотність населення як складова підвищення ресурсної спроможності Національної системи кібербезпеки України. Актуальні питання застосування спеціальних інформаційно-телекомунікаційних систем: матеріали науково-практичної конференції студентів, курсантів, аспірантів, докторантів та молодих вчених (15–16 червня 2021 року) – К.: ІСЗІ КПП ім. Ігоря Сікорського, С.112–113.
6. Герман Д. (2023). Взаємодія алгоритмів штучного інтелекту та ІОТ-технологій: перспективи та виклики цифрового суспільства. Кібербезпека державних інституцій та подолання кризових станів: Збірник тез II Міжнародної науково-практичної конференції, (м. Київ-Вроцлав, травень 2023 року). Київ, С.139-140.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ	17
ВСТУП	18
РОЗДІЛ 1 ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ВИРОБЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЦИФРОВОГО РОЗВИТКУ УКРАЇНИ.....	28
1.1 Теоретичні основи дослідження механізмів формування та реалізації державної політики цифрового розвитку	28
1.2 Нормативно-правове забезпечення державної політики цифрового розвитку в Україні.....	48
1.3.Перспективи застосування концепцій цифрократії та трансгуманізму в галузі публічного управління.....	72
Висновки до розділу 1	79
РОЗДІЛ 2 ЗАРУБІЖНИЙ ТА УКРАЇНСЬКИЙ ДОСВІД ЗАСТОСУВАННЯ МЕХАНІЗМІВ ВИРОБЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЦИФРОВОГО РОЗВИТКУ	84
2.1 Реалізація державної політики у сфері інтеграції України до єдиного цифрового ринку ЄС.....	84
2.2 Штучний інтелект як інструмент цифрового розвитку публічного управління.....	105
2.3 Прогностично-сценарна модель цифрового розвитку України	122
Висновки до розділу 2	131
РОЗДІЛ 3 УДОСКОНАЛЕННЯ МЕХАНІЗМІВ ВИРОБЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЦИФРОВОГО РОЗВИТКУ В УКРАЇНІ.....	138
3.1 Перспективні напрями вироблення державної політики цифрового розвитку України в умовах інтенсифікації інформаційних війн	138
3.2 Запровадження гібридного інтелекту як інструменту цифрового розвитку громадської участі у сфері публічного управління.....	149
3.3 Технологічні перспективи та цифрові інструменти реалізації державної політики цифрового розвитку в Україні	155
Висновки до розділу 3	172
ВИСНОВКИ.....	178
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	185
ДОДАТКИ.....	211

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ЄЦР	– Єдиний цифровий ринок
ІКТ	– Інформаційно-комунікаційні технології
ШІ	– Штучний інтелект
DSA	– Digital Services Act (Акт про цифрові послуги)
DMA	– Digital Markets Act (Акт про цифрові ринки)
DESI	– Digital Economy and Society Index (Індекс розвитку цифрової економіки та суспільства)
ENISA	– European Union Agency for Cybersecurity (Агентство Європейського Союзу з кібербезпеки)
FTTP	– Fiber To The Premises (Оптоволоконний зв'язок до приміщення)
HAPS	– High Altitude Platform Stations (Висотні платформні станції)
ISAC	– Integrated Sensing and Communication (Інтегроване зондування та комунікації)
PETs	– Privacy-Enhancing Technologies (Технології збереження приватності)
RIS	– Reconfigurable Intelligent Surfaces (Реконфігурація інтелектуальних поверхонь)
VHCN	– Very High Capacity Network (Мережа з високою пропускнуою здатністю)
WTA	– World Transhumanist Association (Всесвітня організація трансгуманістів)
ZKP	– Zero-Knowledge Proofs (Доведення з нульовим розголошенням)

ВСТУП

Актуальність теми. У контексті суспільних змін та посилення глобальних викликів, які супроводжують трансформаційний розвиток сучасної України, питання ефективного функціонування системи публічного управління набуває особливої ваги. В умовах кризи, викликаній збройною агресією проти України, управлінські підходи вимагають не просто оновлення, а фундаментального переосмислення як теоретико-методологічних основ, так і практико-орієнтованих політичних, правових, інституціональних, організаційних, економічних, соціальних, технологічних, інформаційних, ресурсних та інших механізмів формування та реалізації державної політики цифрового розвитку. Стрімкий розвиток цифрових технологій, зокрема в таких галузях, як штучний інтелект, квантові обчислення, автономні системи, визначає нову логіку організації управлінських процесів, де ключового значення набувають адаптивність, проактивність та випереджувальна аналітика й здатність до динамічного реагування на зміни середовища.

Від початку повномасштабної збройної агресії проти України перед суспільством постало актуальне завдання – зберегти нашу державу, її територіальну цілісність, промисловість, критично важливу інфраструктуру, а також забезпечити безперебійну та надійну роботу органів державної влади та органів місцевого самоврядування. Справжнім викликом для міжнародної коаліції стало забезпечення належної військової, фінансової та інноваційної підтримки України із залученням різних технологічних ресурсів.

Паралельно з цим, на технологічному горизонті формуються принципово нові інструменти, поширення яких актуалізує появу альтернативних форм управління, які дедалі більше тяжіють до алгоритмізованої моделі, що не вкладається в традиційні вертикальні структури влади. Це вимагає не лише технічної чи організаційної адаптації, а

цілісного науково обґрунтованого підходу до стратегування цифрової трансформації публічного управління.

У схваленій розпорядженням Кабінету Міністрів України від 31 грудня 2024 р. № 1351-р Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року визначено напрями, принципи, цілі та завдання державної політики у сфері цифрового розвитку інноваційної діяльності, а Стратегічною ціллю 18 передбачено розвиток спроможностей держави шляхом впровадження технологій у сфері цифрового врядування (govtech). У Стратегії визначено, що govtech охоплює впровадження цифрових рішень, автоматизацію процесів, використання великих даних, алгоритмів штучного інтелекту та інших передових технологій у галузі публічного управління.

У наукових працях проблематика цифровізації публічного управління досліджувалася у розробках Н. Васюк, Л. Гаєвської, В. Дрешпака [125], С. Квітки [23; 24; 25; 26; 28], О. Карпенка [17; 18; 20; 22; 92; 147; 148; 149], Ю. Карпенко [21]; О. Орлова [41; 42; 43], А. Осьмака [46; 47], Г. Почепцова [53; 54; 55; 56], Я. Цимбаленко [91], І. Чикаренко [33; 34; 35] та П. Шпиги [94]. Наукові розвідки щодо використання ідей цифрократії, трансгуманізму, штучного інтелекту, алгоритмічного управління у різних сферах життєдіяльності людства здійснювалися різними американськими та європейськими ученими, серед яких слід виділити фундаментальні роботи Р. Абрамса [99], М. Амановіч [104], Я. Ван Дійка [195], А. Вільямса [197], П. Данлеві [128], Р. Курцвейла, Дж. Малгена [120], Г. Моравеца, Є. Соренсен, Я. Торфінга [177], Т. Уолліс [196], Ф. Фукуяма, Дж. Хакслі, Д. Хьюза, та Ф. Шумана. Незважаючи на потужний науковий доробок вітчизняних та зарубіжних вчених, а також позитивні практичні результати щодо здійснення інноваційної трансформації системи органів публічної влади, існує низка невирішених проблем, різні суб'єктивні та об'єктивні чинники, що уповільнюють і блокують цифровий розвиток в Україні.

Актуальність запропонованої роботи визначається недостатністю наукового обґрунтування та практичного розроблення механізмів формування

та реалізації державної політики цифрового розвитку в умовах збройної агресії проти України, що не було предметом окремого дисертаційного дослідження у науці державного управління.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційна робота виконана відповідно за комплексним науковим проєктом «Державне управління та місцеве самоврядування» (№ ДР 0199U002827) науково-дослідної роботи «Сервісна діяльність органів публічної влади в умовах розвитку цифрового суспільства» (№ ДР 0199U101449) кафедри інформаційної політики та цифрових технологій Національної академії державного управління при Президентові України, де автором узагальнено зарубіжний досвід цифрової ідентифікація користувачів у сфері протидії поширенню небезпечного контенту в мережі Інтернет. В рамках виконання ініціативної науково-дослідної роботи «Формування та реалізація державної політики реінжинірингу національної економіки» (№ ДР 0123U104290) кафедри національної економіки та публічного управління Київського національного економічного університету імені Вадима Гетьмана дисертантом проаналізовано особливості використання штучного інтелекту як цифрового інструменту реінжинірингу національної економіки в умовах збройної агресії проти України.

Мета і завдання дослідження. Метою дисертаційної роботи є науково-теоретичне обґрунтування механізмів вироблення державної політики цифрового розвитку та розроблення перспективних рекомендацій щодо їх практичного використання в умовах збройної агресії проти України.

Досягнення визначеної мети зумовило вирішення таких *завдань*:

- розкрити існуючі наукові розробки українських та зарубіжних науковців щодо визначення сутності механізмів формування та реалізації державної політики цифрового розвитку;
- проаналізувати особливості нормативно-правового забезпечення державної політики цифрового розвитку в Україні;
- визначити перспективи застосування концепцій цифрократії та

трансгуманізму в галузі публічного управління;

- встановити роль штучного інтелекту як суб'єкту державного управління та надати практичні рекомендації щодо його застосування у сфері публічних закупівель;
- розробити прогностично-сценарну модель цифрового розвитку України та визначити перспективи її практичного впровадження;
- визначити основні траєкторії цифрового розвитку інформаційної безпеки та запропонувати механізми їх подальшої реалізації у сфері публічного управління;
- запропонувати перспективні форми та технології цифрового розвитку публічного управління, надати рекомендації щодо сфери їх подальшого застосування.

Об'єкт дослідження – державна політика цифрового розвитку.

Предмет дослідження – механізми формування та реалізації державної політики цифрового розвитку в Україні.

Методи дослідження. Досягнення мети та вирішення поставлених завдань виконувалися із застосуванням комплексу загальнонаукових та спеціалізованих методів дослідження, які були спрямовані на отримання достовірних, обґрунтованих, точних і об'єктивних результатів, а саме використано:

- пошуково-бібліографічний метод – для теоретичного аналізу, а також систематизації джерел дослідження теоретичних основ дослідження механізмів формування та реалізації державної політики цифрового розвитку;
- методи аналізу та синтезу – для детального вивчення ключових характеристик та особливостей впровадження гібридного інтелекту та визначення його впливу на публічне управління та цифрову партисипацію активних представників громадянського суспільства;
- методи семантики, порівняння та групування – для ідентифікації переваг й недоліків використання симбіозу людського управління та

машинних алгоритмів у діяльності органів публічної влади;

- метод моделювання та стратегічного прогнозування – у розробці прогностично-сценарної модель цифрового розвитку України, що дозволило враховувати альтернативні вектори цифрового розвитку держави та ефективно спланувати (визначати) траєкторії цифрової трансформації органів публічної влади з урахуванням критичних чинників (рівня цифрових компетенцій публічних службовців, інституційної спроможності, інфраструктурної готовності, політичної волі та суспільного запиту);

- методи узагальнення, систематизації та класифікації – для систематизації досвіду впровадження цифрових ініціатив, що дало змогу визначити основні виклики для органів публічної влади, які пов'язані з автоматизованими рішеннями та алгоритмічною прозорістю;

- діалектичний метод – у процесі встановлення взаємозв'язків та відносин між суб'єктами інформаційних процесів в контексті ведення гібридних воєн та забезпечення інформаційної безпеки;

- абстрагування, формалізації та прогностичний методи – для формулювання висновків та надання рекомендацій щодо подальших перспектив вироблення державної політики цифрового розвитку в Україні.

Інформаційну базу дисертації становлять українські, європейські та міжнародні нормативно-правові акти, інформаційні, статистичні та аналітичні матеріали, інтернет-джерела, наукові праці провідних іноземних та українських дослідників, результати власних досліджень.

Наукова новизна отриманих результатів полягає у здійсненні науково-теоретичного обґрунтування механізмів вироблення державної політики цифрового розвитку та розробленні перспективних рекомендацій щодо їх практичного використання в умовах збройної агресії проти України. Зокрема, у дисертації:

уперше:

- розроблено прогностично-сценарну модель цифрового розвитку України на основі поєднання технологічного, інституційного та

користувачького вектор-чинників, що оперує кількома перспективними підходами (еволюційним поступом; адаптивним проривом; ризик-орієнтованою трансформацією; кооперативною інновацією) та представляє собою аналітично-ситуативну конструкцію з п'яти альтернативних сценаріїв («Незалежність та цифрове лідерство»; «Інтеграція та цифрова імплементація»; «Фрагментація та конвенціональна цифровізація»; «Автократія та цифрова ізоляція»; «Дезорганізація та цифрова деградація»), за якими здійснюється проектування політичних, правових, інституціональних, організаційних, економічних, соціальних, технологічних, інформаційних, ресурсних та інших механізмів вироблення (формування та реалізації) державної політики у зазначеній сфері;

- визначено основні траєкторії цифрового розвитку інформаційної безпеки у публічному управлінні («цифрова пропаганда», «цифрові альянси», «цифрова радикалізація», «цифровий контроль»), розкрито їх зміст та обґрунтовано механізми їх реалізації з урахуванням інноваційних та еволюційних змін;

удосконалено:

- регуляторно-правові механізми вироблення державної політики цифрового розвитку у сфері протидії дезінформації через надання практичних рекомендацій щодо моніторингу національних цифрових платформ, контролю використання штучного інтелекту в медіа, обмеження віральності фейкового контенту, протидії бот-мережам, забезпечення прозорості політичної реклами та посилення адміністративного контролю з боку державних регуляторів;

- інструментально-функціональні підходи щодо виявлення сумісності застосування концепцій цифрократії і трансгуманізму у публічному управлінні через наукове обґрунтування спільних цілей, завдань, методів й інструментів застосування технологій цифрового розвитку для підвищення ефективності функціонування різних сфер життєдіяльності суспільства та покращення фізичної, розумової природи людських можливостей (підвищення рівня інтелекту, подовження життя, удосконалення тіла та ін.);

набули подальшого розвитку:

- періодизація нормативно-правового забезпечення державної політики цифрового розвитку України, що дало змогу виокремити її три основні етапи: *усталення* (інформатизація, 1998-2009 рр.) – унормовано використання ІКТ при здійсненні управлінських функцій, становленні електронної інфраструктури публічного управління, автоматизації частини адміністративної діяльності органів державної влади, врегульовано запровадження електронного документообігу та засобів обчислювальної техніки на робочих місцях публічних службовців; *впровадження* (електронне урядування, 2010-2017 рр.) – здійснено оптимізацію процесу надання адміністративних послуг за допомогою унормування процедур використання технічних засобів, врегульовано запровадження єдиної автоматизованої платформи інформаційної взаємодії органів публічної влади з громадянами та суб'єктами господарювання; *просування* (цифрова трансформація, з 2018 р. по т.ч.) – характеризується всебічним та повсюдним застосуванням цифрових технологій у процесі здійснення управлінської діяльності та при прийнятті суспільно-важливих рішень;

- понятійно-категорійний апарат дослідження шляхом введення у науковий обіг науки державного управління нових дефініцій: «гібридний інтелект у публічному управлінні – інноваційна форма цифрового розвитку, яка уособлює симбіоз людського і машинного (штучного) мислення, їх інтегрованих можливостей, потенціалу, партисипації та етичних орієнтирів для вироблення обґрунтованих, неупереджених та оптимальних державно-управлінських рішень»; «алгоритмічне лобіювання – це цифрова форма політичного впливу на публічне управління, яка реалізується за допомогою технологій штучного інтелекту, аналітики великих даних та комунікативних інструментів, здатних модифікувати інформаційні потоки, формувати суспільну думку і зумовлювати процеси ухвалення необхідних рішень»;

- парадигма державної політики цифрового розвитку в Україні, структурний конструкт фундаментальної рамки якої визначається концепцією

(умовами, метою, завданнями та прогнозами), операційно-процедурною складовою – механізмами формування та реалізації (політичними, правовими, інституціональними, економічними, соціальними, організаційними, технологічними, інформаційними, ресурсними), а також змістовним ядром – чинниками, принципами, складовими, факторами, інноваціями, трансформаціями, а головне – очікуваними результатами (продуктами), що досягаються під впливом об’єктивних та суб’єктивних перешкод (ризиків, загроз, проблем).

Практичне значення отриманих результатів дисертаційного дослідження полягає у виробленні пропозицій щодо вдосконалення механізмів вироблення державної політики цифрового розвитку в Україні. Основні положення, висновки та рекомендації використано:

– Комітетом Верховної Ради України з питань бюджету під час підготовки та попереднього розгляду у першому і другому читаннях проекту Закону України «Про внесення змін до Закону України «Про Державний бюджет України на 2023 рік» щодо використання коштів державного фонду регіонального розвитку (реєстраційний № 9165 від 31 березня 2023 року). Зважаючи, що одним із завдань законопроекту було врегулювання питання залучення громадян до участі у відборі інвестиційних програм і проектів та визначенні пріоритетів спрямування коштів державного бюджету на регіональний розвиток, дисертантом (як одним з авторів законопроекту) запропоновано застосувати під час відбору інвестиційних програм і проектів, що мають забезпечуватися за рахунок коштів державного фонду регіонального розвитку, процедури голосування громадян України за відповідні проекти засобами Порталу Дія. Зокрема, враховано такі особливості використання у 2023 році коштів державного фонду регіонального розвитку, визначивши у законопроекті, що «За результатами здійснення попереднього відбору та оцінки на відповідність вимогам законодавства поданих інвестиційних програм і проектів регіонального розвитку, центральний орган виконавчої влади, що забезпечує формування державної регіональної політики, подає їх

для відкритого голосування громадян засобами Єдиного державного веб-порталу електронних послуг (далі – Портал Дія). Під час такого голосування громадянин може віддати один голос за одну інвестиційну програму (проект регіонального розвитку) регіону за місцем реєстрації / місця проживання (внутрішньо переміщена особа – за місцем проживання, визначеним відповідно до законодавства про облік внутрішньо переміщених осіб)» (довідка про впровадження від 05 червня 2025 року № 04-13/12-2025/131354);

– в навчальному процесі кафедри національної економіки та публічного управління Київського національного економічного університету імені Вадима Гетьмана при підготовці та викладанні навчальних дисциплін освітньо-професійної програми «Державна політика та публічне управління» з підготовки здобувачів другого (магістерського) рівня вищої освіти за спеціальністю 281 «Публічне управління та адміністрування», зокрема «Цифрове врядування» та «Сервісна діяльність органів публічної влади», в рамках яких запропоновано науково обґрунтовані підходи щодо реалізації концепції трансгуманізму в галузі державного управління (довідка про впровадження від 08 червня 2023 року № 01/13-404).

Особистий внесок здобувача. Дисертаційне дослідження є самостійною науковою працею, що містить положення, ідеї, розробки, висновки і пропозиції, які характеризуються науковою новизною і належать особисто автору. У наукових працях, опублікованих у співавторстві, використано лише ті ідеї і положення, які є результатом особистих досліджень автора.

Апробація результатів дисертації. Основні положення, висновки та практичні рекомендації дисертаційного дослідження оприлюднено автором на науково-практичних конференціях за міжнародною участю, а саме: «Актуальні питання застосування спеціальних інформаційно-телекомунікаційних систем» (Київ, 2021), «Кібербезпека державних інституцій та подолання кризових станів (Київ-Вроцлав, 2023) та «Інноваційні рішення для відродження України у парадигмі глобальної

конкурентоспроможності» (Київ, 2025, <https://surl.li/koxstj>).

Публікації. За результатами дослідження автором опубліковано самостійно 6 наукових праць загальним обсягом 2,19 д. а. (особисто автору належать 2,01 д. а.), з них: 4 – у наукових фахових виданнях України, 2 – в інших виданнях.

Структура та обсяг дисертації. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертаційної роботи становить 217 сторінок друкованого тексту. Робота містить 2 таблиці на 2 сторінках, 4 рисунки на 7 сторінках, 3 додатки на 7 сторінках. Список використаних джерел налічує 199 найменувань.

РОЗДІЛ 1

ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ВИРОБЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЦИФРОВОГО РОЗВИТКУ УКРАЇНИ

1.1 Теоретичні основи дослідження механізмів формування та реалізації державної політики цифрового розвитку

Актуальність дослідження проблемного поля питань щодо формування та реалізації державної політики цифрового розвитку підтверджується, розробленою нормативно-правовою базою та сформованого у 2020 році тимчасового консультативно-дорадчого органу Кабінету Міністрів України – Міжгалузевої ради з питань цифрового розвитку, цифрових трансформацій і цифровізації [80], а також введенням посад CDTO заступників керівника з питань цифрового розвитку, цифрових трансформацій і цифровізації у центральних органах державної виконавчої влади [8]. У зв'язку з цим, виникає необхідність у здійсненні ґрунтовних наукових розробок, які окреслюють проблемні аспекти досліджуваної сфери.

Однак, актуальними питаннями залишаються: проведення комплексного аналізу нормативно-правової бази з метою виявлення прогалин у законодавстві, щодо регулювання сфери цифрового розвитку, оцінювання відповідності чинних норм сучасним викликам та технологіям, здійснення моніторингу ефективності державної політики цифровізації; удосконалення механізмів формування та реалізації державної політики цифрового розвитку на основі досліджень наукових праць українських та зарубіжних вчених, що дозволить сформулювати пропозиції для вирішення сучасних проблем, сприяючи повоєнному розвитку країни.

Цифровий розвиток і цифрову трансформацію неможливо розглядати окремо від створення новацій, оскільки цифровізація є однією з форм інноваційного розвитку. Сьогодні ключовим аспектом розбудови цифрової

економіки стають не просто нові технології, а саме інвестиції в інновації та наукові дослідження. При цьому, обсяг цих інвестицій виступає одним із головних індикаторів, що відображає потенціал цифровізації країни та її прагнення до впровадження передових технологій. У національній економіці цифровий розвиток відіграє особливо важливу роль у забезпеченні конкурентоспроможності [32], що і підтверджується схваленою у 2018 році Концепцією розвитку цифрової економіки та суспільства України на 2018-2020 роки, основною метою якої стала реалізація швидкісного сценарію цифрового розвитку України [74].

У країнах ЄС поступово формувалися інституційні та нормативно-правові засади для розвитку цифрової економіки та впровадження цифровізації в усі сфери суспільно-економічного життя. Це відбувалося шляхом визначення керівного органу, відповідального за координацію та регулювання процесів цифровізації, формулювання концептуального бачення цих процесів, а також прийняття Стратегії цифрового розвитку та відповідних проєктів і програм за окремими напрямками економіки. Одночасно розроблялися механізми та методики для оцінювання результативності цифровізації з погляду підвищення цифрової конкурентоспроможності європейських країн на світовій арені. Важливим елементом інституційно-організаційних механізмів у публічного управління в країнах ЄС є мінімізація державного впливу і стимулювання цифрового розвитку через ринкові інструменти [95].

Країни-члени ЄС впроваджують власні стратегії та заходи в рамках єдиного Плану дій, у якому визначено сім ключових принципів для майбутніх ініціатив. Дотримання цих принципів покликане забезпечити значні переваги принципу цифрового розвитку, що полягає в тому, що державні адміністрації мають надавати послуги в цифровому форматі, де це можливо, водночас залишаючи відкритими альтернативні канали для тих, хто не може або не хоче користуватися цифровими сервісами. Крім того, державні послуги повинні бути доступними через єдину точку доступу або систему «єдиного вікна», а

також через різні канали комунікації [37]. Слід зазначити, що цифровий розвиток охоплює широкий спектр напрямів, пов'язаних із технологіями, програмним забезпеченням, електронними системами, засобами зв'язку та інформаційно-комунікаційними технологіями. Він включає процеси створення, збору, обробки, зберігання, передачі та використання інформації. Водночас цифровий розвиток спрямований на формування справедливого, відкритого та безпечного цифрового середовища, що є пріоритетом як для політики ЄС, так і для національних урядів [40]. Це, у свою чергу, передбачає створення умов, за яких цифрові технології стають доступними для більшості населення, забезпечуючи при цьому захист персональних даних та належний рівень кібербезпеки. Крім того, важливим аспектом є стимулювання цифрової грамотності населення та зменшення цифрового розриву між різними соціальними групами та регіонами.

Проте існують різні думки щодо досягнення цих цілей. Деякі експерти наполягають на підвищенні прозорості та посиленні регулювання в сфері збору й використання персональних даних, тоді як інші акцентують увагу на розвитку інноваційних технологій і підтримці стартапів [40].

Таким чином сучасний етап розвитку цифрового суспільства в більшості країн світу характеризується стрімкою діджиталізацією економіки та суспільних інститутів, що базується на подальшому впровадженні інформаційно-комунікаційних технологій. Це призводить до формування сучасної системи врядування, адаптованої до умов цифрової ери. Під впливом цих тенденцій виникають нові напрями інноваційної політики, тісно пов'язані з цифровим розвитком [29].

Таким чином, поняття «цифровий розвиток» є багатогранним і складним, а його тлумачення може відрізнитися в залежності від того чи іншого підходу. Проте загальна тенденція свідчить про те, що цифровий розвиток є ключовим чинником збільшення рівня конкурентоспроможності економіки, а також важливим елементом забезпечення безпечного й відкритого цифрового простору [40].

О. Кілієвич розглядає підхід «політика цифрового розвитку» як один із напрямів державної політики, реалізація якого видається можливим через впровадження цифрових новацій у діяльність органів державної влади, бізнесу та населення. Автором аналізуються різні підходи до визначення поняття «цифровий розвиток», при цьому особливу увагу приділено інституалізації політики цифрового розвитку в Україні, а також розкриття змісту цієї політики, а саме її цілей, принципів, інструментів та визначенню ключових проблем. При цьому, важливим є дослідження поточного стану і перспектив цифрового розвитку в Україні, а також визначення перешкод та ризиків, що гальмують ефективну реалізацію такої політики [29].

Можна погодитись з автором, що відповідно до класичних підходів, політику цифрового розвитку як напрям державної політики можна визначити як курс дій органів державної влади, спрямований на вирішення актуальних питань цифровізації у різних сферах життя через впровадження сучасних технологій. Проблемні аспекти формування цієї політики в Україні поділяються на кілька груп: політичні, економічні, технологічні фактори та стан екосистеми цифрового розвитку. При цьому, серед найгостріших викликів автор вважає наявність дефіциту висококваліфікованих фахівців для реалізації цієї політики, недостатнє розуміння керівництвом державних органів важливості комплексного аналізу політики всіма стейкхолдерами, а також нерозвинена інформаційно-технологічна інфраструктура (інтернет, інформаційні системи, великі дані, алгоритми штучного інтелекту, цифрові навички громадян). Крім того, існує потреба у переосмисленні комунікації між владою, суспільством та алгоритмами штучного інтелекту, що є важливим аспектом цифрового розвитку. Врахування цих викликів є необхідною умовою для забезпечення ефективної та стійкої політики цифрового розвитку в Україні [29].

На основі вище зазначеного, ми можемо сформулювати структурний конструкт державної політики цифрового розвитку, парадигма якого набуває подальшого поступу в Україні (рис. 1.1).

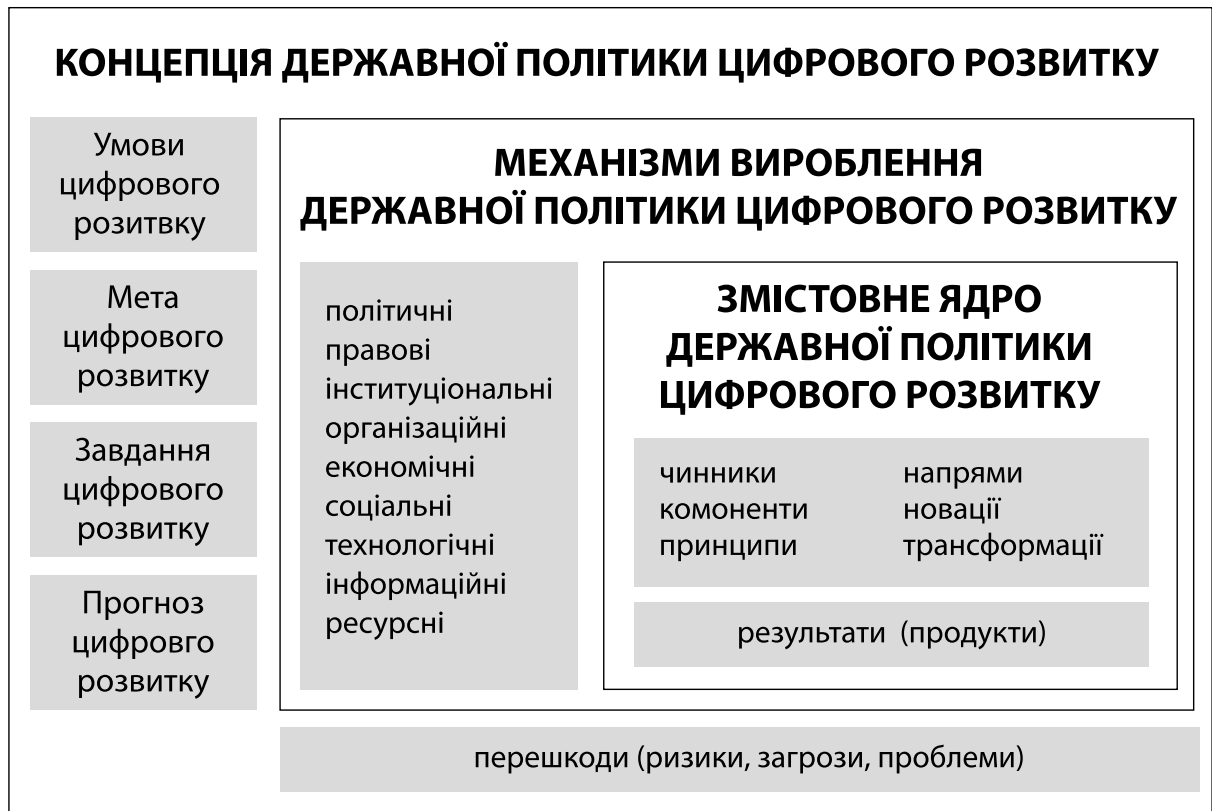


Рис. 1.1 Структурний конструкт державної політики цифрового розвитку в Україні

Джерело: складено автором

Фундаментальну рамку парадигми майбутнього поступу державної політики цифрового розвитку визначає її структурний конструкт, який містить: концепцію (умови, мета, завдання та прогнози), операційно-процедурну складову – механізми формування та реалізації (політичні, правові, інституціональні, організаційні, економічні, соціальні, технологічні, інформаційні, ресурсні), а також змістовне ядро – чинники, принципи, фактори, інновації, трансформації, а головне – очікувані результати (продукти), які одержуються під впливом об’єктивних та суб’єктивних перешкод (ризиків, загроз, проблем).

У результаті аналізу наукових джерел у дослідженні О. Острового систематизовано основні елементи трансформацій та інструменти, що є

актуальними для реалізації державної політики цифрового розвитку в Україні. При цьому, акцентується увага на ключових сферах впровадження цифрових технологій, підкреслюється їхня різноманітність і специфіка. Встановлено основні передумови, що визначають формування політики цифрового розвитку як підґрунтя для вибору ефективних підходів і засобів її реалізації. Автором наголошується, що прогрес інформаційно-комунікаційних технологій, розвиток програмного забезпечення та удосконалення діджитальної інфраструктури створюють сприятливі умови для вироблення належної державної політики, яка повинна базуватись на комплексному підході до вирішення актуальних проблем і враховувати кращі світові практики. На думку автора основними напрямками державної політики цифрового розвитку є удосконалення нормативно-правової бази у сфері цифровізації та її гармонізація з міжнародними стандартами; розбудова цифрової інфраструктури (зокрема фіксованого широкосмугового інтернету та мобільних мереж 4G/5G), а також створення сприятливих умов для приватних ініціатив через податкові стимули; розвиток внутрішнього ринку виробництва, використання й споживання високих технологій, залучення інвестицій для підтримки цифрових інновацій; підвищення рівня кібербезпеки шляхом удосконалення правового регулювання у сфері боротьби з кіберзлочинністю і впровадження відповідних стандартів; стимулювання розвитку наукових досліджень та інтеграції науки з практикою у сфері цифровізації; сприяння повсюдній цифровій освіті та удосконаленню системи підготовки кадрів відповідно до вимог цифрової економіки; формування цифрової культури в суспільстві; розвиток співробітництва з країнами ЄС та підтримка транскордонної взаємодії; забезпечення фінансування цифрових трансформацій шляхом залучення вітчизняних і міжнародних інвестицій та використання коштів міжнародних організацій, які підтримують структурні реформи [44].

Слід відмітити, що у науковій літературі наголошується, що процеси цифровізації супроводжуються значною кількістю викликів і проблем, які

потребують своєчасного вирішення завдяки запровадженню дієвих механізмів державної політики. Науковцями визначено важливу роль державного регулювання у сфері цифрових трансформацій. При цьому, в рамках формування державної політики цифрового розвитку в Україні ініційовано низку законодавчих актів, а на окрему увагу заслуговують процеси інституціонального становлення цифровізації. Орієнтація на світові тенденції сприятиме досягненню високого рівня цифрового розвитку в Україні. На основі аналізу досвіду країн ЄС можна зробити висновок, що публічне управління системою цифровізації переважно здійснюється через економічні механізми із мінімальним застосуванням адміністративних методів. З урахуванням зарубіжного досвіду, сучасних цифрових трендів, а також актуальних викликів і загроз, у працях науковців конкретизовано перспективні напрями розвитку державної політики у сфері цифрових трансформацій, а саме: подальша розробка нормативно-правової бази у сфері хмарних обчислень, реалізації інформаційної безпеки та захисту даних; розширення покриття широкосмугового доступу до Інтернету задля подолання «цифрового розриву»; впровадження сучасних проєктів цифрової трансформації з використанням концесійних моделей і залученням інвестицій; розвиток цифрових технологій і відповідної інфраструктури, зокрема через створення кластерів, наукових парків та промислового інжинірингу; цифровізація суспільного життя, таких як освіта, медицина, міське управління тощо [45].

У працях вітчизняних науковців, присвячених правовим аспектам цифрових трансформацій в Україні, значна частина досліджень зосереджена на цифровізації публічного управління та розвитку цифрової компетентності публічних службовців. Водночас, на думку дослідників, питання нормативно-правового механізму вироблення державної політики цифрового розвитку залишаються недостатньо вивченими [51].

В контексті нашого дослідження, слід зазначити, що у період стрибкоподібної цифрової трансформації важливим викликом є забезпечення належного рівня кіберзахисту критичної інфраструктури. Зростаюча

залежність від цифрових технологій в державному управлінні, критичній інфраструктурі та повсякденному житті підвищує важливість ефективних заходів кібербезпеки. Стійкі інституції державного управління, що мають механізми моніторингу та адаптації, є вирішальними для забезпечення надійної кібербезпеки в умовах цифровізації державних послуг і критичної інфраструктури [81].

Слід відмітити, що окремі науковці у свої дослідженнях наголошують на посиленні європейського та міжнародного впливу на процеси цифрової трансформації в Україні, визначаючи при цьому ключові пріоритети державної політики цифрового розвитку в умовах війни, зокрема необхідність створення єдиного цифрового ринку з ЄС і наближення українського цифрового сектору до міжнародних стандартів. Важливим для наукових досліджень є проведений аналіз розвитку цифрового суспільства в період пандемії COVID-19, яка стала каталізатором цифрових змін, водночас висвітливши проблеми конфіденційності, кібербезпеки, обмеженого фінансування та нестачі ресурсів. Існує тенденція до виокремлення важливих бар'єрів цифрового розвитку в Україні, серед яких домінує проблема недостатності фінансування. Пріоритетні напрями цифрової відбудови та розвитку України на 2022–2025 роки в межах плану United 24 охоплюють цифрову економіку, відновлення інфраструктури, розвиток державних інформаційних ресурсів у хмарних технологіях та електронних реєстрах [31].

Досліджуючи стратегічні документи з цифровізації публічного управління, дослідниками встановлено, що даному напрямку приділяється обмежена увага, за винятком Національної економічної стратегії до 2030 року, де визначено наступні стратегічні цілі щодо цифрового розвитку, зокрема підвищення цифрових навичок, удосконалення електронних державних сервісів та розвиток е-демократії. При здійсненні аналізу основних концепцій, які охоплюють цифровізацію органів публічної влади, дослідники визначають зокрема такі напрями як розвиток систем електронних послуг, цифрової

економіки та суспільства, штучного інтелекту, цифрових компетентностей [51].

Наукова робота М. Хаустової присвячена аналізу ключової ролі держави в процесах цифровізації та обґрунтуванню необхідності формування системної державної політики у цій сфері. При цьому, авторка трактує державну політику цифрового розвитку як узгоджену за цілями систему державно-управлінських заходів, яка базується на чинних нормативно-правових актах і реалізується органами державної влади. Така державна політика спрямована на виконання функцій держави у сфері цифрових трансформацій, розповсюдження цифрових технологій в усі сфери суспільного життя, створення належних умов для цифровізації національної економіки з дотриманням базових принципів, забезпеченням цифрової безпеки, захисту цифрових прав, свобод та інтересів громадян, суспільства і держави [90].

Провідна роль державної політики у сфері цифровізації підтверджується досвідом розвинених країн, які пройшли суттєвий шлях у цьому напрямі та напрацювали ефективні інструменти державного регулювання. Формування національної системи державного управління цифровим розвитком зумовлює потребу дослідження її сучасного стану та визначення перспективних напрямів подальшого розвитку з урахуванням актуальних викликів і загроз [90].

Враховуючи провідну роль держави у цифровізації та виробленні політики цифрового розвитку, важливим є подальше дослідження інституційних, організаційних, та ресурсних засад середовища, в якому враховується потенціал сектору діджитальних технологій.

У працях українських науковців особливу увагу приділено ролі держави у підтримці процесів цифрового розвитку та технологічної трансформації національної економіки. У контексті інституціональної бази пріоритетними завданнями державного управління цифровим розвитком є: забезпечення належної нормативно-правової основи для процесів цифровізації економіки;

удосконалення діяльності інститутів цифрової трансформації; створення та реалізація стратегій, цільових програм і концепцій розвитку діджитальної сфери, а також розбудови цифрового суспільства. Важливо також досягти відповідного рівня стандартизації адміністративних послуг та гарантувати захист прав інтелектуальної власності. При цьому, організаційна платформа повинна забезпечувати цілісність управлінської системи цифровізації та передбачати ефективне функціонування органу, відповідального за координацію та регулювання процесів цифровізації економіки, сприяти дерегуляції та спрощенню процедур отримання дозволів і погоджень для впровадження та розповсюдження цифрових технологій. Крім того, необхідне впровадження механізмів стимулювання розвитку цифрової економіки, налагодження міжфункціональної координації та ефективного партнерства учасників цифрового середовища, запровадження організаційно-консультаційної та інформаційно-методичної підтримки для створення, впровадження, проведення системного моніторингу та контролю розвитку технологічного-сектору [96].

Отже, формування ефективної інституціональної та організаційної основи цифрового розвитку створює передумови для побудови сервісно-орієнтованої публічної служби, яка фокусується на забезпеченні потреб громадян і бізнесу через доступні, зручні та якісні електронні послуги. Водночас цифровізація стає важливим інструментом модернізації окремих секторів національної економіки, сприяючи їхній трансформації відповідно до принципів галузевого цифрового врядування.

Результати проведеного дослідження Н. Савченко підтвердили, що для формування та реалізації сервісно-орієнтованої державної політики активно використовуються різноманітні цифрові технології. Зростання вимог та необхідність посилення орієнтації на сервіс обумовлюють потребу у широкому застосуванні сучасних технологій, які забезпечують ефективний пошук, накопичення та поширення інформації. З'являються нові програмно-

технічні засоби, що активно використовуються користувачами інформації [87].

Проведений аналіз наукової літератури щодо розвитку цифрового врядування в Україні дозволив виявити ряд невирішених питань, що стосуються реалізації механістичного підходу. Основними складовими цифрового врядування є підсистеми методів функціонування цифрових робочих місць; цифрової інфраструктури; цифрових сервісів. Інституціональне поле взаємодії влади та громадськості у сфері цифровізації базується на залученні громадськості; бізнесу та індустрій до створення даних; взаємодії державних цифрових інформаційних ресурсів, та цифрових платформ, а також завдяки набуттю цифрових компетентностей державними службовцями та пересічними громадянами.

Розроблено типологію інструментів цифрового врядування, що дозволяє виокремити алгоритм вибору інструментів за критеріями допустимості, доцільності, результативності та економічної ефективності. Необхідними є усунення законодавчих та інституційних перешкод, що гальмують розвиток цифрового врядування, а також наявність мотивації та стимулів для активної участі всіх суб'єктів публічного управління сферою цифрового розвитку. Окремо слід відмітити, важливість формування попиту бізнес-індустрії на цифрові продукти та послуги, зокрема через впровадження державних масштабних Digital-проектів, у тому числі на базі сучасних моделей державно-приватного партнерства [39].

Важливим для подальшого аналізу теоретичних основ дослідження механізмів реалізації державної політики цифрового розвитку є значущість галузевого аспекту, зокрема в таких сферах, як освіта, охорона здоров'я, культура. Зокрема, впровадження цифрових рішень в соціальній сфері сприятиме покращенню якості послуг, оптимізації ресурсів, зокрема підвищенню рівня доступу до освітніх та медичних послуг.

О. Білик запропоновано методологічний підхід до здійснення державного управління в процесах цифрового розвитку освіти і науки, що

базується на системному підході та розглядається як складна кібернетична система, орієнтована на досягнення та реалізацію відповідних цілей у сфері діджиталізації [2].

У дисертаційному дослідженні Н. Васюк удосконалено систему принципів реалізації державної політики в сфері охорони здоров'я в контексті цифрового розвитку, зокрема через застосування підходів, що забезпечують ефективність прийняття рішень, стандартизацію впровадження цифрових інновацій у галузі охорони здоров'я, а також інтеграцію та інтероперабельність інформаційно-аналітичних систем з іншими секторами, що у свою чергу сприяє адаптивності до змін сучасного цифрового середовища та загальному покращенню функціонування системи охорони здоров'я в умовах цифрових трансформацій [4].

В іншому дослідженні Л. Гаєвська та Н. Васюк актуалізують аспекти реалізації державної політики цифрового розвитку на прикладі сфери охорони здоров'я та визначають шляхи вдосконалення механізмів її впровадження. Авторами проаналізовано цифрові інструменти для реалізації державних механізмів у сфері охорони здоров'я, що дозволило визначити основний напрямок функціонування eHealth як інтеграцію цифрових технологій та систем для зберігання, обробки, обміну та аналізу медичної інформації. Погоджуємося із авторами, що ці інструменти мають вагомий потенціал для поліпшення якості функціонування системи охорони здоров'я, роблячи її більш координованою, доступною, персоналізованою та економною. При цьому, для успішної реалізації цих технологій необхідно забезпечити ефективний обмін медичною інформацією, сприяти співпраці між усіма учасниками системи, захисту даних та інвестуванню в інновацію [5].

Суспільні трансформації та державна політика цифрового розвитку можуть сприяти запобіганню етнічним конфліктам, одночасно відкриваючи нові можливості та нові загрози. Так, С. Квітка та А. Рибченко висвітлюють сучасні аспекти і причини виникнення етнічних конфліктів з урахуванням впливу процесів цифрової трансформації та особливостей реалізації державної

політики цифрового розвитку у боротьбі з ними. Досліджено питання виникнення та розвитку етнічних конфліктів та запропоновані цифрові інструменти вирішення міжетнічних суперечностей через маніпуляцію свідомістю великих мас людей та зменшення гостроти національної самосвідомості, акцентуючи увагу на культурних і традиційних аспектах етнічних меншин. Однак роль цифровізації у забезпеченні етнополітичної рівноваги не завжди можна оцінити як позитивну. Останнім часом міжнародні організації посилили свої зусилля щодо забезпечення свободи вираження думок етнічних груп, доступу до інформації та інклюзивного цифрового розвитку по всьому світу. Це безпосередньо впливає на захист національних інтересів, відкриваючи можливості для створення нових інструментів профілактики міжетнічних розбіжностей, разом з тим провокуючи додаткові загрози, зокрема в сфері тероризму [27].

Т. Васильців та Н. Наконечною визначено основні напрями та інструменти державної політики цифрового розвитку в туристичному секторі. Зокрема, йдеться про: цифровізацію бізнес-процесів суб'єктів господарювання, що формують туристичний комплекс; розвиток системи цифрових комунікацій серед кінцевих споживачів послуг; ефективне застосування інструментів Інтернет-маркетингу на різних рівнях управління. Важливим інструментом, здатним сприяти реалізації цієї стратегії, є активізація процесів цифрової трансформації як на рівні окремих суб'єктів туристичного комплексу, так і на рівні рекреаційних кластерів, дестинацій та комплексної системи в цілому. Для досягнення цього необхідно вирішити кілька стратегічних завдань: створення повноцінної інфраструктури для функціонування сектора цифрової економіки в туристичному комплексі, покращення ресурсної бази для цифровізації суб'єктів туристичної галузі, розширення масштабів цифрових процесів у туристичному секторі, трансформація структурних характеристик галузі та її внеску в економіку, формування ефективних зв'язків між суб'єктами інформаційно-комунікаційних технологій та економічним розвитком національного

туристичного комплексу, а також реалізація національних стратегічних проектів у сфері діджиталізації туризму та його складових [3].

Таким чином, теоретичні підходи українських дослідників включають як визначення категорій, термінів і понять у сфері цифрового розвитку, так і механізмів вироблення відповідної державної політики. Переважна більшість наукових праць окреслює цифровий розвиток як системний процес трансформації суспільних відносин, економіки та державного управління на основі інтеграції цифрових технологій. Основними механізмами вироблення державної політики цифрового розвитку визначено організаційно-правові, інституціональні, інноваційні, та ресурсні механізми, що зокрема включають стратегічне планування, нормативно-правове регулювання, розбудову цифрової інфраструктури, розвиток цифрових компетентностей населення, стимулювання інноваційної діяльності та забезпечення кіберзахисту органів державної влади.

У працях вітчизняних науковців акцентується увага на необхідності міжсекторальної взаємодії держави, бізнесу, наукової спільноти та громадянського суспільства з метою ефективної реалізації стратегічних цілей цифрового розвитку та цифрових трансформацій. При цьому, наукові дослідження підкреслюють важливість забезпечення інноваційного цифрового розвитку, доступу до цифрових технологій для всіх верств населення та ін.

Досліджуючи теоретико-методологічні аспекти формування та реалізації державної політики цифрового розвитку важливим є здійснення аналізу праць зарубіжних вчених, зокрема щодо ролі держави у діджиталізації різних сфер життєдіяльності суспільства.

Діджитальна еволюція, яка відбувалася у сфері публічного управління різних країн світу починаючи з 2000-х років, характеризується зростанням рівня впровадження цифрових технологій як інструментів розвитку та управління, а також застосуванням інструментів Big Data, що супроводжують цей процес [101].

Пандемія COVID-19 значно пришвидшила цифрові зміни у всіх країнах світу. Через встановлені карантинні обмеження значна частина громадського та приватного життя перейшла в онлайн-простір і нові цифрові технології стали незамінними для більшості людей та з метою забезпечення безперервності і функціонування цих сфер [156].

Оскільки розвиток і впровадження цифрових технологій радикально змінюють наш світ, важливим є забезпечити їх сприяння досягненню Цілей сталого розвитку (далі – ЦСР). З цією метою, як зазначено в Білій книзі Великої Британії з міжнародного розвитку, уряди країн повинні сприяти «цифровому розвитку», що означає забезпечення того, щоб цифрова трансформація була інклюзивною, відповідальною та сталою [122].

Можемо погодитися з авторами, що цифрова трансформація не лише змушує організації (установи, підприємства, фірми, компанії) переосмислити свої бізнес-моделі, але й ставить перед урядами країн виклик до вирішення питання про те, як інформаційні технології змінять суспільство сьогодні та в майбутньому. Отже, встановлюючи правові межі та виступаючи інвестором і промоутером вітчизняної цифрової економіки, уряди активно впливають на те, як повинен відбуватися цей трансформаційний процес у кожній країні. Бачення та цілі реалізації цифрової трансформації на державному рівні відображені в розроблених політиках цифрового розвитку.

Важливим етапом, при цьому є, визначення ролі урядів у цифрових трансформаціях та як повинні бути сформовані стратегічні документи щодо цифрового розвитку держави. Автори зазначають, що розробка державної політики цифрового розвитку є подібною в глобальному контексті, але, при цьому, не є диференціатором для країн, що дозволяє їм отримати конкурентну перевагу. Отже, формування та реалізація державної політики цифрового розвитку має майже універсальний характер і лише незначною мірою залежить від національного контексту [188].

І. Пенья-Лопес у своєму дослідженні зосереджує увагу на з'ясуванні того, чи існує потреба в діяльності державного сектору щодо сприяння

формуванню цифрового суспільства та якою має бути пріоритетна роль органів державної влади. Автором визначено етапи цифрового розвитку на рівні країн за допомогою кластерного аналізу. Автор робить висновок, що більшість країн проходять подібний шлях цифрового розвитку, який має тісний зв'язок із соціально-економічним розвитком, зокрема підвищення рівня добробуту населення та економічного зростання; розвиток освіти та наявність цифрової інфраструктури, що майже завжди відповідають високому рівню цифрового розвитку.

Окрім звичних соціально-економічних показників, які безпосередньо впливають на той чи інший рівень цифрового розвитку, автором виявлено, що уряди країн можуть прискорити процес цифрового розвитку у державі через впровадження державної політики щодо цифрового розвитку, а також створення належного режиму економічного стимулювання. Це, у свою чергу, підвищує ймовірність досягнення країною вищого рівня цифрового розвитку [146].

Дослідження показують, що розробка, впровадження та використання цифрових технологій, включаючи штучний інтелект та Інтернет речей, створюють величезні можливості для продуктивності, наукових відкриттів та пом'якшення наслідків зміни клімату, надання державних послуг, нових бізнес-моделей, віддаленої роботи, освіти та охорони здоров'я тощо. Водночас, щоб скористатися перевагами цих розробок виважена державна політика цифрового розвитку повинна передбачити ризики [123].

В той же час, використання цифрових технологій провокує й нові виклики перед державами, зокрема щодо конфіденційності даних; забезпечення безпеки (онлайн-безпеки); подолання цифрової нерівності; забезпечення цілісності інформації та соціальної згуртованості, а також дотримання прав людини в цифрову епоху, справедливості та підзвітності. Отже, державна політика цифрового розвитку повинна забезпечити заходи щодо ефективного використання нових технологій в процесі її формування та

реалізації, водночас управляючи ризиками, які несуть цифрові технології [123; 152].

Заслуговує уваги думка Н. Коко, Ч. Колапінто та В. Фіноттоякі, які зазначають, що попри наявність цифрової трансформації, багато регіонів все ще відстають у цьому процесі. Автори дослідження пояснюють цю невідповідність тим, що політичний консенсус щодо прискорення впровадження новітніх цифрових технологій повинен враховувати різноманітність підприємницьких та соціальних середовищ у різних країнах та регіонах. Погоджуємось із авторами щодо необхідності впровадження та адаптації до місцевих умов кращих світових практик у формуванні та реалізації державної політики цифрового розвитку [157].

Швидкі темпи та міжгалузевий характер цифрової трансформації вимагають дотримання єдиного, цілісного підходу з боку всіх органів державної влади (міністерств чи відомств). ОЕСР – Організація економічного співробітництва та розвитку пропонує країнам Інтегровану політичну рамку «Перехід на цифрові технології» (Going Digital Integrated Policy Framework) [186] та підтримує країни у розробці скоординованої, цілісної та узгодженої державної політики цифрового розвитку за такими напрямками, що охоплюють всі аспекти цифрової трансформації, зокрема доступ до технологій, їх використання, інновації, зайнятість та робочі місця, довіру суспільства та відкритість ринку [123].

Слід зазначити, що національна цифрова стратегія країни слугує інструментом для забезпечення скоординованого та цілісного підходу до розробки державної політики цифрового розвитку. Для того, щоб оцінити чи в повній мірі національна цифрова стратегія країни охоплює сім вимірів Інтегрованої рамкової політики ОЕСР «Перехід на цифрові технології» [186], ОЕСР розробила індикатор комплексності національної цифрової стратегії (national digital strategy comprehensiveness indicator – NDSC) [123].

В цьому контексті, заслуговує уваги Стратегія цифрового розвитку на 2024-2030 роки, яка визначає план уряду Великої Британії щодо співпраці з

країнами, що розвиваються, для створення інклюзивного, відповідального та сталого цифрового майбутнього. Ця стратегія визначає підхід Міністерства закордонних справ, у справах Співдружності та розвитку (FCDO) до міжнародного розвитку в контексті цифрових технологій, які швидко розвиваються [121].

Отже, національна цифрова стратегія держави як інструмент стратегічного планування включає вирішення проблем цифрового розвитку, які необхідно вирішити в процесі її реалізації. Така стратегія має охоплювати всі важливі сфери цифрової трансформації в суспільстві, кінцевою метою якої є сприяння економічному зростанню та добробуту населення.

Слід зазначити, що для підтримки процесу цифрової трансформації уряду Міжамериканський банк розвитку (IDB) розробив Посібник із цифрової трансформації уряду, який автори визначають як своєрідну «енциклопедію цифрового уряду», оскільки класифікує та узагальнює передові знання у цій сфері. Погоджуємося із думкою авторів цього посібника, що досягнення цифрової трансформації потребує міжвідомчого, людиноцентричного підходу. З цією метою необхідно: створити інституційну структуру та систему управління, яка спрямовує, координує й забезпечує реалізацію змін; розробити нормативно-правову базу, що визначає нові цифрові процеси; спроектувати інфраструктуру та інструменти, які закладуть технологічний фундамент для трансформації; сприяти розвитку у громадян цифрових навичок і компетентностей; створити нові цифрові процеси та послуги, які удосконалюють взаємодію органів державної влади з громадянами [113].

Таким чином, на сьогодні можна виділити такі групи країн, кожна з яких перебуває на своєму етапі цифрового розвитку та визначає пріоритети цифрової трансформації [156]:

1. Країни, які мають недостатньо цифрових програм. У них відсутні плани цифрових трансформацій. Такі країни знаходяться на початковому етапі цифрового розвитку.

2. Країни перехідного типу, які зосереджуються на зміцненні цифрових основ, зокрема цифрової інфраструктури та підключення до мережі; розвиток цифрових навичок громадян; розроблення нормативно-правового забезпечення; впровадження цифрового уряду.

3. Розвинені країни, які спрямовані на наявність, доступність та розвиток цифрових технологій та цифрового суспільства.

4. Країни – лідери цифровізації, які досягли високого рівня цифрового розвитку з впровадженням нових технологій, які інноваційно розвиваються та поступово перетворюються на «розумні» й сталі нації.

Упродовж останнього десятиліття цифровізація стала невід’ємним елементом глобального економічного розвитку, а цифрова економіка – новою парадигмою існування України, яка інтегрується до світових ринків і модернізує власну економіку. Базовим вектором економічного зростання стало активне впровадження цифрових інструментів на всіх рівнях: від державного управління до бізнесу. Водночас активне впровадження цифрових технологій супроводжується низкою викликів, пов’язаних із монополізацією даних, зростанням ролі алгоритмічного управління та посиленням державного контролю за економічною активністю. У цьому контексті постає запитання: чи є цифрова економіка в Україні виключно рушієм зростання, чи вона також виступає інструментом контролю?

Передусім, цифрова економіка стає каталізатором інноваційного розвитку. З 2019 року Міністерство цифрової трансформації України реалізує масштабну програму створення «держави у смартфоні» [88], в рамках якої було створено низку платформ і сервісів. Найвідомішим прикладом є застосунок та портал «Дія», що об’єднує понад 20 мільйонів користувачів. Завдяки «Дії» громадяни можуть реєструвати бізнес, отримувати адміністративні послуги, користуватися цифровими документами. Така цифровізація зменшує бюрократичні бар’єри та скорочує транзакційні витрати для бізнесу, стимулюючи легалізацію підприємницької діяльності.

Особливо показовим кейсом є «Дія.City» (<https://city.diia.gov.ua>), запроваджений для розвитку ІТ-сектору. Він створює спеціальні умови для функціонування технологічних компаній, зокрема через зниження податкового навантаження, запровадження гнучких гіг-контрактів і цифрових форм звітності. За короткий період резидентами «Дія.City» стали сотні компаній, а Україна зміцнила свої позиції як потужний експортний центр цифрових послуг.

Також варто відзначити стрімкий розвиток fintech-сектору. Українські цифрові банки, зокрема Monobank (<https://monobank.ua>), стали прикладом успішного поєднання мобільності, автоматизації та персоналізації банківських послуг. За відсутності фізичних відділень Monobank обслуговує понад 7 мільйонів клієнтів, активно використовуючи алгоритми кредитного скорингу та машинне навчання. В цілому, цифрові сервіси стимулюють появу нових ринків, стартапів, робочих місць та підвищують конкурентоздатність української економіки.

Однак паралельно з економічною лібералізацією цифрові інструменти створюють нові моделі контролю, як з боку держави, так і з боку приватних корпорацій. Централізація чутливих даних у цифрових платформах, таких як «Дія», створює ризики зловживання інформацією, моніторингу та обмеження цифрових прав громадян. Попри зручність, така модель має певні ознаки цифрового централізованого нагляду, що потенційно може використовуватись не тільки для убезпечення, а й для певного контролю над економічною поведінкою громадян.

Окремим викликом є питання кібербезпеки та довіри. У 2022–2024 роках зафіксовано серії хакерських атак на державні цифрові сервіси, зокрема на портал «Дія». Попри офіційне спростування витоку персональних даних, інциденти загострили суспільну дискусію стосовно ефективності захисту цифрової інфраструктури, відповідальності держави та прозорості управління даними [85]. На додачу, цифрова нерівність в Україні залишається помітною проблемою: мешканці сільської місцевості, особи старшого віку та

малозабезпечені громадяни мають обмеження доступу до більшості цифрових послуг, що створює ризик маргіналізації частини населення в новій цифровій економіці.

Проблематика цифрової економіки в Україні потребує багаторівневого аналізу. З одного боку, цифровізація створює нові можливості для економічного зростання, відкриває доступ до глобальних ринків та модернізує інститути. З іншого боку – зростає ризик алгоритмізації управління, де визначальним ресурсом стають не фінанси, а дані. Ключовим викликом стає не лише розвиток технологій, а створення інституційної рамки, яка б гарантувала прозорість цифрових процесів, захист даних, цифрові права громадян і відкритість алгоритмів. Лише за дотримання принципів цифрової етики, соціально відповідального врядування та справедливого доступу до технологій, цифрова економіка в Україні зможе стати дійсно інклюзивним інструментом повоєнного відновлення, а не лише новою формою централізованого контролю.

1.2 Нормативно-правове забезпечення державної політики цифрового розвитку в Україні

Упродовж останнього десятиліття цифровий розвиток став частиною людського існування, докорінно змінивши його суть. Цифрові виклики, з якими стикається суспільство, спричинили відповідні зміни як в управлінській науковій думці, так і в практичному плані. На сьогодні тема цифрового розвитку в Україні знаходиться «на передовій» вітчизняних та зарубіжних досліджень. При цьому неодмінним успіхом цифрового розвитку є наявність ефективного нормативно-правового підґрунтя.

Поняття цифрового розвитку в Україні необхідно розглядати як ефективний процес свідомого впливу держави на суспільство, всі його інституції, національну економіку і бізнес з метою впровадження дієвих цифрових технологій у відповідні суспільні відносини. В умовах воєнного

стану особливої актуальності набуває проблема застосування цифрових-технологій. Так, стрімкий розвиток взаємодії у дистанційній формі, що задовольняє різноманітні інтереси учасників суспільних відносин, підштовхує до нових методів управління, що в свою чергу визначає необхідність вирішення нормативно-правового забезпечення державної політики цифрового розвитку. На порядку денному, стоїть питання правового регулювання нових суспільних відносин в умовах цифрових трансформацій, що визначають права людини в цифровому суспільстві, конфіденційність даних, поняття «цифрової особистості» тощо. Як наслідок, під впливом впровадження цифрових технологій, ухвалюються нові правові норми, відповідні законодавчі акти, розвиваються правові інститути та ІТ-сфера в цілому.

Зважаючи на те, що в Україні наразі триває активний процес цифровізації публічного управління, наше дослідження є особливо актуальним. Таку думку підтверджують також і сучасні науковці, які вивчали питання правового забезпечення державної політики цифрового розвитку. Так, професорка кафедри теоретичної юриспруденції Київського національного економічного університету імені Вадима Гетьмана Т. Пікуля аналізуючи правове забезпечення цифрової трансформації в Україні зазначає, що реалізація концепту сервісної держави неможлива без цифровізації самої держави. Крім цього авторка наголошує, що побудова цифрової держави передбачає реорганізацію системи органів публічної влади, реформування державної системи на основі принципів інформаційного суспільства, із урахуванням тих можливостей, які надаються сучасними інформаційно-комунікаційними технологіями і мережевою інфраструктурою [50, с. 62-63].

Поруч з питаннями нормативно-правового забезпечення державної політики цифрового розвитку України доречно зазначити про те, що сьогодні в Україні кількість цифрових послуг та сервісів розширюється з кожним днем. ІТ-технології є інструментом, використання якого при наданні тієї чи іншої послуги можливе тільки в мережі Інтернет. Як доречно зауважує у своїй праці

Т. Пікуля, однією із найбільших проблем виступає відсутність Інтернет-комунікацій у малих населених пунктах, частині автомобільних та залізничних шляхів, гірській місцевості тощо [50, с. 64].

Разом з тим, старший науковий співробітник науково-дослідного інституту правового забезпечення інноваційного розвитку Національної академії правових наук України М. Хаустова акцентує свою увагу на тому, що для державного регулювання розвитку сектора цифровізації суспільства необхідним є формування та дії інституційно-правового, економічного, організаційного, соціально-психологічного та ресурсно-технологічного механізмів з широким переліком методичного інструментарію за кожним із них [89, с.14].

Крім цього, співробітник Хмельницького університету управління та права імені Леоніда Юзькова П. Польовий, розкриваючи нормативно-правовий механізм цифрових трансформацій в органах публічної влади та розвитку цифрових компетентностей публічних службовців наголошує, що цифрові трансформації в суспільстві пов'язані зі стратегічним плануванням, яке набуває особливої актуальності під час вироблення державної політики модернізації сфери публічного управління. Разом з цим вчений підкреслює, що питання цифровізації діяльності органів публічної влади в частині формування цифрових компетентностей публічних службовців знайшли відображення у вітчизняних стратегіях розвитку [52, с. 86].

Зазначені дослідження ще раз доводять, що прийняття відповідної нормативно-правової бази щодо забезпечення сфери цифрового розвитку в Україні окреслить стратегічний курс України щодо процесів опанування громадянами знань, умінь, навичок у сфері цифрових технологій, матиме позитивний вплив на процеси цифровізації в Україні та стане основою для розробки механізмів розвитку людського потенціалу цифрового суспільства, цифрової економіки та її окремих сфер.

В рамках дисертаційного дослідження слід зазначити, що законодавство України, яке регулює громадські відносини, які пов'язані із

реалізацією та впровадженням цифрових-технологій, нараховує відповідну кількість нормативно-правових актів, які розкривають етапи становлення та розвитку законодавства України з питань цифрового розвитку. Чітке формування зазначених етапів дає можливість визначити подальші та необхідні нормативно-правові зміни щодо виведення з обігу застарілих та прийняття нових правових актів. Нині можна виокремити три основні етапи розвитку законодавства у сфері цифрового розвитку України, а саме етапи інформатизації, електронного урядування та цифровізації.

Етап усталення – «інформатизація» (1998 – 2005 роки) – характеризується початком використання засобів інформаційно-комунікаційних технологій при здійсненні управлінських функцій, становленні електронної інфраструктури публічного управління, автоматизації частини адміністративної діяльності органів влади, а також запровадженні електронного документообігу та засобів обчислювальної техніки на робочих місцях публічних службовців.

Упродовж наступного (впроваджувального) етапу – «електронного урядування (2010 – 2017 роки)» – було здійснено оптимізацію процесу надання адміністративних послуг за допомогою технічних засобів (сегментів глобальної та локальних інформаційних мереж), а також запроваджено єдину автоматизовану платформу інформаційної взаємодії органів публічної влади з громадянами та суб'єктами господарювання.

Етап просування – «цифрова трансформація» – розпочався у 2017 році та продовжується по теперішній час, характеризується всебічним та повсюдним застосуванням цифрових технологій у процесі здійснення управлінської діяльності та при прийнятті суспільно-важливих рішень. Так, першим актом етапу цифровізації на законодавчому рівні став Закон України від 05 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України» (введено в дію 09 травня 2018 року) [64], яким визначено правові та організаційні основи забезпечення захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час

використання кіберпростору, за якого забезпечуються розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Разом з тим закон визначив, що державно-приватна взаємодія у сфері кібербезпеки здійснюється, у тому числі, шляхом підвищення цифрової грамотності громадян та культури безпекового поведіння в кіберпросторі, професійних компетенцій, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту.

Законодавчим продовженням цифрового розвитку України став Закон України від 15 липня 2021 року № 1667-IX «Про стимулювання розвитку цифрової економіки в Україні» [70], який визначив організаційні, правові та фінансові засади функціонування правового режиму «Дія Сіті», що запроваджується з метою стимулювання розвитку цифрової економіки в Україні шляхом створення сприятливих умов для ведення інноваційного бізнесу, розбудови цифрової інфраструктури, залучення інвестицій та необхідних спеціалістів.

Справжнім «проривом» у формуванні державної політики цифрового розвитку України на законодавчому рівні став Закон України від 01 грудня 2022 року № 2807-IX «Про Національну програму інформатизації» [63], який визначив особливості реалізації державної політики у сфері інформатизації для забезпечення потреб та розвитку інформаційного суспільства, впровадження інформаційно-комунікаційних та цифрових технологій. Зазначеним законом визначено генерального державного замовника Національної програми інформатизації – Міністерство цифрової трансформації України, унормовано таке поняття як цифровізація, під яким слід розуміти процес впровадження цифрових технологій у всіх сферах суспільного життя.

Серед управлінських рішень Президента України слід виділити Указ Президента України від 03 вересня 2020 року № 371/2020 «Про заходи щодо створення сприятливих умов для розвитку ІТ-індустрії в Україні» [62], зміст якого спрямований на розвиток освіти у галузі знань «Інформаційні технології», інтеграцію кращих світових практик у систему підготовки ІТ-фахівців для підвищення їх конкурентоспроможності на ринку праці, а також на удосконалення організації професійної підготовки, перепідготовки та підвищення кваліфікації зареєстрованих безробітних шляхом залучення закладів освіти, що здійснюють підготовку фахівців у сфері цифрових технологій.

Наступним визначальним рішенням у формуванні правових основ цифрового розвитку в Україні стала прийнята Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» [67], яка серед основних напрямів зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки виділяє наступні умови здійснення цифрової трансформації: забезпечення надання адміністративних послуг через безпечне «єдине вікно» з використанням сучасних інформаційних технологій; поширення цифрової грамотності, а також гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури.

Подальшим концептуальним документом прийнятим Президентом України стала Стратегія воєнної безпеки України (Указ Президента України від 25 березня 2021 року № 121/2021 «Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України») [68], сутність якої спрямована на створення сучасних, мобільних і боєздатних сил оборони, а також забезпечення всеохоплюючої оборони України, захист її суверенітету, територіальної цілісності і недоторканності. Так, з метою запровадження об'єднаного керівництва з підготовки та ведення

всеохоплюючої оборони України Стратегія передбачає упровадження сучасних інформаційних та космічних технологій, автоматизацію управлінських процесів і цифровізацію діяльності в силах оборони України з відповідним рівнем захищеності інформації. Крім цього, з метою нарощування спроможностей Збройних Сил України, сил територіальної оборони у їх складі, інших складових сил оборони до виконання покладених завдань у Стратегії в середньостроковій перспективі затверджено впровадження автоматизованих систем управління військами і зброєю, сучасних технологій зв'язку, телекомунікацій, захисту інформації, розвідки та логістики, цифрової трансформації у воєнній сфері, сфері оборони і військового будівництва.

Слід звернути увагу також на удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони, яке передбачає підвищення ефективності інформаційно-аналітичного забезпечення прийняття управлінських рішень, взаємодії, координації і контролю за діяльністю органів виконавчої влади, правоохоронних органів та військових формувань у сферах національної безпеки і оборони у мирний час, а також в особливий період, у тому числі в умовах воєнного стану, в умовах надзвичайного стану та під час виникнення кризових ситуацій, що загрожують національній безпеці України (Указ Президента України від 18 червня 2021 року № 260/2021 «Про рішення Ради національної безпеки і оборони України від 4 червня 2021 року «Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони»») [69].

Наступним етапом нашого дослідження є аналіз нормативно-правових актів Уряду, які створюють основу розбудови в Україні ефективної цифрової економіки і цифрового ринку та їх подальшу інтеграцію до єдиного цифрового ринку ЄС. І першим таким актом стала Концепція розвитку електронного урядування в Україні, схвалена розпорядженням Кабінету Міністрів України від 20 вересня 2017 року № 649-р [72], яка засвідчила проблеми значного відставання України від світових темпів цифрового розвитку, у тому числі відносно цифрової нерівності у використанні інформаційно-комунікаційних

технологій між органами влади на центральному, регіональному та місцевому рівні. Так, реалізацію та здійснення Концепції розпочато за принципом «цифровий за замовчуванням», який передбачає електронну форму реалізації Концепції як пріоритетну, а планування будь-якої реформи, проєкту чи завдання – із застосуванням інформаційно-комунікаційних технологій. Разом з тим, одним із шляхів і способів розв’язання зазначеної проблеми є розвиток сучасних електронних форм взаємодії, прозорості та відкритості діяльності, залучення громадян до прийняття управлінських рішень.

Наступним нормативно-правовим актом стала Концепція розвитку цифрової економіки та суспільства України на 2018 – 2020 роки, схвалена розпорядженням Кабінету Міністрів України від 17 січня 2018 року № 67-р [74], яка передбачає здійснення заходів щодо впровадження відповідних стимулів для цифровізації економіки, суспільної та соціальної сфер, усвідомлення наявних викликів та інструментів розвитку цифрових інфраструктур, набуття громадянами цифрових компетенцій, а також визначає критичні сфери та проєкти цифровізації, стимулювання внутрішнього ринку виробництва, використання та споживання цифрових технологій. Концепція визначила цифровізацію базовим механізмом економічного зростання завдяки здатності технологій позитивно впливати на ефективність, результативність, вартість та якість економічної, громадської та особистої діяльності, а масштаб і темп цифрових трансформацій – основними характеристиками економічного розвитку України.

Відповідно до Концепції основними цілями цифрового розвитку є: прискорення економічного зростання та залучення інвестицій; трансформація секторів економіки; технологічна та цифрова модернізація промисловості та створення високотехнологічних виробництв; доступність для громадян переваг та можливостей цифрового світу; реалізація людського ресурсу, розвиток цифрових індустрій та цифрового підприємництва.

Державна політика цифрового розвитку України знайшла своє відображення також у сфері навколишнього природного середовища та

екологічного забезпечення. Так, Концепція створення загальнодержавної автоматизованої системи «Відкрите довкілля», схвалена розпорядженням Кабінету Міністрів України від 7 листопада 2018 року № 825-р [76], сучасною проблемою із забезпечення надання вільного доступу до екологічної інформації та до стану навколишнього природного середовища визначила наявність значної кількості несистематизованої та непереведеної у цифровий формат екологічної інформації про стан навколишнього природного середовища на паперових носіях. Передбачається, що зазначену проблему буде вирішено через модернізацію процедури та підвищення якості надання адміністративних послуг у сфері охорони навколишнього природного середовища шляхом їх трансформації у цифровий формат (цифровізації).

Слід зазначити, що 2019 рік став визначальним у нормативно-правовому аспекті щодо розвитку сфер цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, робототехніки та роботизації, а також розвитку інформаційного суспільства України. Так, на початку 2019 року Кабінетом Міністрів України було затверджено засади реалізації органами виконавчої влади принципів державної політики цифрового розвитку (постанова Кабінету Міністрів України від 30 січня 2019 року № 56 [11]), які впроваджуються завдяки:

- відкритості (забезпечення відкритого доступу до відомчих даних (інформації));
- прозорості (використання відкритих зовнішніх інтерфейсів до відомчих інформаційних систем);
- багаторазовості використання (відкритий міжвідомчий обмін рішеннями);
- технологічної нейтральності і портативності даних (доступ до відомчих сервісів і даних);
- орієнтованості на громадян (забезпечення першочергового врахування потреб та очікувань громадян);

- інклюзивності та доступності (забезпечення можливості для всіх громадян користуватися новітніми досягненнями цифрових-технологій);
- безпечності та конфіденційності (забезпечення для громадян і суб'єктів господарювання безпечного та надійного ІТ-середовища);
- багатомовності (надання громадянам і суб'єктам господарювання адміністративних, інформаційних та інших послуг);
- підтримки прийняття рішень (використання новітніх інформаційних технологій для розроблення програмних продуктів);
- адміністративного спрощення (прискорення та спрощення адміністративних процесів шляхом їх цифрового розвитку);
- збереження інформації (забезпечення зберігання рішень, інформації, записів та даних, достовірності та цілісності);
- оцінювання ефективності та результативності.

А у вересні 2019 року Уряд затвердив Положення про Міністерство цифрової трансформації України (постанова Кабінету Міністрів України від 18 вересня 2019 року № 856 [49]), що створило правову основу для його функціонування, визначило засади, цілі та принципи діяльності. Так, Мінцифра відповідно до основних завдань забезпечує формування та реалізацію державної політики у сферах:

- цифровізації, цифрового розвитку, цифрової економіки, інновацій та технологій, впровадження електронного документообігу та розвитку цифрових навичок і цифрових прав громадян;
- відкритих даних, розвитку національних інформаційних ресурсів, публічних електронних реєстрів, інтероперабельності, радіочастотного спектра, цифрових комунікацій, та комерції та бізнесу;
- розвитку ІТ-індустрії, функціонування Дія Сіті, хмарних послуг, надання державних послуг, а також цифрової ідентифікації та електронних довірчих послуг.

Першою ініціативою цього міністерства стало введення в міністерствах, органах публічної влади посади заступника керівника відповідного органу з

питань цифрового розвитку, цифрових трансформацій і цифровізації (CDTO) (постанова Кабінету Міністрів України від 3 березня 2020 року № 194 «Деякі питання діяльності підрозділів з питань цифрового розвитку, цифрових трансформацій і цифровізації центральних та місцевих органів виконавчої влади та заступників керівників центральних органів виконавчої влади, обласних, Київської та Севастопольської міських державних адміністрацій з питань цифрового розвитку, цифрових трансформацій і цифровізації» [8]), що стало дієвим кроком у сфері вироблення державної політики цифрового розвитку в Україні.

Подальшим «правовим кроком» у справі розбудови цифрового розвитку стала програма діяльності новообраного Прем'єр-міністра України Дениса Шмигала (постанова Кабінету Міністрів України від 12 червня 2020 року № 471 «Про затвердження Програми діяльності Кабінету Міністрів України» [61]), яка визначила цифрову трансформацію та розвиток ІТ-сектору ключовими напрямками програми стимулювання, а цифровізацію економіки – одним з ключових напрямів внутрішньої державної політики.

Так, очікуваними результатами та показниками розвитку цифровізації сервісної діяльності органів публічної влади було передбачено збільшення до 200 доступних онлайн державних послуг, користування 60% українців онлайн-послугами, а також збільшення на 30% кількості утворених Центрів надання адміністративних послуг.

За показником цифровізації суспільства передбачалось, що 95% громадян України будуть мати покриття мобільним ширококутовим доступом до Інтернету із швидкістю не менше 2 Мбіт/с, 95% сільських домогосподарств матимуть можливість підключитися до фіксованого ширококутового доступу до мережі Інтернет із швидкістю не менше 100 Мбіт/с, а 95 відсотків закладів соціальної інфраструктури та органів місцевого самоврядування будуть підключені до ширококутового доступу до мережі Інтернет із швидкістю не менше 100 Мбіт/с.

Разом з тим, за показником цифрової грамотності українців очікувалось, що 6 млн. осіб опанують програму цифрової грамотності, 5000 тренерів викладатимуть курс цифрової грамотності, а також буде створено онлайн-платформу з цифрової грамотності, партнерську мережу хабів, а також буде створено онлайн-платформу для дітей, батьків та вчителів з метою інформування та реагування на ризики та загрози в Інтернеті.

Натомість, відповідно до звіту про хід і результати виконання Програми діяльності Кабінету Міністрів України у 2020 році (розпорядження Кабінету Міністрів України від 14 квітня 2021 року № 327-р [58]), за показниками розвитку адміністративних послуг та їх цифровізації було запроваджено в електронній формі та здійснено реінжиніринг 29 пріоритетних послуг (станом на 31 грудня 2020 року доступно 120 електронних послуг), успішно опрацьовано 60 % офлайн та 40 % онлайн заяв щодо державної реєстрації фізичних осіб – підприємців, а також збільшено (у порівнянні з 2019 роком) кількість утворених центрів надання адміністративних послуг на 28 %.

Станом на 2020 рік 83% громадян України мали покриття мобільним широкосмуговим доступом до Інтернету із швидкістю не менше 2 Мбіт/с, 55% сільських домогосподарств мали можливість підключитися до фіксованого широкосмугового доступу до мережі Інтернет із швидкістю не менше 100 Мбіт/с, і всього 23% закладів соціальної інфраструктури та органів місцевого самоврядування підключені до широкосмугового доступу до мережі Інтернет із швидкістю не менше 100 Мбіт/с.

У свою чергу за показником цифрової грамотності українців було встановлено, що станом на 31 грудня 2020 року:

– понад 420 тис. українців переглянуло освітні серіали з цифрової грамотності на платформі «Дія. Цифрова освіта» та понад 31,7 тис. переглянуло освітні серіали та підкасти на платформах «1+1 video» і «Мегого»;

- навчальну програму «Тренери для тренерів» на платформі «Дія. Цифрова освіта» за період з 30 червня по 31 грудня 2020 року пройшло більше 1200 осіб;

- на онлайн-платформі з цифрової грамотності «Дія. Цифрова освіта», зареєструвалося понад 420 тис. користувачів;

- відкрито більше 2000 партнерських хабів «Дія. Цифрова освіта».

Разом з тим, онлайн-платформу для дітей, батьків та вчителів з метою інформування та реагування на випадки ризиків та загроз в Інтернеті у 2020 році створено не було.

У подальшому, з метою вивчення проблемних питань з реалізації державної політики цифрового розвитку у липні 2020 року на засіданні Кабінету Міністрів України було затверджено Положення про Міжгалузову раду з питань цифрового розвитку, цифрових трансформацій і цифровізації та її склад (постанова Кабінету Міністрів України від 8 липня 2020 року № 595 [80]), до якої увійшли 45 представників державних органів на чолі Віце-прем'єр-міністром України з інновацій, розвитку освіти, науки та технологій – Міністром цифрової трансформації, якого призначено її головою. Основними завданнями Міжгалузової ради при цьому було визначено:

- підготовку пропозицій щодо вироблення державної політики цифрового розвитку, а також забезпечення розроблення проєктів концепцій і програм у сфері цифровізації;

- координацію дій органів виконавчої влади під час виконання програм з питань цифрового розвитку, цифрових трансформацій і цифровізації, а також сприяння впровадженню органами виконавчої влади принципів державної політики цифрового розвитку;

- підготовку пропозицій та рекомендацій щодо цільового та ефективного використання державних фінансів та іншої фінансової допомоги під час виконання та реалізації програм з питань цифрового розвитку, цифрових трансформацій і цифровізації органів виконавчої влади та органів місцевого самоврядування.

Необхідно звернути увагу також на цифрову трансформацію соціальної сфери, яка розпочалася у жовтні 2020 року за безпосередньої участі Міністерства соціальної політики та Міністерства цифрової трансформації у частині удосконалення нормативно-правового забезпечення та проведення комплексної цифрової трансформації всіх компонентів системи соціального захисту населення.

Так, з метою забезпечення європейських стандартів функціонування інституцій соціального захисту, надання послуг соціального характеру, фінансової стабільності соціальної сфери, підвищення прозорості та оптимізації її адміністративних видатків у жовтні 2020 року Урядом схвалено Стратегію цифрової трансформації соціальної сфери (розпорядження Кабінету Міністрів України від 28 жовтня 2020 року № 1353-р [78]), реалізація якої здійснюється шляхом виконання актів законодавства у соціальній сфері, розроблення нових актів, необхідних для цифрової трансформації соціальної сфери, реалізації пілотних проєктів із створення Єдиної інформаційної системи соціальної сфери.

Завданнями зазначеної Стратегії було визначено: підвищення ефективності соціального захисту громадян, удосконалення системи управління фінансовими ресурсами соціальної сфери, автоматизація системи її управління, а також технологічний розвиток інформаційних ресурсів соціальної сфери з використанням інноваційних технологій.

Заслуговують на розгляд також проблеми низького рівня цифрової грамотності та поінформованості населення щодо загальних аспектів, можливостей, ризиків та безпеки використання штучного інтелекту. Зазначені проблеми стали основою для схвалення Концепції розвитку штучного інтелекту в Україні (розпорядження Кабінету Міністрів України від 2 грудня 2020 року № 1556-р [75]), яка визначила мету, принципи та завдання розвитку технологій штучного інтелекту в Україні як одного з пріоритетних напрямів у сфері науково-технологічних досліджень. Концепція передбачає, що одним із завдань у сфері загальної середньої освіти є поширення цифрової грамотності

серед школярів (застосування цифрових інструментів для розв’язання прикладних задач, пошук інформації в інтернеті, захист персональних даних, медіаграмотність, цифрова гігієна тощо), а у сфері публічного управління – розвиток технологій штучного інтелекту для цифрової ідентифікації та верифікації осіб, у тому числі для надання державних послуг.

Цифровий розвиток космічної діяльності реалізується завдяки новим комерційним застосуванням, залученню приватної ініціативи, впровадженню нових організаційних форм та посиленню конкуренції. Розвиток зазначених інструментів регулює Концепція Загальнодержавної цільової науково-технічної космічної програми України на 2021-2025 роки, схвалена розпорядженням Кабінету Міністрів України від 13 січня 2021 року № 15-р [71], яка передбачає поетапне створення національної системи космічного спостереження на основі вітчизняних та іноземних орбітальних засобів та інформаційних інструментів, забезпечення сталого розвитку, контролю надзвичайних ситуацій природного та техногенного характеру, співпраці з міжнародною системою GEOSS у розв’язанні глобальних та регіональних проблем.

Необхідно акцентувати увагу також на відсутності концептуальних засад формування державної політики у сфері розвитку цифрових навичок та цифрових компетентностей громадян, що в свою чергу не дозволяло забезпечити розвиток усіх сфер суспільного життя відповідно до сучасних вимог, процесів глобальної цифровізації економіки, сфер життєдіяльності суспільства, які відбуваються у більшості країн світу. Зазначені проблеми стали підставою для схвалення Концепції розвитку цифрових компетентностей (розпорядження Кабінету Міністрів України від 3 березня 2021 року № 167-р [73]), яка визначила пріоритетні напрями і основні завдання з питань розвитку цифрових знань, умінь та навичок, а також підвищення рівня цифрової грамотності населення в умовах розвитку цифрової економіки та суспільства.

Основними завданнями Концепції стало:

- формування та розвиток цифрових компетентностей в суспільстві, а також підвищення рівня обізнаності громадян щодо небезпек в Інтернеті;
- забезпечення правового регулювання з питань формування державної політики розвитку цифрових компетентностей громадян;
- визначення системи та опису складових цифрової компетентності (рамки цифрової компетентності) та створення індикаторів для моніторингу стану розвитку цифрових компетентностей.

В свою чергу виконання вищезазначених завдань передбачає правове регулювання державної політики у сфері розвитку цифрових навичок, затвердження опису цифрової компетентності, розроблення відповідних методичних рекомендацій щодо її застосування, створення системи індикаторів моніторингу, а також проведення інформаційних кампаній, спрямованих на популяризацію цифрових технологій в цілому.

У сфері підготовки професійних кадрів слід виділити рішення Уряду про впровадження Єдиного державного веб-порталу цифрової освіти “Дія. Освіта” (постанова Кабінету Міністрів України від 10 березня 2021 року № 184 [48]), основними завданнями якого визначено:

- надання доступу до освітніх матеріалів, формування відповідного персоналізованого переліку, а також забезпечення можливості формування індивідуальних освітніх траєкторій;
- забезпечення цифрової грамотності людей усіх вікових категорій, проведення відповідного тестування, а також отримання електронних документів, що підтверджують результати проходження навчання;
- поширення ідей цифровізації, доведення інформації щодо новітніх цифрових технологій, відображення новин та результатів досліджень у сфері освіти;
- забезпечення можливості надання пропозицій (зауважень) щодо освітніх матеріалів та процесів дистанційного навчання, та надання інформації про підприємства, установи, організації, які можуть надати доступ до цифрової освіти (центрів цифрової освіти);

– використання методів та механізмів для покращення результатів навчання, а також захист даних (у тому числі персональних), що розміщуються на Веб-порталі цифрової освіти, від несанкціонованого доступу, знищення і модифікації.

Прогрес в розбудові системи управління державними фінансами для забезпечення її відповідності вимогам сучасної ринкової економіки та пріоритетам розвитку України почав з'являтися і у сфері міжбюджетних відносин. Початком такого прогресу стала схвалена у листопаді 2021 року Стратегія здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року (розпорядження Кабінету Міністрів України від 17 листопада 2021 року № 1467-р [77]), завданнями та напрямками реалізації якої є:

– створення багатофункціональної інтегрованої автоматизованої системи та впровадження і підтримка ІТ-продуктів та ІТ-послуг, створення відповідної ІТ-інфраструктури для розвитку ІТ-сервісів та формування підходів до побудови архітектури інформаційно-комунікаційних систем;

– забезпечення електронної інформаційної взаємодії діючих електронних сервісів суб'єктів системи управління державними фінансами із Єдиним державним вебпорталом електронних послуг;

– впровадження та подальший розвиток інформаційної системи управління плануванням та виконанням місцевих бюджетів «LOGICA», а також розвиток (удосконалення) інформаційно-аналітичної платформи електронної верифікації та моніторингу;

– створення нових інформаційних систем управління, забезпечення розмежування прав доступу та надання контрольованого доступу користувачам Єдиної інформаційно-комунікаційної системи управління державними фінансами до інформаційних ресурсів;

– розроблення методів залученості ІТ-персоналу з дотриманням принципу забезпечення рівних гендерних прав та можливостей, а також впровадження в цикл професійної підготовки спеціалістів ІТ-підрозділів

спеціальних курсів, спрямованих на удосконалення якості їх підготовки в галузі прийняття управлінських рішень у критичних ситуаціях;

– забезпечення цілісності інформаційних ресурсів Єдиної інформаційно-комунікаційної системи управління державними фінансами від сучасних кіберзагроз в умовах цифровізації управлінських процесів та необхідності обміну даними.

Наступне рішення Уряду з питань розвитку державної політики цифрового розвитку стало прийняте вже у 2023 році в контексті протидії збройній агресії проти України. Так, відповідно до постанови Кабінету Міністрів України від 4 лютого 2023 року № 139 [9], було підтримано пропозицію Міністерства оборони та Міністерства цифрової трансформації щодо підвищення рівня цифровізації сил безпеки та сил оборони України у період воєнного стану для забезпечення їх оперативної сумісності з відповідними структурами держав-членів НАТО шляхом використання комплексу спеціалізованого програмного забезпечення «Інтеграційна платформа «Дельта» Збройних Сил України», що забезпечує:

– інтеграцію різнотипних інформаційних (автоматизованих) систем для створення єдиного геоінформаційного та інформаційно-аналітичного середовища органів військового управління, військових частин та підрозділів сектору безпеки та оборони України згідно із стандартами НАТО;

– інформаційну сумісність та взаємодію між різнотипними інформаційними (автоматизованими) системами, які використовуються силами безпеки та силами оборони України та/або розробляються в їх інтересах.

Цифровий розвиток антикорупційної складової подальшої реалізації повноважень державними органами та органами місцевого самоврядування сприяє прозорості діяльності та відкриття даних з метою мінімізації корупційних ризиків у їх діяльності. Для цього у березні 2023 року було затверджено Державну антикорупційну програму на 2023-2025 роки (постанова Кабінету Міністрів України від 4 березня 2023 року № 220 [57]),

яка ще раз підкреслила проблему недостатнього рівня цифрової трансформації держави, що у свою чергу негативно впливає на ефективність роботи органів публічної влади, на швидкість та зручність отримання послуг громадянами і бізнесом, а також зумовлює існування ряду корупційних ризиків.

Очікуваними стратегічними результатами такої програми є: розроблення довгострокового національного стратегічного плану цифрового розвитку Державної митної служби та її територіальних підрозділів; цифровізація здійснення процесів примусового виконання рішень; розроблення містобудівної документації у векторній цифровій формі; забезпечення впровадження інструменту цифрового врядування відбудовою (модернізацією) України із публічним доступом до інтерактивної карти робіт; запровадження цифрової автоматизованої системи обліку військовослужбовців; створення цифрової автоматизованої системи наповнення, ведення та управління квартирному обліку військовослужбовців.

Слід виділити також постанову Кабінету Міністрів України від 1 грудня 2023 року № 1317 [10], яка визначила механізм використання функціональних можливостей, призначених для забезпечення потреб в автоматизації та цифровізації процесів, пов'язаних із виконанням посадових обов'язків, та обміну інформацією між працівниками державних органів, а також механізм формування та перевірки електронних службових посвідчень державних службовців органів виконавчої влади і Секретаріату Кабінету Міністрів України та їх електронних копій засобами Єдиного державного вебпорталу електронних послуг, зокрема із використанням мобільного додатка «Портал Дія».

Варто зазначити, щодо необхідності змін у Законі України «Про внесення змін до Закону України "Про Державний бюджет України на 2023 рік" щодо використання коштів державного фонду регіонального розвитку (реєстраційний № 9165 від 31.03.2023 року) зокрема щодо врегулювання питання залучення громадян до участі у відборі інвестиційних програм і проектів та визначенні пріоритетів спрямування коштів державного бюджету

на регіональний розвиток. Запропоновано застосувати під час відбору інвестиційних програм і проектів, що мають забезпечуватися за рахунок коштів державного фонду регіонального розвитку, процедури голосування громадян України за відповідні проекти засобами Порталу Дія. Зокрема, врахувати такі особливості використання у 2023 році коштів державного фонду регіонального розвитку, визначивши, що за результатами здійснення попереднього відбору та оцінки на відповідність вимогам законодавства поданих інвестиційних програм і проектів регіонального розвитку, центральний орган виконавчої влади, що забезпечує формування державної регіональної політики, подає їх для відкритого голосування громадян засобами Єдиного державного веб-порталу електронних послуг (Портал Дія). Під час такого голосування громадянин може віддати один голос за одну інвестиційну програму (проект регіонального розвитку) регіону за місцем реєстрації місця проживання (внутрішньо переміщена особа – за місцем проживання, визначеним відповідно до законодавства про облік внутрішньо переміщених осіб).

У 2024 році слід виділити рішення Уряду, яке було прийнято у серпні місяці (розпорядження Кабінету Міністрів України від 2 серпня 2024 року № 735-р «Деякі питання цифрової трансформації» [12]), яке схвалило пріоритетні напрями та завдання (проекти) цифрової трансформації на 2024-2026 роки, відповідно до яких передбачено:

- запровадження цифрового інструменту для надання електронних публічних послуг у сфері безпеки та оборони (відповідальний за виконання – Міноборони);

- створення, модернізацію, розвиток та забезпечення функціонування Єдиної цифрової інтегрованої інформаційно-аналітичної системи управління процесом відбудови об'єктів нерухомого майна, будівництва та інфраструктури (екосистеми DREAM) (відповідальний за виконання – Мінінфраструктури);

– удосконалення електронної інформаційної взаємодії суб'єктів фінансового моніторингу та цифрових технологій щодо проведення фінансових розслідувань у системі фінансового моніторингу (відповідальні за виконання – Держфінмоніторинг, Мінфін, Національний банк, Мін'юст, Національна комісія з цінних паперів та фондових ринків, Мінцифра);

– створення цифрової платформи «Е-молодь», що міститиме повну та актуальну інформацію про можливості для молоді, інформаційно-комунікаційних технологій для адміністрування і забезпечення реалізації пілотного проєкту «Гроші ходять за послугою» (відповідальний за виконання – Мінмолодьспорт);

– впровадження цифрових технологій для боротьби з маніпулюваннями, пов'язаними із спортивними змаганнями, присвоєнням спортивних звань в Україні, забезпечення функціонування електронного реєстру спортивних рекордів з визнаних в Україні видів спорту (відповідальний за виконання – Мінмолодьспорт);

– створення інформаційно-комунікаційної системи у сфері фізичної культури і спорту, цифрових технологій для публічного відображення інформації про національні і міжнародні спортивні заходи та результати спортсменів, проведення трансляцій та зберігання відповідних медіа-матеріалів (відповідальний за виконання – Мінмолодьспорт);

– створення відомчої системи цифрового радіозв'язку, а також модернізацію інформаційної системи надання адміністративних послуг Державної служби України з надзвичайних ситуацій (відповідальні за виконання – МВС, ДСНС);

– цифровий розвиток у сфері охорони життя та здоров'я людини через спеціалізовані веб-сервіси;

–модернізацію центральної ланки цифрової платформи «Безпечна країна», та комплексної системи захисту інформації Єдиної цифрової відомчої електронної комунікаційної мережі МВС з урахуванням загальних вимог до кіберзахисту об'єктів критичної інфраструктури;

– запровадження цифрових технологій для підготовки і проведення публічних закупівель у сфері інформатизації (відповідальні за виконання – Мінцифри, Мінекономіки);

– введення в експлуатацію інструменту цифрового управління відбудовою (модернізацією) України (відповідальні за виконання – Мінінфраструктури, Мінцифри, Агентство відновлення).

Щодо цифрового розвитку сфери ЖКХ важливо згадати постанову Кабінету Міністрів України від 3 вересня 2024 року № 1039 «Про реалізацію експериментального проекту щодо створення та впровадження цифрової інтегрованої інформаційно-аналітичної системи «Єдина платформа житлово-комунальних послуг» [66], яка має на меті створення єдиної уніфікованої інформаційної системи, що дасть змогу автоматизувати процеси, пов'язані з наданням та отриманням послуг, а також проведення реінжинірингу процесів та процедур, пов'язаних із наданням та отриманням послуг, зокрема шляхом їх цифровізації.

На окрему увагу заслуговує розпорядження Кабінету Міністрів України від 5 вересня 2023 року № 774-р «Про затвердження переліку показників Індексу цифрової економіки та суспільства (DESI)» [60], положення якого є індикатором запровадження європейських підходів до цифрового розвитку, що у свою чергу забезпечить соціально-економічну трансформацію України та її регіонів, дозволить розширити права і можливості кожного громадянина України, а також посилить українські підприємства. DESI (the Digital Economy and Society Index) – індекс цифрової економіки та суспільства, що є стандартним інструментом вимірювання цифрової продуктивності у країнах Європейського Союзу. За допомогою цього індексу відстежується прогрес країн-членів ЄС щодо цифрової конкурентоспроможності, а вони, у свою чергу, отримують можливість пріоритезувати свої потреби в реформах та інвестиціях. Впровадження показників DESI в Україні надасть можливість: відстежувати прогрес України за рівнем цифрової продуктивності; порівнювати відповідні показники з державами-членами ЄС; визначати сфери,

де країна відстає; коригувати державну політику та вживати необхідних заходів для підвищення цифрової продуктивності; визначати сфери пріоритетних інвестицій.

Підсумовуючи аналіз нормативно-правового забезпечення державної політики цифрового розвитку в Україні слід відзначити наступне:

- на цей час в Україні частково наявне законодавство для ефективної побудови цифрового суспільства та економіки;
- серед державно-правових документів у сфері цифрового розвитку переважають директивні акти (концепції, положення, стратегії), які у переважній більшості мають планувальний характер та містять обов’язкові для виконання вказівки. Разом з тим, нормативні акти (відповідні плани, програми тощо) у сфері цифрового розвитку, які б розкривали порядок реалізації зазначених директивних актів, починають тільки з’являтися;
- незважаючи на прийняті за останні декілька років різноманітні директивні документи, які спрямовані на цифровий розвиток суспільства та економіки, не розробленими залишаються акти стратегічного характеру. Так, не вирішеним питанням є розробка Національної стратегії цифровізації та Концепції цифрового розвитку органів публічної влади;
- потребує врегулювання питання цифрових відносин за межами України, а також гармонізації вітчизняного «цифрового» законодавства з правовими нормами Європейського Союзу.

На сьогодні, предметом цифрового розвитку є широке коло суспільно-загальних відносин, яке повинно урегульовуватися за допомогою права. Так, на сьогодні в Україні вже запущено такі е-послуги: паспорт разом з ПІН, цифрове посвідчення громадянина, MobileID, SmartID, mobile app, е-пенсія, електронний кабінет е-Малятко, е-резидентство, банківський рахунок для бізнесу онлайн, кабінет забудовника, прописка дитини онлайн, електронні вибори, ID-картка з електронним підписом. Разом з тим, реформа системи державного управління в напрямі цифрового розвитку держави повинна корелюватися із заходами щодо:

- створення дієвої та ефективної нормативно-правової бази для діяльності держави у цифровій сфері;
- законності та легітимності дій держави у віртуальному просторі, у тому числі щодо формування основних інформаційних прав та свобод людини і громадянина;
- забезпечення інформаційної прозорості в діяльності органів державної влади і місцевого самоврядування;
- зниження адміністративних бар'єрів і обмежень, що можуть унеможливити реалізацію громадянами України законних прав на одержання і поширення інформації;
- визначення національних інтересів держави у кіберпросторі.

Узагальнюючи зазначене, для подолання нормативно-правових викликів у сфері цифрового розвитку необхідно:

- на національному рівні:
 - посилити цифровий розвиток шляхом зменшення цифрового «розриву» та створення надійних ІТ-технологій для всіх;
 - посилити захист конфіденційності даних шляхом впровадження кращих систем та алгоритмів;
 - забезпечити подальший розвиток державно-приватного партнерства на основі людиноцентричного підходу;
 - підвищити рівень статистичних систем для відстеження процесів впровадження цифрових технологій та їх соціально-економічних наслідків у динаміці;
- на регіональному рівні:
 - забезпечити впровадження ефективних онлайн-послуг (або доступних послуг) за одне відвідування ЦНАПу;
 - забезпечити доступ до швидкісного Інтернету в кожному населеному пункті;
 - надати безкоштовну допомогу та можливість населенню користуватися цифровими послугами;

– на місцевому рівні:

забезпечити координацію дій з питань розвитку ІТ-навичок та цифрових компетентностей;

створити соціальні ініціативи, спрямовані на підвищення рівня цифрових ІТ-навичок та компетентностей для представників різних цільових груп населення;

запровадити програми, спрямовані на підвищення рівня обізнаності громадян щодо небезпек у цифровому середовищі, а також на формування культури нетерпимого ставлення до порушення прав, свобод та безпеки в ІТ-середовищі.

1.3 Перспективи застосування концепцій цифрократії та трансгуманізму в галузі публічного управління

Процеси глобальної цифрової трансформації відбуваються інтенсивно та екстенсивно, оскільки цифрові технології займають нішу прогресу, забезпечуючи ефективну діяльність органів публічної влади та підвищуючи продуктивність національних економік. Кожного дня в усьому світі в геометричній прогресії зростає кількість комп'ютерів, стає доступнішим Інтернет, розробляються нові потужні новації для збирання, зберігання та обробки даних, які згодом використовуються для прийняття управлінських рішень. Разом з тим, збільшуються й обсяги інформації, яка поширюється у мобільних додатках та соціальних мережах за допомогою цифрових технологій. Соціальні медіа стали значущою частиною життя сучасної особистості та перетворилися на платформи з обміну думками та ідеями. Ці зміни є базою для запровадження терміну «цифрократія» у понятійно-категорійний апарат науки державного управління.

Уперше поняття «цифрократія» зустрічається у роботах відомого американського футуролога А. Тофлера, зокрема у його книзі «Шок майбутнього» [189], де використовується для опису зростаючого впливу

цифрових технологій на економіку та суспільство. Згодом цей термін почали застосовувати у сфері наукових досліджень та у практичній діяльності органів влади, бізнес-організацій та громадських об'єднань.

М. Андерсон [105], активно досліджував питання діджитальних технологій та електронної комерції доводячи, що цифрократія змінює способи співпраці представників великого та середнього бізнесу із своїми клієнтами, а також процеси взаємодії між собою. Разом з тим, науковець обґрунтовує вплив цифрових технологій на ринок праці та зміни, що впроваджуються у процеси суспільного розвитку.

Ф. Шуманн та Р. Гібсон займаються дослідженням впливу соціальних мереж та інших цифрових технологій на публічне управління, політичну участь та громадську активність [175]. На їхню думку цифрові технології можуть як підтримувати, так і обмежувати громадянську партисипацію у політичному житті країни. З одного боку, цифрові технології дозволяють людям зручно спілкуватись між собою, організовувати акції і т.п., а також висловлювати свої думки та політичні переконання. З іншого боку, цифрові технології сприяють утворенню ефекту «інформаційної бульбашки», і де люди обирають можливість спілкуватись лише з тими, хто поділяє їх погляди та переконання. Негативним наслідком цього є відсутність можливості чути інші точки зору різних представників інших спільнот. Вчені провели експеримент, суть якого полягає у визначенні впливів віртуального обговорення у соціальних мережах та на сайтах політичних форумів на довіру громадян до влади. В експерименті взяло участь 800 респондентів, які були поділені на дві групи: контрольна та експериментальна. Перед усіма учасниками експерименту було двічі поставлено одні й ті ж самі запитання стосовно їх відношення до деяких політичних питань та подій (до початку та після закінчення експерименту). Учасники експериментальної групи користувались виключно соціальними мережами та цифровими ресурсами політичних форумів упродовж двох тижнів, а учасники контрольної групи довільно використовували різні джерела інформації та засоби комунікації у режимі

повсякденного життя. Дослідники встановили, що учасники експериментальної групи, які взяли участь у віртуальних обговореннях, більшою мірою довіряли уряду та демократичніше стали сприймати його політику після проведення експерименту, ніж учасники контрольної групи. Разом з тим, учасники, які брали участь у віртуальних обговореннях були більш налаштованими змінити свою думку, ніж учасники контрольної групи.

Сама концепція цифрократії активно застосовується у багатьох країнах світу. Наприклад, для зменшення корупційних ризиків Естонія використовує діджитальні технології в публічному управлінні, зокрема запровадивши різні платформи та сервіси цифрової участі (<https://www.valimised.ee>), у яких використовують ID-картки та інструменти електронного голосування з метою активного залучення громадян до процесів цифрового врядування. Подібні платформи для голосування застосовуються також у Данії та Норвегії, уряди яких, окрім того, активно використовують ще й соціальні мережі для забезпечення швидкої комунікації з громадянами. В Ісландії створено платформу «Better Reykjavik» (<https://betrireykjavik.is>) для жителів Рейк'явіку, що дозволяє пропонувати та обговорювати проекти, які у майбутньому можуть бути задіяні до реалізації стратегії розвитку міста. Варто зазначити, що практично у кожній країні світу на місцевому рівні існують подібні портали.

Враховуючи зазначене, можна сказати що цифрократія є новою формою влади, яка базується на використанні цифрових технологій та мереж для прийняття управлінських рішень, керування та контролю за різними процесами. Цифрократія передбачає використання алгоритмів штучного інтелекту та інших технологій автоматизації процесів публічного управління для реалізації у різних секторах національної економіки. Загалом цифрократія дозволила вивести публічне управління на сучасний рівень суспільних відносин. Цифрові технології дозволяють органам державної влади збирати та обробляти великі обсяги даних з різних джерел, що дозволяє більш детально аналізувати інформацію та приймати обґрунтовані державно-управлінські

рішення. Цифрові системи також допомагають аналізувати та моніторити показники роботи державних установ та виявляти проблеми які можуть виникати. Також цифрові технології допомагають при покращенні комунікації між громадянами та органами місцевого самоврядування. За допомогою мобільних додатків органи влади можуть швидко надавати інформацію про публічні послуги та застосовувати інструменти зворотного зв'язку. При цьому використання цифрових технологій спонукає будь-яку владу приймати інноваційні нормативні акти, що значно зменшують бюрократію при отриманні адміністративних послуг. Цифрократія змінила спосіб життя людей та привела до змін в культурній та економічній сфері. Активно розвивається електронна комерція та інтернет-бізнес, що дозволяє відкривати та розвивати нові ринки та робочі місця. Цифрові технології допомагають ефективніше управляти організаціями та збільшувати прибутковість бізнесу.

Цифрократія змінила та трансформує суспільні відносини, розширюючи можливості та впливаючи на створення нових парадигм людського розвитку. Одним із проявів таких змін є поява такого явища як трансгуманізм. Трансгуманізм є філософсько-науковою концепцією, яка пропонує використовувати нові цифрові технології (генна інженерія, кріоніка, штучний інтелект, нанотехнології, імплантація цифрових засобів) для збільшення потенційних можливостей людини та покращення її фізичного стану. В ідеалі ці технології повинні уповільнювати (або зовсім усувати) процеси старіння, підвищити тривалість життя, поліпшити когнітивні та сенсорні здібності людини [159].

Термін «трансгуманізм» уперше з'явився в есе Дж. Хакслі [138]. На його думку соціальні інститути у майбутньому зможуть конкурувати з еволюцією у вдосконаленні людського виду. Концепцію Дж. Хакслі, який обмежував трансгуманізм лише покращенням стану людей через соціальні та культурні зміни, розвинули ті, хто вважав, що людство може технологічно розширити межі своїх фізичних можливостей. Ідея трансгуманізму почала об'єднувати науковців, які прагнули акумулювати новітні наукові досягнення у сфері

комп'ютерних технологій, генної інженерії, кріоконсервації та інших новацій.

У 1986 році К. Дрекслер опублікував науково-публіцистичну працю «Engines of Creation» [126], у якій спрогнозував перспективи ери нанотехнологій та можливості їхнього використання у створенні різних матеріалів та пристроїв молекулярного рівня, виробництво яких має високий потенціал для вирішення складних технологічних завдань із забезпечення життєдіяльності людства. Разом з тим, К. Дрекслер відзначив важливість безпеки використання таких технологій та змодельовав можливі наслідки їх нерегульованого використання. Вважається, що саме ця книга стала основою для подальших досліджень у галузі нанотехнологій та першим кроком у напрямі розуміння їх ризиків та переваг.

Автор книги «Democratic Transhumanism 2.0» Д. Хьюз [137] є не тільки прихильником концепції трансгуманізму, але засновником Інституту етики та нових технологій (Institute for Ethics and Emerging Technologies, <https://ieet.org>) – некомерційного аналітичного центру, якій просуває ідею застосування можливостей технологічного прогресу для збільшення свободи, удосконалення та процвітання людини в умовах розвитку цифрового суспільства. Співробітники інституту вважають, що технологічний прогрес може стати необхідним каталізатором людського розвитку лише за умови гарантування, що технології будуть безпечними та рівномірно розподіленими у світі. Також в інституті досліджують етичні аспекти технологічного розвитку та пропонують конкретні рішення у цій галузі. У своїх роботах, Д. Хьюз активно продукує етичні, правові та соціальні дослідження розвитку технологій, зокрема штучного інтелекту, генної інженерії, біотехнологій. Разом з тим, автор звертає увагу на проблеми розширення людських прав у зв'язку з розвитком технологій, зокрема права на покращення фізичних та розумових можливостей за допомогою цифрових трансформацій.

Відомий канадський робототехнік Г. Моравец у своїх роботах вважає, що людина повинна активно залучатися до покращення своєї природної продуктивності за допомогою широкого спектру новітніх технологій, таких як

інженерія генів, штучний інтелект, розумні машини тощо. Автор переконаний, що за їх допомоги людина здатна зробити «кращу версію себе» [155] з високим рівнем інтелекту, фізичних та розумових здібностей.

В одній із своїх перших книг «Ера духовних машин» американський футуролог Р. Курцвейл передбачив, що машини не лише перевершать людський інтелект, але й зможуть «розвивати свободу волі, отримувати емоційний та духовний досвід» [150]. У наступній книзі «Сингулярність наближається» [151] теорія автора набула подальшого розвитку завдяки передбаченню неминучої сингулярності технологічного процесу до 2045 року, наслідком якого стане «злиття» людського та штучного інтелекту, а всі проблеми, пов'язані з хворобами, старінням та смертю будуть вирішені.

У 1998 році Н. Бостром і Д. Пірс заснували Всесвітню організацію трансгуманістів (WTA), яка виступала за використання технологій для розширення людських можливостей та покращення якості життя. Згодом, необхідність відобразити більш широке та різноманітне бачення трансгуманізму, що включає в себе не лише технології, а й культурні, соціальні, політичні та етичні аспекти спонукало засновників до її перейменування у 2008 році на «Humanity+» (<https://www.humanityplus.org>). Сьогодні ця організація просуває концепцію трансгуманізму як окрему галузь науки.

Теорія трансгуманізму знайшла підтримку у дослідників з Кремнієвої долини, зокрема Л. Пейджа, Дж. Безоса, І. Маска. У 2013 році Л. Пейдж заснував дослідницьку компанію «Calico Life Sciences» (LLS, <https://www.calicolabs.com>), місією якої було краще зрозуміння біології старіння та тривалості життя з метою використання отриманих знань для розробки технологій щодо його подовження. Ця організація не є традиційною біотехнологічною компанією чи академічною установою, однак вона об'єднує у собі кращі риси обох інституцій, не обмежуючи джерела фінансування. Для досягнення необхідних результатів потрібно здійснювати довгострокові дослідження у сфері базової біології старіння з використанням та створенням

передових технологій.

У 2002 році І. Маск заснував корпорацію з виробництва обладнання для потреб космічної галузі «SpaceX» (<https://www.spacex.com>) з метою організації у майбутньому людських поселень на Місяці та Марсі, а також у 2016 році створив нейротехнологічну компанію «Neuralink» (<https://neuralink.com>) для розробки мозкових чіпів-імплантів (інтерфейсів).

У липні 2022 року компанія з виробництва мозкових чіпів «Synchron» (<https://synchron.com>) на чолі з Т. Окслі оголосила про успішний експеримент у США з імплантації чіпа в мозок пацієнта з бічним аміотрофічним склерозом. Особливість технології полягає у розробленому ендоваскулярному мозковому комп'ютерному інтерфейсі, який дозволяє отримати доступ до кожного з відділів мозку за допомогою кровоносних судин. Ця платформа стала революційною та відкривала нові можливості у лікуванні неврологічних захворювань (нейроінтервенційна електрофізіологія). Така технологія трансформує три медичні вертикалі: нейропротезування, нейромодуляцію та нейродіагностику.

Разом з тим, інші науковці висловлюють занепокоєння щодо феномену розвитку трансгуманістичних технологій, оскільки їх подальше використання зможе призвести до штучного виникнення суспільної нерівності. У статті опублікованій у журналі «Foreign Policy» американський політичний та економічний теоретик Ф. Фукуяма назвав трансгуманізм найнебезпечнішою ідеєю у світі і попередив, що розвиток біотехнологій може мати жахливі наслідки для прав людини. Він зауважив, що значні економічні розбіжності між країнами можуть спонукати «удосконалених» індивідів вимагати більших прав над «тими, хто залишився фізично незмінними» [190].

Дехто із застереженням порівнює трансгуманізм з євгенікою (рухом за удосконалення природи людини) через обґрунтовані побоювання, що новітні технології можуть бути використані для створення «надлюдей». Наприклад, синтетичне виробництво гормонів та застосування біонічних імплантів і протезів можуть бути корисні для людей з захворюваннями або

інвалідностями, але разом з тим, можуть бути використані для покращення продуктивності досягнень у спортсменів без жодних медичних проблем. Однак найбільш поширеною критикою концепції застосування трансгуманізму є побоювання щодо виникнення певного підвищення суспільного дисбалансу, пов'язаного із соціальною нерівністю. Так, «удосконалені» люди почнуть вимагати більших прав над звичайними людьми, що може призвести до втрати цінностей, що пов'язані із людською природою, а також імовірність виникнення ризику зниження значення людської особистості.

Тому, розуміння чи є майбутнє у реалізації концепцій цифрократії та трансгуманізму в галузі публічного управління залежить від того, як будуть вирішені етичні та соціальні питання, пов'язані з використанням цифрових технологій для поліпшення людських можливостей. Перспективою подальших досліджень є вироблення механізмів вирішення проблем балансу переваг трансгуманізму та ризиків й етичних викликів задля подальшого суспільного розвитку, а також вироблення нових механізмів управління майбутнім.

Висновки до розділу 1

Розкрито існуючі наукові розробки українських та зарубіжних вчених щодо визначення сутності механізмів формування та реалізації державної політики цифрового розвитку, що дало змогу визначити проблематику діджиталізації публічного управління, а саме: недостатність опанування цифрових компетенцій державними службовцями та посадовими особами місцевого самоврядування; неналежність забезпечення кібербезпеки критичної інфраструктури та захисту цифрових прав і свобод громадян. У дослідженнях аналізується досвід країн ЄС, що підкреслює доцільність орієнтації на економічні механізми державного регулювання цифровізації із мінімальним застосуванням адміністративних методів.

Незважаючи на вагомі наукові здобутки вітчизняних учених, подальших досліджень потребують: розробка механізмів адаптації кращих зарубіжних практик цифровізації до українських реалій; реалізація належної державної політики у сфері інтеграції України до єдиного цифрового ринку ЄС; визначення ключових інструментів здійснення цифрової та кібердипломатії; здійснення моніторингу соціально-економічних наслідків цифрової трансформації у розрізі регіонів України; дослідження етичних, правових та соціальних викликів, пов'язаних із впровадженням штучного інтелекту, в тому числі і як інструменту зниження корупційних ризиків у сфері публічних закупівель; вивчення впливу цифрової освіти на підвищення конкурентоспроможності людського капіталу в умовах цифрової економіки, зокрема визначення ключових напрямів та механізмів реалізації медіаграмотності серед населення; перспективи застосування концепцій цифрократії та трансгуманізму в галузі публічного управління; виокремлення ключових напрямів та механізмів реалізації захисту державних інституцій від дезінформаційних атак; вироблення стратегічних напрямів державної політики цифрового розвитку України в умовах інтенсифікації ведення інформаційних воєн.

Проаналізовано особливості нормативно-правового забезпечення державної політики цифрового розвитку України, що дало змогу виокремити його три основні етапи: усталення (інформатизація, 1998-2009 рр.), впровадження (електронного урядування, 2010-2017 рр.) та просування (цифрова трансформація, з 2018 р. по т.ч.).

Констатовано зростання кількості та якості цифрових послуг/сервісів завдяки нормативному розширенню сфери застосування ІТ й можливостей їх онлайн надання. зокрема реалізовано: паспорт разом з ППН, цифрове посвідчення громадянина, MobileID, SmartID, mobile app, е-пенсія, е-Малятко, е-резидентство, банківський рахунок для бізнесу онлайн, кабінет забудовника, прописка дитини онлайн, електронні вибори, ID-картка з електронним підписом.

Здійснено аналіз нормативно-правового забезпечення державної політики цифрового розвитку України, яке є основою для розвитку людського потенціалу, цифрової економіки та її окремих сфер, формування цифрових компетентностей громадян, розбудови електронної демократії і ресурсного капіталу, забезпечення координації дій на рівні органів публічної влади, а також підвищення рівня обізнаності у сфері державної кібербезпеки.

В результаті здійсненого аналізу особливостей нормативно-правового забезпечення державної політики цифрового розвитку України слід відзначити: фрагментарність чинного законодавства, яке лише частково сприяє ефективній цифровізації діяльності органів публічної влади; домінування директивних актів (концепцій, положень, стратегій), які у переважній більшості мають планувальний характер та містять обов'язкові для виконання заходи, разом з тим виявлено недостатність наявності відповідних планів, програм та проєктів щодо цифрового розвитку різних сфер життєдіяльності суспільства, які б розкривали порядок реалізації зазначених директив; недостатню розробленість актів стратегічного характеру, які б були спрямовані на управлінський розвиток цифрової трансформації, а саме відсутність Національної стратегії цифровізації та Концепції цифрового розвитку органів державної влади та органів місцевого самоврядування; неврегульованість питань цифрових відносин за межами України, а також гармонізації українського «цифрового» законодавства з правовими нормами ЄС. Також виявлено неврегульованість реалізації цифрових комунікацій на місцевому рівні, що залишає невирішеними проблеми із забезпечення Інтернет-покриттям більшої частини авто- та залізничних магістралей, гірської місцевості та інших віддалених територій України.

Обґрунтовано, що реформа системи державного управління у сфері цифрового розвитку України повинна здійснюватися з урахуванням: забезпечення інформаційної прозорості діяльності органів державної влади і органів місцевого самоврядування, законності та легітимності дій держави у віртуальному просторі, захисту основних інформаційних прав та свобод

людини і громадянина; зниження адміністративних бар'єрів і обмежень; відстоювання національних інтересів України у кіберпросторі; створення дієвої та ефективної нормативно-правової бази для діяльності держави у цифровій сфері.

Доведено, що прийняття належної нормативно-правової бази у сфері цифрового розвитку окреслить стратегічний курс України щодо процесів опанування громадянами знань, умінь, навичок у сфері цифрових технологій, а також матиме позитивний вплив на процеси розвитку цифрового суспільства. Запропоновано розвивати нормативно-правове забезпечення у таких сегментах цифрового розвитку як: захист конфіденційності даних через впровадження систем та алгоритмів штучного інтелекту; державно-приватне партнерство на основі людино-центричного підходу; розширення переліку доступних державних онлайн-послуг; забезпечення доступу до швидкісного Інтернету в кожному населеному пункті країни; розвиток цифрових компетентностей.

Визначено перспективи застосування концепцій цифрократії та трансгуманізму в галузі публічного управління, що дало змогу стверджувати, що цифрократія стає новою формою влади, яка дозволить трансформувати галузь публічного управління до нового інноваційного рівня суспільних відносин завдяки цифровим технологіям та комунікативним мережам прийняття рішень. Цифрократія передбачає використання алгоритмів штучного інтелекту та інших технологій автоматизації процесів публічного управління та адміністрування. Обґрунтовано спільність/різницю наукових підходів щодо застосування концепцій «цифрократія» та «трансгуманізм». Доведено, що концепції цифрократії та трансгуманізму мають спільну мету – удосконалити та покращити життя людства за допомогою діджиталізації технологічного розвитку, але їх сфера та інструментально-функціональні підходи фокусуються на різній природі застосування. Зазначено, що методи, інструменти та засоби цифрократії орієнтовані на підвищення ефективності функціонування різних сфер суспільства (публічне управління, національна

економіка, освіта, охорона здоров'я та ін.). Визначено, що концепція трансгуманізму завдяки застосуванню новітніх технологій спрямована на покращення фізичної та розумової природи людських можливостей (підвищення рівня інтелекту, подовження життя, удосконалення тіла та ін.). Визначено основні складові наукового дискурсу щодо можливостей подальшого застосування концепцій трансгуманізму в галузі публічного управління, а саме наголошено на необхідності дослідження переваг, ризиків та етичних аспектів її розвитку.

Основні результати розділу 1 опубліковано в наукових працях автора:

1. Герман, Д., & Карпенко, Ю. (2022). Перспективи застосування концепцій цифрократії та трансгуманізму в галузі публічного управління. *Аспекти публічного управління*, 10(6), 19-23. <https://doi.org/10.15421/152239>
2. Герман, Д. (2025). Особливості нормативно-правового забезпечення державної політики цифрового розвитку України. *Аспекти публічного управління*, 13(1), 82-92. <https://doi.org/10.15421/152510>

РОЗДІЛ 2

ЗАРУБІЖНИЙ ТА УКРАЇНСЬКИЙ ДОСВІД ЗАСТОСУВАННЯ МЕХАНІЗМІВ ВИРОБЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЦИФРОВОГО РОЗВИТКУ

2.1 Реалізація державної політики у сфері інтеграції України до єдиного цифрового ринку ЄС

На сучасному етапі євроінтеграційного поступу України особливої актуальності набуває завдання гармонізації національної системи публічного управління із стандартами Європейського Союзу. Цифрова трансформація, яка охоплює всі сфери діяльності органів публічної влади, вимагає не лише адаптації до європейського спільного доробку (*acquis communautaire*), а й активного використання новітніх цифрових технологій, які вже стали фундаментом стратегічних програм ЄС, зокрема Digital Decade Policy Programme 2030 [119].

Прийняті Євросоюзом акти, як-от Artificial Intelligence Act [169], Data Governance Act [166], Digital Services Act [165], eIDAS 2.0 [170], Data Act [167] та Cybersecurity Act [164], окреслюють не тільки правові вимоги, а й нову етичну, технологічну та операційну парадигму цифрового врядування, орієнтованого на прозорість, безпеку та людиноцентризм.

Новітні технології – штучний інтелект, блокчейн, цифрові двійники, квантові мережі – розширюють можливості публічного управління. Сучасна держава має бути не лише користувачем, а й модератором інновацій: формувати запити, координувати дії, встановлювати етичні стандарти.

З одного боку, сучасні виклики загострюють потребу у національних рішеннях, які не лише відповідають європейським стандартам (зокрема вимогам EU Cybersecurity Act [164] та NIS2 Directive [124]), а й розвивають власну стійку цифрову архітектуру. З іншого боку, криза породжує унікальне

«вікно можливостей» для впровадження інновацій у системі публічного управління, адже саме в екстремальних умовах формуються нові моделі взаємодії між державою, громадянами та цифровими сервісами.

Пріоритетний курс на євроінтеграцію є важливим аспектом участі України у функціонуванні Єдиного цифрового ринку ЄС (далі – ЄЦР). Для нашої країни перехід до ЄЦР відкриває низку перспектив і значних переваг, зокрема зменшення наявних бар'єрів у цифровій торгівлі з країнами ЄС через регуляторне зближення у цифровій сфері, а також прискорення цифрової трансформації відповідно до європейських стандартів.

Центр аналізу міжнародної торгівлі «Trade+» та громадська організація «Український центр європейської політики» провели дослідження, яке виявило низку переваг реалізації державної політики цифрового розвитку, а саме [15]:

- підвищення рівня економічної продуктивності за рахунок розширеного доступу до передових європейських цифрових технологій та інновацій, автоматизації організаційних і виробничих процесів;
- скорочення трансакційних витрат для бізнесу та державного сектору у наслідок переходу на безпаперові операції;
- оптимізація цифрової торгівлі між Україною та ЄС за рахунок зменшення регуляторних, інформаційних та організаційних бар'єрів, а також покращення логістичних процесів, які сприятимуть зниженню торговельних витрат;
- запровадження передових європейських практик для підвищення якості, прозорості та ефективності цифрового врядування;
- стимулювання розвитку інноваційних галузей через впровадження сучасних цифрових технологій, зокрема штучного інтелекту, хмарних платформ і сервісів, великих даних;
- підвищення рівня добробуту населення завдяки ширшому доступу до цифрових інноваційних продуктів і послуг, а також посиленню захисту прав споживачів онлайн-сервісів.

Таким чином, інтеграція до ЄЦР буде мати суттєвий вплив на цифровий розвиток та підвищення конкурентоспроможності України у світі.

Проте, окрім позитивних аспектів, це також зобов'язуватиме Україну впроваджувати низку заходів щодо адаптації національного законодавства до норм та стандартів ЄС, забезпечення технічної та інституційної спроможності країни для сумісності систем у цифровій сфері, а також збільшення державних інвестицій у фізичну інфраструктуру цифрового врядування та широкопasmового інтернету.

Щодо бізнесу, це означатиме зміни у правилах регулювання, які передбачають посилений захист прав споживачів, зокрема у сфері обробки персональних даних, а також зростання конкуренції з боку європейських компаній. Втім, такі зміни є необхідними для побудови спільного економічного простору з ЄС і, з огляду на стрімкий розвиток цієї сфери, потребують невідкладних дій. Якщо ці процеси не будуть реалізовані вчасно, це може призвести до виникнення додаткових регуляторних бар'єрів і розбіжностей, що в свою чергу, негативно позначиться на цифровій торгівлі та загальному економічному співробітництві між Україною та Європейським Союзом.

Загалом, сучасний стан цифрового розвитку України свідчить про ряд позитивних зрушень, що відображається у різних міжнародних рейтингах, а саме у:

- Індексі ООН з розвитку електронного урядування EGDI (E-Government Development Index);
- Індексі електронної участі (E-Participation Index);
- Індексі мережевої готовності NRI (Networked Readiness Index);
- Індексі цифрової конкурентоспроможності WDCR (World Digital Competitiveness Ranking).

Їх детальний аналіз та позиції України зазначені у табл. 2.1.

Таблиця 2.1

Позиції України в основних міжнародних рейтингах цифрового розвитку

Індекс	Характеристика	Місце України
Індекс ООН з розвитку електронного урядування EGDІ	Індекс використовується з метою оцінювання рівня розвитку е-уряду в країнах-членах ООН, який проводиться раз на два роки. Також, цей індекс є складеним показником 3 важливих вимірів: надання онлайн-послуг, забезпечення телекомунікаційним зв'язком і розвиток людського потенціалу.	82 місце – 0,61650 (2018 рік) 69 місце – 0,71190 (2020 рік) 46 місце – 0,80290 (2022 рік) 30 місце – 0,88407 (2024 рік)
Індекс електронної участі E-Participation Index	Індекс оцінювання рівня електронної участі громадян у процесах прийняття державно-управлінських рішень.	75 місце – 0,68540 (2018 рік) 46 місце – 0,80950 (2020 рік) 57 місце – 0,60230 (2022 рік) 1 місце – 1,00000 (2024 рік)
Індекс мережевої готовності NRI	NRI є складеним показником за допомогою якого оцінюється застосування та вплив ІКТ в економіках світу. Щорічно випускається звіт та публікуються дані, які включають карту мережевої готовності 133 економік на основі: технологій, людських ресурсів, управління та взаємодії.	67 місце зі 121 – 48,92 (2019 рік) 64 місце зі 134 – 49,43 (2020 рік) 50 місце зі 131 – 55,71 (2022 рік) 43 місце зі 133 – 55,32 (2024 рік)
Індекс цифрової конкурентоспроможності WDCR	За допомогою індексу оцінюється ступінь впровадження та вивчення країнами цифрових технологій за трьома основними факторами: знання; технології; майбутня готовність.	58 місце з 63 – 51,292 (2018 рік) 60 місце з 63 – 55,255 (2019 рік) 58 місце з 63 – 48,807 (2020 рік) 54 місце з 64 – 50,073 (2021 рік)

Джерело: сформоване автором на основі джерела [130-142]

Проаналізувавши дані табл. 2.1, можна зробити певні висновки про сучасний стан цифрового розвитку в Україні у періоді з 2018 по 2024 роки. Розглядаючи показник EGDI, спостерігається позитивна динаміка упродовж зазначеного періоду. У 2018 році Україна займала 82 місце зі 193 країн, але надалі її позиції покращувалися, а саме: у 2020 році – 0,71190 (69 місце), 2022 рік – 0,80290 (46 місце), 2024 рік – 0,88407 (30 місце). Крайній показник є високим, оскільки середнє світове значення цього індексу становило 0,6382, що свідчить про певне випередження Україною глобального рівня цифрового розвитку. Щодо середнього рівня в країнах Європи він дорівнює 0,8493, що також свідчить про позитивну динаміку цифрового розвитку в Україні. Окрім цього, Україна займає перше місце Східної Європи, що свідчить про швидкі темпи цифровізації та може стати прикладом для багатьох країн світу [130].

Дані Індексу електронної участі також свідчать про позитивну динаміку за проаналізований період. З 2018 по 2024 рік показники коливалися у діапазоні від 0,69 до 1,0, що свідчить про те, що рівень електронної участі громадян у процесах прийняття державно-управлінських рішень є доволі високим, що сприяло Україні стати світовим лідером за цим показником [131].

Дані Індексу мережевої готовності (NRI) також відображають покращення позиції України щодо підвищення рівня середнього доходу серед населення. Аналізуючи окремі компоненти NRI, такі як «люди», «технології», «управління» та «вплив», Україна має показник вище середнього серед всіх країн ЄС. За результатами 2024 року Україна займає 43 місце зі 133 країн світу. Щодо, показників за окремими значеннями найкращим напрямом розвитку для України є «людські ресурси», за яким показник склав 51,83 (28 місце серед країн світу), а значення показників «технології» склав 48,96 (44 місце), та «вплив» – 57,34 (51 місце), стовп «управління» – 63,14 (56 місце) відповідно. Останні два компонента містять максимальний потенціал для удосконалення. Недостатніми в Україні є показники розвитку цифрової інфраструктури, цифрової конкурентоспроможності бізнесу, а найбільшої уваги потребує

покращення якості життя та забезпечення сталого розвитку. За показниками сталого розвитку міст та громад Україна займає 104 місце, а за доступністю чистої енергії – 113, що свідчить про суттєві проблеми у цих сферах [185].

Щодо Індексу цифрової конкурентоспроможності (WDCR), упродовж 2018–2021 років суттєвих змін не відбулося. Україна стабільно входила до десяти країн із найгіршими показниками серед 64 держав, що оцінювалися в рейтингу. З 2022 року через обмежену доступність даних, Україну виключили з рейтингу, що унеможливило точну оцінку її позицій. Проте, з огляду на тенденції позитивної динаміки щодо цифрового розвитку України, можна припустити, що її позиції у WDCR могли б суттєво покращитися.

Існуючі позитивні зміни можна пов'язати з наступними чинниками:

- по-перше, визначення цифрового розвитку як одного із ключових пріоритетів державної політики України;
- по-друге, створення у 2019 році профільного ЦОВВ – Міністерства цифрової трансформації України;
- по-третє, активізація інтеграції України до Єдиного цифрового ринку ЄС, у рамках якого було реалізовано низку заходів, спрямованих на гармонізацію українського законодавства з європейськими нормами та стандартами.
- по-четверте, активна взаємодія України з ЄС у сфері цифровізації, зокрема через фінансування та підтримку різних ініціатив і міждержавних програм.

Створення Міністерства цифрової трансформації України позитивно вплинуло на інтеграцію України до ЄЦР [49]. Враховуючи рекомендації Європейської Комісії, Мінцифра у 2020 році представила оновлену Дорожню карту інтеграції України до ЄЦР ЄС (далі – Дорожня карта). Зокрема, даний документ передбачав впровадження 141 заходу з метою імплементації 75 правових актів ЄС до грудня 2023 року [36]. Ключовими результатами її виконання стали: імплементація Кодексу електронних комунікацій ЄС; реформування регуляторних органів у сфері телекомунікаційних послуг;

впровадження європейських систем у сфері електронних довірчих послуг, кіберзахисту та кібербезпеки; впровадження мережі 5G та широкосмугового Інтернету; розвиток електронної комерції; впровадження єдиного європейського номера екстреної допомоги. Зокрема, на рис. 2.1 представлено відсотковий рівень виконання заходів Дорожньої карти станом на 01 березня 2025 року.

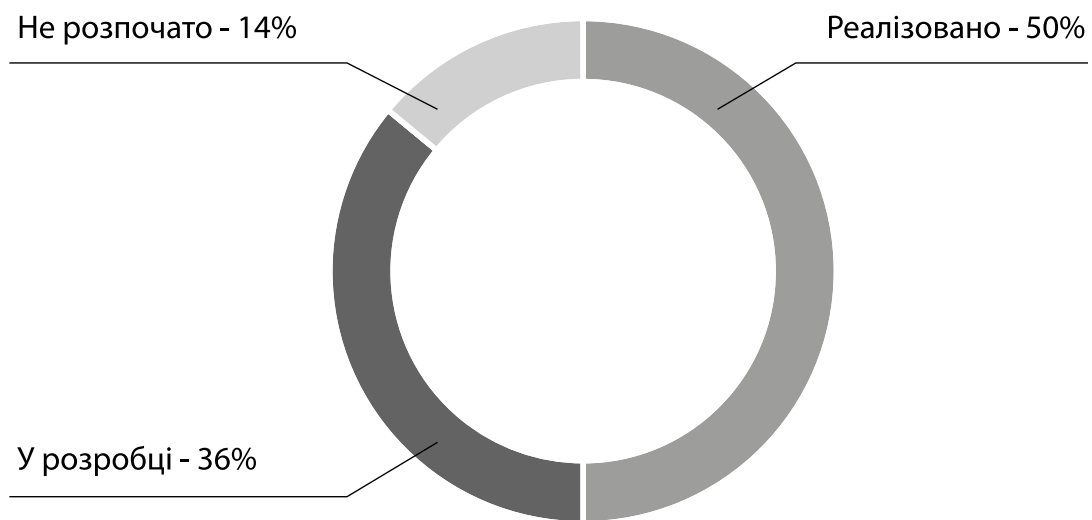


Рис. 2.1 – Виконання Плану Заходів Дорожньої карти інтеграції України до Єдиного цифрового ринку ЄС

Джерело: побудовано автором на основі джерела [13]

Таким чином, реалізовано повністю лише 12 проєктів (50%), у стані розробки перебуває 12 проєктів, що складає 36%, а не розпочатими залишається ще 15% (3 проєкти) [13].

Стосовно повністю реалізованих проєктів було досягнуто ряд позитивних зрушень щодо: адаптації українського законодавства до норм ЄС в частині конкуренції на ринках телекомунікацій; забезпечення правового захисту послуг, що базуються чи включають умовний доступ; узгодження системи безпеки електронних довірчих послуг; врегулювання питання інформаційних послуг, відкритого доступу до Інтернету та повторного використання даних; долучення до низки програм ЄС у сфері цифрової

трансформації; спрощення доступу до об'єктів, захищених авторськими правами; врегулювання онлайн-автентифікації для платіжних послуг; визначення законодавчих норм у сфері цифрового контенту, послуг та захисту прав споживачів тощо [13].

Ще 66 завдань в рамках плану Дорожньої карти перебувають на стадії реалізації, більшість з них виконана на 50%, зокрема: гармонізація законодавства щодо телекомунікаційних мереж та послуг (64%); спрощення процедур отримання дозволів на телекомунікаційні послуги (67%); забезпечення відкритого та конкурентного ринку (83%); адаптації радіочастотного спектру відповідно до норм ЄС (67%); законодавчих змін у сфері кібербезпеки (80%); забезпечення доступності державних вебсайтів та мобільних додатків (71%); удосконалення законодавства щодо захисту прав споживачів, обробки персональних даних та безпеки дітей в Інтернеті (50%). Однак, нерозпочатими завданнями залишаються: законодавче врегулювання транскордонної мобільності онлайн-контенту; усунення гео-блокування та екстериторіального ліцензування цифрових послуг [13].

Підсумовуючи зазначимо, що Україна активно інтегрується до ЄЦР ЄС, однак для завершення процесів повноцінного приєднання необхідно виконати низку проєктів та вирішити неврегульованих питань. Окрім того, Дорожня карта наразі є застарілою та потребує оновлення, а також розробки нової Стратегії у сфері інтеграції України до Єдиного цифрового ринку ЄС, оскільки терміни виконання Плану заходів вже завершився.

Для надання рекомендацій щодо удосконалення інструментарію державної політики у сфері інтеграції України до єдиного цифрового ринку ЄС доцільним є проведення аналізу щодо досвіду вироблення державної політики на прикладі окремих країн-членів ЄС.

Раніше для оцінки ролі цифрової економіки в країнах-членах ЄС використовувався Індекс розвитку цифрової економіки та суспільства (Digital Economy and Society Index, DESI). Цей індекс складався з 5 вимірів: «людський капітал», «зв'язок», «використання Інтернету», «інтеграція цифрових

технологій», «цифрові державні послуги». Аналіз цих складових допомагав моніторити та оцінювати можливості у сфері цифрової конкурентоспроможності. На основі цього надавалися рекомендації для урядів країн-членів ЄС, що сприяли більш узгодженому та ефективному плануванню національних стратегій цифрового розвитку. Проте, останній звіт публікувався у 2022 році, а у 2023 році відповідно до Політичної програми цифрового десятиліття до 2030 року індекс DESI було інтегровано до звіту «Стан цифрового десятиліття», який використовується для моніторингу прогресу в досягненні цифрових цілей [179].

Саме тому, вважаємо за доцільне проаналізувати саме Звіт 2024 року Траєкторії Цифрового десятиліття [1], який демонструє зміни в ЄС стосовно цифрових трансформацій у чотирьох ключових сферах: цифрова інфраструктура, цифрові навички, цифровізація державних послуг і цифровізація бізнесу. Також, у цьому документі представлено ключові чинники та виклики, а також їх вплив на конкурентоспроможність. Також, у звіті 2024 року оцінюються Стратегічні дорожні карти цифрового десятиліття, ухвалені на рівні країн-членів ЄС у 2023 році. У звіті представлено оцінку зусиль у сфері цифровізації, пропонуються рекомендації щодо її покращення, а також публікуються данні щодо дотримання Європейської декларації цифрових прав і принципів.

У 2022 році в межах Цифрового десятиліття ЄС було ухвалено Європейську декларацію про цифрові права та принципи (далі – Декларація) [133] – ключовий рамковий документ, який визначає основні цифрові права та принципи, які відображають цінності ЄС. Ця Декларація є своєрідною дорожньою картою реалізації цифрових трансформацій в ЄС на основі людиноцентричного, безпечного та сталого підходу. Документ не лише закріплює фундаментальні права громадян у цифровій сфері, але й містить зобов'язання для держав-членів ЄС щодо діяльності у ключових напрямках цифрового розвитку. Декларація є дороговказом для громадян стосовно дотримання цифрового законодавства ЄС.

Комісія стежить за застосуванням цифрових прав і принципів в ЄС і публікує свій щорічний моніторинг разом зі Звітом про стан цифрового десятиліття. Звіт про моніторинг дозволяє оцінити, наскільки країни-члени дотримуються обраного курсу, а також сприяє поширенню передових цифрових практик на рівні ЄС.

Окрім того, ЄС керується принципами Декларації у міжнародних відносинах формуючи глобальну цифрову трансформацію, базовим пріоритетом, якої є забезпечення прав людини та демократичні цінності. Принципи Декларації сформовані навколо шести ключових напрямів, які відображено на рис. 2.2 [133].

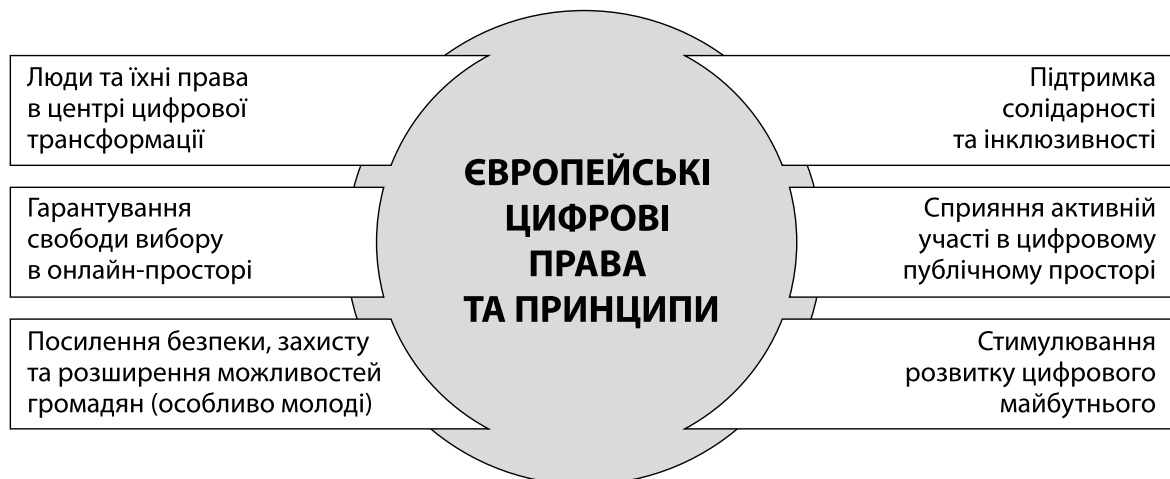


Рис. 2.2 Ключові напрями Європейської декларації про цифрові права та принципи

Джерело: сформовано автором на основі джерела [133]

Відповідно до зазначених напрямів Декларації усі мешканці ЄС повинні отримати максимальні переваги від цифрової трансформації, зокрема [133; 180]:

1. Люди та їхні права в центрі цифрової трансформації. Основна сутність цього напрямку полягає у тому, що цифрові технології мають захищати права людей, підтримувати демократію та гарантувати відповідальність усіх цифрових учасників ЄЦР.

2. Підтримка солідарності та інклюзивності. Другий напрям визначає, що технології мають об'єднувати, а не роз'єднувати суспільство, і що кожен повинен мати доступ до Інтернету, цифрових навичок, цифрових державних послуг і справедливих умов праці у цифровому середовищі.

3. Гарантування свободи вибору в онлайн-просторі. Основна сутність третього напрямку полягає у тому, що люди повинні користуватися безпечним онлайн-середовищем, бути захищеними від незаконного та шкідливого контенту та мати можливість застосовувати нові технології, що розвиваються, наприклад такі як штучний інтелект.

4. Сприяння активній участі в цифровому публічному просторі. У рамках четвертого напрямку визначено, що громадяни повинні мати можливість брати активну участь у демократичному процесі на всіх рівнях і контролювати використання своїх персональних даних.

5. Посилення безпеки, захисту та розширення можливостей громадян (особливо молоді). П'ятий напрям визначає, що цифрове середовище має бути безпечним для усіх вікових категорій, надаючи їм необхідні цифрові навички та інструменти для свого захисту.

6. Стимулювання сталого розвитку цифрового майбутнього. Шостий напрям визначає те, що користувачі цифрових технологій повинні підтримувати сталість і екосистему впливу своїх пристроїв на навколишнє середовище та енергоспоживання.

Таким чином, на основі цих напрямів має ґрунтуватися побудова Цифрового десятиліття ЄС. Відповідно до положень Декларації, національні уряди країн-членів ЄС зобов'язані законодавчо впроваджувати ці норми, що передбачає гармонізацію регуляторних актів, адаптацію механізмів державної політики до європейських стандартів та інтеграцію цифрових прав у національні стратегії цифрового розвитку.

Також, одним із важливих додатків Звіту 2024 року Траєкторії Цифрового десятиліття є «Короткі звіти 27 держав-членів ЄС» [1], в яких аналізується рівень їхнього прогресу у сфері цифровізації. Для детальнішого

аналізу дослідження європейських практик нами було обрано Данію, Естонію та Польщу здійснено смарт-аналіз коротких звітів цих країн про стан цифрового розвитку за 2024 рік.

Данія є одним із провідних лідерів у сфері цифрового розвитку, перевершуючи середні показники у ЄС за більшістю критеріїв у межах цілей Цифрового десятиліття. Країна має стовідсоткове покриття 5G-мережами своєї території, та на 97,2% забезпечує доступ населення до високошвидкісного Інтернету, що робить її одним із лідерів у розбудові цифрової інфраструктури. На 84,2% забезпечено надання цифрових послуг для громадян, та на 88,7% для бізнесу.

Високим є рівень володіння населення базовими цифровими навичками, який у 2024 році складає 69,6%, в той час коли середній показник серед країн ЄС – 55,6%. Також, Данія активно впроваджує штучний інтелект та хмарні технології у бізнес сферу, а 75,3% малих та середніх підприємств володіють принаймні базовим рівнем цифрової інтенсивності. Країна оснащена потужною цифровою інфраструктурою та передовими науково-дослідними центрами, зокрема у сфері робототехніки, нанотехнологій, квантових технологій, сенсорних систем та виробництва чіпів. Окрему увагу у Данії приділено використанню цифрової трансформації для розумної екологізації. Країна активно розвиває стандартизацію, цифровізацію та автоматизацію даних, спрямованих на підтримку бізнесу, державних установ і громадян для ефективного управління ресурсами та зменшення негативного впливу на довкілля.

У 2023 році Естонія досягла помітного прогресу у сфері цифровізації, що підтверджується високими показниками у різних напрямках, зокрема, цифровізації державних послуг (95,8% цифрових послуг для громадян та 98,8% для бізнесу), цифрових навичках – 62,6%, тоді як середній рівень серед країн ЄС – 55,6%, а також ініціативах у сфері кібербезпеки. У країні високий рівень доступу до e-Health записів – 97,5% громадян мають доступ до

цифрових медичних записів, що є найвищим показником у ЄС. Також, у Естонії 52,6% підприємств використовують хмарні технології.

За даними Спеціального дослідження Євробарометра «Цифрове десятиліття 2024» (Digital Decade Eurobarometer), 81% естонців вважають, що цифровізація популярних державних і приватних послуг полегшує їм життя, що значно перевищує середній показник серед країн ЄС (73%), що свідчить про високу довіру населення до цифрових сервісів та максимальний рівень ефективності їх впровадження.

Разом з тим, Естонія сприяє розширенню цифрової інфраструктури, у 2024 році загальне покриття мережею 5G складає 87,5%, у порівнянні з 2023 роком – 43,3% (річний прогрес у цій сфері дорівнює 102%). Проте зазначений показник дещо нижчий за середній рівень серед країн ЄС – 89,3%.

Польща продовжує впевнено рухатися шляхом цифрової трансформації, демонструючи значний прогрес у сфері гігабітного підключення, цифровізації малих та середніх підприємств, а також розвитку цифровізації державних послуг. У 2024 році показник стаціонарної мережі високої пропускної здатності (VHCN) склав 81,1% (середній рівень серед країн ЄС – 78,8%), покриття оптоволоконним зв'язком до приміщення (FTTP) – 75,4% (середній рівень серед країн ЄС – 64%), покриття мережею 5G – 71,9%, що є нижчим ніж середній рівень серед країн ЄС – 89,3%, однак демонструє позитивну динаміку.

Країна досягла успіхів у своїй схемі цифрової ідентифікації (36,5% населення використовували e-ID для доступу до державних послуг, що є вищим за середній показник ЄС – 36,1%). Водночас цифровізація державних послуг потребує подальшого вдосконалення, адже наразі лише 63,7% державних сервісів доступні онлайн для громадян (проти 79,4% у середньому в ЄС), а для бізнесу цей показник становить 72,9%, що також нижче середнього європейського рівня (85,4%). Однак, за показником доступу до e-Health записів, який склав 90%, Польща випереджає середній європейський рівень (79,1%).

Окрім цифровізації державних сервісів, польський уряд та приватні підприємства активно впроваджують енерго- та ресурсоефективні цифрові рішення у своїй діяльності, спрямовуючи інвестиції на розвиток сталої цифрової інфраструктури та технологій. Попри значний прогрес, країні варто зосередитися на подальшому розширенні 5G-покриття, покращенні якості цифрових державних послуг та підвищенні рівня цифрових навичок населення.

На основі аналізу можна зазначити, що Данія продукує досягнення цілей ЄС у рамках Цифрового десятиліття з огляду на її успішну цифровізацію, за рахунок прогресу в цифровізації державних послуг для бізнесу та збільшення кількості спеціалістів цифрової індустрії. Проте, є проблеми з цифровізацією малих та середніх підприємств, зокрема через низький рівень впровадження передових технологій, наприклад таких як штучний інтелект. У своїй національній дорожній карті цифрового розвитку Данія запланувала заходи з посилення конкурентоспроможності підприємств, покращення державних послуг і просування «зеленої» сфери.

У 2023 році ухвалена оновлена Стратегія цифровізації на 2024-2027 роки, у рамках якої передбачено виділити 100 млн. євро на ініціативи, що спрямовані на надання технологічних знань учням початкових шкіл, на збільшення використання цифрових технологій, таких як штучний інтелект, робототехніка, а також для екологічних трансформацій. Також, у Данії є ряд інших стратегій, які формують цілі щодо розвитку цифрового середовища. Пріоритетом цифрового розвитку надалі стане розширення покриття високошвидкісного широкосмугового зв'язку сільських територій; підвищення рівня готовності у сфері кібербезпеки; використання штучного інтелекту; подальша цифровізація малих і середніх підприємств та сфери державного управління.

Особливу увагу буде приділено розробці цифрових рішень для сектору охорони здоров'я та активізації науково-дослідних робіт; посилення цифрового залучення та збільшення спеціалістів у IT-сфері [118].

Щодо Естонії, то цифровізація є одним з основних пріоритетів країни, про що свідчить національний Цифровий порядок денний на 2030 рік, ухвалений у 2021 році. Зазначена, цифрова стратегія зосереджується на трьох сферах: цифровий стан, кібербезпека та розвиток цифрової інфраструктури. Державна політика цифрового розвитку в Естонії реалізується тут комплексно, однак наразі відсутні окремі стратегії, які стосуються розвитку напівпровідникової промисловості, нано- та квантових технологій. Також, в країні існують проблеми у сфері покриття гігабітним Інтернетом та цифровізації малих і середніх підприємств, оскільки лише 55,9 % з них мають базовий рівень цифрової інтенсивності, що є значно нижчим за європейські показники (90%) [132].

Щодо внеску країни у реалізацію Цифрового десятиліття ЄС, то відповідно до представленої Національної дорожньої карти, амбіції Естонії залишаються відносно стриманими. Документ передбачає обмежені зусилля для досягнення цифрових цілей ЄС, що стало підставою для надання низки рекомендацій. Уряд Естонії має у своїй Національній дорожній карті встановити цілі і заходи щодо ключових показників ефективності Цифрового десятиліття, визначити джерела та обсяг фінансування заходів, та провести консультації із зацікавленими сторонами щодо розробки дорожньої карти.

Окрім загальних рекомендацій щодо вдосконалення цифрової політики, короткий звіт Естонії окреслює низку конкретних заходів. Так, у сфері цифрової інфраструктури країні рекомендовано продовжити розширення мереж 5G, VHCN та FTTP. У сфері кібербезпеки необхідно активніше впроваджувати 5G Cybersecurity Toolbox, що забезпечить стабільність і безпеку цифрових комунікацій. Також, Естонії варто розробити національну стратегію для розвитку напівпровідникової галузі та квантових обчислень, а також сприяти цифровізації МСП з особливим акцентом на аналітику даних та штучний інтелект.

Проаналізувавши досвід Польщі, який представлено в Короткому звіті країни про цифровий стан за 2024 рік, можна зазначити, що країна має значний

потенціал для покращення ефективності щодо сприяння досягненню цілей та завдань Цифрового десятиліття ЄС. Уряд країни спрямовує значні фінансові ресурси на покращення зв'язку, використання цифрових технологій МСП та розвитку цифрових державних послуг для підвищення конкурентоспроможності польської економіки. Польща планує інвестувати у розвиток виробництва напівпровідників та братиме участь у проєктах зі створення квантових комп'ютерів. Відповідно до Плану відновлення та стійкості Польщі, країна виділяє на реалізацію політики цифрового розвитку 7,4 млрд. євро. Основну частину інвестицій буде спрямовано на розгортання широкосмугового зв'язку, покращення цифрових навичок населення, цифровізації державних послуг, а також на сферу електронної охорони здоров'я та кібербезпеку країни. Також, у рамках програми політики згуртованості буде виділено додатково ще 5,7 млрд. євро на цифрову трансформацію країни [162].

Польща демонструє амбітні плани, та має намір докласти значних зусиль для досягнення цілей Цифрового десятиліття, через подолання недоліків щодо реалізації цифрових компетенцій та здійсненні цифровізації підприємств. Уряду Польщі було надано ряд рекомендацій стосовно розвитку цифрової інфраструктури та підключення.

Окрім цього, Польщі слід адаптувати національне законодавство до Європейського кодексу електронних комунікацій, посилити заходи щодо розгортання мережі 5G (особливо вздовж основних транспортних коридорів), забезпечити доступ нових учасників до частотного спектра для розвитку інноваційних B2B- та B2C-рішень, та заохочувати операторів прискорити розгортання автономних опорних мереж 5G. У сфері кібербезпеки Польща має продовжити впровадження 5G Cybersecurity Toolbox, що забезпечить захист та стійкість 5G-інфраструктури. Необхідно, забезпечити активне впровадження хмарних технологій нового покоління, які розробляються в межах IPCEI-CIS (Important Projects of Common European Interest in Cloud Infrastructure and Services). Для підвищення рівня цифрових компетенцій населення необхідно

запланувати заходи щодо покращення базових навичок серед молоді шляхом модернізації цифрового обладнання у школах, підвищення кваліфікації викладачів ІКТ та внесення змін в навчальні програми для підвищення привабливості STEM-дисциплін. Для вирішення проблеми дефіциту ІКТ-фахівців необхідно зробити програми цифрової освіти більш доступними, а також активно залучати жінок до технологічної сфери шляхом популяризації цифрових професій [162].

Проаналізувавши, досвід Данії, Естонії, та Польщі можна зробити висновок, що ці країни мають різний рівень цифрового розвитку, проте усі вони прямують до єдиних стандартів у рамках цілей Цифрового десятиліття ЄС. Дане дослідження дозволяє визначити кращі європейські практики та ключові виклики, з якими стикаються уряди цих країн в процесі реалізації цифрової політики ЄС. Зокрема, Естонія та Данія демонструють високі результати у порівнянні з середнім рівнем в ЄС, що свідчить про результативну реалізацію державної політики цифрового розвитку. Ці країни розвивають цифрову інфраструктуру, реалізують заходи щодо підвищення рівня цифрових компетенцій населення та збільшення кількості фахівців ІТ-сектору, а також створюють умови щодо безпечного користування цифровим середовищем відповідно до Європейської декларації про цифрові права та принципи. Досвід Польщі демонструє, що незважаючи на нижчі показники цифровізації, країна активно впроваджує реформи з метою досягнення стратегічних цілей ЄС у цифровій сфері. Завдяки реалізації комплексних заходів Польща прагне зміцнити конкурентоспроможність своєї економіки та прискорити цифрову трансформацію країни.

Саме тому, такий досвід є корисним, адже допоможе визначити оптимальні напрями державної політики, адаптувати найкращі практики та прискорити процес інтеграції України до єдиного цифрового ринку ЄС. Особливу увагу профільним органам публічної влади України варто зосередити на цілях та ключових показниках ефективності Цифрового десятиліття, рекомендаціях, наданих країнам-членам ЄС, та положеннях

Європейської декларації про цифрові права та принципи. Адже вчасне, урахування цих аспектів сприятиме формуванню сучасного бачення цифрової трансформації та допоможе визначити оптимальні заходи для гармонізації цифрового середовища України до європейських стандартів.

Як вже було зазначено, Україна наразі динамічно розвивається в цифровому секторі, та спрямовує значні зусилля на шляху до Євроінтеграції. Зокрема, в кінці лютого 2025 року відбулось засідання представників Кабінету Міністрів України та Європейської комісії, під час якого було обговорено поточний стан євроінтеграційних проєктів.

Загалом, Європейська комісія позитивно оцінює успіхи України у сфері цифровізації, проте у Звіті щодо прогресу України в межах Пакету розширення 2024 було наголошено на проблемах та визначено ключові напрями розвитку цієї сфери на 2025 рік. Також, на цій зустрічі було досягнуто домовленості щодо співпраці у наступних напрямках, а саме: інтеграція України до індексу DESI; забезпечення доступу України до кіберрезерву ЄС у межах програми «Цифрова Європа»; удосконалення українського законодавства у сфері надання цифрових послуг на основі Digital Services Act та Digital Markets Act; співпраця з ЄС у сфері штучного інтелекту та імплементація EU AI Act [86].

Серед проблемних аспектів, які були визначені у Звіті можна зазначити наступні [194]:

По-перше, це наявність регуляторних та правових бар'єрів, які суттєво ускладнюють співпрацю українських та європейських компанії щодо надання цифрових послуг. Загалом, Україна розпочала процес узгодження національного законодавства з нормами ЄС у сфері надання цифрових послуг для гармонізації з Актом про цифрові послуги (DSA), але все ще не має чіткої дорожньої карти, яка визначатиме подальші кроки та заходи з нарощування спроможності для відповідності DSA.

Окрім того, існує потреба щодо гармонізації законодавства відповідно до оновленого Регламенту про європейську цифрову ідентичність, а також має бути уточнено правила в окремих сферах (наприклад, відповідність GDPR або

еквівалентному рівню захисту персональних даних, а також деяким положенням Директиви ЄС щодо безпеки мережевих та інформаційних систем (NIS2) для забезпечення взаємного визнання схем електронної ідентифікації держав-членів ЄС та України.

По-друге, відсталість цифрової інфраструктури у порівнянні з країнами ЄС, наприклад частка домогосподарств з доступом до інтернету в Україні складає – 79%, тоді коли середній рівень в ЄС – 92%. До того ж, суттєвим негативним чинником, який впливає на поглиблення проблеми руйнування цифрової інфраструктури у зв'язку із військовою агресією проти України, що зумовлює необхідність її відновлення та підвищення стійкості мереж. Щодо питань у сфері телекомунікаційної інфраструктури, з огляду на діючі безпекові обмеження, Україна розпочала підготовку щодо реалізації заходів щодо регулювання політики радіочастотного спектра, зокрема звільнення діапазону 700 МГц від телевізійного мовлення для мобільного зв'язку. Окрім того, пріоритетним напрямом на 2025 рік має стати виконання умов ЄС щодо роумінгу, що дозволить Україні приєднатися до зони "роумінг як вдома" (Roam like at home).

По-третє, існує необхідність посилення заходів у сфері кібербезпеки, Україна повинна продовжувати імплементацію заходів 5G Cybersecurity Toolbox, зокрема щодо оцінки ризиків постачальників та запровадження відповідних обмежень і/або виключень для постачальників із високим рівнем ризику. Команда реагування на комп'ютерні надзвичайні події CERT-UA вживає заходів у рамках загальної структури кібердіалогу Україна-ЄС для поглиблення інституційної співпраці з європейськими партнерами, зокрема з Агентством ЄС з кібербезпеки (далі – ENISA).

У результаті 9 листопада 2023 року був підписаний робочий договір між ENISA, Національним координаційним центром кібербезпеки (далі – НКЦК) та Державною службою спеціального зв'язку та захисту інформації (далі – ДССЗІ), і наразі триває його реалізація. Окрім того, є потреба у розширенні заходів щодо захисту критичної цифрової інфраструктури.

Отже, окреслені вище проблемні аспекти потребують нагальної уваги з боку профільних органів публічної влади для визначення курсу дій щодо їх подолання. Загалом, вирішення цих проблем допоможе прискорити інтеграцію України до єдиного цифрового ринку ЄС, що є стратегічним завданням для нашої країни. Державна політика у цій сфері вимагає комплексного підходу та адаптації європейських стандартів до національного цифрового середовища. Саме тому, пропонуємо наступні напрями удосконалення механізмів вироблення державної політики у сфері інтеграції України до ЄЦР:

– потрібно удосконалювати нормативно-правову базу для усунення регуляторних та правових бар'єрів з нормами ЄС. Доцільним у цьому напрямі буде розроблення подальшої Стратегії інтеграції України до ЄЦР, яка включатиме імплементацію регуляторних актів ЄС, зокрема Акту про цифрові послуги (DSA) [165], Директиви ЄС щодо безпеки мережевих та інформаційних систем (NIS2) [124], Регламенту про європейську цифрову ідентичність [168], Акту про цифрові ринки (DMA) [84], врегулювання питання транскордонної мобільності послуг онлайн-контенту відповідно до Регламенту (ЄС) 2017/1128 [82], положення Регламенту (ЄС) 2018/302 щодо сфери усунення невиправданого гео-блокування та інших форм дискримінації [83], та Європейської декларації про цифрові права та принципи [14]. Це дозволить усунути правові відмінності українського правового поля від норм ЄС, та пришвидшить процес приєднання нашої країни до європейського цифрового середовища;

– необхідно спрямовувати зусилля щодо покращення цифрової інфраструктури, що зменшить відсталість нашої країни у порівнянні з ЄС. В рамках цього доцільно запроваджувати заходи щодо розширення доступу до високошвидкісного Інтернету (особливо у сільській місцевості), впровадження 5G-мереж, а також залучення інвестицій у сферу цифрових сервісів, що сприятиме підвищенню конкурентоспроможності України. У сфері телекомунікаційної інфраструктури потрібно реалізувати заходи щодо

регулювання політики радіочастотного спектра, та забезпечити повне впровадження норм ЄС щодо роумінгу;

– здійснювати заходи щодо підтримки цифровізації бізнесу в Україні, зокрема, стимулювати та надавати консультаційну підтримку, врахувати позиції бізнес-спільноти під час розробки законодавчих змін, а також впроваджувати безкоштовні навчальні програми, які допоможуть підприємцям швидше освоювати передові цифрові технології, такі як великі дані, штучний інтелект, хмарні сервіси, тощо;

– удосконалити сферу кібербезпеки шляхом подальшої імплементації заходів 5G Cybersecurity Toolbox, забезпечення відповідності європейським стандартам інформаційної безпеки, адаптації кращих європейських практик, проведення інформаційних кампаній з населенням щодо обізнаності у сфері кібербезпеки та цифрової гігієни, співпраці в цій сфері з європейськими інституціями та країнами-членами ЄС з метою посилення цифрової захищеності України;

– сприяти покращенню рівня цифрових компетенцій населення, зокрема у цьому напрямку необхідно виконувати рекомендації надані Європейською комісією країнам-членам ЄС у рамках Звіту Про стан Цифрового десятиліття, а саме: здійснювати заходи щодо покращення цифрового обладнання в школах та вищих навчальних закладах, запровадити внесення змін в навчальні програми (розроблення дисциплін щодо основ цифрової грамотності), удосконалювати наявні навчальні платформи та розширювати доступ населення до безкоштовних онлайн-курсів, створювати стимули для навчання та перекваліфікації фахівців ІТ-сектору, усі ці заходи позитивно впливатимуть на зростання цифрових компетентностей населення, підвищення економічної активності та розширення можливостей для працевлаштування в сфері ІТ.

2.2 Штучний інтелект як інструмент цифрового розвитку публічного управління

У XXI столітті стрімкий розвиток цифрових технологій докорінно трансформував механізми прийняття управлінських рішень, розширивши коло суб'єктів вироблення державної політики цифрового розвитку. Особливої уваги заслуговує феномен впровадження технологій штучного інтелекту (ШІ), який із допоміжного інструменту аналітика перетворюється на активного учасника управлінського процесу. Застосування алгоритмів ШІ у таких сферах як обробка масивів даних (Big Data), прогнозування поведінки громадян, таргетована політична реклама, автоматизоване управління державними сервісами – формує нову реальність. Алгоритми здійснюють як опосередкований, так і системний вплив на процеси публічного управління. Зростає роль приватних корпорацій, які володіють технологіями ШІ, у формуванні державної політики. Саме на цьому перетині – між державою, приватним сектором і цифровими алгоритмами – виникає явище алгоритмічного лобіювання. Йдеться про вплив на публічне управління через дані, рекомендації, цифрові платформи та аналітичні інструменти, що не завжди є прозорими або підконтрольними демократичним інститутам. Таким чином, аналіз ШІ не тільки як технології, а й як потенційного суб'єкта управління, є надзвичайно актуальним у контексті трансформацій сучасної держави, цифрового суверенітету та збереження демократичних процедур.

Умови та особливості лобіювання у публічному управлінні відображено у працях українських та зарубіжних науковців. Зокрема, у класичному розумінні, лобіювання – це діяльність, спрямована впливати на процеси прийняття рішень у публічному секторі з боку недержавних акторів (бізнесу, громадських організацій, асоціацій тощо) задля реалізації певних інтересів [38]. У західній політичній теорії лобіювання є легітимною формою участі в політичному процесі. Українські дослідники акцентують на потребі врегулювання лобістської діяльності в контексті транспарентності та

добročесності публічного управління. Серед іноземних авторів, які розглядали лобізм у системі управління, варто згадати Д. Трумена [192], який підкреслював роль груп інтересів у демократичному процесі, Р. Даля [114], який розглядав лобіювання як частину плюралістичної демократії, К. Молоні [154], який звертає увагу на зміну форм лобіювання в епоху цифрових комунікацій. В українському контексті важливий внесок зробили Ю. Коваленко який досліджує алгоритмічні системи та їх вплив на соціальні процеси, моделюванням поведінки в контексті штучного інтелекту [30], О. Карпенко – визначає особливості правових засад застосування цивілізованого лобізму у публічному управлінні [19], а В. Гончаренко – аналізує правові аспекти цифровізації публічного управління, вплив алгоритмічних систем на правові та політичні процеси, правову регуляцію цифрових лобістських практик [6].

З урахуванням важливих змін в законодавстві України особливої актуальності набуває дослідження алгоритмічного лобіювання як інструменту впливу у сфері публічного управління.

З розвитком цифрових технологій традиційні підходи до лобіювання зазнають трансформації – цифрові платформи та алгоритмічні системи дедалі частіше виступають не лише як канали комунікації, а як самостійні механізми впливу на формування та реалізацію державної політики.

Традиційна модель суспільно-владних відносин складається з трьох груп учасників: органи публічного управління; приватний сектор (бізнес, фінансові групи); громадянське суспільство (ГО, профспілки, активісти).

Класична політична теорія розглядає політичних акторів як учасників процесу розподілу влади та ресурсів. У цифрову добу це уявлення розширюється. За даними досліджень Ш. Зубофф [199], цифрові корпорації отримують владу не лише економічну, але й політичну – через контроль над даними і поведінковим прогнозуванням.

Б. Шнайер у своїй праці «Data and Goliath» (2015) [174] аналізує феномен алгоритмічного посередництва, яке трансформує традиційні форми

суспільного впливу, формуючи нову реальність, у якій алгоритмічне управління має більшу значущість, ніж вплив демократичних інституцій.

Ці процеси породжують феномен «алгоритмічного суверенітету» [171], коли суб'єкти державної політики втрачають здатність автономно формувати її порядок денний без участі цифрових платформ. Поняття «алгоритмічне управління» (algorithmic governance) поступово входить у дискурс вироблення державної політики цифрового розвитку. У дослідженнях М. Хілдебранд [136] обґрунтовується, що алгоритми, які приймають або рекомендують рішення на основі обробки великих даних, формують нову архітектуру управління – «by design», тобто заздалегідь запрограмовану. Інші автори, зокрема Ф. Поскуаль [161], наголошують на непрозорості алгоритмів, які використовуються у сфері безпеки, медицини, фінансів і все частіше – у публічному секторі.

В ЄС вже кілька років тривають дебати навколо «AI Act» (Закону про штучний інтелект) [169], запропонованого Європейською комісією у 2021 році. Документ передбачає рівні ризику використання ШІ, зокрема – в публічному управлінні, правосудді та правопорядку. Саме на рівні ЄС алгоритми розглядаються як структурні фактори впливу на державу.

В Україні поки що бракує науково-обґрунтованих рішень щодо використання ШІ як суб'єкту управління, однак вже є перші спроби практичної реалізації стосовно його залучення. У проектах «Дія», «єМалятко», «єЗвернення» можна побачити елементи автоматизованого прийняття рішень, хоча публічний дискурс поки зосереджений більше на зручності, ніж на політичних наслідках.

На нашу думку, алгоритмічне лобіювання – це цифрова форма політичного впливу на публічне управління, яка реалізується за допомогою технологій штучного інтелекту, аналітики великих даних та алгоритмів, здатних модифікувати інформаційні потоки, формувати суспільну думку і впливати на прийняття рішень у сфері публічного управління. На відміну від класичних форм лобізму, що передбачають безпосередню взаємодію

зацікавлених груп з представниками влади (зустрічі, подання пропозицій, неформальні комунікації), алгоритмічне лобіювання здійснюється опосередковано – через цифрову архітектуру впливу: пріоритетні системи, маніпуляцію даними, персоналізовану інформацію та соціальні медіа.

На думку К. Янг [198], алгоритми відіграють дедалі важливішу роль у «софт-управлінні» поведінкою, де управління не ґрунтується на примусі, а здійснюється шляхом технологічного спрямування впливу на суспільство через цифрове середовище. До основних механізмів алгоритмічного впливу на суспільство відносять:

1. Алгоритмічну селекцію інформації. Платформи, що використовують ІІІ (Meta, Google, X/Twitter, TikTok), визначають контент користувачів. Це створює «фільтрувальні бульбашки» (filter bubbles) та ефект резонансу, які можуть бути використані для політичної мобілізації або маніпуляції. Наприклад алгоритмічне просування політичного контенту у мережі «Facebook» під час виборів у США 2016 року призвело до змін електоральних настроїв [193].

2. Мікротаргетинг на основі даних. Компанії можуть здійснювати індивідуальне таргетування громадян, використовуючи їхню онлайн-поведінку, для впливу на уподобання, переваги, громадську думку. Відомий приклад – скандал пов'язаний «Cambridge Analytica», коли дані понад 87 мільйонів користувачів «Facebook» було використано для створення психологічних цільових аудиторій та профілів виборців [144].

3. Автоматизовані алгоритмічні рекомендації органам публічної влади. Системи штучного інтелекту використовуються органам публічної влади як “нейтральні аналітики”, які здатні ефективно обробляти дані для прийняття рішень – у сфері безпеки, охорони здоров'я, урбаністики, соціальної політики тощо. Проте такі системи часто створюються приватними корпораціями, які переслідують власні інтереси. Як приклад у 2021 році нідерландський уряд був змушений відмовитись від автоматизованої системи боротьби з шахрайством «SyRI» після того, як суд визнав її непрозорою та дискримінаційною [187].

4. Стандартизація оптимального управління. Приватні компанії, які володіють інструментами ШІ, одночасно формують технічні стандарти для оцінювання ефективності управлінських рішень. Це дозволяє бізнесу хоч і опосередковано, але впливати на процеси нормотворчості органів законодавчої влади, визначаючи рамки “оптимального” управління. Так, Google у співпраці з Єврокомісією фінансувала дослідження у сфері ШІ для державних послуг, результати яких згодом було включено в експертні звіти щодо регулювання ШІ.

Алгоритмічне лобіювання здійснюється не лише технологічними компаніями, але й через корпоративні мережі впливу (наприклад, «Accenture», «Palantir», «McKinsey»), індустріальні об'єднання (зокрема, «DigitalEurope», що активно впливає на політику ЄС щодо ШІ), незалежні дослідницькі центри, які фінансуються гігантами ІТ-індустрії (наприклад, «Center for Humane Technology»). У дослідженні «Corporate Europe Observatory» [181] зазначається, що у 2021 році технологічні компанії витратили понад 97 мільйонів євро на лобіювання в ЄС, здебільшого у сфері цифрового регулювання.

Феномен алгоритмічного лобіювання становить певну загрозу для прозорості, підзвітності та інклюзивності публічного управління. Основна небезпека полягає у прихованому впливі на процеси ухвалення державно-управлінських рішень, що відбувається поза межами традиційного політичного поля та класичних механізмів демократичного контролю.

По-перше, алгоритмічний вплив є переважно прихованими для більшості громадян, оскільки здійснюється через інфраструктури цифрових платформ, які не мають чіткого політичного позиціонування та сприймаються як технічні чи комерційні інструменти. Таким чином, «алгоритмічні рекомендації» набувають статусу де-факто стосовно рішень суб'єктів вироблення державної політики, залишаючись водночас поза межами суспільної уваги.

По-друге, алгоритмічне лобіювання виходить за межі існуючих рамок

антикорупційного та лобістського законодавства, оскільки не є прямим втручанням у політичний процес через фізичних агентів або політичних посередників. Замість цього вплив здійснюється за допомогою великих масивів даних, персоналізованих таргетингових компаній і автоматизованих управлінських рішень.

По-третє, така форма впливу викривлює політичну конкуренцію, надаючи перевагу акторам, які мають доступ до значних обсягів поведінкових даних та високорозвинених алгоритмічних інструментів ШІ. Це сприятиме виникненню нової форми інформаційної асиметрії, де політичні ресурси концентруються не у державних інституціях чи громадянському суспільстві, а у приватних цифрових платформах і транснаціональних технологічних корпораціях.

По-четверте, наявність таких процесів створює передумови для «цифрового неокolonіалізму», в межах якого країни, особливо з обмеженим технічним потенціалом, стають залежними від рішень, запропонованих або імплементованих комерційними алгоритмічними системами, розробленими за межами їх юрисдикції.

Впровадження непрозорих алгоритмічних систем без відповідного регуляторного супроводу загрожує посиленню цифрової нерівності, спотворенню політичної конкуренції та підризу фундаментальних громадянських прав. Алгоритми можуть не лише репрезентувати політичні упередження, а й створювати нові форми виключення та маніпуляції [158].

Тому, особливої уваги потребує питання забезпечення прозорості алгоритмів. Однією з визначальних характеристик сучасних моделей штучного інтелекту є феномен так званої «чорної скриньки» (black box) – коли логіка прийняття рішень є складною для інтерпретації не лише для зовнішніх спостерігачів, а й для самих розробників. Це суттєво ускладнює процес встановлення відповідальності за помилки, упередженості або маніпуляцій в алгоритмічних системах, що мають вплив на суб'єктів вироблення державної політики та суспільні процеси. У випадку системи «COMPAS», яка

використовувалась у США для прогнозування рівня рецидивізму злочинців, алгоритм виявився упередженим до афроамериканців, однак власники алгоритмів не змогли однозначно пояснити, яким чином вони функціонують [106].

Одним з негативних аспектів застосування алгоритмічного лобіювання є цілеспрямований вплив на суспільні настрої через соціальні мережі, що здійснюється шляхом:

1. Формування емоційних наративів: формування контенту, який викликає сильні емоції, спрямованого на посилення маніпуляції масовою свідомістю.
2. Створення ілюзії підтримки певних ідей: використання бот-мереж та астротурфінгу для штучної імітації масової підтримки супротиву до певних суспільних ініціатив та політичних позицій.
3. Психографічний мікротаргетинг: застосування аналізу особистісних характеристик користувачів для персоналізованого впливу на їхні політичні уподобання.

Згідно з дослідженням «Oxford Internet Institute» [143], організовані комунікативні кампанії цифрової дезінформації з політичною метою були зафіксовані у 81 країні. Ці кампанії часто здійснювалися як державними структурами, так і приватними фірмами, що спеціалізуються на маніпуляції громадською думкою через соціальні медіа. Разом з цим, особливої актуальності набуває використання можливостей ШІ у галузі публічного управління та адміністрування. Дослідженням проблематики впровадження штучного інтелекту у діяльність органів публічної влади займалися чимало зарубіжних науковців, особливо слід відзначити праці А. Агравала [100], Й. Баха [107], П. Догерті [163], С. Дж. Рассела [173], К. Шваба [176].

Комплексне застосування інструментів Інтернету речей (далі – IoT) та алгоритмів ШІ поступово набуває подальшого розвитку у дослідженнях сфери сучасних цифрових технологій. Такий підхід сприяє революціонізації ефективності, результативності, комфорту та зручності багатьох сфер

людської життєдіяльності, включаючи промисловість, медицину, транспорт, енергетику, освіту та багато інших.

За оцінками зарубіжних дослідників до централізованих хмарних додатків до 2025 року було підключено понад 150 мільярдів пристроїв, зокрема планшетів та смартфонів [103].

IoT як система з'єднаних віртуальною мережею фізичних пристроїв здатна обмінюватись даними без втручання людини. Застосування алгоритмів ШІ в такому контексті полягає у здійсненні аналізу великих даних (Big Data), які отримуються з цих пристроїв для виявлення шаблонів та взаємозалежностей з метою прийняття результативних управлінських рішень на основі цих даних. Одним із перспективних напрямів цифрового розвитку є створення більш ефективних та високоінтелектуальних систем взаємодії ШІ та IoT. Впровадження алгоритмів ШІ в IoT-пристрої дозволить останнім не лише збирати дані, але й аналізувати їх у режимі реального часу, що у свою чергу оптимізуватиме процеси управління, прогнозування подій та реагування на них. Наприклад у сфері містобудування, мережа IoT-сенсорів може збирати дані про трафік та забруднення повітря, а завдяки алгоритмам AI можна буде аналізувати дані для оптимізації систем функціонування громадського транспорту та керування екологічними заходами.

Однак разом із перевагами є й певні ризики та виклики. Одним з них є забезпечення конфіденційності даних та їх безпека. Із збільшенням кількості підключених пристроїв до IoT-мережі зростає також й кількість кібератак та порушень приватності, що в свою чергу вимагає розробки та впровадження надійних систем цифрового захисту.

Науковці Р. Булак та М. Огієла запропонували алгоритм ШІ, який використовуватиме особисті характеристики користувача та контекстні особливості їх автентифікації. Цей алгоритм кодує всі отримані дані в один інформаційний модуль, який згодом використовуватиметься для встановлення особи користувача. Вчені вважають, що використання такого персоналізованого контекстно-залежного протоколу може підвищити

надійність автентифікації користувача, особливо на пристроях з обмеженими обчислювальними потужностями [111].

Взаємодія між ШІ та IoT відкриває нові потужні перспективи для розвитку сучасного цифрового суспільства. Проте щоб максимально використати потенціал цієї взаємодії необхідно усвідомлювати існуючі загрози та враховувати нові виклики, які виникають перед людством зокрема у сфері безпеки даних з метою забезпечення стійкого та сталого розвитку цих цифрових технологій для покращення якості життя людства. Ще одним важливим аспектом реалізації державної політики цифрового розвитку стала трансформація системи публічних закупівель в Україні.

З початку військових дій на території України функціонування цифрової системи публічних закупівель «ProZorro» було призупинено через «чутливість» інформації, яку вона вміщувала, зокрема адреси замовників, підрядників, деякі інші персональні дані, що могли бути використані окупантами для розшуку їх власників. Згодом, після ухвалення Постанови Кабінету Міністрів України «Про затвердження особливостей здійснення публічних закупівель товарів, робіт і послуг для замовників, передбачених Законом «Про публічні закупівлі», на період дії правового режиму воєнного стану в Україні та протягом 90 днів з дня його припинення або скасування» № 157 від 17 лютого 2023 року [59] розпочалося відновлення обов'язкового використання процедур електронних закупівель, а саме:

- змінено вимоги до публікації замовниками звіту про виконання договору про закупівлю;
- скорочено кількість підстав для здійснення закупівель без використання системи «ProZorro»;
- уточнено інформацію, яку замовник може не публікувати в річних планах закупівель та оголошеннях про торги, якщо її оприлюднення загрожує безпеці;
- дозволено публікувати тексти договорів та всі додатки до них, у разі проведення закупівель без використання електронної системи (з можливістю

приховання «чутливої» інформації про постачальника, адресу доставки, у разі якщо така інформація може загрожувати безпеці);

– уточнено випадки та підстави відхилення пропозицій постачальників товарів російського та білоруського походження (зокрема тих компаній, які належать громадянам цих країн).

Процес публічних закупівель органами державної влади розпочинається в останні місяці року, що передує року закупівель. Замовники можуть ознайомитися із обсягами виділених коштів на наступний бюджетний рік, одразу після затвердження бюджету. Перевагою такого планування є те, що закупівельну процедуру можна провести вже на початку року (зокрема це стосується продовження ліцензій на програмне забезпечення). У разі виявлення помилок в документації, або якщо торги з якихось причин не відбудуться, замовник матиме певний час для проведення процедури повторних торгів.

Для відповідальних осіб за проведення організацією публічних закупівель, які планують бюджет на наступний рік, було б корисно мати чітке уявлення про те, що саме їм потрібно буде закупити. Предметом закупівель можуть бути різні, роботи, товари та послуги, наприклад: ремонтні роботи, комунальні послуги, інтернет, програмне забезпечення, комп'ютерна техніка, ліцензії та інше, приблизну вартість та умови постачання/надання/виконання яких необхідно знати заздалегідь для планування та виконання бюджету. Такий підхід має декілька переваг. По-перше, він дає можливість заздалегідь підготуватися до процедури публічних закупівель з урахуванням можливості повторного проведення відкритих торгів. По-друге, це дозволяє чітко визначити граничний поріг обсягів закупівель у році планування. На практиці складно ідеально досягнути оптимального підходу. Зазвичай фінансове планування зводиться лише до того, що за основу використовується план минулого року, який корелюється відповідно до показників інфляції. Такий спосіб планування є недостатньо точним і не враховує всіх умов та потреб у змінах, які можуть виникнути упродовж наступного бюджетного року.

Поширеним плануванням обсягів публічних закупівель органами державної влади є застосування так званого принципу «top-down» («зверху вниз»), за якого загальний бюджет органу державної влади затверджується зверху без достатньої уваги до урахування реальних потреб. Це призводить до незбалансованого розподілу ресурсів та неефективного планування публічних закупівель. Тому, для покращення ефективності фінансового планування необхідно враховувати реальні потреби органу державної влади, залучати до формування бюджету високопосадовців та підпорядковані їм підрозділи, які фактично впливають на це, а також використовувати гнучкі та точні методи планування з метою забезпечення оптимального використання ресурсів та успішного виконання поставлених завдань у закупівельному процесі.

Ефективне фінансове планування є необхідною умовою для забезпечення безперервної та результативної роботи органів державної влади, бюджетування яких погоджується з профільними міністерствами або іншими центральними органами виконавчої влади. Наслідком цього є той факт, що передбачуваний обсяг бюджетного фінансування часто зменшується без урахування реальних потреб замовників, що створює проблеми недофінансування і безпосередньо впливає на якість планування та ефективність публічних закупівель. Одним з основних недоліків «top-down» підходу є те, що у затвердженому бюджеті відсутня деталізація щодо конкретних предметів закупівель, на які зменшуються витрати. Фінансування зменшується без урахування реальних потреб органів державної влади, що призводить до незбалансованого розподілу коштів і може перешкоджати забезпеченню необхідних ресурсів для їх ефективної роботи.

Такий підхід має й інші недоліки, зокрема, незважаючи на затверджений бюджет, його формування може обмежувати можливість оптимізації витрат та використання переваг повторного проведення відкритих торгів. Неналежне фінансове планування однозначно позначається на якості та швидкості виконання функцій держави та наданні населенню управлінських послуг. Замовникам складно визначити потреби, точно оцінити та сформулювати опис

предмета договору (контракту), який оптимально відповідатиме необхідним управлінським рішенням, а також умовам виконання державних контрактів. Нарешті, замовники стикаються з певними труднощами у передбаченні можливих та суттєвих змін, які можуть відбутися під час виконання умов договору на постачання робіт, товарів і послуг (наприклад, такі фактори як зміна ціни на сировину та поява на ринку інших технологій повинні бути враховані).

Закон України «Про публічні закупівлі» у редакції від 01 січня 2023 року [65] передбачає заходи для полегшення виконання цих завдань. Наприклад, за результатами торгів, перед ініціюванням процедури укладання контракту замовники можуть провести попередні ринкові консультації. Під час цих консультацій вони в змозі звернутися за порадою до незалежних експертів, або до інших учасників ринку та потенційних постачальників (підрядників). Замовники також можуть дозволити подавати тендерні пропозиції, включаючи, відповідно до основних положень технічного завдання, інший метод виконання договору (контракту), ніж той, що визначено. У деяких окремих випадках замовникам також дозволено використовувати переговорні процедури укладання контрактів. Ці рішення є корисними, однак базуються лише на інформації та пропозиціях, наданих невеликою кількістю суб'єктів: учасниками початкових ринкових консультацій та учасниками тендеру, які подають варіанти пропозицій або беруть участь у переговорах. Це потребує значних витрат часу та ресурсів.

В контексті вирішення зазначених проблем актуальними є можливості ІІІ у процесі підготовки та здійснення публічних закупівель органами державної влади. Здатність аналізувати великі обсяги (масиви) даних та прогнозувати майбутні тенденції за визначено обмежений період часу без необхідності залучення зовнішніх експертних організацій є потенційними перевагами використання ІІІ.

До початку збройної агресії проти України в онлайн-платформі «ProZorro», яка розпочала функціонувати з 2016 року [16] щодня

публікувалася інформація про проведення від 3000 до 5000 нових тендерів. Однією з основних цілей запровадження системи «ProZorro» стало усунення корупційного чинника у сфері публічних закупівель, які здійснювалися органами державної влади.

У 2018 році Державна аудиторська служба України розпочала виявляти підозрілі закупівлі у системі «ProZorro» шляхом запровадження алгоритму їх автоматичного оцінювання на відповідність 35 корупційним ризик-індикаторам, зокрема порушення процедури проведення торгів, перевищення встановлених термінів розгляду, наявність великої кількості лотів у тендері, а також відсутність: належних повноважень у суб'єкта торгів; кваліфікованих електронних підписів; необхідних тендерних документів; укладеного договору; опису предмету публічної закупівлі тощо [7]. Державні аудитори через спеціальні електронні кабінети в оболонці системи «ProZorro» стали отримували інформацію про ті закупівлі, які підлягають перевірці через їх відповідність значній кількості ризик-індикаторів. Ці індикатори додавались, а тому чим більше позначалася їх відповідність, тим більша була ймовірність того, що процедура проведення тендеру щодо здійснення публічних закупівель підлягатиме аудиторській перевірці. З метою уникнення перевірок недоброчесні замовники та учасники торгів розпочали застосувати різні шахрайські методи для спотворення відповідності ризик-індикаторам.

Для того, щоб потенційні корупціонери не змогли адаптуватися до наявних критеріїв підозрілості командою експертів «Transparency International Ukraine» було вирішено запровадити більш гнучку аудиторську систему III для моніторингу та контролю державних закупівель – «DoZorro» з алгоритмом самонавчання та змінними складовими визначення ризик-індикаторам [1]. «DoZorro» базується на програмному забезпеченні, яке вчиться ідентифікувати тендери з високим ризиком корупції та значно відрізняється від системи сталих ризик-індикаторів. Результати першого бета-тесту в 2018 році показали, що штучний інтелект виявив на 26% більше тендерів з несправедливим вибором переможця, на 37% більше тендерів, де учасники

були несправедливо дискваліфіковані, і на 29% більше випадків змови між учасниками торгів [97].

У 2019 році на Всесвітньому економічному форумі [115] було оприлюднено перші в світі рекомендації щодо потенціалу штучного інтелекту у здійсненні державних закупівель. Алгоритми рішень штучного інтелекту можуть ефективніше ніж людина відстежувати та аналізувати максимально складні та великі набори даних про публічні закупівлі задля автоматизації закупівельного процесу та вирішення завдань різної складності.

В Україні було докладено значних зусиль для цифровізації процесів та процедур здійснення публічних закупівель. Однак закупівельний процес все ще залишається адміністративно обтяжливими, а його процедури є персистентними та часоємними, через необхідність заповнення складних форм, які вимагають значних людських ресурсів від замовника та всіх учасників тендеру. Для послідовного впровадження ШІ слід враховувати передусім ті його технології й алгоритми, які будуть використовуватися для зниження корупційних ризиків, підвищення результативності операцій та ефективності процедур проведення тендерів у процесі здійснення публічних закупівель. Відповідно до цього, визначимо основні переваги алгоритмів та технологій ШІ за умови їх впровадження у сферу публічних закупівель, що сприятиме заощадженню бюджету для замовників та/або отримання прибутку для постачальників:

- *інформування потенційних учасників закупівельного процесу у відповідності до норм чинного законодавства, наприклад публікація даних про предмет закупівлі, вимоги та критерії відбору тощо;*

- *моніторинг великих масивів даних відкритих тендерів та збір інформації про проведення закупівлі (ціна, умови поставки, якість робіт, товарів і послуг), що дозволить управляти ризиками та забезпечувати високу якість закупівель з метою оперативного відстеження змін, які відбуваються (непрогнозована зміна вартості робіт, товарів і послуг; зменшення кількості учасників торгів; виявлення недобросовісного постачальника тощо);*

– *планування, здійснення аналітичної та прогностичної діяльності* шляхом формування планів та звітності про ефективність закупівельної діяльності, здійснення аналізу шаблонів та профілів закупівельних організацій і учасників тендеру, оцінка та прогнозування потреб у різних роботах, товарах і послугах за допомогою алгоритмів машинного навчання на основі аналізу різних критеріїв;

- *роботизація трудомістких, рутинних, стандартних, типових та повторюваних операцій* з метою усунення «людського фактору» та вивільнення трудових ресурсів, необхідних для виконання більш складних процедур й стратегічних завдань у сфері публічних закупівель;

- *оптимізація та/або узгодження внутрішніх операцій закупівельного процесу*, таких як обробка документів, перевірка дотримання закупівельних процедур, введення даних та відстеження термінів виконання;

- *розробка стратегій з управління закупівельним процесом* з метою визначення нових ринків та/або постачальників робіт, товарів і послуг, а також виявлення потенційних корупційних ризиків.

Разом з тим, варто відзначити, що алгоритми ШІ можуть сприяти отриманню експертами з публічних закупівель додаткової інформації, яка генеруватиметься на основі надскладних та великих наборів даних. Наразі технології ШІ застосовуються у сфері публічних закупівель як окремі програмні рішення (наприклад, спеціалізовані чат-боти, які розроблені для допомоги у вирішенні конкретних проблем), однак у майбутньому їх потенціал може суттєво підвищити результативність діяльності структурних підрозділів органів державної влади, відповідальних за проведення публічних закупівель.

Прикладом практичного використання чат-боту є віртуальний помічник «PAIGE» (Procurement Answers and Information Guided Experience), розроблений компанією «Civic Chatbots», який з 2018 року успішно використовується співробітниками Управління з адміністрування контрактів відділу публічних закупівель муніципалітету міста Сан-Франциско для

допомоги у розв'язанні завдань різної складності у сфері публічних закупівель ІТ-продуктів [153].

На нашу думку, подібні чат-боти мають потужний потенціал для забезпечення прозорості, відкритості та послідовності закупівельної діяльності органами публічної влади, а на етапі підготовки проведення закупівельних процедур зможуть надавати замовникам покрокові інструкції у процесі складання тендерної документації, що унеможливить виникнення більшості помилок та суттєво заощадить їх час. Завдяки використанню технології машинного навчання (machine learning, ML) такі чат-боти зможуть аналізувати типові помилки та існуючі проблеми щодо закупівельних процесів, допомагати учасникам відкритих торгів правильно заповнити та своєчасно подати свої пропозиції у відповідності до норм чинного законодавства у сфері публічних закупівель. В частині ефективного управління внутрішніми (замовники) так і зовнішніми (виконавці) запитами, чат-боти зможуть стати транспарентною комунікативною платформою для подання інформації, її обробки та забезпечення зворотного зв'язку, виключаючи «людський фактор», що суттєво обмежить безпосередню комунікацію між замовником та учасниками тендеру, забезпечить здорову конкуренцію та сприятиме уникненню можливих корупційних ризиків. Таким чином, впровадження чат-ботів на основі штучного інтелекту у сфері публічних закупівель може мати низку переваг, головним чином корисних для підвищення рівня ефективності та результативності закупівельної діяльності органів публічної влади. Використання цього інструменту може зіткнутися з певними проблемами, наприклад, пов'язаними з відсутністю достатньої кількості даних і низьким рівнем цифровізації державного сектора. Всі зазначені переваги чат-ботів III перевищують потенційні перешкоди та ризики щодо їх впровадження.

Неможливо забезпечити стовідсоткове впровадження III у сферу публічних закупівель, однак на шляху до максимізації рівня їх залучення пропонуємо:

1. Вдосконалити механізм підготовки процедур відкритих торгів та укладання договорів (контрактів) через впровадження ІІІ-системи оцінювання та аналізу даних усіх попередніх торгів та контрактів, для того, щоб на їх основі розробити оптимальний алгоритм нових процедур, якій містить:

- планування потреб (обсягів) публічних закупівель шляхом аналізу та оцінювання накопичених даних та характеристик робіт, товарів і послуг, які будуть необхідні у майбутньому й дозволять забезпечити наявність достатньої кількості пропозицій, а також запобігти їх дефіциту за певними категоріями або номенклатурою;

- підготовку документації шляхом її роботизованого генерування та автоматизованого адаптування для проведення відкритих торгів на основі стандартів і вимог, що суттєво спростить процес підготовки та зменшить ймовірність виникнення можливих помилок;

- оптимізацію умов договору (контракту) шляхом аналізу його варіативності, з урахуванням корупційних ризиків, встановлених термінів, ціни та інших факторів, що допоможе створити максимально вигідні умови для замовника та постачальника.

2. Визначати роботи, товари і послуги, які краще підходять для проведення відкритих торгів, їх необхідний обсяг та оптимальну вартість за допомогою оптимізаційних алгоритмів та машинного навчання ІІІ через:

- сегментацію товарів, робіт і послуг шляхом вивчення їх асортименту та визначення тих, які за своїми характеристиками та обсягом найкраще підходять для проведення відкритих торгів;

- аналіз та оцінювання попиту на основі даних про попит на різні товари, роботи і послуги, враховуючи те, які з них є найбільш популярними, та визначаючи оптимальний обсяг для торгів, відповідно до потреб організації;

- визначення для замовника оптимальної (прийнятної) ціни на роботи, товари і послуги, що виставляються на торги, шляхом аналізу цінової динаміки, тенденцій цільового ринку.

2.3 Прогностично-сценарна модель цифрового розвитку України

Особливої актуальності набуває формування прогностично-сценарної моделі цифрового розвитку, яка має враховувати альтернативні сценарії, гнучкість правової системи, сумісність цифрових платформ та значення цифрового суверенітету як ключового чинника національної спроможності. Потреба у побудові прогностично-сценарної моделі задля вироблення державної політики цифрового розвитку України з урахуванням багатовекторності технологічних інновацій, потенційних сценаріїв змін та адаптації органів влади до умов невизначеності, спричинена необхідністю виявити та оцінити майбутні траєкторії трансформації українського суспільства, а також визначити інструменти формування відповідальної, динамічної та відкритої системи публічного управління, здатної ефективно реагувати на виклики цифрової ери. Зазначена модель представляє собою аналітично-ситуативну конструкцію проєктування певних траєкторій застосування політичних, правових, економічних, соціальних, інституціональних, організаційних, технологічних та ресурсних механізмів вироблення державної політики. Стратегічною рамкою планування визначимо 2050 рік, до якого можливі різні сценарії розвитку України з урахуванням ризиків глобального та національного контекстів.

Дедуктивно-індуктивний підхід до сценарного планування передбачає аналіз різних складових механізмів формування та реалізації державної політики цифрового розвитку. Міжнародна взаємодія, наявність дієвої стратегії та неухильність реалізації політичного курсу на діджиталізацію разом із забезпеченням динамічного зростання показників цифрової економіки, підвищенням рівня інвестиції в інфраструктуру, інтеграцією гібридних технологій у публічне управління, опануванням професійних компетентностей з кібербезпеки стають ключовими чинниками альтернативних сценаріїв моделювання інноваційних змін в Україні залежно

до ухвалених державно-управлінських рішень.

Складна конструкція моделі інтегрує методи стратегічного прогнозування, багатофакторного аналізу змін та сценарного моделювання з метою ефективного планування траєкторій цифрової трансформації держави. З іншого точки зору, вона виконує функцію концептуально-інструментального підґрунтя для ухвалення обґрунтованих управлінських рішень орієнтуючись на довгострокові тенденції, невизначеності та ризики, які можуть впливати на ефективність, стійкість і справедливість функціонування публічного сектору в умовах євроінтеграції та збройної агресії проти України. Модель передбачає різні сценарії з урахуванням критичних чинників: темпів інституційної адаптації, рівня діджитальних компетенцій населення, стану технологічної інфраструктури країни, політичної волі та суспільного запиту до цифрових трансформацій.

Прогностично-сценарна модель цифрового розвитку України (рис.2.3) складається з п'яти альтернативних сценаріїв, а саме:

- Сценарій 1: «Незалежність та цифрове лідерство»;
- Сценарій 2: «Інтеграція та цифрова імплементація»;
- Сценарій 3: «Фрагментація та конвенціональна цифровізація»;
- Сценарій 4: «Автократія та цифрова ізоляція»;
- Сценарій 5: «Дезорганізація та цифрова деградація».

Сценарії 1-4 напряду залежать від сталості політичного курсу країни на цифровізацію, на відміну від Сценарію 5, який спричинений бездіяльністю у цій сфері центральних органів державної влади, що неминуче призведе до невизначеності, хаосу, дезорганізації та деградації.

Для застосування ефективних та результативних механізмів державної політики цифрового розвитку важливим є досягнення національного консенсусу (Сценарії 1-3) щодо єдності поглядів стосовно важливості та значущості діджиталізації для еволюції суспільства, економіки та публічного управління.

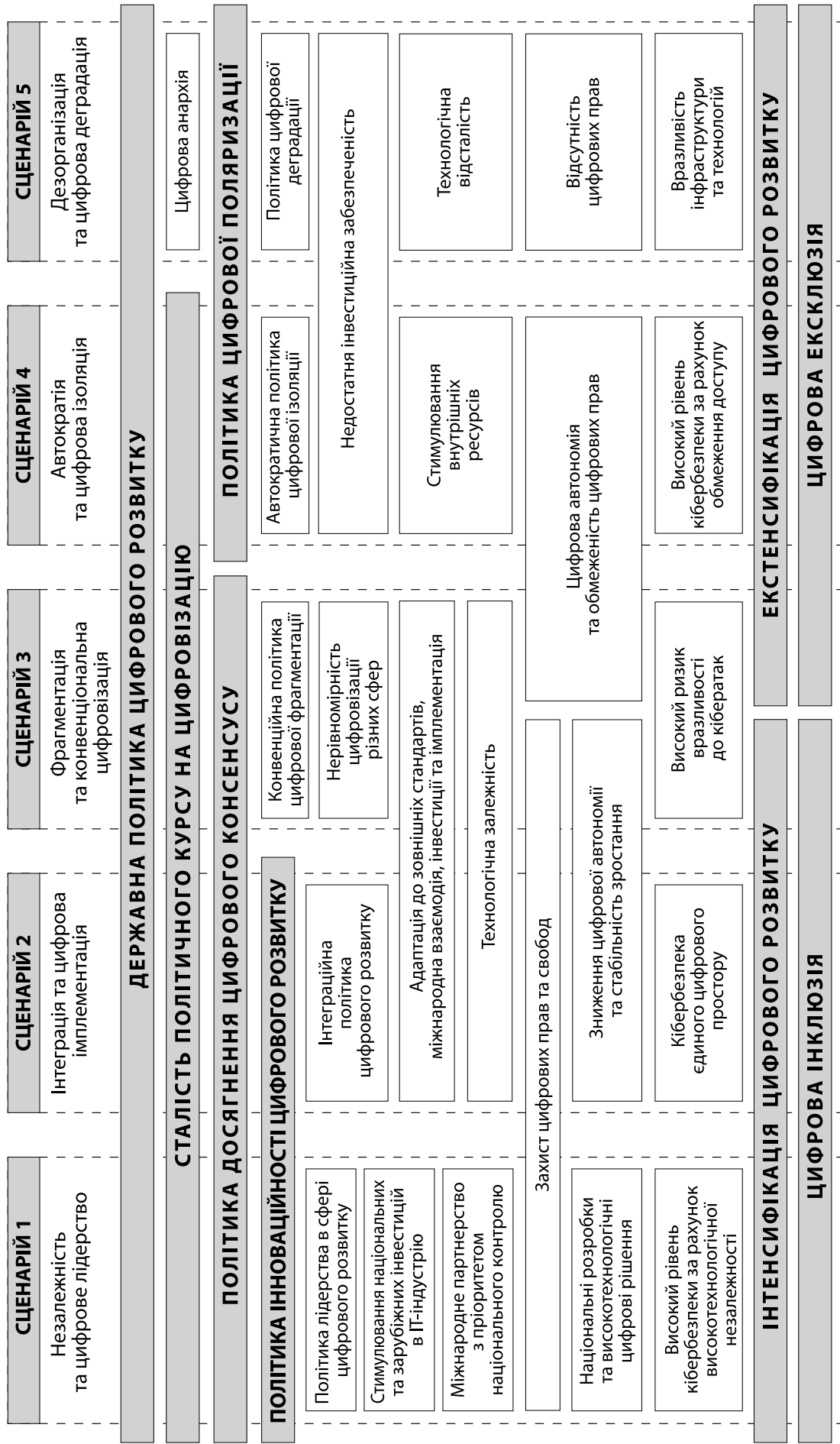


Рис. 2.3 Прогностично-сценарна модель вироблення (формування та реалізації) державної політики цифрового розвитку України

Натомість цифрова поляризація (Сценарії 4-5) спричинює такі негативні наслідки як недовіра до державних інституцій, підвищення рівня соціальної напруги, а також становить загрозу для демократичних процесів в країні. Ознаками цифрової поляризації є виникнення феноменів «інформаційної бульбашки» та «ехо-камер», які разом із таргетингом та алгоритмами соціальних мереж посилюють розбіжності й радикалізацію у поглядах населення, сприяють поширенню дезінформації, обмежують доступ до різних точок зору завдяки штучному формуванню цільових аудиторії «за інтересами». Політика інноваційності цифрового розвитку здебільшого притаманна Сценаріям 1-2, що сприяє застосуванню проривних та високотехнологічних комплексних рішень, таких як нанотехнології, роботизація, гібридний інтелект, алгоритмічне управління та ін.

У цьому контексті цифровий розвиток трактується не лише як процес впровадження нових технологій, а як системна еволюція управлінських практик, адміністративних процедур, на основі нормативно-правових засад, що реалізується через цільові інтервенції державної політики та взаємодії з громадянами. Прогностично-сценарна модель базується на принципі динамічної адаптивності, оскільки передбачає не просто стратегічний план, а здатність держави швидко реагувати на зовнішні виклики шляхом переорієнтації ресурсів відповідно до обраного сценарію розвитку.

Інноваційність вектору державної політики цифрового розвитку визначає схожість Сценаріїв 1 та 2, також обов'язковою умовою просування яких є забезпечення захисту інформаційних (цифрових) прав та свобод населення. Політика лідерства у сфері цифрового розвитку визначає поступ Сценарію 1, якому притаманне стимулювання національних та іноземних інвестицій в ІТ-індустрію, міжнародне партнерство з пріоритетом національного контролю, першочергове стимулювання українських розробок програмних продуктів (наприклад на основі вітчизняних стартапів та гнучких підходів до створення програмних продуктів), а також досягнення високого рівня захищеності цифрового середовища країни від кіберзагроз за рахунок

впровадження закритих високотехнологічних цифрових рішень.

Євроінтеграційна політика визначає цифровий розвиток за Сценарієм 2, базовими складовими якого є міжнародна взаємодія, адаптація та імплементація України до стандартів ЄС, а також технологічна залежність та зниження цифрової автономії. Натомість позитивною ознакою стає стабільність зростання та входження до єдиної системи кіберзахисту європейського цифрового простору.

Розвиток відповідно до Сценарію 3 здебільшого притаманний сучасному стану діджиталізації та спричинений виробленням конвенційної політики цифрової фрагментації, яка відображається нерівномірністю впровадження інновацій у різні сфери. Глибока технологічна залежність, високій ризик вразливості до кібератак та часткове обмеження цифрових прав і свобод громадян спричинені різними суб'єктивними та об'єктивними факторами, які пов'язані з наслідками введення воєнного стану в Україні.

Негативними та малоймовірними вбачаються Сценарії 4 та 5, але які можуть виникнути за умови відмови від політичної, економічної, технологічної та іншої ресурсної підтримки України з боку стратегічних партнерів – країн ЄС та США.

У практичному вимірі прогностично-сценарна модель передбачає формування цифрових дорожніх карт на основі змішаних методів форсайту, аналізу даних до та після реалізації обраного сценарію, моніторингу негативних сигналів, а також системи раннього попередження про загрози та ризики. У перспективі така модель сприятиме створенню гнучких державних стратегій, що враховують одночасно швидкоплинні технологічні тренди, системні ризики, вимоги нормативного узгодження з європейським правом та потреби післявоєнної відбудови. Також, її можна покласти за основу розробки національної рамки цифрової трансформації сфери публічного управління, що включає сценарне картографування, цифрову стратегію ризик-менеджменту, вироблення механізмів превентивної державної політики у сфері кібербезпеки та прогнозно-орієнтовані регуляторні інструменти, які забезпечують

гнучкість, легітимність та результативність цифрових реформ у взаємозв'язку з демократичними цінностями та публічною підзвітністю.

Прогностично-сценарна модель включає три взаємозалежні функціональні чинники: технологічний вектор, що формалізує вплив ключових перспективних технологій; інституційний вектор, який визначає здатність органів публічної влади інтегрувати ці технології у практики врядування та користувацький вектор, що відображає ступінь залученості фізичних і юридичних осіб до одержання цифрових сервісів.

Модель оперує кількома можливими підходами цифрового розвитку:

- еволюційний поступ (Сценарії 2, 3) – помірне впровадження технологій та інерційне моделювання з фокусом на автоматизацію базових функцій;
- адаптивний прорив (Сценарії 1, 2) – динамічне впровадження технологій у сферах стратегічного планування й адміністрування;
- ризик-орієнтована трансформація (Сценарії 3, 4) – акцент на стійкість, безпеку й конфіденційність у відповідь на гібридні загрози;
- кооперативна інновація (Сценарії 1, 2, 3) – масове розгортання інновацій через державно-приватне партнерство, інноваційні пілотні проекти та цифрову участь.

Цифровий розвиток публічного управління в Україні відбувається в умовах високої динаміки та невизначеності. Залежно від обраного сценарію, інтеграція новітніх технологій у систему державного управління має різний рівень складності, інтенсивності та функціонального навантаження. Така гнучкість дозволяє будувати стратегії, що відповідають як ресурсному потенціалу держави, так і здатності органів публічної влади впроваджувати цифрові новації.

Важливу роль відіграє зовнішній контекст: безпекова ситуація (збройна агресія проти України), рівень гармонізації законодавства з правом та стандартами ЄС, кіберзагрози, виклики кризових явищ або шлях до самоізоляції тощо. Для вибору оптимального сценарію цифрового розвитку

необхідна адаптивна, сценарно-чутлива система публічного управління, здатна реагувати на зміни та підтримувати стабільність суспільних екосистем.

Сьогодні державне управління стикається з різними викликами глобальних протистоянь, економічної нестабільності, зростанням конкуренції за цифровий суверенітет та очікуваннями громадян щодо прозорості й ефективності публічного управління. Це вимагає нових управлінських інструментів, здатних діяти гнучко, стратегічно та в реальному часі. Цифрова трансформація має виходити за межі автоматизації, нині мова йде вже про зміну логіки та ідеології прийняття управлінських рішень. Такі зміни базуються на аналітичних платформах, системах прогнозування та штучному інтелекті, які дозволяють моделювати сценарії розвитку та адаптувати управлінські дії до нових обставин.

Ефективність та результативність таких рішень неможлива без розвитку цифрових компетенцій на усіх рівнях влади. Потрібен міждисциплінарний підхід, що об'єднує знання з адміністративної аналітики, цифрової соціології, ризикології та теорії публічного управління. В результаті цього формується нова парадигма публічного управління – проактивна, адаптивна та інтегрована. Цифрова трансформація публічного управління не може обмежуватись лише технічними оновленнями. Воно передбачає глибоке переосмислення принципів керованості, відкритості та довіри. Інноваційні технології мають не лише оптимізувати процеси, а й сприяти переходу до відкритого, інклюзивного та людино-центричного публічного управління. У цьому контексті особливо актуальним є створення науково обґрунтованої прогностично-сценарної моделі цифрового розвитку України, яка має поєднувати стратегічне бачення з прикладними інструментами, бути адаптивною, передбачуваною та сприяти реалізації діджитальної стратегії, яка відповідає викликам сучасності.

Сучасний розвиток публічного управління в Україні потребує подвійної трансформації – внутрішньої адаптації до динамічних викликів і зовнішньої інтеграції в європейський цифровий простір. Це включає як гармонізацію

національного законодавства з нормами ЄС у сфері цифрової безпеки, захисту даних та штучного інтелекту, так і створення власних інституційно-технологічних основ для впровадження інновацій.

У складному політичному та безпековому середовищі реалізація Сценарію 2 виходить за межі інтеграції готових цифрових рішень та потребує вирішення завдань в рамках продукування ідей національного цифрового лідерства (Сценарій 1) у східно-європейському просторі. Україна дедалі більше демонструє власні розробки та ініціативи щодо цифрової ідентифікації (наприклад розповсюдження застосунку «Дія» у Польщі як «Diia.pl» або «mObywatel»), електронного документообігу, кібероборони та прозорого адміністрування, що визнається міжнародними партнерами.

Розбудова національної системи цифрового врядування дає Україні змогу не лише імплементувати європейські норми, а й впливати на їх формування. Це стосується сфер штучного інтелекту, квантової безпеки, цифрової ідентичності, електронної демократії та децентралізованих фінансових систем. Стратегічна мета для України – бути активним суб'єктом європейської політики цифрового розвитку, здатним формувати майбутні правила цифрової взаємодії.

Водночас збройна агресія проти України актуалізувала безпековий аспект цифрової трансформації до рівня стратегічного пріоритету. Повномасштабне вторгнення росії супроводжується ескалацією кіберінформаційного тиску, атаками на критичну інфраструктуру, спробами деструктивного впливу на державні електронні реєстри, а також маніпуляціями в цифровому інформаційному просторі, спрямованими на підрив громадської довіри. Ці виклики вимагають перегляду демократичних підходів та виключно інноваційних шляхів цифрового розвитку публічного управління (Сценарії 1,2) на користь Сценаріїв 3,4, які поєднують технологічну ізольованість, фрагментарність, адаптивність, багаторівневність, захищеність та стійкість до асиметричних загроз.

У цьому вимірі особливої ваги набувають такі напрями, як стратегічна

кібербезпека, захист персональних даних, інформаційна резистентність органів державної влади, а також побудова інфраструктури довіри на основі технологій, що забезпечують анонімність і використання доказів без розкриття. Застосування таких рішень дозволяє підвищити надійність функціонування державних цифрових сервісів, мінімізувати ризики несанкціонованого втручання в адміністрування публічних ресурсів та забезпечити сталість ключових елементів управлінської системи навіть у кризових ситуаціях.

Оптимальний сценарій вироблення державної політики цифрового розвитку має спиратися не лише на інструментальний ресурс технологій, а й поєднувати стратегічне бачення (ідеологію інноваційності) з безпековою рефлексією, організаційну гнучкість з адміністративною відповідністю, європейську інтегрованість з проактивним державотворенням у цифровому просторі, що забезпечить стійкість до зовнішніх атак та високий рівень довіри до інститутів публічної влади в умовах збройної агресії проти України.

Сучасний етап цифрового розвитку публічного управління в Україні характеризується суперечністю між потребою гармонізації з нормативно-правовими актами та технологічними стандартами ЄС і водночас недостатньою стратегічною, інституційною та нормативною готовністю до впровадження національних інновацій. Чинні підходи здебільшого адаптивні та не враховують можливостей України діяти як технологічний лідер, або ініціатор, випереджаючи європейські практики.

Це створює запит на формування проактивної, прогностично орієнтованої моделі цифрового розвитку, яка б поєднувала вимоги євроінтеграції з національними можливостями лідерства в галузі цифрового врядування. Розробка прогностично-сценарної моделі не є меню вибору між інтеграцією до європейських стандартів та пріоритетним впровадженням перспективних технологій, оскільки будь-який з інноваційних сценаріїв зможе зміцнити позицію України як цифрового лідера в майбутньому європейському політико-технологічному просторі.

Висновки до розділу 2

Констатовано, що Україна перебуває на етапі активної реалізації державної політики інтеграції до єдиного цифрового ринку ЄС. У цьому контексті впроваджуються низка заходів, які спрямовані на регуляторне зближення з нормами ЄС, розвиток цифрової інфраструктури та покращення рівня цифрових компетенцій населення. Незважаючи на позитивну динаміку щодо покращення позицій України у провідних міжнародних цифрових рейтингах, невирішеними залишаються низка питань, що гальмують її повноцінну інтеграцію.

Проведений аналіз досвіду європейських країн свідчить про різний рівень їх цифрового розвитку, незважаючи на те, що національні уряди орієнтуються на спільні стандарти в межах реалізації цілей Цифрового десятиліття ЄС. Дослідження дозволяє виявити ефективні практики імплементації європейської політики цифрового розвитку, зокрема на прикладі Данії та Естонії, які демонструють високі показники індексів цифровізації. Основна увага урядів цих країн зосереджується на розвитку цифрової інфраструктури, підвищенні цифрових компетенцій населення, зростанні кількості ІТ-фахівців та забезпеченні безпечного цифрового середовища відповідно до положень Європейської декларації про цифрові права та принципи. Польща попри нижчі показники, активно впроваджує цифрові реформи задля досягнення стратегічних орієнтирів ЄС, що сприяє підвищенню її економічної конкурентоспроможності та цифрової трансформації. Досвід зазначених країн дозволяє окреслити пріоритетні напрями державної політики цифрового розвитку України та прискорити інтеграцію до Єдиного цифрового ринку ЄС.

Запропоновано першочергові напрями удосконалення механізмів вироблення державної політики у сфері інтеграції України до ЄЦР, а саме необхідно: адаптувати нормативно-правову бази відповідно до європейських стандартів; реалізувати європейські ініціативи щодо модернізації цифрової

інфраструктури; якісно оновити систему кіберзахисту органів публічної влади за рахунок використання високотехнологічних цифрових рішень; стимулювати цифрову трансформацію бізнесу за рахунок залучення іноземних інвестицій; поглиблювати цифрові компетенції населення. Належна реалізація цих напрямів буде позитивно впливати на рівень конкурентоспроможності країни, зміцнювати позиції України у європейському цифровому просторі та забезпечить сталість її подальшого цифрового розвитку.

Встановлено роль штучного інтелекту як нового суб'єкту державного управління завдяки аналізу можливостей алгоритмічного лобіювання впливати на прийняття державно-управлінських рішень та змінювати механізми політичної взаємодії. На основі практичних прикладів застосування алгоритмічного таргетування на виборах у США, Бразилії та Індії через великі цифрові платформи (Facebook, Google, X) доведено їх ефективність та результативність у формуванні суспільної (громадської) думки. Доведено небезпечність алгоритмічних впливів на демократію завдяки відсутності підзвітності, застосуванню алгоритмічного спотворення реальності та поступове перетворення держави на «цифрового заручника» маніпулятивних технологій. Надано рекомендації щодо формування багаторівневої системи регуляції алгоритмічного лобіювання (доступна прозорість алгоритмів для державних органів та громадян; інституційний контроль за алгоритмічними рішеннями; етична відповідальність компаній дотримуватися принципів чесності, недискримінації та соціальної відповідальності при обробці даних; міжнародна гармонізація стандартів створення визнаних норм щодо обмеження алгоритмічної влади) та пропозиціями для України щодо демократичного контролю за алгоритмами (прийняття нормативних актів про прозорість алгоритмів; сформувати незалежний наглядовий орган з питань алгоритмів ІІІ; запровадження «права на відмову» від алгоритмічної персоналізації, зокрема в політичній рекламі та новинних стрічках).

Визначено основні переваги застосування штучного інтелекту для зниження корупційних ризиків у сфері публічних закупівель та надано

практичні рекомендації щодо максимізації рівня впровадження його алгоритмів та технологій на основі дослідження нормативних, організаційних та технологічних особливостей здійснення публічних закупівель у період дії правового режиму воєнного стану в Україні. Визначено недоліки застосування принципу «top-down» для фінансового плануванні обсягів публічних закупівель органами державної влади. Констатовано, що закупівельний процес продовжує бути адміністративно обтяжливим, а його процедури є персистентними та часоємними, через необхідність заповнення складних форм, які вимагають значних людських ресурсів. Доведено, що для послідовного впровадження штучного інтелекту слід враховувати передусім переваги його технологій й алгоритми, які будуть використовуватися для зниження корупційних ризиків, підвищення ефективності та результативності публічних закупівель.

Наведено основні переваги алгоритмів та технологій штучного інтелекту за умови їх впровадження у сферу публічних закупівель, що сприятиме заощадженню бюджету для замовників та/або отримання прибутку для постачальників (своєчасне та належне інформування потенційних учасників закупівельного процесу; моніторинг великих масивів даних відкритих тендерів; планування, здійснення аналітичної та прогностичної діяльності; роботизація трудомістких, рутинних, стандартних, типових та повторюваних операцій; оптимізація та/або узгодження внутрішніх операцій закупівельного процесу; розробка стратегій з управління закупівельним процесом). Доведено, необхідність використання чат-ботів, побудованих на основі спеціальних програмних рішень штучного інтелекту, які завдяки використанню технології «machine learning» зможуть аналізувати типові помилки та існуючі проблеми закупівельних процесів, допомагати учасникам відкритих торгів правильно заповнити та своєчасно подати свої пропозиції. Чат-боти зможуть стати прозорою комунікативною платформою для подання, обробки інформації та забезпечення зворотного зв'язку, виключаючи «людський фактор», що суттєво обмежить безпосередню комунікацію між замовником та

учасниками тендеру, забезпечить здорову конкуренцію та сприятиме уникненню можливих корупційних ризиків. Надано практичні рекомендації для максимізації рівня впровадження алгоритмів та технологій штучного інтелекту, а саме необхідно: для розробки оптимальних алгоритмів закупівельних процедур вдосконалити механізм підготовки процедур відкритих торгів та укладання контрактів через впровадження системи оцінювання та аналізу даних попередніх торгів та контрактів; обирати роботи, товари і послуги, які краще підходять для проведення відкритих торгів, їх необхідний обсяг та оптимальну вартість за допомогою оптимізаційних алгоритмів та машинного навчання.

Розроблено прогностично-сценарну модель цифрового розвитку України, що представляє собою аналітично-ситуативну конструкцію з п'яти альтернативних сценаріїв (Сценарій 1 – «Незалежність та цифрове лідерство»; Сценарій 2 – «Інтеграція та цифрова імплементація»; Сценарій 3 – «Фрагментація та конвенціональна цифровізація»; Сценарій 4 – «Автократія та цифрова ізоляція»; Сценарій 5 – «Дезорганізація та цифрова деградація») за якими здійснюється проектування політичних, правових, інституціональних, організаційних, економічних, соціальних, технологічних, інформаційних, ресурсних та інших механізмів вироблення (формування та реалізації) відповідної державної політики.

У практичному вимірі прогностично-сценарна модель передбачає не лише технологічну модернізацію цифрової інфраструктури країни, створення гнучких державних стратегій, а й трансформацію управлінської парадигми: від реактивного (кризового) адміністрування до динамічного, адаптивного, проактивного, стратегічно вмотивованого публічного управління, яке ґрунтується на застосуванні змішаних методів алгоритмічного прогнозування, форсайту, моніторингу, аналізі та оцінці даних, забезпеченні кіберзахисту та інституційної гнучкості.

Особливість дослідницького підходу до розробки прогностично-сценарної моделі полягає у поєднанні трьох функціональних вектор-чинників

цифрового розвитку – *технологічного* (формалізує вплив ключових перспективних технологій), *інституційного* (визначає здатність органів публічної влади інтегрувати технології у єдиній системі цифрового врядування) та *користувацького* (відображає ступінь залученості фізичних і юридичних осіб до одержання цифрових сервісів), що сприятиме не лише ефективності впровадження комплексних діджитальних рішень, а й їх обґрунтованості, доцільності, легітимності, інклюзивності та відповідності демократичним цінностям цифрового суспільства. Модель оперує кількома можливими перспективними підходами щодо подальшого цифрового розвитку: *еволюційним поступом* (Сценарії 2-3) – помірне впровадження технологій та інерційне моделювання з фокусом на автоматизацію базових функцій; *адаптивним проривом* (Сценарії 1-2) – динамічне впровадження технологій у сфери стратегічного планування й адміністрування; *ризик-орієнтованою трансформацією* (Сценарії 3, 4) – акцент на стійкість, безпеку й конфіденційність у відповідь на гібридні загрози; *кооперативною інновацією* (Сценарії 1, 2, 3) – масове розгортання інновацій через державно-приватне партнерство, інноваційні пілотні проєкти та цифрову участь.

Запропонована прогностично-сценарна модель цифрового розвитку України є концептуально-інструментальним підґрунтям стратегічного планування й наукового обґрунтування управлінських рішень, їх адаптації до тенденцій технологічної трансформації, ризиків глобальної нестабільності та довгострокових безпекових невизначеностей, що впливають на ефективність, результативність і стійкість функціонування органів публічної влади.

В умовах євроінтеграційних процесів, збройної агресії проти України та в умовах повоєнного відновлення модель сприятиме вчасній ідентифікації актуальних ризиків і критичних загроз, створенню ефективної системи їх раннього виявлення та попередження, розробці цифрових дорожніх карт та впровадженню адаптивних управлінських рішень, які посилять стійкість функціонування органів публічного управління.

З огляду на вищезазначене, виникає необхідність удосконалення

нормативно-правових, функціонально-організаційних та ресурсних механізмів вироблення державної політики цифрового розвитку в Україні, а саме першочерговим вбачається:

- включити до стратегічних цілей Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року, ухваленої розпорядженням кабінету Міністрів України від 31 грудня 2024 р. № 1351-р, необхідність першочергової адаптації українського законодавства до базових цифрових актів ЄС (AI Act, DGA, Data Act, eIDAS 2.0) з обов'язковими дорожніми картами щодо їх детальної імплементації;

- розробити Концепцію технологічного (інноваційного) лідерства України у сфері цифрового розвитку, яка визначатиме пріоритетні напрями випереджального впровадження перспективних та проривних цифрових технологій з урахуванням національних потреб, міжнародних стандартів та етичних рамок;

- створити й інституалізувати систему моніторингу, аналізу, оцінювання, та прогностичного моделювання цифрової спроможності (зрілості) органів публічної влади, що дозволить своєчасно коригувати управлінські процеси відповідно до темпів змін та новацій у технологічному середовищі;

- сформувати міжсекторальну раду з питань цифрового лідерства та етичного врядування, як дорадчого органу при Міністерстві цифрової трансформації України з функціями стратегічної експертизи щодо взаємодії з інституціями ЄС.

Основні результати розділу 2 опубліковано в наукових працях автора:

1. Карпенко, О., Карпенко, Ю., & Герман, Д. (2023). Штучний інтелект як інструмент зниження корупційних ризиків у сфері публічних закупівель. *Аспекти публічного управління*, 11(2), 129-135. <https://doi.org/10.15421/152328>

2. Герман Д. (2023). Взаємодія алгоритмів штучного інтелекту та ІОТ-технологій: перспективи та виклики цифрового суспільства. Кібербезпека державних інституцій та подолання кризових станів: Збірник тез II Міжнародної науково-практичної конференції, (м. Київ-Вроцлав, травень 2023 року). Київ, С.139-140.

3. Герман, Д., & Пузько, М. (2024). Особливості використання штучного інтелекту у сфері культури та креативних індустрій: державно-управлінський аспект. Університетські наукові записки, 3(99), 23-36. <https://doi.org/10.37491/UNZ.99.3>

РОЗДІЛ 3

УДОСКОНАЛЕННЯ МЕХАНІЗМІВ ВИРОБЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЦИФРОВОГО РОЗВИТКУ В УКРАЇНІ

3.1 Перспективні напрями вироблення державної політики цифрового розвитку України в умовах інтенсифікації інформаційних війн

Цифровізація докорінно змінила характер інформаційних війн, перетворивши їх на багатовимірну систему впливу, що охоплює алгоритмічні маніпуляції, фільтрацію та пріоритезацію контенту, персоналізований таргетинг, автоматизоване створення інформації та використання бот-мереж для спотворення суспільного дискурсу. У світі, де цифрові комунікації стають основним джерелом отримання інформації, такі технології значно ускладнюють виявлення дезінформаційних кампаній та реагування на них.

У цьому контексті надзвичайно важливим стає прогнозування подальшої еволюції цифрових інформаційних війн, зокрема визначення їх динаміки та впливу маніпулятивних технологій на інформаційне протистояння.

Серед можливих сценаріїв розвитку інформаційних війн особливу увагу слід приділити глобалізації таких конфліктів, що відбувається внаслідок зростання ролі соціальних мереж, використання ШІ для створення маніпулятивного контенту та впровадження нових кібероперацій. Соціальні платформи стали сферою комунікативного протистояння, оскільки забезпечують миттєве поширення контенту, створюючи ефект масштабної інформаційної хвилі. Водночас алгоритмічні системи впливу та автоматизовані ботоферми значно підсилюють тиск на суспільну думку.

Одним із ключових викликів стає розвиток автономних інформаційних агентів, таких як боти, керовані ШІ, які здатні в реальному часі аналізувати суспільні настрої та адаптувати комунікативні кампанії відповідно до змін у середовищі. Використання методів глибокого навчання та аналізу великих масивів даних дозволяє таким системам генерувати ефективні комунікативні

стратегії, що орієнтовані на конкретні цільові аудиторії. Такий підхід значно підвищує точність та ефективність інформаційного впливу, роблячи його майже непомітним для кінцевого споживача цифрового контенту.

Зростаючою загрозою є персоналізована пропаганда, коли ІІІ генерує індивідуалізовані інформаційні кампанії, використовуючи поведінкові дані користувачів. Аналіз цифрових слідів, таких як історія пошуку, соціальні взаємодії та уподобання, дає змогу створювати психологічно адаптовані меседжі, які мають значно вищий рівень ефективності порівняно з традиційними формами дезінформації. Як вже було зазначено у п. 2.2 використання таких методів відкриває нові можливості для маніпуляцій суспільною свідомістю, адже вони націлені на індивідуальні когнітивні особливості кожної людини.

Ще однією небезпечною тенденцією є технологія «реального діпфейку», яка дозволяє створювати фальшиві відео- та аудіоматеріали в режимі реального часу. Це ускладнює можливість відрізнити правдиву інформацію від сфабрикованої, підриваючи довіру до всіх джерел комунікації. Завдяки використанню глибоких нейронних мереж створення реалістичних підробок виступів політичних лідерів, офіційних заяв чи журналістських репортажів стає дедалі доступнішим, що може суттєво впливати на формування суспільних уподобань та прихильностей.

У контексті міждержавного інформаційного протистояння дедалі більшої значущості набуває створення цифрових альянсів та формування стратегічної координації між державами. Інформаційні війни перестають бути локальним феноменом, інтегруючись до глобальних геополітичних процесів.

Політичні сугестори використовують цифрові технології для маніпуляції виборчими процесами, зміцнення власних геополітичних позицій та послаблення супротивників. У відповідь на це формується міжнародне співробітництво у сфері цифрової безпеки, що включає обмін аналітичними даними, координацію дій у сфері кібероборони та розробку спільних стандартів для протидії дезінформації.

У сучасних умовах зростає також небезпека радикалізації через цифрові платформи. Інформаційний простір стає дедалі більш поляризованим, що сприяє формуванню «інформаційних бульбашок», в яких користувачі взаємодіють лише з контентом, що підтверджує їхні переконання. Це ускладнює доступ до альтернативних точок зору та стимулює посилення соціальної напруженості.

Подальший розвиток цієї тенденції може спричинити появу віртуальних квазідержав і цифрових спільнот, що діятимуть незалежно від традиційних державних інституцій, створюючи нові виклики для регулювання глобального інформаційного простору.

Протидія дезінформації та цифровим загрозам стає стратегічним пріоритетом для держав та міжнародних організацій. У цьому контексті розвивається концепція фактчекінгових груп громадських активістів та спеціалізованих установ, які займаються виявленням та нейтралізацією маніпулятивного контенту і виявленням інформаційних атак.

Водночас розширюється використання технологій ШІ для виявлення фейкової інформації та автоматизованого блокування деструктивних кампаній у соціальних мережах.

Таким чином, еволюція інформаційних війн у цифрову епоху потребує комплексного підходу до забезпечення національної безпеки. Інтеграція технологічних, політичних та міжнародних стратегій є необхідною для ефективного реагування на сучасні загрози. Розвиток цифрових альянсів, запровадження технологічних рішень для боротьби з дезінформацією та підвищення медіаграмотності населення стануть ключовими елементами інформаційної стійкості держав у XXI столітті.

У таблиці 3.1 нами визначено, за якими траєкторіями поточні інформаційні процеси можуть еволюціонувати в майбутньому, зважаючи на розвиток цифрових технологій та зміну підходів до ведення гібридних воєн та забезпечення інформаційної безпеки.

Таблиця 3.1

**Траєкторії цифрового розвитку інформаційних процесів в контексті
ведення гібридних воєн та забезпечення інформаційної безпеки**

Напрями	Сучасний стан	Прогнозований розвиток
1. Глобальні інформаційні війни та цифрова пропаганда	Використання ІІІ для генерації та поширення дезінформації. Соціальні мережі як основне поле для розгортання інформаційних атак. Маніпуляція суспільною думкою через ботоферми та алгоритмічні системи.	Збільшення ролі автономних ІІІ-ботів, які аналізують ситуацію в реальному часі та змінюють наративи. Виникнення «реального дідфейку» – можливість створення відео та аудіо в реальному часі, що ускладнює відрізнєння правди від вигадки. Персоналізована пропаганда, адаптована до поведінкових даних кожного користувача.
2. Міждержавні інформаційні війни та цифрові альянси	Цифрові технології використовуються державами для впливу на політичні процеси інших країн. Застосування кібероперацій як частини інформаційних воєн.	Формування цифрових військових блоків і альянсів для координації інформаційних воєн. Використання цифрових "проксі-альянсів", що діють в інтересах сильніших геополітичних гравців. Цифрова інтеграція військових дій із масованими інформаційними кампаніями для введення противника в оману.
3. Автоматизація інформаційних воєн та цифрова радикалізація	Інформаційні маніпуляції спричиняють поляризацію суспільств. Соціальні платформи використовуються для поширення різних у тому числі радикальних ідеологій.	Виникнення віртуальних держав та цифрових спільнот без фізичних кордонів. Використання «меметичного» програмування для впливу на масову свідомість. Імплантація/спотворення помилкових спогадів за допомогою інтерактивного цифрового медіаконтенту, що формує альтернативну реальність для окремих цільових груп населення
4. Цифровий контроль та боротьба з дезінформацією	Цифровий розвиток механізмів перевірки фактів (fact-checking) та ініціатив в інформаційному середовищі. Використання ІІІ для автоматизованої ідентифікації фейків.	Формування глобальних цифрових «спільнот», які координують боротьбу з дезінформацією. Використання блокчейн-технологій для перевірки достовірності новин. Впровадження персоналізованого аудитора – інтелектуальних систем, що аналізує контент, який споживає користувач, та попереджує про можливі маніпуляції.

Джерело: складено автором.

Зокрема, у прогнозованому розвитку можна побачити значне збільшення впливу ІІІ, розширення цифрових альянсів та нові способи радикалізації через інформаційні технології. Крім того, технології, такі як блокчейн, забезпечуватимуть перевірку достовірності інформації, а персональні системи аналізу контенту можуть стати важливим інструментом для попередження маніпуляцій у майбутньому.

Аналіз напрямів цифрового розвитку інформаційної безпеки дає змогу сформулювати ключові виклики для вироблення відповідної державної політики в умовах збройної агресії проти України. Розглянемо основні траєкторії (вектори, напрями) розвитку ситуації.

Напрямок, що має умовну назву «Цифрова пропаганда», передбачає збереження нинішніх тенденцій. Він охоплює подальший розвиток цифрових технологій і збереження основних тенденцій, що вже сформувалися у сфері інформаційних воєн. В рамках цього напрямку одним із ключових викликів для держави є пошук балансу між забезпеченням свободи слова і протидією дезінформації, що набуває дедалі масштабніших форм в умовах цифровізації. У зв'язку з цим, ефективна протидія дезінформації вимагає вироблення нових механізмів верифікації контенту. Однак, ці заходи не повинні призводити до надмірної цензури у повоєнний період, що може обмежити основні права громадян на вільний обмін інформацією.

Однією з основних загроз цього напрямку є активне використання ІІІ для маніпуляції суспільною думкою, який здатний генерувати та поширювати фальшиві новини, дипфейки й інші форми дезінформації, яка впливає на громадську думку, політичні процеси та національну безпеку. Оскільки технології ІІІ розвиваються набагато швидше за правову базу, що намагається їх регулювати, виробники державної політики стикаються з новими викликами. Відставання ухвалення правових норм від тенденцій технологічного прогресу створює прогалини законодавства, що ускладнює боротьбу з новими цифровими загрозами.

Ще одним важливим аспектом є персоналізація інформаційних атак. Завдяки розвитку великих даних і алгоритмів ШІ виникають нові можливості для цілеспрямованого впливу на окремі соціальні групи. Така персоналізація інформаційних атак ускладнює їх виявлення та нейтралізацію, що потребує розробки нових, адаптованих до сучасних умов, механізмів протидії дезінформації.

Для ефективного реагування на ці загрози необхідно вдосконалювати методи медіаграмотності, критичного аналізу й перевірки джерел інформації. Крім того, важливо нормативно врегулювати діяльність цифрових платформ, аби запобігти поширенню шкідливого контенту без порушення демократичних принципів свободи слова та вираження думок.

Одним із ключових завдань є також розбудова ефективних механізмів швидкого реагування на інформаційні загрози. Створення спеціалізованих органів або агентств, які б займалися моніторингом та аналізом комунікативних кампаній, спрямованих проти національних інтересів держави, дозволить оперативно реагувати на нові виклики й забезпечить більш ефективний інформаційний захист від цифрових загроз.

Напрямок «цифрових альянсів» передбачає активну участь України в глобальних спільнотах, що стає важливим аспектом вироблення міжнародної політики. В умовах глобалізації та цифрової трансформації важливо знайти оптимальний баланс між збереженням інформаційної суверенності та необхідністю міжнародної координації в галузі інформаційної безпеки. Необхідно враховувати внутрішні потреби та зовнішні вимоги, обумовлені глобальними цифровими процесами.

Основною загрозою в рамках цього напрямку є використання інформаційних воєн союзниками України у власних інтересах. Іноді політичні, економічні та стратегічні амбіції окремих країн можуть призвести до того, що інформаційна політика використовується як інструмент для досягнення власних цілей, що може бути несумісне з національними інтересами України. Додатковою загрозою є втрата контролю над частиною національного

інформаційного простору у процесі проведення міжнародних інформаційних кампаній, що може порушити інформаційну незалежність країни.

Іншою проблемою є використання так званих квазі-альянсів (проксі-держав) для ведення агресивних інформаційних операцій. Це дозволяє державам-агресорам приховувати свою причетність до атак, що ускладнює їх виявлення та нейтралізацію, створюючи загрозу для національної безпеки та стабільності інформаційного простору України.

Для мінімізації цих загроз Україні необхідно проводити власну стратегію кібердипломатії, яка повинна стати основою зовнішньої політики в сфері кібербезпеки та інформаційних воєн, зокрема визначати можливості для співпраці з міжнародними партнерами й забезпечити захист національних інтересів. Важливим також є постійне забезпечення удосконалення інформаційної безпеки державних інституцій задля гарантування стійкості системи державних інституцій до зовнішніх і внутрішніх інформаційних атак.

Напрямок «цифрової радикалізації» інформаційних воєн передбачає значний вплив новітніх технологій на інформаційне середовище, що ставить під загрозу традиційні методи контролю та протидії дезінформації. Розвиток ШІ відкриває нові можливості для маніпуляції інформацією, що вимагає адаптації механізмів вироблення державної політики до нових умов і розробки більш ефективних інструментів забезпечення національної безпеки. Основною загрозою є використання ШІ для масового створення маніпулятивного контенту й дипфейків. Зі швидким розвитком технологій штучний інтелект здатний генерувати фальшиві новини, відео та аудіо, що може вводити громадськість в оману і ставити під загрозу політичну стабільність. Автоматизовані інформаційні атаки на основі алгоритмів ШІ можуть бути настільки швидкими й масштабними, що державні інституції не встигатимуть їх адекватно аналізувати й реагувати на них.

Напрямок концентрації «цифрового контролю» є серйозною загрозою для інформаційних потоків, які зосереджуються у руках великих технологічних корпорацій. Саме такі корпорації мають доступ до великих обсягів даних і

потужних алгоритмів для маніпуляції інформацією. Це може призвести до ситуації, коли приватні компанії, а не держави, визначатимуть, яка інформація буде доступною для громадян, що створює ризики національній безпеці, демократичним процесам та свободі слова.

Для ефективної протидії цим загрозам необхідно інвестувати в розробку державних алгоритмів для розпізнавання дезінформації. Це дозволить швидше виявляти маніпуляції й фальшиві новини, а також оперативно реагувати на інформаційні атаки. Важливим кроком є впровадження регуляторних норм щодо використання ШІ в медіа, що створить правову основу для контролю за застосуванням технологій штучного інтелекту в інформаційному просторі.

Фрагментація цифрового простору та інформаційної ізоляції передбачає серйозні виклики для глобальної комунікації та міжнародної співпраці. Загроза розшарування світового інформаційного простору й посилення «інформаційних залізних завіс» ускладнює забезпечення вільного доступу до інформації та ефективного обміну даними. В умовах реалізації цього напрямку важливо знайти шляхи для збереження відкритості інформаційного середовища при одночасному захисті національних інтересів України.

Однією з найбільших загроз є втрата глобальної відкритості Інтернету. Якщо країни почнуть активно контролювати інформаційний простір, це може призвести до ізоляції окремих держав у світовому інформаційному просторі. Виникнення паралельних цифрових екосистем обмежить доступ до ключових технологій та знань, що поставить під загрозу технологічний розвиток країни.

Для протидії цим викликам необхідно збалансувати інформаційну відкритість із захистом національного інформаційного простору. Важливим кроком є створення національних цифрових платформ, що зменшить залежність від зовнішніх ресурсів і посилить контроль держави над внутрішнім інформаційним середовищем. Крім того, потрібно активно працювати над створенням міжнародних коаліцій для підтримки відкритого інформаційного середовища, які допоможуть зберегти глобальну відкритість Інтернету.

Підсумовуючи викладене, можемо констатувати, що майбутнє інформаційних воєн визначатиметься здатністю держав адаптуватися до умов розвитку цифрових суспільств. Водночас, ефективність протидії інформаційним загрозам залежатиме не лише від технологічного потенціалу держав, а й від здатності стейкхолдерів формувати стратегічні підходи до управління інформаційним простором. Важливу роль відіграватиме розробка комплексних заходів, що поєднують технологічні, правові та організаційні механізми цифрового розвитку у сфері протидії дезінформації та інформаційним маніпуляціям. Успішна реалізація відповідної державної політики вимагатиме балансування між забезпеченням національної безпеки та збереженням принципів відкритості й свободи інформації в глобальному цифровому середовищі.

Важливою складовою державної політики цифрового розвитку є налагодження співпраці між органами державної влади та компаніями-власниками технологічних платформ, що має відбуватися у форматі постійного діалогу щодо удосконалення механізмів протидії інформаційним загрозам. У цьому аспекті доцільним є створення платформи оперативного реагування на дезінформацію, яка б включала представників державних органів, цифрових платформ та незалежних експертів для обговорення та впровадження спільних заходів боротьби з маніпулятивним контентом.

Ключовим напрямом правового регулювання має стати забезпечення прозорості політичної реклами у цифровому просторі, що передбачає обов'язкове розкриття інформації про замовників, джерела фінансування та механізми мікротаргетингу політичної агітації. Також необхідно запровадити архіви політичної реклами, які дозволять громадським організаціям та дослідникам здійснювати моніторинг її впливу на виборчі процеси.

Рис. 3.1 ілюструє наші рекомендації щодо механізмів вироблення ефективної державної політики цифрового розвитку у сфері протидії дезінформації.

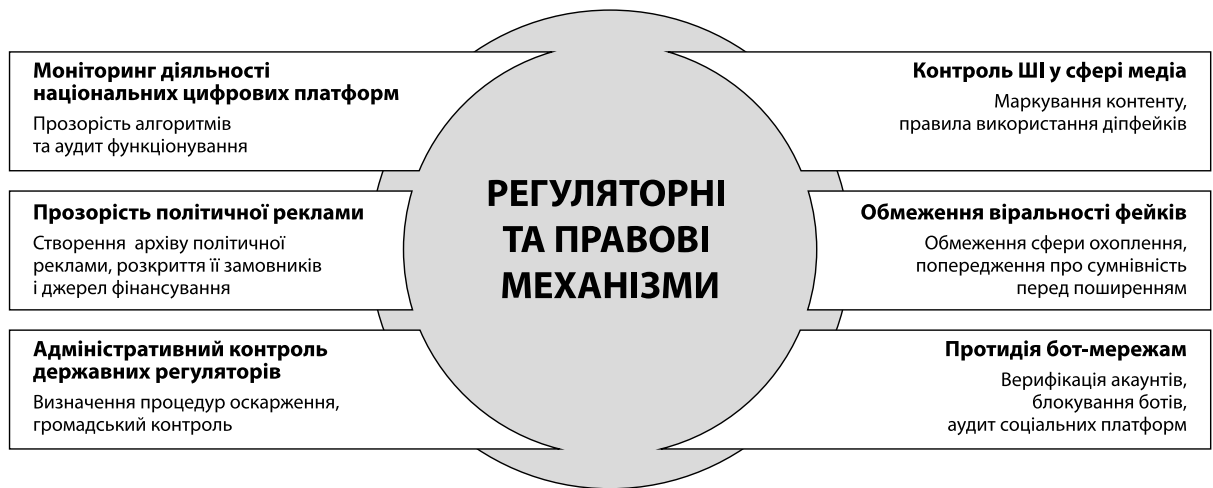


Рис. 3.1 Регуляторні та правові механізми вироблення державної політики цифрового розвитку у сфері протидії поширенню дезінформації

Джерело: складено автором.

Таким чином, розбудова ефективної системи публічного управління цифровим розвитком потребує поєднання законодавчих, організаційних, технологічних, ресурсних та етичних підходів. Відповідальна взаємодія публічних службовців, власників цифрових платформ та представників громадянського суспільства є запорукою формування належного інформаційного середовища, яке одночасно відповідатиме демократичним стандартам та захищатиме національні інтереси України.

Проте, крім нормативно-правового та регуляторного захисту, цифрова протидія інформаційним загрозам неможлива без міжнародного співробітництва. Дезінформаційні кампанії, що використовують цифрові технології, не мають географічних кордонів і часто координуються на глобальному рівні, що вимагає відповідної багатосторонньої відповіді. В умовах поширення дезінформації через транскордонні комунікаційні платформи, зростання впливу маніпулятивних наративів та активного використання кіберінструментів для інформаційних атак міжнародна координація у сфері цифрової дипломатії стає стратегічно необхідною. Для України необхідно розширювати міжнародне співробітництво, удосконалювати дипломатичні механізми забезпечення національної безпеки

та активно використовувати інструменти «м'якої сили» для протидії деструктивним впливам.

Глобальна співпраця у сфері цифрової дипломатії передбачає інтеграцію України у міжнародні ініціативи з протидії дезінформації та посилення взаємодії з міжнародними організаціями, що працюють у цій сфері. В ЄС вироблено низку стратегічних механізмів, спрямованих на боротьбу з цифровими загрозами, серед яких «Digital Services Act» (далі – DSA), що регулює діяльність цифрових платформ, а також спеціалізовані аналітичні центри, такі як «East StratCom Task Force» та «EUvsDisinfo», які займаються виявленням, аналізом і спростуванням дезінформації. Взаємодія з європейськими партнерами, адаптація української політики до стандартів ЄС у сфері цифрової безпеки та участь у спільних заходах із боротьби з інформаційними загрозами дозволять Україні розширити свої можливості у сфері стратегічних комунікацій та інформаційного захисту.

Важливим напрямом міжнародної діяльності є співпраця з НАТО у сфері кібербезпеки, зокрема через активну участь у діяльності Кооперативного центру кібероборони НАТО (CCDCOE). Ця взаємодія забезпечить доступ до передових методів аналізу інформаційних загроз, розширить можливості стратегічного планування цифрової безпеки та підвищить рівень оперативного обміну інформацією щодо дезінформаційних атак. Водночас посилення участі України у міжнародних коаліціях, таких як «Counter Disinformation Coalition», Глобальний альянс для захисту демократії (далі – GAD) та Ініціатива з кіберстійкості G7, сприятиме координації дій з міжнародними партнерами для розробки спільних заходів реагування на інформаційні загрози.

Поряд із багатосторонньою дипломатією важливе значення має двостороннє співробітництво з державами, що мають успішний досвід протидії цифровим загрозам. Країни Балтії, Польща, Фінляндія та інші держави, які зазнавали масованих інформаційних атак, розробили ефективні стратегії боротьби з дезінформацією, що можуть бути адаптовані для українських реалій. Посилення співпраці на рівні урядів, спільні навчальні

програми, обмін досвідом щодо тактик цифрової агресії сприятимуть підвищенню кіберстійкості України.

Не менш важливою складовою міжнародної кібердипломатії є взаємодія з глобальними цифровими платформами, які відіграють ключову роль у формуванні суспільних наративів. Такі компанії, як «Meta», «Google», «Twitter» та «Telegram», значною мірою впливають на поширення інформації та можуть сприяти або, навпаки, перешкоджати боротьбі з дезінформацією, залежно від своєї політики модерації контенту. У зв'язку з цим необхідним є створення інституціоналізованої системи співпраці між державними органами України та технологічними корпораціями, що дозволить оперативно реагувати на дезінформаційні кампанії, блокувати маніпулятивний контент та забезпечувати прозорість алгоритмів.

3.2 Запровадження гібридного інтелекту як інструменту цифрового розвитку громадської участі у сфері публічного управління

Сьогодні суспільство постає перед вибором: з одного боку – це нові технологічні можливості для партисипації громадян, з іншого – загрози втрати людської суб'єктності через застосування алгоритмічного управління та непрозорості цифрових процесів. Тому важливим є науковий пошук методів узгодження алгоритмічної відповідальності та цифрової етики, а також виявлення інструментів ефективного делегування окремих адміністративних функцій системам штучного інтелекту поряд із збереженням людського потенціалу у діяльності органів публічної влади. Тому особливої актуальності у сучасній науці державного управління набувають дослідження феноменів гібридного інтелекту та алгоритмічного врядування. Враховуючи результати дослідження алгоритмів та технологій штучного інтелекту (п. 2.2) та можливості їх подальшого впливу на суспільні трансформації, новою перспективною формою цифрового розвитку є гібридний інтелект, під яким у публічному управлінні слід розуміти симбіоз людського і машинного

мислення, їх інтегрованих можливостей та етичних орієнтирів для вироблення обґрунтованих, неупереджених та оптимальних державно-управлінських рішень.

Будь-які трансформації громадянського суспільства в умовах цифровізації повинні досліджуватися на перетині фокусів декількох наукових дискурсів, а саме: цифрового врядування, політики застосування алгоритмів, е-демократії та технологічної етики. У рамках цифровізації державного управління такі іноземні вчені як П. Данліві [127] та Х. Маргеттс [129] звертають увагу на поступову зміну традиційних інституційних структур під впливом ІКТ. Окрема увага у науковій літературі приділяється електронній участі громадян (e-participation), яка розглядається як інноваційний засіб активізації суспільства через онлайн-інструменти, та водночас піддається критиці за ризик створення ілюзії залученості [116]. З появою більш складних цифрових систем алгоритми прийняття рішень та технології інтелектуального управління формують нове аналітичне поле, відоме як алгоритмічне управління (algorithmic governance).

К. Бейтуллаху-Міхалопулос та М.-В. Флорен ставлять під сумнів справедливість та підзвітність вплив алгоритмів на розподіл ресурсів, прийняття рішень і доступ до послуг [108]. У цьому контексті особливе занепокоєння викликає закритість та непрозорість таких цифрових систем, оскільки їх рішення важко оскаржити, а іноді навіть зрозуміти.

У сфері інформатики, бізнес-аналітики та когнітивних наук активно розробляється концепція гібридного інтелекту [117], яка у науковому дискурсі паралельно з'являється і як інтеграція людського та машинного мислення в процесах публічного управління. Застосування гібридного інтелекту у контексті залучення громадянського суспільства відкриває новий вимір про те, яким чином можливо збалансувати машинну ефективність з людською етикою, відповідальністю та участю.

Американські вчені Л. Беннетт та А. Зегерберг досліджуючи трансформацію громадянського суспільства у цифрову епоху [109]

акцентують на появі нових форм «мережевого активізму», гнучких структур самоорганізації, а також цифрових прав, зокрема права на дані, приватність та онлайн-участь. Проте у сучасних наукових джерелах не знайшли свого відображення питання впливу саме гібридного інтелекту на політичну суб'єктність громадян.

Таким чином, актуальність дослідження цієї проблематики полягає в необхідності інтегрувати концепт гібридного інтелекту у розвиток громадянського суспільства та публічного управління, враховуючи позитивні та негативні наслідки такої інтеграції. Невирішеними залишаються питання обґрунтування подальшої ролі та суб'єктності представників громадянського суспільства у публічному управлінні під впливом застосування технологій гібридного інтелекту.

Для осмислення трансформації громадянського суспільства в умовах застосування гібридного інтелекту необхідно розглянути кілька ключових концептів, що дозволяють структуровано проаналізувати взаємодію між людиною, державою та цифровими системами управління.

У традиційному розумінні громадянське суспільство – це сукупність незалежних від держави організацій, ініціатив та індивідів, що здійснюють контроль, мобілізацію та представлення інтересів громадян [112]. У цифровому контексті це поняття доповнюється такими новими формами як мережева діяльність, онлайн-активізм, діджитал-волонтерство та залучення суспільства до краудсорсингу державної політики [8]. Громадянське суспільство від посередника між громадянами і державою стає учасником вироблення державної політики цифрового розвитку.

Гібридний інтелект (hybrid intelligence) є системою взаємодії людини та штучного інтелекту, в якій обидві сторони доповнюють одна одну у прийнятті рішень. У публічному управлінні ця концепція вказує на поступове делегування частини адміністративних функцій алгоритмічним системам при збереженні людського контролю. На думку Д. Делерманна [117] гібридний інтелект передбачає кооперацію, де алгоритмічні потужності здатні

поєднуватися з людською етикою, емоційним та критичним мисленням.

Під алгоритмічним врядуванням (управлінням) розуміється використання автоматизованих систем (ШІ, машинного навчання та великих даних) для здійснення аналізу, прогнозування та прийняття державно-управлінських рішень. Алгоритмічне врядування трансформує владу, рішення якої можуть ухвалюватися поза людським контролем або без забезпечення достатньої прозорості [198]. У такій конфігурації виникають питання щодо необхідності забезпечення алгоритмічної відповідальності (responsibility), дискримінаційного ризику та підзвітності таких систем.

У теоріях цифрової демократії все більшого значення набуває поняття технократичного суспільства [145], яке функціонує завдяки здатності громадян діяти, реагувати та впливати на владу в умовах цифрової взаємодії з державою. Участь у петиціях, бюджетуванні, врядуванні через цифрові платформи, а також володіння знаннями про алгоритми відтепер постійно впливає на життя пересічних громадян.

Таким чином, поєднання класичного уявлення про громадянське суспільство з сучасними концептами гібридного інтелекту та алгоритмічного врядування (управління) дозволяє досліджувати не лише технологічну сторону цифровізації, а й політико-етичні наслідки такого делегування владних повноважень.

Поява гібридного інтелекту в державному управлінні створює не лише нові інструменти для залучення громадян, а й спричинює нові виклики щодо подальшого збереження демократичного контролю, етичної відповідальності та соціальної рівності. Розглянемо основні загрози, з якими стикається громадянське суспільство у новій технологізованій управлінській екосистемі.

1. *Алгоритмічна непрозорість та втрата підзвітності.* Більшість систем алгоритмічного врядування (управління) функціонують за принципом «чорної скриньки» – тобто логіка прийняття рішень залишається недоступною для громадськості, а іноді навіть для замовника (державних службовців), що може створювати дискримінаційну ситуацію, оскільки незрозумілим є

процедура ухвалення того чи іншого рішення (наприклад, це може бути не достатньо обґрунтована відмова в соціальній допомозі).

2. *Цифрова нерівність, виключність та елітизм.* Хоча цифрові технології потенційно розширюють доступ до участі громадян, на практиці вони можуть посилювати певну соціальну нерівність. Громадяни, які не володіють цифровими компетентностями, не мають належного доступу до інтернету та сучасних пристроїв (особливо на віддалених територіях) ризикують опинитися поза межами нових форм партисипації. Виникає ризик появи «цифрового елітизму», коли право голосу матимуть лише ті, хто володіє технічним знанням і ресурсами.

3. *Делегування та розмиття відповідальності.* Коли частина управлінських рішень перекладається на алгоритми, виникає проблема у становленні відповідального за помилкові або дискримінаційні рішення. Виникає необхідність щодо правового регулювання алгоритмічної відповідальності.

4. *Зменшення простору для громадського контролю.* Алгоритмізація процесів може звужити зону впливу та втручання для громадськості, оскільки автоматизовані рішення ухвалюватимуться без попередніх консультацій, відкритих слухань чи зворотного зв'язку. Якщо цифрова держава функціонує як технократична система, громадянське суспільство ризикує втратити не лише вплив, а й сенс свого існування як противага автократії влади.

5. *Ризик маніпуляцій та поширення цифрового популізму.* Гібридний інтелект, що використовується для аналізу громадської думки, соціальних мереж або участі в опитуваннях, може бути спрямований для планування тактичних, оперативних та стратегічних цілей. Однак, існує загроза «алгоритмічного популізму», коли цифрові дані використовуються для створення ілюзії урахування громадської думки.

Ці виклики вимагають переосмислення не лише технічних параметрів цифрового врядування, а й фундаментальних основ демократії в цифрову епоху: прозорості, участі, підзвітності та справедливості.

Попри численні виклики, які спричиненні цифровим розвитком державного управління, гібридний інтелект сприяє виникненню нових можливостей для розвитку громадянського суспільства як активного виробника державної політики. Результативне поєднання людського та машинного потенціалу здатне оптимізувати адміністративні процеси, та посилити громадську участь лише за умови відповідного нормативного, інституціонального та організаційного врегулювання.

Цифрові сервіси нового покоління (наприклад, «GovTech» та «CivicTech») дають змогу громадянам не лише інформувати державу про свої потреби, а й безпосередньо впливати на управлінські рішення шляхом проведення цифрових консультацій, опитувань, голосувань, краудсорсингу ідей. Успішний приклад тайванського «vTaiwan» (<https://info.vtaiwan.tw>) демонструє потенціал змістовної участі, коли цифрові інструменти слугують платформою для інклюзивного та раціонального діалогу між громадянським суспільством та державою.

Розробка та впровадження відкритого коду (open source) і відкритих алгоритмів (explainable AI) дає змогу громадянському суспільству здійснювати аудит цифрових процесів. Низка країн вже експериментує у сфері застосування незалежного аудиту до алгоритмічного управління. Залучення різних NGO, комітетів з етики та цифрових омбудсменів до перевірки автоматизованих систем III підсилює демократичний контроль і відновлює довіру до цифрової держави.

Громадянське суспільство відіграє ключову роль у формуванні цифрової грамотності, критичного мислення та обізнаності про права в діджитальному просторі. Розвиток цифрової емансипації означає перехід від пасивного користування сервісами до участі у створенні, удосконаленні та контролі алгоритмів публічного управління. Програми цифрової освіти, проведення «публічних хакатонів», а також популяризація етичного дизайну цифрових технологій є важливими інструментами посилення громадської участі.

Інноваційність підходів до вироблення політики цифрового розвитку

передбачає залучення громадськості ще на етапі розробки комплексних цифрових рішень. Моделі «co-design» або «participatory AI» дозволяють залучати громадян, активістів, експертів і розробників до спільного проектування алгоритмічних систем, що знижує ризик упередженості та зміщує фокус від технократичної ефективності до соціальної справедливості.

У гібридному середовищі з'являються нові спільноти самоорганізації громадян, наприклад децентралізовані автономні організації, блокчейн-ініціативи з управління спільними ресурсами, колективні краудфандингові платформи для здійснення місцевого самоврядування. Це дає змогу громадянському суспільству не лише реагувати на результати вироблення державної політики цифрового розвитку, а й генерувати альтернативні управлінські моделі політичних мереж, які можуть конкурувати між собою.

Таким чином, громадянське суспільство в умовах запровадження гібридного інтелекту постає не як пасивний спостерігач, а як активний учасник і співавтор цифрового розвитку країни. Його роль полягає в забезпеченні етичних, інклюзивних, та інших загальнолюдських цінностей, а також відповідальності в технократичному середовищі.

3.3 Технологічні перспективи та цифрові інструменти реалізації державної політики цифрового розвитку в Україні

Цифровізація публічного управління обов'язково передбачає маніпулювання суспільною свідомістю, однак нові діджитальні технології сприяють й самоідентифікації кожного індивіда. Повсюдність цифрових трансформацій спричинює зміни у масовій свідомості населення.

Одержуючи нові знання та маючи рівний доступ до будь-якої інформації в мережі, чому, безумовно сприяють соціальні медіа, люди усвідомлюють своє значення та нові можливості. Це ускладнює діяльність зовнішніх та внутрішніх маніпуляторів, яким стає набагато складніше впливати та маніпулювати цільовими аудиторіями країни.

Успішною в управлінській діяльності людиною майбутнього стане той, хто завдяки розвинутому системному мисленню, високому рівню креативних здібностей, особистісним комунікативним якостям, сформованій когнітивній гнучкості та досконалому опануванню цифровими технологіями вмітиме досягати необхідних результатів.

Зазначимо, що після опанування навичок цифрової грамотності та запровадження тотальної кіберосвіти відбудеться цифрова селекція суспільства, яке почне формуватися з інших людей, які й стануть суб'єктами нового «цифрового» суспільства.

Цифрова освіта повинна не тільки навчати, виховувати та сприяти просвітництву, а й формувати цінності та традиції українського суспільства. Однак, разом із здобуттям цифрової компетентності поряд з подоланням наслідків цифрового розриву відбувається формування віртуальної залежності у більшості населення, яка стає потужнішою за потреби у звичайних людських емоцій та спілкуванні наживо. Окрім того, постійна присутність індивіда в соціальних мережах й медіа-каналах сприяє його психологічній залежності від них та визначає його інформаційний вибір.

Вимушене дистанційне навчання стає фундаментальною основою реалізації сучасної освіти, яке разом із зручністю, несе цілий спектр різних ризиків. Більшає тих, хто під час навчання воліє шукати потрібну інформацію онлайн, а не на сторінках паперових підручників.

Відсутність основних засад вироблення державної політики у сфері розвитку цифрових навичок та цифрових компетенцій громадян не дозволяє на належному рівні забезпечити в Україні розвиток усіх сфер суспільного життя відповідно до сучасних вимог, процесів глобальної цифровізації економіки, сфер життєдіяльності суспільства, які відбуваються у більшості країн світу, а тому виникає необхідність забезпечення готовності суспільства до таких процесів, опанування населенням належного рівня цифрової компетентності.

Кібербезпека цифрового середовища набуває особливого актуального

значення для сучасного українського суспільства. Основним завданням розвитку Національної системи кібербезпеки є підвищення рівня її ресурсної спроможності задля гарантування стійкості функціонування цифрової інфраструктури органів державної влади та безпеки всього кіберпростору України.

Посилення ресурсних спроможностей Національної системи кібербезпеки повинне відбуватися завдяки усвідомленню населенням України існуючих безпекових викликів та загроз в цифровому середовищі, вмінню користуватись сучасними безпековими кіберзасобами та удосконалювати навички цифрової гігієни.

Під час стрімких глобальних трансформацій зростає інтерес до наукового осмислення та технологічного конструювання цифрових рішень, здатних визначити майбутню архітектуру цифрового врядування. Наукові інституції, міжнародні організації та провідні корпорації ІТ-індустрії впроваджують нові підходи до інтелектуалізації управлінських процесів, насамперед через створення автономних систем ухвалення рішень, самокерованих інтерфейсів та децентралізованих цифрових платформ. Ці інновації поступово виходять за межі суто прикладного технічного виміру й трансформуються в елементи нової техносоціальної реальності, яка змінює уявлення про природу публічного управління, державну організацію та способи взаємодії громадян з владними інституціями. У цьому контексті цифрові технології модернізують державно-управлінські функції та стають каталізаторами змін та переосмислення суспільно-владних відносин, визначають роль органів влади в еволюційних процесах, а також здійснюють переформатування логіки публічного управління в умовах не тільки постіндустріального, а вже постцифрового суспільства.

В 2024 році Всесвітній економічний форум оприлюднив аналітичний звіт щодо десяти проривних технологій, які здатні змінити соціальні, економічні та управлінські практики упродовж найближчих п'яти років [191]. У звіті, побудованому на основі аналізу понад 300 пропозицій експертів з

усього світу на основі даних про інвестиційні та наукові тренди, особливо відзначено ті технології, які можуть мати значний вплив на трансформацію публічного управління, зокрема: технології збереження приватності, реконфігуровані інтелектуальні поверхні, інтегровані сенсори, імерсивні технології тощо. У звіті «The Future of Jobs Report 2025» здійснено аналіз змін глобального ринку праці під впливом технологічних, макроекономічних, екологічних та демографічних змін, які становляться визначальними драйверами трансформації сфери зайнятості населення до 2030 року [135].

На підставі аналізу звіту *Stanford Emerging Technology Review 2025* [178], можемо виокремити технології, які є не лише науковими проривами, що можуть істотно трансформувати публічне управління, а й стають векторними чинниками розвитку цифрової держави, сприяючи формуванню нових підходів до вироблення державної політики та захисту національних інтересів України та суспільного добробуту.

У межах наукового дискурсу науки державного управління такі технології доцільно розглядати як інструменти цифрового розвитку функціонування органів публічної влади, що впливають на результативність, ефективність, транспарентність та інноваційність національної економіки. Серед перспективних технологій, які поступово стають інструментами публічного управління, можемо відзначити:

- *штучний інтелект* (перевагами є здатність до автоматизованої обробки великих обсягів даних, аналітичного супроводу управлінських рішень, моделювання альтернативних сценаріїв вироблення державної політики та забезпечення когнітивної взаємодії між системою і користувачем);
- *криптографія разом з постквантовими алгоритмами та технологіями конфіденційних обчислень* (є фундаментальним інструментом захисту цифрової ідентичності громадян, безпечної роботи інтегрованих державних реєстрів та забезпечення надійності цифрових сервісів);
- *лазерні технології моніторингу та діагностики*. (можуть стати основою інфраструктури «розумних міст», підтримуючи роботу аеро-фото-

ГІС-систем, безконтактного вимірювання рівня забруднення та аналітики об'єктів критичної інфраструктури задля підвищення якості життя громадян);

– *біосумісні сплави, сенсорні пластмаси та 3D-конструкції* (здатні знизити витрати на будівництво критичної інфраструктури та мають значний потенціал для використання у сфері виробництва військових технологій); нейротехнології (відкривають нові горизонти оптимізації процесів прийняття рішень, прогнозування суспільної поведінки та адаптації державних сервісів під потреби громадян, створюючи більш інклюзивну систему управління); автономні, мобільні, маніпулятивні інтелектуальні роботи та дрони з комп'ютерним зором і автономною логістикою (інструменти екстреного реагування, дистанційного моніторингу й автоматизованого управління задля зміцнення цифрової стійкості держави).

– *технології* децентралізованої генерації, зберігання та споживання енергії (адаптивні моделі енергоуправління, стратегій енергетичної незалежності та кліматичної адаптації критичної інфраструктури).

На основі аналізу звіту «Everybody is Looking into the Future!» [134], який здійснено в рамках спільного проєкту прогнозування нових технологій та революційних інновацій «ANTICIPINNOV» Європейської інноваційної ради і Дослідницького центру Європейської Комісії можемо виокремити у окремі групи пріоритетних технологій, які зможуть забезпечити подальший стрибкоподібний цифровий розвиток України в умовах євроінтеграційних процесів у поствоєнний період:

1. Технології цифрової індустрії, як то: технології штучного інтелекту (для автоматизації сервісної діяльності органів публічної влади, аналізу кіберзагроз), квантових обчислень (для створення безпечних квантових каналів зв'язку між державними інформаційними системами), метасередовища (для навчання публічних службовців, візуалізації рішень та залучення громадян до просторового планування та діджитальних двійників (для моделювання розвитку територій, об'єктів інфраструктури та розрахунку еконавантаження).

2. *Зелені інновації* – технології, орієнтовані на: забезпечення високого рівня енергоефективності (розгортання розподіленої генерації енергії); декарбонізацію (за рахунок біоінженерії та ефективного управління ресурсами); регенеративного (відновлюваного) господарювання; моніторингу ґрунтів та водних ресурсів на основі IoT; застосування нових матеріалів (біобетон, низьковуглецевий цемент) у будівництві для зменшення викидів CO₂; впровадження систем цифрового управління транспортним трафіком у містах; використання алгоритмічного управління вітровими електростанціями; автоматизованого контролю за екосистемами.

3. *Цифрові інструменти у сфері охорони здоров'я* – технології, що інтегрують біоінженерію, персоналізовану телемедицину, нанотехнології та молекулярну робототехніку з використанням сенсорних пристроїв та інтернету для віддаленого моніторингу; застосування 3D-друку для виготовлення біоімплантів та тканин в рамках державних програм; формування цифрових медичних карток з використанням біочіпів та штучного інтелекту; застосування біообчислювальних систем у медичних закладах та центрах громадського здоров'я для моделювання реакцій на медикаментозне лікування; інклюзивна підтримка вразливих груп населення через інтегровані сенсорні рішення, що інтегруються в соціальні програми (наприклад, онкохворих).

4. *Технології збереження приватності* (Privacy-Enhancing Technologies, далі – PETs) – являють собою інноваційні технологічні рішення (набір інструментів, методів та підходів), що здійснюють збирання, зберігання, обробку та передавання інформації без розкриття ідентифікаційних характеристик особи (базуються на принципах анонімізації, криптографічного захисту, децентралізації обчислювальних процесів та є гомоморфно зашифрованими синтетичними даними. Основним напрямом розвитку збереження приватності PETs є технологія доведення з нульовим розголошенням (Zero-Knowledge Proofs, далі – ZKP), суть якої полягає в можливості підтвердити істинність певного твердження без необхідності

розкриття змісту самої інформації. Зазначений підхід забезпечує високий рівень безпеки даних у сфері публічного управління.

5. Інтегроване зондування та комунікації (Integrated Sensing and Communication, далі – ISAC), які поєднують функції сенсингу (моніторингу та збору інформації про навколишнє середовище) та передачі даних між пристроями у єдину технологічну платформу, що дозволить прискорити зв'язок (взаємодію) складових елементів критичної інфраструктури, підвищити енергоефективність територій, а також забезпечити швидку реакцію на зміни та адаптивну трансмісію сигналів у контексті динамічних управлінських сценаріїв.

Зазначимо, ISAC інтегрує процес виявлення та просторового визначення місцезнаходження пасивних (непідключених) об'єктів у мережу мобільного зв'язку, розширюючи функціональність мережі за межі простого зв'язку. Повторне використання більшої частини мережевого обладнання, розгорнутого для зв'язку, може забезпечити безперебійне впровадження ISAC [172] та широкий спектр нових послуг, таких як високоточна локалізація, розпізнавання жестів та активності, пасивне виявлення та відстеження об'єктів, а також візуалізація та реконструкція середовища («network as a sensor», мережа як датчик). З іншого боку, можливості високоточної локалізації, візуалізації та реконструкції середовища, отримані в результаті сенсорного зондування в режимі реального часу є важливим для втілення концепції цифрового двійника [102].

Варто зазначити, що активно впроваджуються у практику публічного управління блокчейн-технології для прозорості державних послуг, інтеграції децентралізованих реєстрів, інструменти токенизації державних активів і цифрових валют, а також Web3-рішення та генеративні моделі штучного інтелекту (GenAI) для автоматизації аналітичних процесів і підготовки управлінських рішень.

Зазначені технології не лише відповідають європейським нормативним орієнтирам, а й мають високий потенціал для масштабування в умовах

цифрового розвитку діяльності органів публічного управління.

У додатку А наведено функціонально-технологічні складові цифрового розвитку України.

Серед усього спектру перспективних технологій цифрового розвитку України, які на сьогодні є найбільш близькими до практичного впровадження у сфері публічного управління та на яких варто, на нашу думку зосередитись в розрізі першочергового впровадження, доцільно виокремити такі діджитальні рішення як: технології збереження ідентифікації та приватності без розкриття; технології нового покоління мобільного зв'язку та цифрових комунікацій, а також імерсивні технології.

Як зазначалося вище у сучасних умовах інтенсивної цифровізації публічного управління гостро постає питання захисту приватності громадян, особливо враховуючи стрімке зростання обсягів персональних даних, що обробляються органами державної влади та органами місцевого самоврядування. Виникає необхідність у запровадженні таких інструментів, які забезпечують ефективну обробку та аналіз даних без порушення норм конфіденційності, а також без додаткових ризиків, пов'язаних із кіберзагрозами, технічним та людським факторами. PETs стають базовим інструментом модернізації системи управління даними державного сектору. У публічному управлінні перспективним є використання синтетичних даних для моделювання адміністративних реєстрів з метою генерування аналітики або машинного навчання без застосування реальних персональних даних.

Гомоморфне шифрування забезпечує здійснення безпечної обробки зашифрованих даних, відкриваючи шлях до якісного нового рівня захищеності процесів цифрової взаємодії між державними установами без спільного доступу до персональних баз даних. Це є ключовим для реалізації концепції «інтероперабельності» інформаційних систем органів публічної влади та створення ефективної моделі обміну даними в рамках ідеї «держава як платформа».

Водночас розподілені системи машинного навчання і прийняття рішень

дозволяють обробляти управлінську інформацію без передачі «чутливих» даних за межі локальних мереж органів місцевого самоврядування, що має важливе значення для посилення автономії територіальних громад.

Інституціоналізація технологій захисту приватності забезпечує захист ідентифікації громадян, удосконалює процеси надання адміністративних послуг і оптимізує міжвідомчу взаємодію через захищені цифрові канали. У сфері охорони здоров'я ці технології дозволяють обробляти медичні дані без ризику розкриття лікарської таємниці, що є важливим для формування профілактичних програм і прогнозування ризиків епідеміологічних загроз. У цифровій освіті та соціальному захисті PETs сприяють персоналізації даних, зберігаючи при цьому їх конфіденційність. У сфері інформаційної безпеки вони застосовуються для аналізу відкритих джерел і виявлення інформаційних атак, не порушуючи конституційних прав та свобод громадян.

Водночас ефективне впровадження PETs вимагає оновлення організаційно-правових підходів до управління даними. Зокрема, необхідно впроваджувати технологічно нейтральне регулювання, яке дає змогу адаптуватися до технічних змін без частих змін нормативних актів. Важливим є закріплення принципу «приватність за дизайном» як обов'язкового елемента розробки нових цифрових рішень. Крім того, успіх імплементації PETs напряду залежить від розвитку цифрової культури публічних службовців, що включає панування не лише специфічних технічних навичок, а й розуміння етичних, правових та управлінських аспектів роботи з даними.

Технології збереження приватності стає не просто технічним інструментом захисту інформації, а й важливим механізмом впливу на формування довіри до державних інституцій. Ці технології сприяють підвищенню рівня транспарентності процесів цифрового розвитку публічного управління, особливо в умовах повоєнного відновлення України та її євроінтеграції. PETs можуть стати стратегічним ресурсом для вироблення державної політики цифрової доброчесності, яка об'єднуватиме спільні інтереси держави та людини. Натомість, технологія доведення з нульовим

розголошенням відкриває нові можливості для створення конфіденційних цифрових сервісів без розкриття персональних даних, що суттєво знижує ризики витоку інформації та несанкціонованого доступу. ZKP також має значний потенціал у сфері онлайн голосування, поєднуючи анонімність виборця з достовірністю результатів, що може зміцнити довіру до інструментів цифрової демократії. Крім того, ця технологія розширює можливості у сфері публічних фінансів, оскільки ZKP може гарантувати прозорість і правомірність транзакцій, контрактів і тендерів без розкриття комерційної інформації. Наприклад, це забезпечує баланс між відкритістю закупівельних операцій та захистом економічних інтересів учасників тендерних процедур.

Важливою для ZKP є реалізація концепції самокерованої ідентичності («self-sovereign identity»), завдяки якій користувач контролює доступ до своїх даних і передає лише необхідну інформацію під час здійснення кожної адміністративної процедури. Водночас впровадження ZKP вимагає комплексного оновлення нормативної бази, технічних стандартів і опанування фахівцями певних цифрових компетенцій, зокрема щодо розуміння криптографічного захисту. У контексті гармонізації українського законодавства з нормативними актами ЄС (Digital Europe Programme, AI Act), застосування ZKP є значущим інструментом зміцнення цифрового суверенітету та відповідності європейським стандартам у сфері кібербезпеки та захисту приватності. У рамках розвитку європейського цифрового простору та впровадження eIDAS 2.0 Україна має унікальну можливість інтегрувати ZKP у національні системи ідентифікації, зокрема Дія.ID.

Розкриваючи переваги застосування технологій інтегрованих сенсорних та комунікаційних систем як інструменту цифрового розвитку публічного управління зазначимо, що вони відкривають нові можливості для модернізації транспортного, енергетичного та телекомунікаційного секторів критичної інфраструктури, забезпечуючи безперервний моніторинг та швидке реагування на можливі відхилення, що особливо важливо в умовах гібридних

загроз і збройної агресії проти України.

У процесі управління містом ISAC-технології слугують основою смарт-інфраструктури, дозволяючи автоматично відстежувати рівень забруднення та шуму, рух громадського транспорту тощо. Одержані дані сприяють об'єктивному аналізу та відповідно ухваленню обґрунтованих рішень у сфері планування, екології та організації міських сервісів (наприклад, від інтелектуального освітлення до транспортної логістики). В екологічній сфері ISAC забезпечують високий рівень верифікації даних про шкідливі викиди, стан якості ґрунтів і води, передаючи відповідні показники у режимі реального часу до міських центрів обробки інформації. Це підвищує достовірність даних екологічного моніторингу та дозволяє застосовувати необхідні превентивні заходи. Також, такі системи сприяють ухваленню інтелектуальних рішень щодо управління громадським транспортом.

У сфері охорони здоров'я сенсорні мережі допомагають контролювати різні критично важливі індикатори функціонування медичних закладів (від заповненості пацієнтами до умов мікроклімату, що дає змогу змодельовати їхню готовність до надзвичайних ситуацій, зокрема пандемій.

Технології ISAC не лише розширюють технічні можливості управління, а й формують нову архітектуру цифрового врядування – чутливу до змін, побудовану на емпіричних даних, орієнтовану на довіру та швидке реагування. У перспективі вони стають основою адаптивного та стійкого публічного адміністрування в умовах високої технологічної динаміки.

Інтенсифікація цифрового розвитку публічного управління супроводжується зростаючою потребою в нових підходах до просторового планування, управління міським середовищем, архітектурного та інфраструктурного моделювання. Одним із таких підходів, що поєднує технологічну інноваційність із підвищенням прозорості управлінських рішень, є використання імерсивних технологій, зокрема засобів віртуальної, доповненої та змішаної реальності. Їх застосування в державно-управлінському процесі передбачає створення цифрових моделей територій та

об'єктів – так званих цифрових твінів (двійників), які надають можливість візуалізувати різні альтернативи розвитку, моделювання сценаріїв, а також верифікацію управлінських рішень на етапі їх підготовки. Така практика посилює обґрунтованість просторового управління та забезпечує його відповідність реальним потребам громадян.

Для стратегічного планування використання таких технологій створює додаткові можливості, зокрема через інституалізацію цифрових механізмів партисипації. Візуалізація урбаністичних проєктів у форматі тривимірного цифрового моделювання підвищує прозорість прийняття рішень, полегшує комунікацію з громадськістю та дозволяє враховувати соціальні, екологічні та транспортні аспекти ще до початку реалізації запланованих проєктів. Здатність імерсивних середовищ акумулювати просторову інформацію з реєстрів, кадастрів, транспортних і сервісних систем сприяє формуванню єдиного аналітичного поля для діяльності місцевих органів влади. У цьому контексті технології доповненої реальності виконують функцію інтегративного середовища для управління урбанізованим простором, де цифрові дані стають активним ресурсом управлінської взаємодії.

У сфері інфраструктурного розвитку імерсивні рішення дозволяють моделювати об'єкти ще до початку їхнього будівництва, тим самим знижуючи ризики проєктних помилок, оптимізуючи бюджетне планування та забезпечуючи ефективну взаємодію між учасниками інфраструктурного процесу – органами публічної влади, підрядниками та громадою. Застосування технологій цифрового моделювання набуває особливої ваги в межах реалізації проєктів державно-приватного партнерства, оскільки дозволяє здійснювати симулятивну оцінку економічної доцільності, технічної реалізованості та соціального впливу кожного інфраструктурного рішення. В результаті застосування імерсивних технологій підвищується рівень довіри між суб'єктами публічного управління, а також легітимності процесу прийняття рішень і забезпечується реалізація державної політики цифрового розвитку у сфері інвестицій та будівництва.

Імерсивні технології також формують нову модель експлуатації та технічного моніторингу об'єктів державної та комунальної власності. Створення цифрових твінів (двійників) дозволить здійснювати дистанційні інспекції технічного стану будівель і споруд, оптимізувати планові та позапланові ремонти, а також підвищувати рівень готовності до виникнення надзвичайних ситуацій. Управління активами, яке реалізовано на основі імерсивних середовищ, забезпечує своєчасний доступ до даних про об'єкт, автоматизоване формування технічної документації, а також моніторинг життєвого циклу кожного об'єкту з урахуванням енергетичних, екологічних та соціальних факторів. Така модель сприяє ефективному витрачання бюджетних ресурсів, скороченню часу на інспекційні дії та переходу до превентивного управління публічними.

Значний потенціал імерсивні технології мають і в контексті розвитку кадрового забезпечення публічного управління. Імерсивні симулятивні середовища дозволяють створювати нові умови професійного навчання, у яких відпрацьовуються різні складні сценарії управління об'єктами щодо дотримання умов безпеки, використання спеціалізованих цифрових інструментів тощо. Це сприяє підвищенню якості підготовки фахівців у сфері урбаністики та місцевого управління. За умов обмеженості доступу до об'єктів або специфічного обладнання, симулятивне навчання стає ефективною альтернативою традиційному навчанню та може бути інтегроване у процес підготовки здобувачів вищої освіти за спеціальністю D4 «Публічне управління та адміністрування», зокрема в рамках магістерських освітньо-професійних програм з цифрового врядування.

Забезпечуючи візуалізацію урбаністичних, екологічних чи інфраструктурних рішень, імерсивні технології сприяють поглибленню участі громадян в ухваленні рішень та удосконалюють існуючий інструментарій цифрової демократії. Через можливість наочного ознайомлення з потенційними змінами в середовищі проживання, громадяни отримують інструмент не лише для висловлення позиції, але й для її аргументації в межах

демократичних процедур. Відтак зростає рівень публічної легітимності управлінських рішень, зміцнюється довіра до діяльності органів публічної влади, а сам процес публічного управління стає гнучким та чутливим до зворотного зв'язку з населенням.

Імерсивні технології виступають не лише як засіб технологічного оновлення інструментарію цифрового врядування, а як складова формування нової парадигми просторового управління, орієнтованого на сталий розвиток, ефективність, партисипативність і відкритість. Успішна інтеграція цих технологій потребує нормативного закріплення статусу цифрових твінів як управлінського інструменту підтримки інноваційних рішень у діяльності органів публічної влади. У стратегічній перспективі такі технології можуть стати платформою для інтеграції просторових, аналітичних і управлінських процесів у єдине адаптивне цифрове середовище публічного управління в Україні.

Цифрові твіни є віртуальною копією певного процесу, ресурсу, системи або фізичного простору, яка динамічно відображає та імітує поведінку свого реального аналогу. Завдяки сучасному програмному забезпеченню моделювання можна зрозуміти прогнозовану поведінку цифрового твіна в певних умовах. Тобто, відстежується, яким чином цифровий твін реагує на зміни навколишнього середовища або цілеспрямовані впливи на нього [93]. У широкому сенсі технологія цифрових твінів є процесом використання потоків даних для створення цифрового представлення реального активу з метою покращення співпраці, доступу до інформації та прийняття рішень. Іншими словами, завдяки поєднанню технології моделювання та даних, зібраних з датчиків та моніторингових записів, створюється віртуальний твін справжнього об'єкта чи процесу [160].

Цінність цифрових твінів полягає у здатності працювати з достовірними даними та прогнозними моделями. Зокрема, моделювання цифрових копій територіальних громад дозволяє відстежувати зміни забудови, стан довкілля, транспортну доступність і якість інфраструктури, що сприяє ухваленню

обґрунтованих рішень у містобудуванні, землекористуванні та екологічному регулюванні.

У межах політики відкритих даних і концепції Smart City цифрові твіни сприяють створенню сервісів реального часу, що потребує інтеграції інформаційних систем, стандартизації даних, застосування хмарних технологій, а також підвищення рівня цифрових компетентностей публічних службовців. Особливе значення цифрові твіни мають для відновлення деокупованих територій, особливо під час ліквідації наслідків руйнувань. Завдяки використанню 3D-моделей можна візуалізувати довоєнний стан, визначити пріоритети необхідної відбудови, оцінити та запланувати обсяги відновлювальних робіт, а також оптимізувати та зробити прозорими необхідні фінансові витрати, що критично важливо для контролю з боку громадськості та здійсненню моніторингу виділеної міжнародної допомоги задля збереження суспільної довіри. Цифрові твіни створюють основу для публічного управління на базі даних («data-driven governance») та підвищують якість вироблених рішень.

У контексті цифрового розвитку діяльності органів державної влади технології зв'язку і діджитальних комунікацій нового покоління відіграють визначальну роль та уособлюють використання трьох взаємопов'язаних технологічних рішень: шостого покоління мобільного зв'язку (далі – 6G), реконфігураційних інтелектуальних поверхонь (Reconfigurable Intelligent Surfaces, далі – RIS) та висотних платформних станцій (High Altitude Platform Stations, далі – HAPS). Комплексне застосування цих рішень створює передумови для формування проривної інфраструктури майбутнього, здатної підтримувати передові сервіси цифрової держави, забезпечувати гнучкість, просторовість та інклюзивність публічного управління. У сукупності ці комплексні діджитальні рішення формують інноваційну архітектуру комунікаційного середовища, що має потенціал стати основою сервісної та децентралізованої системи цифрового врядування в Україні.

Технологія 6G забезпечує надвисоку пропускну здатність, мінімальну

затримку сигналу та гіпермасштабоване підключення пристроїв, створює умови для реалізації когнітивно-чутливих функцій публічного управління, зокрема в галузі моніторингу, кризового реагування, кібербезпеки та розумного планування територій у режимі реального часу. Це вже не просто шосте покоління мобільності, а еволюційне вдосконалення характеристик мереж зв'язку, передусім – фундаментальна зміна побудови комунікаційної взаємодії, що передбачає симбіоз фізичного, цифрового та когнітивного просторів. У порівнянні з попередніми поколіннями, 6G забезпечує терабітну швидкість передачі даних, ультранизьку затримку (менше 1 мілісекунди), високу щільність підключень (до 10 млн пристроїв на квадратний кілометр), а також інтеграцію з системами штучного інтелекту, квантової криптографії, доповненої реальності, цифрових твінів і розподілених обчислень. Це створює якісно нові можливості для реалізації управлінських функцій у реальному часі, зокрема в таких напрямках як прогнозно-сценарне моделювання, автоматизоване управління інфраструктурою, ситуаційне регулювання державно-управлінських процесів та безперервна аналітика великих даних у межах державних реєстрів.

Однак повноцінне розгортання потенціалу 6G вимагає доповнення його функціональними інструментами керованого формування середовища передачі сигналу. У цьому контексті технологія RIS виконує роль ключового елементу фізичного середовища цифрової трансформації, оскільки дозволяє керовано змінювати властивості поверхонь (відбивання, заломлення, фазове зміщення електромагнітних хвиль), тим самим перетворюючи пасивні об'єкти інфраструктури (будівлі, споруди, архітектурні фасади) у активні компоненти комунікаційної системи. У публічному управлінні це відкриває можливості для забезпечення безперервного зв'язку в урбанізованих середовищах, де традиційна мережа часто зазнає перешкод; для інтелектуального управління інформаційними потоками; для посилення функціонування «розумних» об'єктів державної власності, а також для екологічного зменшення енергоспоживання в процесі цифрового обміну. Поєднання 6G і RIS

забезпечує стійке високошвидкісне покриття навіть у щільно забудованих територіях або в умовах динамічного навантаження на мережу. Це створює передумови для функціонування смарт-сервісів на рівні громад, ефективного адміністрування міської інфраструктури, впровадження партисипативного планування з використанням технологій доповненої реальності, а також безпечного доступу громадян до персоналізованих публічних послуг.

Третій компонент інтегрованої зв'язкової архітектури – HAPS – виконує критичну функцію забезпечення цифрової присутності держави у важкодоступних або стратегічно важливих територіях, виконуючи роль мобільних ретрансляторів та інтелектуальних вузлів розподіленого зв'язку. Завдяки розміщенню на висотах 18–25 км, HAPS-системи забезпечують широке та гнучке покриття без потреби у розгалуженій наземній інфраструктурі, що має важливе значення для забезпечення зв'язку у гірських, прикордонних або на деокупованих територіях, для оперативного розгортання сервісів у випадках надзвичайних ситуацій, а також для підтримки інтегрованих систем безпеки, територіального моніторингу, екологічного контролю та геопросторового адміністрування. HAPS можуть забезпечити швидке розгортання публічних сервісів, підтримку ресурсів цифрового врядування на рівні територіальних громад, а також гнучке управління ресурсами в умовах недостатньо розвиненої наземної інфраструктури.

У функціональній взаємодії «6G–RIS–HAPS» формується нове інтелектуальне-комунікаційне середовище публічного управління, яке характеризується здатністю до автономної адаптації, децентралізованої координації та сервісної орієнтації. Така інфраструктура може забезпечити: підтримку соціально-чутливих державних послуг та реагування на потреби громадян; цифровий розвиток систем прогнозування соціально-економічних ризиків через обробку даних у режимі реального часу; розгортання платформ цифрової партисипації населення з підтримкою доповненої реальності; формувати нові канали доступу до адміністративних послуг для вразливих або ізольованих груп населення.

Водночас впровадження комплексного середовища «6G–RIS–HAPS» вимагає оновлення нормативно-правового регулювання, включно з адаптацією стандартів спектральної політики, визначенням етичних рамок використання персоналізованих сервісів, розробкою інституційних механізмів координації управління інформаційною інфраструктурою та створенням моделей державно-приватного партнерства в секторі інтелектуального зв'язку. Особливого значення набуває розвиток цифрової компетентності публічних службовців, спроможності громад до керування локальними RIS-рішеннями, а також гармонізація державних стратегій цифрової трансформації з глобальними стандартами 6G. Таким чином, триєдина технологічна взаємодія комунікаційного середовища «6G–RIS–HAPS) є стратегічним активом цифрового розвитку публічного управління, який відкриває нові горизонти для досягнення діджитальної інклюзії, ефективності, відкритості та оперативної адаптивності адміністративних процесів органів публічної влади.

Висновки до розділу 3

1. Визначено основні траєкторії цифрового розвитку інформаційної безпеки у публічному управлінні з урахуванням інноваційних та еволюційних змін, охарактеризовано їх сутність, запропоновано механізми їх подальшої реалізації у сфері публічного управління, а саме:

- *«цифрова пропаганда»* (забезпечення балансу між захистом свободи слова і протидією дезінформації; вироблення нових механізмів верифікації контенту, протидії дезінформації та швидкого реагування на інформаційні загрози;. вдосконалення методів медіаграмотності, критичного аналізу й перевірки джерел інформації);

- *«цифрові альянси»* (забезпечення оптимального балансу між збереженням інформаційної суверенності та необхідністю міжнародної координації в галузі інформаційної безпеки; ухвалення національної стратегії цифрової дипломатії задля міжнародної співпраці та забезпечення захисту

національних інтересів України; удосконалення державної системи інформаційної безпеки задля гарантування її стійкості до зовнішніх і внутрішніх інформаційних загроз; створення цифрових коаліцій та здійснення стратегічної координації між державами у сфері інформаційної безпеки через обмін аналітичними даними, узгодження дій та розробку спільних стандартів для протидії дезінформації);

- *«цифрова радикалізація»* (адаптація державної політики до нових можливостей меметичного програмування у сфері масового створення маніпулятивного контенту й діпфейків з метою розробки більш ефективних інструментів забезпечення національної безпеки; впровадження регуляторних норм щодо використання ШІ в медіа, що створить правову основу для контролю їх застосування в інформаційному просторі);

- *«цифровий контроль»* (протидія приватним компаніям/корпораціям, які у власних інтересах маніпулятивно визначатимуть доступний для громадян інформаційний контент; інвестування в розробку державних алгоритмів для розпізнавання дезінформації, що дозволить швидше виявляти маніпуляції й фальшиві новини, а також оперативно реагувати на інформаційні атаки; забезпечення балансу інформаційної відкритості та захист національного інформаційного простору через створення національних цифрових платформ, які зменшать залежність від зовнішніх ресурсів і посилять контроль держави над внутрішнім інформаційним середовищем).

Доведено, що сучасна еволюція інформаційних воєн завдяки багатовимірності цифрового розвитку публічного управління потребує комплексного підходу до забезпечення ефективного реагування на створення нового високотехнологічного рівня загроз у сфері інформаційної безпеки України.

Запропоновано практичні рекомендації щодо удосконалення регуляторно-правових механізмів вироблення державної політики цифрового розвитку у сфері протидії поширенню дезінформації, а саме:

- здійснення моніторингу діяльності національних цифрових

платформ (забезпечення прозорості алгоритмів та проведення аудиту функціонування);

- контроль використання ІІІ в медіа (маркування контенту, унормування правил та сфер використання дипфейків);
- обмеження віральності фейкового контенту (обмеження сфери охоплення, попередження про сумнівність перед поширенням);
- протидія бот-мережам (верифікація акаунтів, блокування ботів, аудит соціальних платформ);
- адміністративний контроль з боку державних регуляторів (визначення процедур оскарження, забезпечення громадського контролю);
- забезпечення прозорості політичної реклами (з обов'язковим розкриттям інформації про замовників, джерел фінансування та інструментів мікротаргетингу політичної агітації);
- запровадження архіву політичної реклами.

Обґрунтовано, що результативне ведення інформаційної війни визначатиметься спроможністю державних інституцій адаптуватися до умов функціонування цифрового суспільства, ефективно протидіяти інформаційним загрозам через зміцнення технологічного потенціалу та здатністю стейкхолдерів державної політики сформувати стратегічні підходи до управління інформаційним простором. Необхідним вбачається створення інституціоналізованої системи співпраці між державними органами України, великими технологічними корпораціями ІТ-індустрії та глобальними цифровими платформами, що дозволить оперативно реагувати на дезінформаційні кампанії, блокувати маніпулятивний контент та забезпечувати прозорість будь-яких алгоритмів.

Таким чином, сучасна динаміка розвитку інформаційних воєн вимагає від України комплексної державної стратегії, що поєднує інноваційні технології, нормативне регулювання, міжнародну кооперацію та активну участь громадянського суспільства у формуванні інформаційного імунітету.

Доведено, що новими формами цифрового розвитку публічного

управління є гібридний інтелект та алгоритмічне врядування, які можуть радикально змінювати умови існування і функціонування інституту громадянського суспільства, в результаті чого виникають нові можливості для залучення населення, підвищення прозорості та інноваційної співпраці з державою. Визначено основний ризик, що полягає у поступовій роботизації управління, коли автоматизовані системи змінюють усталені адміністративні процедури та механізми громадського контролю. За таких умов громадянське суспільство має адаптуватися до цифрової реальності та відігравати стратегічну роль у її формуванні, у якості захисника прав, свобод та прозорості у відносинах між людьми та машинами. Доведено, що демократія гібридного інтелекту неможлива без активної участі громадян, здатних розуміти, оцінювати, і впливати на алгоритми, які управляють процесами розвитку суспільного життя. Висунуто гіпотезу, що майбутнє публічного управління залежить не тільки від технологічних інновацій, а й від дієвого діалогу між громадянським суспільством і державою щодо меж, принципів і цілей цифрового розвитку. Перспективним напрямом подальших наукових досліджень вбачається створення моделей спільного алгоритмічного управління (co-government), механізмів аудиту, гібридного управління та способів захисту цифрових прав і свобод у пост алгоритмічному суспільстві.

Запропоновано перспективні комплексні технологічні рішення цифрового розвитку галузі публічного управління (технології збереження приватності без розкриття ідентифікаційних характеристик особи; технології зондування та комунікацій; інтегровані технології нового покоління зв'язку, цифрові твіни та інші імерсивні технології візуалізації та моделювання різних інфраструктурних об'єктів), які розширюють можливості комунікаційного середовища органів публічної влади, формує нову інтелектуальну, адаптивну та стійку архітектуру цифрового врядування – чутливу до змін, захищену від загроз зовнішнього втручання, побудовану на емпіричних даних, орієнтовану на довіру та швидке реагування. Обґрунтовано, що гібридний інтелект та алгоритмічне врядування здатні радикально трансформувати взаємодію

органів публічної влади з інститутами громадянського суспільства, в результаті чого виникають нові можливості для залучення населення, підвищення прозорості та інноваційної співпраці з державою.

Рекомендовано використовувати перспективні технологічні рішення цифрового розвитку у різних сферах галузі публічного управління, зокрема:

- *технології збереження приватності без розкриття ідентифікаційних характеристик особи (PETs)* на основі криптографічних алгоритмів та синтетичних даних із застосуванням методу доведення одного твердження іншому з нульовим розголошенням (ZKP) – генерування аналітики без застосування персональних даних; реалізації концепції самокерованої ідентичності («self-sovereign identity»); створення конфіденційних цифрових сервісів; захист анонімності онлайн-голосування для виборців; забезпечення балансу між відкритістю операцій та захистом економічних інтересів учасників публічних закупівель; впровадження у національну систему ідентифікації (Дія.ID) в рамках розвитку європейського цифрового простору та eIDAS 2.0.

- *інтегрування технології зондування та комунікації (ISAC)* – прискорення взаємодії складових елементів інфраструктурних об'єктів; підвищення енергоефективності окремих територій; удосконалення транспортного, енергетичного та телекомунікаційного секторів критичної інфраструктури; модернізація смарт-інфраструктури (автоматизоване відстеження рівня забруднення повітря та шуму, якості ґрунтів і води, управління інтелектуальним освітленням та транспортною логістикою, контроль критично важливих індикаторів функціонування медичних закладів);

- *імерсивні технології візуалізації та моделювання, зокрема цифрові твіни (Digital Twins), які забезпечують симулятивно-аналітичну інтеграцію фізичного та віртуального середовищ* – стратегічне планування; моделювання ситуацій для прийняття управлінських рішень, візуалізації їх наслідків та оптимізації використання ресурсів; використання у сфері просторового

планування, управління інфраструктурою, моніторингу об'єктів критичної інфраструктури, розробки стратегій сталого розвитку, а також у галузях охорони здоров'я, освіти, енергетики, енергопостачання та транспорту.

– *інтегровані технології нового покоління зв'язку як платформи комплексного застосування шостого покоління мобільного зв'язку (6G), реконфігураційних інтелектуальних поверхонь (RIS) та висотних платформних станцій (HAPS)* – підтримка соціально-чутливих державних послуг та реагування на потреби громадян; цифровий розвиток систем прогнозування соціально-економічних ризиків через обробку даних у режимі реального часу; розгортання платформ цифрової партисипації населення з підтримкою доповненої реальності; формування нових каналів доступу до адміністративних послуг для вразливих або ізольованих груп населення.

Основні результати розділу 3 опубліковано в науковій праці автора:

1. Карпенко О.В., & Герман Д.В. (2021). Цифрова грамотність населення як складова підвищення ресурсної спроможності Національної системи кібербезпеки України. Актуальні питання застосування спеціальних інформаційно-телекомунікаційних систем: матеріали науково-практичної конференції студентів, курсантів, аспірантів, докторантів та молодих вчених (15–16 червня 2021 року) – К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, С.112–113.

ВИСНОВКИ

У дисертаційній роботі вирішено нове наукове завдання, яке полягає у науково-теоретичному обґрунтуванні механізмів вироблення державної політики цифрового розвитку та розробленні перспективних рекомендацій щодо їх практичного використання в умовах збройної агресії проти України. В результаті проведеної роботи досягнута її мета та розв'язані поставлені завдання, що дозволяє зробити такі загальні висновки.

1. Розкрито існуючі наукові розробки українських та зарубіжних вчених щодо визначення сутності механізмів формування та реалізації державної політики цифрового розвитку, що дало змогу визначити наступну проблематику: недостатність опанування цифрових компетенцій публічними службовцями; неналежність забезпечення кібербезпеки критичної інфраструктури та захисту цифрових прав і свобод громадян. Визначено, що, подальших досліджень потребують: розробка механізмів адаптації кращих зарубіжних практик цифровізації до українських реалій; реалізація належної державної політики у сфері інтеграції України до єдиного цифрового ринку ЄС; визначення ключових інструментів здійснення цифрової та кібердипломатії; здійснення моніторингу соціально-економічних наслідків цифрової трансформації у розрізі регіонів України; дослідження етичних, правових та соціальних викликів, пов'язаних із впровадженням штучного інтелекту, в тому числі і як інструменту зниження корупційних ризиків у сфері публічних закупівель; перспективи застосування концепцій цифрократії та трансгуманізму в галузі публічного управління; виокремлення ключових напрямів та механізмів реалізації захисту державних інституцій від дезінформації; вироблення стратегічних напрямів державної політики цифрового розвитку України в умовах інтенсифікації ведення інформаційних воєн.

2. Проаналізовано особливості нормативно-правового забезпечення державної політики цифрового розвитку України, що дало змогу виокремити

його три основні етапи: усталення (інформатизація, 1998-2009 рр.), впровадження (електронного урядування, 2010-2017 рр.) та просування (цифрова трансформація, з 2018 р. по т.ч.). Констатовано зростання кількості та якості цифрових послуг/сервісів завдяки нормативному розширенню сфери застосування ІТ й можливостей їх онлайн надання. Здійснено аналіз нормативно-правового забезпечення державної політики цифрового розвитку України, яке є основою для розвитку людського потенціалу, цифрової економіки, формування цифрових компетентностей громадян у сфері державної кібербезпеки, розбудови цифрової демократії і ресурсного капіталу, забезпечення координації дій на рівні органів публічної влади. Виявлено неврегульованість реалізації цифрових комунікацій на місцевому рівні, що залишає невирішеними проблеми із забезпечення Інтернет-покриттям більшої частини авто- та залізничних магістралей, гірської місцевості та інших віддалених територій України. Обґрунтовано, що цифровий розвиток України повинен здійснюватися з урахуванням створення дієвої та ефективної нормативно-правової бази у цифровій сфері, насамперед для забезпечення: інформаційної прозорості діяльності органів публічної влади, законності та легітимності дій держави у віртуальному просторі, захисту основних інформаційних прав та свобод людини; зниження адміністративних бар'єрів і обмежень; відстоювання національних інтересів України у кіберпросторі. Запропоновано розвивати нормативно-правове забезпечення у таких сегментах цифрового розвитку як: захист конфіденційності даних через впровадження систем та алгоритмів штучного інтелекту; державно-приватне партнерство на основі людино-центричного підходу; розширення переліку доступних державних онлайн-послуг; розвиток цифрових компетентностей.

3. Визначено перспективи застосування концепцій цифрократії та трансгуманізму в галузі публічного управління, що дало змогу стверджувати, що цифрократія стає новою формою влади, яка дозволить трансформувати галузь публічного управління до нового інноваційного рівня суспільних відносин завдяки цифровим технологіям та комунікативним мережам

прийняття рішень. Цифрократія передбачає використання алгоритмів штучного інтелекту та інших технологій автоматизації процесів публічного управління та адміністрування. Обґрунтовано спільність/різницю наукових підходів щодо застосування концепцій «цифрократія» та «трансгуманізм». Доведено, що концепції цифрократії та трансгуманізму мають спільну мету – удосконалити та покращити життя людства за допомогою діджиталізації технологічного розвитку, але їх сфера та інструментально-функціональні підходи фокусуються на різній природі застосування. Зазначено, що методи, інструменти та засоби цифрократії орієнтовані на підвищення ефективності функціонування різних сфер суспільства (публічне управління, національна економіка, освіта, охорона здоров'я та ін.). Визначено, що концепція трансгуманізму завдяки застосуванню новітніх технологій спрямована на покращення фізичної та розумової природи людських можливостей (підвищення рівня інтелекту, подовження життя, удосконалення тіла та ін.).

4. Встановлено роль штучного інтелекту як суб'єкту державного управління завдяки аналізу можливостей алгоритмічного лобіювання впливати на прийняття рішень та змінювати механізми політичної взаємодії. На основі практичних прикладів застосування алгоритмічного впливу доведено його ефективність у формуванні громадської думки, а також небезпечність завдяки відсутності підзвітності, застосуванню алгоритмічного спотворення реальності та поступовому перетворенню держави на «цифрового заручника» маніпулятивних технологій. Надано рекомендації щодо формування багаторівневої системи регуляції алгоритмічного лобіювання та пропозиції щодо демократичного контролю за алгоритмами.

Визначено основні переваги застосування штучного інтелекту для зниження корупційних ризиків у сфері публічних закупівель на основі дослідження нормативних, організаційних та технологічних особливостей здійснення публічних закупівель у період дії правового режиму воєнного стану в Україні. Доведено, що для послідовного впровадження штучного інтелекту слід враховувати передусім переваги його технологій й алгоритмів,

які будуть використовуватися для зниження корупційних ризиків, підвищення ефективності та результативності публічних закупівель. Визначено основні переваги алгоритмів та технологій штучного інтелекту за умови їх впровадження у сферу публічних закупівель, що сприятиме заощадженню бюджету для замовників та/або отримання прибутку для постачальників (своєчасне та належне інформування потенційних учасників закупівельного процесу; моніторинг великих масивів даних відкритих тендерів; планування, здійснення аналітичної та прогностичної діяльності; роботизація трудомістких, рутинних, стандартних, типових та повторюваних операцій; оптимізація та/або узгодження внутрішніх операцій закупівельного процесу; розробка стратегій з управління закупівельним процесом). Доведено, необхідність використання чат-ботів, побудованих на основі спеціальних програмних рішень штучного інтелекту, які завдяки використанню технології «machine learning» зможуть аналізувати типові помилки та існуючі проблеми закупівельних процесів, допомагати учасникам відкритих торгів правильно заповнити та своєчасно подати свої пропозиції. Надано практичні рекомендації для максимізації рівня розробки оптимальних алгоритмів закупівельних процедур (вдосконалити механізм підготовки процедур відкритих торгів та укладання контрактів через впровадження системи оцінювання та аналізу даних попередніх торгів та контрактів; обирати роботи, товари і послуги, які краще підходять для проведення відкритих торгів, їх необхідний обсяг та оптимальну вартість за допомогою оптимізаційних алгоритмів та машинного навчання).

5. Розроблено прогностично-сценарну модель цифрового розвитку України, що представляє собою аналітично-ситуативну конструкцію з п'яти альтернативних сценаріїв («Незалежність та цифрове лідерство»; «Інтеграція та цифрова імплементація»; «Фрагментація та конвенціональна цифровізація»; «Автократія та цифрова ізоляція»; «Дезорганізація та цифрова деградація»), за якими здійснюється проєктування політичних, правових, інституціональних, організаційних, економічних, соціальних, технологічних,

інформаційних, ресурсних та інших механізмів вироблення (формування та реалізації) відповідної державної політики. У практичному вимірі прогностично-сценарна модель передбачає технологічну модернізацію цифрової інфраструктури країни, створення гнучких державних стратегій, а також трансформацію управлінської парадигми: від реактивного (кризового) адміністрування до динамічного, адаптивного, проактивного, стратегічно вмотивованого публічного управління, яке ґрунтується на застосуванні змішаних методів алгоритмічного прогнозування, форсайту, моніторингу, аналізі та оцінці даних, забезпеченні кіберзахисту та інституційної гнучкості.

Особливість дослідницького підходу до розробки прогностично-сценарної моделі полягає у поєднанні трьох функціональних вектор-чинників цифрового розвитку – *технологічного, інституційного та користувацького*, що сприятиме ефективності впровадження комплексних діджитальних рішень та їх обґрунтованості, доцільності, легітимності, інклюзивності та відповідності демократичним цінностям цифрового суспільства. Модель оперує кількома можливими перспективними підходами щодо подальшого цифрового розвитку: *«еволюційним поступом»*, *«адаптивним проривом»*, *«ризик-орієнтованою трансформацією»* та *«кооперативною інновацією»*.

Запропонована прогностично-сценарна модель цифрового розвитку України є концептуально-інструментальним підґрунтям стратегічного планування й наукового обґрунтування управлінських рішень, їх адаптації до тенденцій технологічної трансформації, ризиків глобальної нестабільності та довгострокових безпекових невизначеностей, що впливають на ефективність, результативність і стійкість функціонування органів публічної влади.

В умовах євроінтеграційних процесів, збройної агресії проти України та в умовах повоєнного відновлення модель сприятиме вчасній ідентифікації актуальних ризиків і критичних загроз, створенню ефективної системи їх раннього виявлення та попередження, розробці цифрових дорожніх карт та впровадженню адаптивних управлінських рішень, які посилять стійкість функціонування органів публічного управління.

6. Визначено основні траєкторії цифрового розвитку інформаційної безпеки у публічному управлінні («цифрова пропаганда», «цифрові альянси», «цифрова радикалізація» та «цифровий контроль») з урахуванням інноваційних та еволюційних змін, охарактеризовано їх сутність, запропоновано механізми їх подальшої реалізації у сфері публічного управління. Запропоновано практичні рекомендації щодо удосконалення регуляторно-правових механізмів вироблення державної політики цифрового розвитку у сфері протидії поширенню дезінформації, а саме: здійснення моніторингу діяльності національних цифрових платформ (забезпечення прозорості алгоритмів та проведення аудиту функціонування); контроль використання ІІІ в медіа (маркування контенту, унормування правил та сфер використання дипфейків); обмеження віральності фейкового контенту (обмеження сфери охоплення, попередження про сумнівність перед поширенням); протидія бот-мережам (верифікація акаунтів, блокування ботів, аудит соціальних платформ); адміністративний контроль з боку державних регуляторів (визначення процедур оскарження, забезпечення громадського контролю); забезпечення прозорості політичної реклами (з обов'язковим розкриттям інформації про замовників, джерел фінансування та інструментів мікротаргетингу агітації, запровадження архіву політичної реклами).

7. Запропоновано перспективні форми (гібридний інтелект та алгоритмічне врядування) та комплексні технологічні рішення (технології збереження приватності без розкриття ідентифікаційних характеристик особи; технології зондування та комунікацій; інтегровані технології нового покоління зв'язку, цифрові твіни та інші імерсивні технології візуалізації та моделювання різних інфраструктурних об'єктів) цифрового розвитку галузі публічного управління, що розширює технічні можливості комунікаційного середовища органів публічної влади, формує нову інтелектуальну, адаптивну та стійку архітектуру цифрового врядування – чутливу до змін, захищену від загроз зовнішнього втручання, побудовану на емпіричних даних, орієнтовану на довіру та швидке реагування.

Визначено пріоритетні сфери використання перспективних технологічних рішень цифрового розвитку галузі публічного управління (генерування аналітики без застосування персональних даних; реалізація концепції самокерованої ідентичності; створення конфіденційних цифрових сервісів; захист анонімності онлайн-голосування для виборців; забезпечення балансу між відкритістю операцій та захистом економічних інтересів учасників публічних закупівель; впровадження у національну систему ідентифікації (Дія.ID); взаємодія складових елементів інфраструктурних об'єктів; підвищення енергоефективності територій; удосконалення транспортного, енергетичного та телекомунікаційного секторів критичної інфраструктури; модернізація смарт-інфраструктури; стратегічне планування; моделювання ситуацій для прийняття управлінських рішень, візуалізації їх наслідків та оптимізації використання ресурсів; просторове планування; підтримка соціально-чутливих державних послуг; розгортання платформ цифрової партисипації населення з підтримкою доповненої реальності; формування нових каналів доступу до адміністративних послуг для вразливих або ізольованих груп населення).

З огляду на вищезазначене, виникає необхідність удосконалення механізмів вироблення державної політики цифрового розвитку в Україні, а саме першочерговим вбачається: включити до стратегічних цілей Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року необхідність адаптації українського законодавства до базових цифрових актів ЄС (AI Act, DGA, Data Act, eIDAS 2.0) з обов'язковими дорожніми картами щодо їх детальної імплементації; розробити Концепцію технологічного лідерства України у сфері цифрового розвитку; створити й інституалізувати систему моніторингу, аналізу, оцінювання, та прогностичного моделювання цифрової спроможності (зрілості) органів публічної влади; сформувати міжсекторальну раду з питань цифрового лідерства та етичного врядування, як дорадчого органу при Міністерстві цифрової трансформації України з функціями стратегічної експертизи щодо взаємодії з інституціями ЄС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Алгоритми «зради»: як штучний інтелект DoZorro знаходитиме порушення в ProZorro. URL: <https://ti-ukraine.org/news/algoritmy-zrady-yak-shtuchnyj-intelekt-dozorro-znahodytyme-porushennya-v-ProZorro/> (дата звернення: 14.04.2025).
2. Білик О. О. Формування та реалізація механізмів електронного управління регіональною системою освіти : монографія. Вінниця : ТОВ «НіланЛТД», 2024. 392 с. URL: <https://docs.academia.vn.ua/handle/123456789/1774> (дата звернення: 14.04.2025)
3. Васильців Т., Наконечна, Н. Інструменти державної політики активізації процесів діджиталізації туристичного комплексу України. *Herald of Khmelnytskyi National University. Economic Sciences*. 2024. № 326(1). С. 444-448. URL: <https://heralds.khmnua.edu.ua/index.php/heralds/article/view/432> (дата звернення: 14.04.2025)
4. Васюк Н. О. Трансформаційний механізм формування та реалізації державної політики у сфері охорони здоров'я : дис. ... канд. екон. наук : 25.00.02 / Васюк Наталія Олегівна ; М-во освіти і науки України, Київ. нац. екон. ун-т ім. Вадима Гетьмана. Київ, 2024. 573 с. URL: <https://ir.kneu.edu.ua/handle/2010/47585> (дата звернення: 14.04.2025)
5. Гаєвська Л. А., Васюк Н. О. Вітчизняний досвід реалізації державної політики цифрового розвитку (на прикладі сфери охорони здоров'я). Інвестиції: практика та досвід. 2025. № 6. С. 161-167. URL: <https://nayka.com.ua/index.php/investplan/article/view/5947/6010> (дата звернення: 14.04.2025)
6. Гончаренко В. Правові аспекти використання інформаційних технологій у публічному секторі. *Право України*. 2014. №3. С. 25–30.
7. Держаудитслужба починає моніторинг закупівель ProZorro з ризик-індикаторами. URL: <https://dozorro.org/news/u-prozorro-zapracuyovali-rizik-indikatori-dlya-poshuku-pidozrilih-tenderiv> (дата звернення: 14.04.2025).

8. Деякі питання діяльності підрозділів з питань цифрового розвитку, цифрових трансформацій і цифровізації центральних та місцевих органів виконавчої влади та заступників керівників центральних органів виконавчої влади, обласних, Київської та Севастопольської міських державних адміністрацій з питань цифрового розвитку, цифрових трансформацій і цифровізації: постанова Кабінету Міністрів України від 3 березня 2020 р. № 194. URL: <https://zakon.rada.gov.ua/laws/show/194-2020-%D0%BF#Text> (дата звернення: 14.04.2025).

9. Деякі питання підвищення рівня цифровізації сил безпеки та сил оборони України у період воєнного стану : Постанова Каб. Міністрів України від 04.02.2023 № 139. URL: <https://zakon.rada.gov.ua/laws/show/139-2023-п#Text> (дата звернення: 14.04.2025).

10. Деякі питання цифровізації діяльності державних органів : Постанова Каб. Міністрів України від 01.12.2023 № 1317 : станом на 11 берез. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/1317-2023-п#Text> (дата звернення: 14.04.2025).

11. Деякі питання цифрового розвитку : Постанова Каб. Міністрів України від 30.01.2019 № 56 : станом на 8 квіт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/56-2019-п#Text> (дата звернення: 14.04.2025).

12. Деякі питання цифрової трансформації : Розпорядж. Каб. Міністрів України від 17.02.2021 № 365-р : станом на 2 серп. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/365-2021-р#Text> (дата звернення: 14.04.2025).

13. Дорожня карта інтеграції України до Єдиного цифрового ринку ЄС. URL: <https://thedigital.gov.ua/projects/evrointegraciya/roadmap> (дата звернення: 17.02.2025)

14. Європейська декларація про цифрові права та принципи для цифрового десятиліття 2023/C 23/01. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOC_2023_023_R_0001 (дата звернення: 21.04.2025)

15. Інтеграція України у Єдиний цифровий ринок ЄС. Потенційні економічні переваги. URL: https://ucep.org.ua/wp-content/uploads/2021/01/dig_ukraine_eu_15.12.2020-_WEB_3.pdf (дата звернення: 17.02.2025)

16. Інформація про реформу публічних закупівель (2016). URL: <https://me.gov.ua/Documents/Detail?lang=uk-UA&id=1197d60b-5c7b-45ef-bf3a-e08d4cf11cba&title=InformatsiiaProReformupublichniZakupivli> (дата звернення: 14.04.2025).

17. Карпенко О., Животова К. Медійний простір та особливості реалізації державної політики протидії дезінформації в умовах воєнного стану. *Studenckie Prace Prawnicze, Administratywistyczne i Ekonomiczne. Wydawnictwo Uniwersytetu Wrocławskiego*. Wydawnictwo «Szermierz». 2023. Tom 45. P. 9-21. URL: <https://doi.org/10.19195/1733-5779.45.1> (дата звернення: 14.04.2025)

18. Карпенко О.В. Державна кіберосвіта та інструменти підвищення рівня цифрової компетентності населення України. *Вісник НАДУ. Серія "Державне управління"*. 2020. № 4 (91). С. 95–102.

19. Карпенко О.В. Про доцільність впровадження в Україні інституту цивілізованого лобізму державно-управлінських рішень. Демократичне врядування. Вип. 7. Львів: ЛПІДУ НАДУ. 2011. URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2022/feb/26956/karpenko.pdf> (дата звернення: 20.04.2025)

20. Карпенко О.В., Васюк Н.О., Осьмак А.С. Штучний інтелект як цифровий інструмент проектного підходу в місцевому самоврядуванні. *Стратегія економічного розвитку України*. 2024. № 55. С. 189-200. DOI: <https://doi.org/10.33111/sedu.2024.55.189.200> (дата звернення: 14.04.2025)

21. Карпенко О.В., Карпенко Ю.В., Осьмак А.С., Качмарський Є.І. Державна підтримка технологій штучного інтелекту у наданні медичної допомоги при онкологічних захворюваннях: досвід США. *Університетські наукові записки*. 2024. № 1(97), С. 59-71. DOI: <https://doi.org/10.37491/UNZ.97.5> URL: https://unz.univer.km.ua/article/view/97_59-7 (дата звернення: 14.04.2025)

22. Карпенко О.В., Федірко Н.В. Цифрова трансформація vs оптимізація: інноваційні можливості для держави та бізнесу в процесі здійснення публічних закупівель. *Економіка та підприємництво*. 2022. №48. С.39-58. DOI: https://doi.org/10.33111/EE.2022.48.KarpenkoO_FedirkoN (дата звернення: 14.04.2025)

23. Квітка С., Карпенко О. Вплив цифровізації на державне управління у сфері протидії міжнаціональним конфліктам. *Аспекти публічного управління*. 2022. №10(5). С. 62-68. DOI: <https://doi.org/10.15421/152236> (дата звернення: 14.04.2025)

24. Квітка С., Корсун В., Магиляс Ю. Цифрова трансформація публічного управління: перспективні напрямки досліджень. *Аспекти публічного управління*. 2024. №12(3). С. 50-58. DOI: <https://doi.org/10.15421/152437> (дата звернення: 14.04.2025)

25. Квітка С., Миргородська М. Цифрова трансформація системи охорони здоров'я: фактори впливу на якість життя населення. *Аспекти публічного управління*. 2024. №12(1). С.14-21. DOI: <https://doi.org/10.15421/152402> (дата звернення: 14.04.2025)

26. Квітка С., Новіченко Н., Бардах О. Штучний інтелект у муніципальному управлінні: вектори розвитку. *Аспекти публічного управління*. 2021. №9(4) С. 85-94. DOI: <https://doi.org/10.15421/152140> (дата звернення: 14.04.2025)

27. Квітка С., Рибченко А. Реалізація державної політики цифрового розвитку щодо боротьби з етнічними конфліктами. *Аспекти публічного управління*. 2022 № 10(6). С. 5-13. URL: <https://aspects.org.ua/index.php/journal/article/view/964/939> (дата звернення: 14.04.2025)

28. Квітка С., Титаренко О., Мазур О. Оцінка стану цифрового розвитку адміністративно-територіальних одиниць Дніпропетровської області. *Аспекти публічного управління*. 2019. №7(11). С.15-25. DOI: <https://doi.org/10.15421/151952> (дата звернення: 14.04.2025)

29. Кілієвич О. І. Державна політика цифрового розвитку як новий напрям інноваційної політики в умовах цифровізації економіки та інформатизації суспільства. *Прикладні системи та технології в інформаційному суспільстві*: зб. Тез доповідей і наук. повідомл. учасників V Міжнародної науково-практичної конференції (Київ, 30 вересня 2021 р.) / за заг. ред. В.Л. Плєскач, І.І. Гарко, В.Л. Міронової. К.: Київський нац. ун-т ім. Тараса Шевченка, 2021. 288 с. С.95-103. URL: https://www.researchgate.net/profile/Grigoriy_Gnatienko/publication/383500586_AISTIS_20211/links/66d079bdf84dd1716c70a5e7/AISTIS-20211.pdf#page=95 (дата звернення: 14.04.2025)

30. Коваленко Ю. Алгоритмічні моделі поведінки в системах штучного інтелекту. Моделювання та обчислювальні технології. 2016. №8 (3). С. 45–52.

31. Кужда Тетяна, Луциків Іванна. Дослідження стану та перспектив цифрового розвитку в Україні. *Галицький економічний вісник*. 2022. № 5–6 (78–79). С. 146-155. URL: <https://galicianvisnyk.tntu.edu.ua/pdf/78-79/1119.pdf> (дата звернення: 14.04.2025)

32. Луняк В. Шляхи вдосконалення механізмів публічного управління у сфері цифровізації в контексті забезпечення інноваційного розвитку. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2024. № (9). С. 84–90. URL: <https://pa.journal.in.ua/index.php/pa/article/view/158> (дата звернення: 14.04.2025)

33. Маматова Т., Chykarenko I., Chykarenko O., Kravtsova T., Kravtsov O. Information Systems in Project Management of The Public Sphere. *International Journal of Computer Science and Network Security*. 2021. Vol. 21. № 8. Р. 141–148. DOI: <https://doi.org/10.22937/IJCSNS.2021.21.8.19> (дата звернення: 14.04.2025)

34. Маматова Т., Чикаренко І., Бородин Є. Цифрові платформи Smart Specialisation Platform та Espon: структура та можливості для регіонів і громад ЄС. *Аспекти публічного управління*. 2022. №10(6). С. 37-45. DOI: <https://doi.org/10.15421/152242> (дата звернення: 14.04.2025)

35. Маматова Т., Чикаренко, І. Використання штучного інтелекту у процесах розвитку стратегічних і проєктних компетентностей публічних управлінців. *Публічне управління та місцеве самоврядування*. 2023. №4. С. 45–53. DOI: <https://doi.org/10.32782/2414-4436/2023-4-7> (дата звернення: 14.04.2025)

36. Мінцифра представила оновлену Дорожню карту інтеграції до Єдиного цифрового ринку ЄС. URL: <https://thedigital.gov.ua/news/mintsifra-predstavila-onovlenu-dorozhnyu-kartu-integratsii-do-edinogo-tsifrovogo-rinku-es> (дата звернення: 17.02.2025)

37. Мохова Ю. Л. Державні механізми розвитку електронного урядування в умовах цифрових трансформацій України. Дисертація на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.02 – механізми державного управління. Чорноморський національний університет імені Петра Могили, м. Миколаїв, 2021. 490 с. URL: <https://chmnu.edu.ua/wp-content/uploads/Disertatsiya-5.pdf> (дата звернення: 14.04.2025)

38. Нестерович В.Ф. Етимологія та феномен поняття «лобіювання»: гносеологічний вимір. Бюлетень Міністерства юстиції України. 2010. № 1. С. 40-51.

39. Никифоров А. Є. Інструментарій сервісно-орієнтованих механізмів цифрового урядування. Державне управління: удосконалення та розвиток. 2022. № 10. DOI: <http://doi.org/10.32702/2307-2156.2022.10.2> (дата звернення: 14.04.2025)

40. Орищук В. В. Категорійний апарат у сфері цифрового розвитку. *Публічне управління та митне адміністрування*. 2023. № 1 (36). С.94-103. URL: <http://customs-admin.umsf.in.ua/archive/2023/1/14.pdf> (дата звернення: 14.04.2025)

41. Орлов О., Живилю Є., Нестеренко В. Нормативно-правові аспекти електронного документообігу в системі державного управління сектору

оборони держави. *Аспекти публічного управління*. Том 13. № 1. 2025. DOI: <https://doi.org/10.15421/152512> (дата звернення: 14.04.2025)

42. Орлов О.В., Дунаєв І.В. Національне правове регулювання цифрової економіки і інформаційних платформ. *Актуальні проблеми державного управління*. 2023. № 1(62). С. 6-20. DOI: <https://doi.org/10.26565/1684-8489-2023-1-01> (дата звернення: 14.04.2025)

43. Орлов О.В., Хмельницький А.В. Адаптації цифрових продуктів з елементами штучного інтелекту до роботи із запитом щодо доступу до публічної інформації. *Публічне управління і адміністрування в Україні*. 2024. Вип 39. DOI: <https://doi.org/10.32782/pma2663-5240-2024.39.22> (дата звернення: 14.04.2025)

44. Островий О. В. Передумови формування державної політики цифрового розвитку. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління*. 2021. Том 32 (71) № 6. С. 37-43.

45. Островий, О. Формування державної політики цифрового розвитку: сучасні тенденції та перспективи. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування*. 2022. № (3). С. 85-91. URL: <https://www.journals.ksauniv.ks.ua/index.php/public/article/view/122> (дата звернення: 14.04.2025)

46. Осьмак А., Карпенко Ю., Качмарський Є. Інтероперабельність критеріїв оцінювання сервісів виявлення дезінформації в умовах цифровізації публічного управління. *Аспекти публічного управління*. 2024. №12(1). С. 6-13. DOI: <https://doi.org/10.15421/152401> (дата звернення: 14.04.2025)

47. Осьмак А., Карпенко Ю., Семененко І. Використання інструментів штучного інтелекту в мережевому управлінні: переваги, ризики та розвиток. *Аспекти публічного управління*. 2023. №11(3). С. 38-42. DOI: <https://doi.org/10.15421/152333> (дата звернення: 14.04.2025)

48. Питання Єдиного державного веб-порталу цифрової освіти “Дія. Цифрова освіта” : Постанова Каб. Міністрів України від 10.03.2021 № 184 :

станом на 1 черв. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/184-2021-п#Text> (дата звернення: 14.04.2025).

49. Питання Міністерства цифрової трансформації : Постанова Каб. Міністрів України від 18.09.2019 № 856 : станом на 18 лют. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/856-2019-п#Text> (дата звернення: 14.04.2025).

50. Пікуля Т. О. Правове забезпечення цифрової трансформації в Україні. *Науковий вісник Ужгородського національного університету. Серія : Право*. 2024. Вип. 81(1). С. 61-67.

51. Польовий П. В. Нормативно-правовий механізм цифрових трансформацій в органах публічної влади та розвитку цифрових компетентностей публічних службовців. Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування. 2022. Том 33 (72) № 4. С. 84-93. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2022/4_2022/14.pdf (дата звернення: 14.04.2025)

52. Польовий П. В. Нормативно-правовий механізм цифрових трансформацій в органах публічної влади та розвитку цифрових компетентностей публічних службовців. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Публічне управління та адміністрування*. 2022. Т. 33(72), № 4. С. 84-93.

53. Почепцов Г. Г. Від покемонів до гібридних війн: нові комунікативні технології ХХІ століття. Г. Г. Почепцов. – К., 2017. 260 с.

54. Почепцов Г. Г. Сенси і війни: Україна і Росія в інформаційній і смисловій війнах. Г. Г. Почепцов. К., 2016. 316 с.

55. Почепцов Г. Г. Сучасні інформаційні війни. Г. Г. Почепцов. – К., 2016. 498 с.

56. Почепцов Г. Г. Токсичний інфопростір. Як зберегти ясність мислення і свободу дії. Г. Г. Почепцов. – Х.: Віват, 2022. 384 с.

57. Про затвердження Державної антикорупційної програми на 2023-2025 роки : Постанова Каб. Міністрів України від 04.03.2023 № 220 : станом

на 6 листоп. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/220-2023-п#Text> (дата звернення: 14.04.2025).

58. Про затвердження звіту про хід і результати виконання Програми діяльності Кабінету Міністрів України у 2020 році : Розпорядж. Каб. Міністрів України від 14.04.2021 № 327-р. URL: <https://zakon.rada.gov.ua/laws/show/327-2021-р#Text> (дата звернення: 14.04.2025).

59. Про затвердження особливостей здійснення публічних закупівель товарів, робіт і послуг для замовників, передбачених Законом України “Про публічні закупівлі”, на період дії правового режиму воєнного стану в Україні та протягом 90 днів з дня його припинення або скасування : Постанова Каб. Міністрів України від 12.10.2022 № 1178 : станом на 1 квіт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/1178-2022-п#Text> (дата звернення: 14.04.2025).

60. Про затвердження переліку показників Індексу цифрової економіки та суспільства (DESI) : Розпорядж. Каб. Міністрів України від 05.09.2023 № 774-р. URL: <https://zakon.rada.gov.ua/laws/show/774-2023-р#Text> (дата звернення: 14.04.2025).

61. Про затвердження Програми діяльності Кабінету Міністрів України: Постанова Каб. Міністрів України від 12.06.2020 № 471. URL: <https://zakon.rada.gov.ua/laws/show/471-2020-п#Text> (дата звернення: 14.04.2025).

62. Про заходи щодо створення сприятливих умов для розвитку ІТ-індустрії в Україні : Указ Президента України від 03.09.2020 № 371/2020. URL: <https://zakon.rada.gov.ua/laws/show/371/2020#Text> (дата звернення: 14.04.2025).

63. Про Національну програму інформатизації : Закон України від 01.12.2022 № 2807-IX. URL: <https://zakon.rada.gov.ua/laws/show/2807-20#Text> (дата звернення: 14.04.2025).

64. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII: станом на 3 квіт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 14.04.2025).

65. Про публічні закупівлі : Закон України від 25.12.2015 № 922-VIII : станом на 23 жовт. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/922-19#Text> (дата звернення: 14.04.2025).

66. Про реалізацію експериментального проекту щодо створення та впровадження цифрової інтегрованої інформаційно-аналітичної системи “Єдина платформа житлово-комунальних послуг” : Постанова Каб. Міністрів України від 03.09.2024 № 1039. URL: <https://zakon.rada.gov.ua/laws/show/1039-2024-п#Text> (дата звернення: 14.04.2025).

67. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України" : Указ Президента України від 14.09.2020 № 392/2020 : станом на 7 січ. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text> (дата звернення: 14.04.2025).

68. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України" : Указ Президента України від 25.03.2021 № 121/2021. URL: <https://zakon.rada.gov.ua/laws/show/121/2021#Text> (дата звернення: 14.04.2025).

69. Про рішення Ради національної безпеки і оборони України від 4 червня 2021 року «Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони» : Указ Президента України від 18.06.2021 № 260/2021. URL: <https://zakon.rada.gov.ua/laws/show/260/2021#Text> (дата звернення: 14.04.2025).

70. Про стимулювання розвитку цифрової економіки в Україні : Закон України від 15.07.2021 № 1667-IX : станом на 1 січ. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/1667-20#Text> (дата звернення: 14.04.2025).

71. Про схвалення Концепції Загальнодержавної цільової науково-технічної космічної програми України на 2021-2025 роки : Розпорядж. Каб. Міністрів України від 13.01.2021 № 15-р. URL: <https://zakon.rada.gov.ua/laws/show/15-2021-р#Text> (дата звернення: 14.04.2025).

72. Про схвалення Концепції розвитку електронного урядування в Україні : Розпорядж. Каб. Міністрів України від 20.09.2017 № 649-р. URL:

<https://zakon.rada.gov.ua/laws/show/649-2017-p#Text> (дата звернення: 14.04.2025).

73. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації : Розпорядж. Каб. Міністрів України від 03.03.2021 № 167-р. URL: <https://zakon.rada.gov.ua/laws/show/167-2021-p#Text> (дата звернення: 14.04.2025).

74. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації : Розпорядж. Каб. Міністрів України від 17.01.2018 № 67-р : станом на 17 верес. 2020 р. URL: <https://zakon.rada.gov.ua/laws/show/67-2018-p#Text> (дата звернення: 14.04.2025).

75. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядж. Каб. Міністрів України від 02.12.2020 № 1556-р : станом на 29 груд. 2021 р. URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text> (дата звернення: 14.04.2025).

76. Про схвалення Концепції створення загальнодержавної автоматизованої системи “Відкрите довкілля” : Розпорядж. Каб. Міністрів України від 07.11.2018 № 825-р : станом на 17 верес. 2020 р. URL: <https://zakon.rada.gov.ua/laws/show/825-2018-p#Text> (дата звернення: 14.04.2025).

77. Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації : Розпорядж. Каб. Міністрів України від 17.11.2021 № 1467-р : станом на 11 квіт. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/1467-2021-p#Text> (дата звернення: 14.04.2025).

78. Про схвалення Стратегії цифрової трансформації соціальної сфери : Розпорядж. Каб. Міністрів України від 28.10.2020 № 1353-р. URL: <https://zakon.rada.gov.ua/laws/show/1353-2020-p#Text> (дата звернення: 14.04.2025).

79. Про утворення Міжгалузевої ради з питань цифрового розвитку, цифрових трансформацій і цифровізації: постанова Кабінету Міністрів України від 8 липня 2020 р. № 595. URL: <https://zakon.rada.gov.ua/laws/show/595-2020-%D0%BF#Text> (дата звернення: 14.04.2025)

80. Про утворення Міжгалузевої ради з питань цифрового розвитку, цифрових трансформацій і цифровізації : Постанова Каб. Міністрів України від 08.07.2020 № 595 : станом на 4 квіт. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/595-2020-п#Text> (дата звернення: 14.04.2025).

81. Радченко А. А., Круглов В. В. Удосконалення механізмів державного управління кібербезпекою в Україні. *Розвиток сучасного українського суспільства у соціологічному вимірі*. С.223-226. URL: https://www.researchgate.net/profile/Vitalij-Kruglov/publication/387222600_UDOSKONALENNA_MECHANIZMIV_DERZAVNOGO_UPRAVLINNA_KIBERBEZPEKOU_V_UKRAINI/links/676479e0c1b0135465e930f5/UDOSKONALENNA-MECHANIZMIV-DERZAVNOGO-UPRAVLINNA-KIBERBEZPEKOU-V-UKRAINI.pdf (дата звернення: 10.04.2025)

82. Регламент (ЄС) 2017/1128 Європейського Парламенту та Ради від 14 червня 2017 року про транскордонну портативність онлайн-контент-послуг на внутрішньому ринку. URL: <https://eur-lex.europa.eu/eli/reg/2017/1128/oj/eng> (дата звернення: 21.04.2025)

83. Регламент (ЄС) 2018/302 Європейського Парламенту та Ради від 28 лютого 2018 року про вирішення проблеми необґрунтованого геоблокування та інших форм дискримінації на основі громадянства, місця проживання або місця заснування клієнтів на внутрішньому ринку. URL: <https://eur-lex.europa.eu/eli/reg/2018/302/oj/eng> (дата звернення: 21.04.2025)

84. Регламент (ЄС) 2022/1925 Європейського Парламенту та Ради від 14 вересня 2022 року про конкурентні та чесні ринки в цифровому секторі та про внесення змін до Директив (ЄС) 2019/1937 та (ЄС) 2020/1828 (Закон про цифрові ринки). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/>

?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC (дата звернення: 21.04.2025)

85. Російські хакери зламали державні реєстри України. Що відомо. BBC News Україна. 20.12.2024. URL: <https://www.bbc.com/ukrainian/articles/c7ve1298ndgo> (дата звернення: 10.04.2025)

86. Рухаємось до Єдиного цифрового ринку ЄС. Комітет з питань цифрової трансформації. URL: https://www.rada.gov.ua/news/news_kom/259113.html (дата звернення: 23.02.2025)

87. Савченко Н. В. Формування та реалізація сервісно-орієнтованої державної політики зайнятості в умовах розбудови цифрового суспільства. Теорія та практика державного управління. 2017. № 2(57). С. 165-170. URL: https://library.nlu.edu.ua/POLN_TEXT/NADU/TPDU/TPDU-57-2017.pdf#page=165 (дата звернення: 10.04.2025)

88. Україні презентували бренд «держави у смартфоні». LB.ua. 27.09.2019. URL: https://lb.ua/news/2019/09/27/438454_ukraine_prezentovali_brend.html (дата звернення: 10.04.2025).

89. Хаустова М. Г. Поняття цифровізації: національні та міжнародні підходи. *Право та інновації*. 2022. Вип. № 2 (38). С. 7–18.

90. Хаустова М. Державна політика в сфері цифровізації: теоретичний аспект. Матеріали конференцій МЦНД. (26.08.2022; Чернівці, Україна). 2022. С. 76–81. URL: <https://archive.mcnd.org.ua/index.php/conference-proceeding/article/view/217> (дата звернення: 10.04.2025)

91. Цимбаленко Я. Ю., Карпенко О. В. Цифрові інструменти запобігання корупції. *Інвестиції: практика та досвід*. 2023. № 2 (2023). С.68-73. DOI: <https://doi.org/10.32702/2306-6814.2023.2.68> (дата звернення: 10.04.2025)

92. Цифрове врядування: монографія О. В. Карпенко, Ж. З. Денисюк, В. В. Наместнік [та ін.]; за ред. О. В. Карпенка. Київ: ІДЕЯ ПРИНТ. 2020. 336с. URL: https://elib.nakkkim.edu.ua/bitstream/handle/123456789/4638/Monografia_Tsyfrove_vryadyvannya_2020.pdf?sequence=1&isAllowed=y (дата звернення: 10.04.2025)

93. Шкурак Людмила. Що таке цифрові двійники та як ця технологія змінює світ. URL: <https://ain.ua/2025/05/20/shho-take-cifrovi-dviiniki-i-iak-sia-technologie-zminiue-svit/> (дата звернення: 25.05.2025)

94. Шпиґа П.С., Карпенко О.В., Осьмак А.С., Карпенко Ю.В., Качмарський Є.І. Інструменти реінжинірингу державного управління у сфері охорони здоров'я: штучний інтелект та цифрові системи персональної ідентифікації пацієнтів. *Електронний журнал. Державне управління: удосконалення та розвиток*. 2024. № 5. DOI: <https://doi.org/10.32702/2307-2156.2024.5.2> (дата звернення: 10.04.2025)

95. Штець, Т. Ф. Світовий досвід впровадження механізмів державного регулювання розвитку сектора цифрової економіки. *Вчені записки Університету «КРОК»*. 2019. № 1 (53). С. 84–89. URL: <https://snku.krok.edu.ua/index.php/vcheni-zapiski-universitetu-krok/article/view/149/169> (дата звернення: 10.04.2025)

96. Щупаківський Р. Інституційні та організаційні аспекти середовища формування і реалізації потенціалу сектора інформаційно-комунікаційних технологій. *Modeling the development of the economic systems*. 2023. № (3). С. 109–114. URL: <https://mdes.khmnu.edu.ua/index.php/mdes/article/view/224> (дата звернення: 10.04.2025)

97. Як штучний інтелект DoZorro моніторить закупівлі. URL: <https://dozorro.org/blog/yak-shtuchnij-intelekt-dozorro-monitorit-zakupivli> (дата звернення: 14.04.2025).

98. 2024 State of the Digital Decade package. URL: <https://digital-strategy.ec.europa.eu/en/policies/2024-state-digital-decade-package> (Accessed: 23.02.2025)

99. Abrams R., "Uncovering the Network-Centric Organization." Ph.D. dissertation. University of California. Irvine. 2009. URL: <https://www.proquest.com/docview/304856743?pq-origsite=gscholar&fromopenview=true>

100. Agrawal A. The Economics of artificial Intelligence. McKinsey. Retrieved June 30, 2018. URL: <https://www.mckinsey.com/business->

functions/mckinsey-analytics/our-insights/the-economics-of-artificial-intelligence (Accessed: 28.02.2025)

101. Al Dahdah M, Quet M. Between Tech and Trade, the Digital Turn in Development Policies. *Development* (Rome). 2020. №63(2-4). P. 219-225. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC7653448/?utm> (Accessed: 21.04.2025)

102. Alireza Bayesteh, Jia He, Yan Chen, Peiying Zhu, Jianglei Ma, Ahmed Wagdy Shaban, Ziming Yu, Yunhao Zhang, Zhi Zhou, Guangjian Wang. Integrated Sensing and Communication (ISAC) – From Concept to Practice. Ottawa Wireless Advanced System Competency Centre, Wireless Technology Lab. URL: <https://www-file.huawei.com/-/media/corp2020/pdf/publications/huawei-research/issue2/isac-en.pdf?la=en> (Accessed: 17.05.2025)

103. Amanatidis, Petros, Dimitris Karampatzakis, George Iosifidis, Thomas Lagkas, and Alexandros Nikitas. 2023. "Cooperative Task Execution for Object Detection in Edge Computing: An Internet of Things Application" *Applied Sciences* 13, no. 8: 4982. DOI: <https://doi.org/10.3390/app13084982>

104. Amanowicz M. A Shared cybersecurity awareness Platform. *Journal of telecommunications and informational technology*. 2021. №3. P. 32-41. DOI: <https://doi.org/10.26636/jtit.2021.154421> (Accessed: 21.04.2025)

105. Anderson M. Alteryx Self-Service Analytics Data Science & Automation. Emerging & Disruptive Technologies for Defense, 2023, March 21–22. URL: <https://www.ciocoverage.com/alteryx-self-service-analytics-data-science-automation/> (Accessed: 14.04.2025).

106. Angwin, J., Larson, J., Mattu, S., & Kirchner, L. Machine Bias—There's Software Used across the Country to Predict Future Criminals. And It's Biased against Blacks. ProPublica, Online Edition. 2016. URL: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> (Accessed: 21.04.2025)

107. Bach J. Artificial General Intelligence and Organizational Intelligence (On the Singularity of AI). *Proceedings of 8th European Conference on Computing and Philosophy*, ECAP 10, Munich, Germany. 2010.

108. Bejtullahu-Michalopoulos K., Florin M.-V. The Governance of Decision-Making Algorithms. Lausanne: EPFL International Risk Governance Center. 2018. 32p. URL: https://www.researchgate.net/publication/329319807_The_Governance_of_Decision-Making_Algorithms (Accessed: 21.04.2025)
109. Bennett W. L., Segerberg A. The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics. *Information, Communication & Society*. 2012. T. 15. № 5. P. 739–768. DOI: <https://doi.org/10.1080/1369118X.2012.670661> (Accessed: 21.04.2025)
110. Bennett, W. L., & Segerberg, A. The logic of connective action: Digital media and the personalization of contentious politics. *Information, Communication & Society*. 2012. №15(5). P.739–768. DOI: <https://doi.org/10.1080/1369118X.2012.670661> (Accessed: 21.04.2025)
111. Bułat, Radosław, and Marek R. Ogiela. 2023. "Personalized Context-Aware Authentication Protocols in IoT" *Applied Sciences* 13, no. 7: 4216. DOI: <https://doi.org/10.3390/app13074216> (Accessed: 21.04.2025)
112. Cohen, J. L., & Arato, A. Civil society and political theory. Cambridge, MA: *The MIT Press*. 1992. URL: <http://ereserve.library.utah.edu/Annual/POLS/3960/Orchard/cohen.pdf> (Accessed: 21.04.2025)
113. Cubo, Aitor, José Luis Hernández Carrión, Miguel Porrúa, and Benjamin Roseth. Government Digital Transformation Guide. 2022. URL: <https://publications.iadb.org/en/government-digital-transformation-guide> (Accessed: 21.04.2025)
114. Dahl R. A. Who governs?: Democracy and power in American city. New Haven : Yale University Press, 1974. 355 p.
115. Data Science in the New Economy. A new race for talent in the Fourth Industrial Revolution. Centre for the New Economy and Society. URL: https://www3.weforum.org/docs/WEF_Data_Science_In_the_New_Economy.pdf (Accessed: 14.04.2025)

116. Davies J., Procter R. Online Platforms of Public Participation – a Deliberative Democracy or a Delusion? arXiv preprint arXiv. 2009.14074, 2020. URL: <https://arxiv.org/abs/2009.14074> (Accessed: 21.04.2025)
117. Dellermann D., Ebel P., Söllner M., Leimeister J. M. Hybrid Intelligence. *Business & Information Systems Engineering*. 2019. T. 61. № 5. P. 637–643. DOI: <https://doi.org/10.1007/s12599-019-00595-2> (Accessed: 21.04.2025)
118. Denmark 2024 Digital Decade Country Report. URL: <https://digital-strategy.ec.europa.eu/en/node/12863/printable/pdf> (Accessed: 23.02.2025)
119. Digital Decade Policy Programme 2030. URL: <https://digital-strategy.ec.europa.eu/en/library/digital-decade-policy-programme-2030> (Accessed: 10.05.2025)
120. Digital Democracy: The Tools Transforming Political Engagement. J.Simon, T. Bass, V. Boelman, G. Mulgan. Nesta. 2017. URL: <https://www.nesta.org.uk/report/digital-democracy-the-tools-transforming-political-engagement> (Accessed: 21.04.2025)
121. Digital development strategy 2024 to 2030. GOV.UK. 2024. URL: <https://www.gov.uk/government/publications/digital-development-strategy-2024-to-2030?utm> (Accessed: 21.04.2025)
122. Digital Development Strategy 2024-2030. UK International Development. 2024. URL: <https://assets.publishing.service.gov.uk/media/6613e7f7c4c84d4b31346a68/FCDO-Digital-Development-Strategy-2024-2030.pdf?utm> (Accessed: 21.04.2025)
123. Digital transformation. The OECD (Organisation for Economic Co-operation and Development). URL: <https://www.oecd.org/en/topics/policy-issues/digital-transformation.html?utm> (Accessed: 21.04.2025)
124. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with

EEA relevance) Text with EEA relevance URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng> (Accessed: 21.04.2025)

125. Dreshpak V.M., Kovalov V.G., Kritenko O.O., Shevchenko N.I., Babachenko N.V. Communication of EU public servants in the digital environment during the Covid-19 Pandemic. *Amazonia Investiga*. 2022. №11(51), P. 171-182. DOI: <https://doi.org/10.34069/AI/2022.51.03.16> (Accessed: 21.04.2025)

126. Drexler K. Engines of Creation. New York : Anchor Press Doubleday, 1986. URL: https://royallib.com/read/dreksler_erik/mashini_sozdaniya.html#0 (Accessed: 14.04.2025).

127. Dunleavy P. Why is it so hard to achieve organisational innovation in government. *LSE Public Policy Group Working Paper*. 2015.

128. Dunleavy Patrick, Margetts Helen, Bastow Simon, Tinkler Jane, Digital Era Governance: IT-Corporations. The State and E-Government. Oxford : Oxford University Press. 2006. 302 p.

129. Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. Acquiring and Managing Government IT. Digital Era Governance: IT Corporations, the State, and e-Government.. *Oxford University Press*. 2006. P.41–63. DOI: <https://doi.org/10.1093/acprof:oso/9780199296194.003.0002> (Accessed: 21.04.2025)

130. E-Government Development Index Ukraine. URL: <https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine> (Accessed: 17.02.2025)

131. E-Participation Index Ukraine. URL: <https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine> (Date of access: 17.02.2025)

132. Estonia 2024 Digital Decade Country Report. URL: <https://digital-strategy.ec.europa.eu/en/node/12840/printable/pdf> (Accessed: 23.02.2025)

133. European Digital Rights and Principles. URL: <https://digital-strategy.ec.europa.eu/en/policies/digital-principles> (Accessed: 23.02.2025)

134. Farinha, J., Vesnic Alujevic, L., Alvarenga, A. and Polvora, A., Everybody is looking into the Future! A literature review of reports on emerging technologies and disruptive innovation, Publications Office of the European Union, Luxembourg. 2023. doi:10.2760/144730. JRC134319 URL: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC134319/JRC134319_01.pdf (Accessed: 17.05.2025)
135. Future of Jobs Report 2025 URL: https://reports.weforum.org/docs/WEF_Future_of_Jobs_Report_2025.pdf (Accessed: 17.05.2025)
136. Hildebrandt M. Law for Computer Scientists and Other Folk. Oxford University Press, 2020. URL: <https://global.oup.com/academic/product/law-for-computer-scientists-and-other-folk-9780198860884?cc=pl&lang=en&> (Accessed: 21.04.2025)
137. Hughes J. Democratic Transhumanism 2.0. 2002. URL: <http://www.changesurfer.com/Acad/DemocraticTranshumanism.htm> (Accessed: 14.04.2025).
138. Huxley J. Transhumanism. *Journal of Humanistic Psychology*. 1968. Vol. 8, № 1. P. 73–76. DOI: <https://doi.org/10.1177/002216786800800107> (Accessed: 14.04.2025).
139. IMD World Digital Competitiveness Ranking 2018. URL: <https://cedakenticomedia.blob.core.windows.net/cedamediacontainer/kentico/media/general/publication/pdfs/wcydigitalranking2018.pdf> (Accessed: 17.02.2025)
140. IMD World Digital Competitiveness Ranking 2019. URL: <https://conapri.org/wp-content/uploads/2020/09/imd-world-digital-competitiveness-rankings-2019.pdf> (Accessed: 17.02.2025)
141. IMD World Digital Competitiveness Ranking 2020. URL: <https://imd.cld.bz/IMD-World-Digital-Competitiveness-Ranking-2020> (Accessed: 17.02.2025)
142. IMD World Digital Competitiveness Ranking 2021. URL: <https://imd.cld.bz/Digital-Ranking-Report-2021/200/> (Accessed: 17.02.2025)

143. Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation. Oxford Internet Institute. URL: <https://www.oii.ox.ac.uk/news-events/reports/industrialized-disinformation-2020-global-inventory-of-organized-social-media-manipulation/> (Accessed: 21.04.2025)
144. Isaak J., Hanna M. J. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*. 2018. Vol. 51, no. 8. P. 56–59. DOI: <https://doi.org/10.1109/mc.2018.3191268> (Accessed: 21.04.2025)
145. Isin, E. F., & Ruppert, E. Being digital citizens. London: Rowman & Littlefield International. 2015 URL: https://research.gold.ac.uk/id/eprint/29321/7/Isin%20and%20Ruppert%20%282020%29%20Being%20Digital%20Citizens_Second%20Ed_OA.pdf?utm_ (Accessed: 21.04.2025)
146. Ismael Peña-López. Policy-making for digital development: the role of the government. In Proceedings of the 4th ACM/IEEE International Conference on Information and Communication Technologies and Development (ICTD '10). Association for Computing Machinery. 2010. New York. USA. Article 32. P. 1–10. URL: https://ictlogy.net/articles/20101214_ismael_pena-lopez_policy-making_digital_development_role_government_paper.pdf?utm (Accessed: 21.04.2025)
147. Karpenko O., Zaporozhets T., Tsedik M., Vasiuk N., Osmak A. Digital Transformations of Public Administration in Countries with Transition Economies. *European Review*. 2023. №31(6). P.569–588 DOI: <https://doi.org/10.1017/S1062798723000522> (Accessed: 21.04.2025)
148. Karpenko O. V. Digital transformation and good data governance in Ukraine. *Вісник НАДУ. Серія “Державне управління”*. 2018. № 4 (91). С. 157–162.
149. Korol V., Dmytryk O., Karpenko O., Riadinska V., Basiuk O., Kobylnik D., Moroz V., Safronova O., Alisov E., Mishchenko T. Elaboration of recommendations on the development of the state internal audit system when applying the digital technologies. *Eastern-European Journal of Enterprise Technologies*. 2022. №1(13(115)). P.39–48. URL: <https://doi.org/10.15587/1729-4061.2022.252424> (Accessed: 21.04.2025)

150. Kurzweil R. The Age of Spiritual Machines When Computers Exceed Human Intelligence. New York : Penguin Books, 2000. URL: <https://archive.org/details/ageofspiritualm000kurz/page/n7/mode/2up> (Accessed: 14.04.2025).
151. Kurzweil R. The Singularity Is Near When Humans Transcend Biology. New York: Viking Adult, 2005. URL: <http://www.singularity.com/bookexcerpts.html> (Accessed: 14.04.2025).
152. Lewis Lloyd. Policy making in a digital world. How data and new technologies can help government make better policy. The Institute for Government. 2020. 52 p. URL: <https://www.instituteforgovernment.org.uk/sites/default/files/publications/policy-making-digital-world.pdf?utm> (Accessed: 21.04.2025)
153. Meet PAIGE, San Francisco's promising young IT procurement chatbot. URL: <https://statescoop.com/san-francisco-procurement-chatbot/> (Accessed: 14.04.2025)
154. Moloney K., Lobbying in the 21st. Transparency, Integrity and Access Century, 2007 URL: https://www.oecd.org/en/publications/lobbying-in-the-21st-century_c6d8eff8-en.html (Accessed: 20.04.2025)
155. Moravec H. P. Sensor Fusion In Certainty Grids For Mobile Robots. USA: Carnegie-Melton University Pittsburgh, 1989. URL: https://link.springer.com/chapter/10.1007/978-3-642-74567-6_19 (Accessed: 14.04.2025).
156. National digital transformation strategy – mapping the digital journey. The Digital Regulation Platform. 2023. URL: <https://digitalregulation.org/national-digital-transformation-strategy-mapping-the-digital-journey/?utm> (Accessed: 21.04.2025)
157. Nunzia Coco, Cinzia Colapinto, Vladi Finotto. Bridging conflicting frames in policies for digital transformation. Science and Public Policy. 2023. № 51(2). URL: https://www.researchgate.net/publication/375595464_Bridging_conflicting_frames_in_policies_for_digital_transformation (Accessed: 21.04.2025)
158. O'Neil C. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown Pub, 2016. 272 p.

159. Ostberg R. Transhumanism social and philosophical movement. *Britannica Encyclopaedia*. URL: <https://www.britannica.com/topic/transhumanism> (Accessed: 14.04.2025).
160. Overview: What is Digital Twin Technology? September 12, 2022. URL: https://altair.com/blog/articles/overview-what-is-digital-twin-technology?_gl=1*1wiqcrz*_gcl_au*NTczMTEzNDQ2LjE3NDkzMtYxMTI (Accessed: 25.05.2025)
161. Pasquale F. *Black Box Society*. Harvard University Press, 2015. 260 p. URL: <https://raley.english.ucsb.edu/wp-content/Engl800/Pasquale-blackbox.pdf> (Accessed: 21.04.2025)
162. Poland 2024 Digital Decade Country Report URL: <https://digital-strategy.ec.europa.eu/en/node/12822/printable/pdf> (Accessed: 23.02.2025)
163. Purdy M. & Daugherty P. How AI boosts industry profits and innovation. 2017. URL: https://www.accenture.com/_acnmedia/PDF-84/Accenture-AI-Industry-Growth-Full-Report.pdf. (Accessed: 28.02.2025)
164. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) URL: <https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng> (Accessed: 21.04.2025)
165. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj> (Accessed: 21.04.2025)
166. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868> (Accessed: 21.04.2025)

167. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance) URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854&qid=1749155653401> (Accessed: 21.04.2025)

168. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1183> (Accessed: 21.04.2025)

169. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689> (Accessed: 21.04.2025)

170. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG (Accessed: 21.04.2025)

171. Reviglio U., Agosti C. Thinking Outside the Black-Box: The Case for “Algorithmic Sovereignty” in Social Media. *Social Media + Society*. 2020. Vol. 6, no. 2. P. 205630512091561. DOI: <https://doi.org/10.1177/2056305120915613> (Accessed: 20.04.2025)

172. Robert Baldemair. Integrated Sensing and Communication URL: <https://www.ericsson.com/en/blog/2024/6/integrated-sensing-and-communication> (Accessed: 17.05.2025)

173. Russell S. J., Norvig P. *Artificial Intelligence: A Modern Approach*. 2nd ed. Upper Saddle River, New Jersey: Prentice Hall, 2003, 24p.

174. Schneier B. Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World. Recorded Books, Inc. and Blackstone Publishing. 2015. 295p.
175. Schumann Ph., Gibson R. K. Internet Discussion Citizen Trust in Government and Public Opinion Change An Experimental Study. *Journal of public discussions*. 2017. Vol. 13, № 2.
176. Schwab K. The fourth industrial revolution. Cologny. Geneva Switzerland: World Economic Forum, 2016. 172p.
177. Sorensen E., Torfing J. The democratic anchorage of governance networks. *Scandinavian Political Studies*. 2005. №28 (3). P. 195–218. DOI: <https://doi.org/10.1111/j.1467-9477.2005.00129.x> (Accessed: 21.04.2025)
178. Stanford Emerging Technology Review. URL: https://setr.stanford.edu/sites/default/files/2025-01/SETR2025_web-240128.pdf (Accessed: 17.05.2025)
179. The Digital Economy and Society Index (DESI). URL: <https://digital-strategy.ec.europa.eu/en/policies/desi> (Accessed: 23.02.2025)
180. The European Declaration on Digital Rights and Principles. URL: <https://digital-strategy.ec.europa.eu/en/factpages/digital-rights-and-principles> (Accessed: 23.02.2025)
181. The lobby network: Big Tech's web of influence in the EU. 19. Corporate Europe Observatory. 2021. URL: <https://corporateeurope.org/en/2021/08/lobby-network-big-techs-web-influence-eu> (Accessed: 21.04.2025)
182. The Network Readiness Index 2019. URL: <https://www.insead.edu/sites/default/files/assets/dept/globalindices/docs/nri-2019.pdf> (Accessed: 17.02.2025)
183. The Network Readiness Index 2020. URL: <https://download.networkreadinessindex.org/reports/data/2020/nri-2020.pdf> (Accessed: 17.02.2025)
184. The Network Readiness Index 2022. URL: https://download.networkreadinessindex.org/reports/nri_2022.pdf (Accessed: 17.02.2025)

185. The Network Readiness Index Ukraine 2024. URL: <https://networkreadinessindex.org/country/ukraine/> (Accessed: 17.02.2025)
186. The OECD Digital Government Policy Framework Six dimensions of a Digital Government. OECD Public Governance Policy Papers. OECD Publishing, Paris. 2020. No.02. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/10/the-oecd-digital-government-policy-framework_11dd6aa8/f64fed2a-en.pdf?utm (Accessed: 21.04.2025)
187. The year that was not saved by automated systems – 2021 in review. AlgorithmWatch. URL: <https://algorithmwatch.org/en/annual-review-2021/> (Accessed: 21.04.2025)
188. Tobias Mettler, Gianluca Miscione, Claus D. Jacobs, Ali A. Guenduez. Same same but different: How policies frame societal-level digital transformation. Government Information Quarterly. 2024. Volume 41. Issue 2. URL: <https://www.sciencedirect.com/science/article/pii/S0740624X24000248?utm> (Accessed: 21.04.2025)
189. Toffler A. Future Shock. New York : Random House, 1970. URL: <https://cdn.preterhuman.net/texts/literature/general/Alvin%20Toffler%20-%20Future%20Shock.pdf> (Accessed: 14.04.2025).
190. Toffler A. Transhumanism Special Report. Foreign Policy. 2009. URL: <https://foreignpolicy.com/2009/10/23/transhumanism/> (Accessed: 14.04.2025).
191. Top 10 Emerging Technologies of 2024. URL: https://www3.weforum.org/docs/WEF_Top_10_Emerging_Technologies_of_2024.pdf (Accessed: 17.05.2025)
192. Truman D. B. The governmental process: Political interests and public opinion. New York : Knopf, 1951. 544 p.
193. Tufekci Z. Algorithmic harms beyond facebook and google: emergent challenges of computational agency. Colorado Technology Law Journal. 2015. Vol. 13. P. 203-218. URL: <https://ctlj.colorado.edu/wp-content/uploads/2015/08/Tufekci-final.pdf> (Accessed: 21.04.2025)

194. Ukraine 2024 Report. 2024 Communication on EU enlargement policy
URL: https://enlargement.ec.europa.eu/document/download/1924a044-b30f-48a2-99c1-50edeac14da1_en?filename=Ukraine%20Report%202024.pdf (Accessed: 23.02.2025)
195. Van Dijk J. A. Digital Democracy: Vision and Reality. *Public Administration in the Information Age: Revisited*. IOS-Press. 2013. URL: https://www.utwente.nl/en/bms/vandijk/research/itv/itv_plaatje/Digital%20Democracy-%20Vision%20and%20Reality.pdf (Accessed: 21.04.2025)
196. Wallis T., Leszczyna R. EE-ISAC—Practical cybersecurity solution for the energy sector. *Energies*. 2022. 15. 2170. DOI: <https://doi.org/10.3390/en15062170> (Accessed: 21.04.2025)
197. Williams A. Digital-era policy making. A. Williams, H. Hay. *Governance in the Digital Economy*. 2000. 27 p.
198. Yeung K. Algorithmic regulation: A critical interrogation. *Regulation & Governance*. 2017. Vol. 12, no. 4. P. 505–523. DOI: <https://doi.org/10.1111/rego.12158> (Accessed: 21.04.2025)
199. Zuboff S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, USA : Public Affairs, 2019. 704 p.

ДОДАТКИ

Додаток А

Функціонально-технологічні складові цифрового розвитку України

Технологія	Функції технології для публічного управління	Функції технології для національної безпеки / військової сфери	Функції технології для споживачів управлінських послуг
Штучний інтелект (AI)	автоматизація процесів управління аналітика рішень кіберзахист реєстрів та сервісів	автономізація наступальних та спеціальних операцій виявлення ворожих впливів аналіз бойових даних; підтримка рішень під час бойових дій	інтелектуальні сервіси адаптація сервісів до потреб громадян безпечна взаємодія
Цифрові технології та промисловість	оптимізація промисловості цифровий аудит виробництва	контроль ВПК; цифрова підтримка логістики ЗСУ розробка оборонних ІТ-рішень	надійність сервісів цифровий доступ до послуг
Зелені інновації (Green)	контроль викидів управління ризиками катастроф екомоніторинг	захист водних/повітряних об'єктів під час бойових дій автономне енергозабезпечення	прогнозування стану довкілля захист від забруднень
Блокчейн	реєстрація прав власності незмінність даних цифрова ідентичність	перевірка прав власності на деокупованих територіях захист військових баз	доступ до реєстрів захищені транзакції
Web3-рішення	побудова децентралізованих систем публічного управління	забезпечення цифрової демократії у воєнний час автономні сервіси управління	доступ до DAO-систем захист ідентичності цифрова участь
Генеративні моделі (GenAI)	автоматизація документообігу корекція політик масові комунікації	генерація стратегій протидії ворогу створення сценаріїв реагування	створення шаблонів швидка підготовка заяв, звернень, запитів
Робототехніка	автоматичне реагування на надзвичайні події; інфраструктурна допомога	наступальні та спеціальні операції розмінування військова логістика евакуаційна підтримка	асистивні сервіси автоматизоване обслуговування в громадах

Нейронауки	управління людським ресурсом в органах публічної влади зменшення стресу у службовців	реабілітація військових нейростимуляція рішень у бойових умовах	підтримка психічного здоров'я персоналізована взаємодія
Напівпровідникові технології	обробка критичних обсягів даних у режимі реального часу	мобільні платформи зв'язку ЗСУ стійкість систем ППО	стабільність та підвищення захисту електронних сервісів
Космічні технології	просторове планування територій супутниковий моніторинг	розвідка та прогнозування атак контроль переміщення військ тактичний зв'язок	візуалізація територіальних змін геоінформування населення
Сталі енергетичні технології	стале енергозабезпечення енергетичний аудит	автономне живлення оборонних об'єктів, енергобезпека	енергостійкість житла попередження про енергозагрози
Health Tech	універсальний медичний нагляд інтеграція систем охорони здоров'я	військова телемедицина підтримка рішень у військовій медицині	Е-картка здоров'я телемедичні послуги
Перехресні технології	мультидисциплінарне управління змінami кризове планування	мобілізація інновацій на потреби ЗСУ міжгалузовий обмін	єдине цифрове середовище взаємодії
PETs / ZKP	захист реєстрів, документообігу та виборчих процесів	прихована верифікація даних безпека мобілізаційних баз	приватність персональних даних анонімні звернення
ISAC	інфраструктурний моніторинг в реальному часі розвиток IoT	виявлення диверсій спостереження за бойових дронів антидронові системи	оповіщення про загрози реактивне управління безпекою
6G–RIS–HAPS	комунікація в умовах руйнування інфраструктури	зв'язок тактичного рівня автономна інфраструктура ЗСУ	резервний зв'язок телекомунікації у кризових умовах
Імерсивні технології	симуляції для навчання служб оперативного реагування	військові навчальні полігони XR; планування операцій	навчання громадян дій під час воєнного стану захисне моделювання
Цифрові твіни (Digital Twins)	віртуальне дублювання об'єктів органів публічної влади моделювання прийняття рішень	передбачення військових загроз тестування реакцій інфраструктури	підготовка до надзвичайних ситуацій прогнозування впливів

Джерело: сформоване автором на основі аналізу джерел [93; 102; 134; 135; 160; 172; 178]

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Статті у наукових фахових виданнях України

1. Герман, Д., & Карпенко, Ю. (2022). Перспективи застосування концепцій цифрократії та трансгуманізму в галузі публічного управління. *Аспекти публічного управління*, 10(6), 19-23. <https://doi.org/10.15421/152239>
2. Карпенко, О., Карпенко, Ю., & Герман, Д. (2023). Штучний інтелект як інструмент зниження корупційних ризиків у сфері публічних закупівель. *Аспекти публічного управління*, 11(2), 129-135. <https://doi.org/10.15421/152328>
3. Герман, Д., & Пузько, М. (2024). Особливості використання штучного інтелекту у сфері культури та креативних індустрій: державно-управлінський аспект. *Університетські наукові записки*, 3(99), 23-36. <https://doi.org/10.37491/UNZ.99.3>
4. Герман, Д. (2025). Особливості нормативно-правового забезпечення державної політики цифрового розвитку України. *Аспекти публічного управління*, 13(1), 82-92. <https://doi.org/10.15421/152510>

В інших виданнях

5. Карпенко О.В., & Герман Д.В. (2021). Цифрова грамотність населення як складова підвищення ресурсної спроможності Національної системи кібербезпеки України. Актуальні питання застосування спеціальних інформаційно-телекомунікаційних систем: матеріали науково-практичної конференції студентів, курсантів, аспірантів, докторантів та молодих вчених (15–16 червня 2021 року) – К.: ІСЗЗІ КПП ім. Ігоря Сікорського, С.112–113.
6. Герман Д. (2023). Взаємодія алгоритмів штучного інтелекту та ІОТ-технологій: перспективи та виклики цифрового суспільства. Кібербезпека державних інституцій та подолання кризових станів: Збірник тез II Міжнародної науково-практичної конференції, (м. Київ-Вроцлав, травень 2023 року). Київ, С.139-140.

Довідки про впровадження результатів дисертаційного дослідження

КОМІТЕТ ВЕРХОВНОЇ РАДИ УКРАЇНИ
з питань бюджетувул. М. Грушевського, 5, м. Київ, 01008, www.rada.gov.ua

ДОВІДКА

про впровадження результатів дисертаційного дослідження
аспіранта кафедри національної економіки та публічного управління Київського
національного економічного університету імені Вадима Гетьмана

ГЕРМАНА Дениса Вадимовича

на тему: «Механізми формування та реалізації державної політики цифрового
розвитку в Україні» на здобуття ступеня доктора філософії за спеціальністю 281
«Публічне управління та адміністрування»

Довідка засвідчує те, що Комітетом Верховної Ради України з питань бюджету під час підготовки та попереднього розгляду у першому і другому читаннях проекту Закону України «Про внесення змін до Закону України "Про Державний бюджет України на 2023 рік" щодо використання коштів державного фонду регіонального розвитку (реєстраційний № 9165 від 31.03.2023 року) були використані пропозиції дисертанта до нього.

Зважаючи, що одним із завдань законопроекту було врегулювання питання залучення громадян до участі у відборі інвестиційних програм і проектів та визначенні пріоритетів спрямування коштів державного бюджету на регіональний розвиток, дисертантом (як одним з авторів законопроекту) запропоновано застосувати під час відбору інвестиційних програм і проектів, що мають забезпечуватися за рахунок коштів державного фонду регіонального розвитку, процедури голосування громадян України за відповідні проекти засобами Порталу Дія. Зокрема, врахувати такі особливості використання у 2023 році коштів державного фонду регіонального розвитку, визначивши у законопроекті, що «за результатами здійснення попереднього відбору та оцінки на відповідність вимогам законодавства поданих інвестиційних програм і проектів регіонального розвитку, центральний орган виконавчої влади, що забезпечує формування державної регіональної політики, подає їх для відкритого голосування громадян засобами Єдиного державного веб-порталу електронних послуг (далі – Портал Дія). Під час такого голосування громадянин може віддати один голос за одну інвестиційну програму (проект регіонального розвитку) регіону за місцем реєстрації місця проживання (внутрішньо переміщена особа – за місцем проживання, визначеним відповідно до законодавства про облік внутрішньо переміщених осіб)».

Голова Комітету

Роксолана ПІДЛАСА

Апарат Верховної Ради України
04-13/12-2025/131354 від 05.06.2025

1907341



Україна

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
імені Вадима Гетьмана

03057, м. Київ, пр-т Берестейський (пр-т Перемоги), 54/1. e-mail: office@kneu.edu.ua
Тел.: (044) 456-50-55, (044) 371-61-19. ЄДРПОУ: 02070884

08.06.2023 № 04/13-404

На № _____

ДОВІДКА

про впровадження результатів дисертаційного дослідження
Германа Дениса Вадимовича за темою «Механізми формування та
реалізації державної політики цифрового розвитку в Україні»
в навчальний процес Київського національного економічного університету
імені Вадима Гетьмана

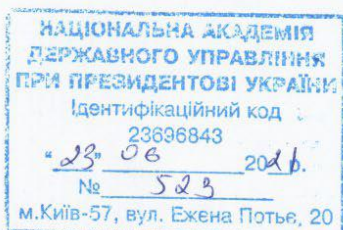
Довідка видана у підтвердження того, що результати дисертаційного дослідження сформульовані в роботі Германа Дениса Вадимовича за темою «Механізми формування та реалізації державної політики цифрового розвитку в Україні» використано в навчальному процесі кафедри національної економіки та публічного управління Київського національного економічного університету імені Вадима Гетьмана» при підготовці та викладанні навчальних дисциплін освітньо-професійної програми «Державна політика та публічне управління» з підготовки здобувачів другого (магістерського) рівня вищої освіти за спеціальністю 281 «Публічне управління та адміністрування», зокрема «Цифрове врядування» та «Сервісна діяльність органів публічної влади». Заслуговують на увагу запропоновані здобувачем науково обґрунтовані підходи щодо реалізації концепції трансгуманізму в галузі державного управління.

Проректор
з науково-педагогічних робіт,
доктор економічних наук, професор



Анатолій КОЛОТ

001641

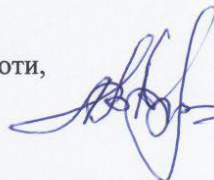


ДОВІДКА про участь у науково-дослідних роботах

Видана ГЕРМАНУ Денису Вадимовичу з підтвердженням про те, що він дійсно брав участь у виконанні науково-дослідних робіт за комплексним науковим проектом “Державне управління та місцеве самоврядування” (державний реєстраційний номер 0199U002827) Національної академії державного управління при Президентові України, а саме:

- у 2021 році – виконавець на громадських засадах (наказ від 15 березня 2021 року № 182-ос “Про залучення до виконання науково-дослідних робіт”) науково-дослідної роботи “Сервісна діяльність органів публічної влади в умовах розвитку цифрового суспільства”, державний реєстраційний номер 0119U101449.

Керівник науково-дослідної роботи,
д.держ.упр., доцент

 Олександр КАРПЕНКО

Т.в.о. директора Інституту
експертно-аналітичних
та наукових досліджень
к.держ.упр., доцент

 Наталія КЛИМЕНКО

Підпис 
засвідчую:
“15” 06 2021





МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА
проспект Берестейський, 54/1, м. Київ, 03057, e-mail: office@kneu.edu.ua
Тел.: +38 (044) 456-50-55, +38 (044) 371-61-19. Код згідно з ЄДРПОУ: 02070884

11.06.2025 № 01/13-570

На № _____

ДОВІДКА про участь у науково-дослідній роботі

Довідка видана аспіранту кафедри національної економіки та публічного управління ГЕРМАНУ Денису Вадимовичу з підтвердженням про те, що він дійсно брав участь у виконанні ініціативної науково-дослідної роботи «Формування та реалізація державної політики реінжинірингу національної економіки» (державний реєстраційний номер 0123U104290) у період з вересня 2023 року по червень 2025 року, яка виконується в Київському національному економічному університеті імені Вадима Гетьмана.

В рамках науково-дослідної роботи ГЕРМАНОМ Денисом Вадимовичем проаналізовано особливості використання штучного інтелекту як цифрового інструменту реінжинірингу національної економіки в умовах збройної агресії проти України.

Перший проректор



Андрій ОМЕЛЬЧЕНКО

005901