Олена ДИКАНЬ[1],
доктор економічних наук, професор, завідувач кафедри менеджменту, публічного управління та HR-технологій, ORCID: https://orcid.org/0000-0002-2087-9257
Юлія КРИХТІНА[1],
доктор наук з державного управління, доцент, професор кафедри менеджменту, публічного управління та HR-технологій, ORCID: https://orcid.org/0000-0002-6595-4759
Арсеній КОВАЛЬОВ[1],
здобувач третього (освітньо-наукового) рівня вищої освіти, кафедра фінансів, обліку і аудиту, ORCID: https://orcid.org/0009-0003-5428-0722

[1] *Український державний університет залізничного транспорту*

Прийняття: 15/05/2026
Рецензія: 22/05/2026
Публікація: 29/05/2026

JEL Класифікатор:
H83, O33, O38, D73

ISSN 2786-5339 (print)
ISSN 2786-5347 (online)

DOI: https://doi.org/10.53920/ES-2026-2-2

ЦИФРОВЕ ВРЯДУВАННЯ В СИСТЕМІ ПІДВИЩЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ ДЕРЖАВИ

Мета дослідження полягає в обґрунтуванні ролі цифрового врядування у підвищенні конкурентоспроможності держави з урахуванням ризиків кібербезпеки, нерівного доступу до цифрових сервісів і цифрового розриву. Методологія дослідження спирається на системний та інституційний аналіз, узагальнення міжнародних підходів до цифрового урядування, ризик-орієнтоване групування та структурно-функціональне пояснення зв'язків між цифровими сервісами, довірою і державною спроможністю. Результати дослідження свідчать, що цифрове врядування посилює конкурентоспроможність держави через скорочення адміністративних витрат, прискорення сервісних процедур, розвиток роботи з даними, прозорість, електронну участь і зміцнення довіри до публічних інституцій. Наукова новизна полягає в обґрунтуванні ризик-орієнтованої рамки, яка поєднує безпекову, інклюзивну, інституційно-довірчу та координаційну площини цифрового врядування. Практичне значення результатів полягає у можливості використання запропонованої матриці для аудиту електронних послуг, підготовки цифрових стратегій, програм цифрової грамотності та оцінювання сервісної якості публічного управління.

Ключові слова: *цифрове врядування, конкурентоспроможність держави, ризики цифрового врядування, кібербезпека, цифровий розрив, цифрова інклюзія, електронні послуги, довіра громадян.*

Olena DYKAN, Yuliia KRYKHTINA, Arsenii KOVALOV

DIGITAL GOVERNANCE IN THE SYSTEM OF ENHANCING STATE COMPETITIVENESS

The purpose of the study is to substantiate the role of digital governance in strengthening state competitiveness, with attention to cybersecurity risks, unequal access to digital services, and the digital divide. The methodology is based on systemic and institutional analysis, synthesis of international approaches to digital government, risk-oriented grouping, and structural-functional interpretation of the links between digital services, public trust, and state capacity. The study shows that digital governance supports state competitiveness through lower administrative costs, faster service procedures, wider use of public-sector data, transparency, electronic participation, and stronger trust in public institutions. Its competitive effect depends on institutional coordination, resilient digital infrastructure, protection of registers and personal data, and the ability of public authorities to provide clear, accessible, and secure services for different user groups. Scientific novelty lies in a risk-oriented framework that combines the security, inclusive, institutional-trust, and coordination dimensions of digital governance. This framework presents digital transformation as a managerial factor of competitiveness and as a field of risks that require monitoring, preventive regulation, and user-oriented communication. The practical value of the results lies in the possibility of applying the proposed matrix to audit electronic services, prepare digital strategies, design digital literacy programmes, and assess the service quality of public administration.

Keywords: *digital governance, state competitiveness, risks of digital governance, cybersecurity, digital divide, digital inclusion, electronic services, citizens' trust.*

Постановка проблеми. Цифрове врядування дедалі частіше розглядається як складова державної спроможності, що впливає на швидкість управлінських дій, передбачуваність адміністративних процедур і відкритість взаємодії органів влади з громадянами та бізнесом. У міру переходу від окремих електронних послуг до узгодженого середовища, де дані, реєстри, канали комунікації, сервісні процедури та механізми участі громадян працюють у межах спільної управлінської архітектури, конкурентоспроможність держави пов'язується з якістю інституцій, витратами часу на адміністративний контакт, рівнем довіри, захистом даних і досяжністю послуг для різних груп населення.

Міжнародні підходи до цифрового урядування, зокрема документи OECD, наголошують на поєднанні цифрового проєктування, державного

сектору на основі даних, платформеної організації, відкритості, орієнтації на користувача та проактивності [1]. Індекс цифрового уряду (Digital Government Index) 2023 засвідчує потребу в узгодженій та людиноцентричній цифровій трансформації публічного сектору [2]. Дані United Nations E-Government Survey 2024 підтверджують підвищення рівня цифрового урядування у світі, одночасно фіксуючи стійкі розриви у доступі, навичках і якості використання цифрових можливостей [3]. Тому цифровізацію доцільно оцінювати, зважаючи на те, наскільки вона реально спрощує контакт людини з державою, скорочує витрати часу на адміністративні процедури, зберігає захист даних і робить сервіси зрозумілими для різних груп користувачів.

Актуальність проблеми зростає через поєднання сервісних переваг цифрового врядування з новими управлінськими ризиками. Централізація даних, електронна ідентифікація, міжреєстровий обмін, хмарні сервіси, цифрові платежі та онлайн-портали підвищують зручність послуг, однак збільшують наслідки кібератак, витоків даних, помилок у реєстрах і збоїв у роботі цифрових компонентів.

У контексті підвищення конкурентоспроможності держави цифрове врядування доцільно розглядати через його вплив на якість публічних інституцій, швидкість адміністративних процедур, прозорість управлінських рішень, доступність послуг і довіру до держави. Розвиток електронних сервісів створює можливості для зменшення бюрократичного навантаження на громадян та бізнес, однак потребує надійної цифрової інфраструктури, захищених реєстрів, узгодженого обміну даними між органами влади та зрозумілих процедур користування послугами.

В українських умовах зазначені вимоги ускладнюються воєнними загрозами, кібератаками, територіальними відмінностями у цифровій доступності та різним рівнем цифрової підготовки користувачів. Це формує проблему дослідження, пов'язану з оцінюванням цифрового врядування як чинника конкурентоспроможності держави з урахуванням сервісних переваг, управлінських обмежень і ризиків цифрової залежності.

Аналіз останніх досліджень і публікацій. Питання цифрового врядування, електронних державних сервісів, цифрової інфраструктури, безпеки даних та інклюзії досліджуються у працях зарубіжних авторів і документах міжнародних організацій. OECD подає цифровий уряд як систему узгодженої роботи даних, платформ, регуляторних рішень і сервісної орієнтації [1]. Зв'язок цифрового уряду з конкурентоспроможністю аналізує D. Sagarik, який пов'язує його розвиток з інституційною якістю, цифровими інструментами та підтримкою інноваційного середовища [4]. T. Mettler,

G. Miscione, C. D. Jacobs та A. A. Guenduez звертають увагу на практичне виконання цифрових стратегій, управлінську дисципліну й результат для користувача [5]. Окрему увагу приділено цифровій публічній інфраструктурі, що охоплює цифрову ідентичність, базові реєстри, обмін даними, цифрові платежі та спільні компоненти сервісного середовища [6]. Організаційні зміни у публічному секторі досліджують N. Haug, S. Dan та I. Mergel, пов'язуючи цифровізацію з переглядом адміністративних процесів, ролей службовців і вимог до управлінських компетентностей [7].

Довіру, приватність і сприйняття цифрових ризиків вивчають P. Gupta, A. Hooda, A. Jeyaraj, J. J. M. Seddon та Y. K. Dwivedi, які доводять вплив цих чинників на готовність громадян користуватися електронним урядом [8]. Y. Li та H. Shang показують зв'язок позитивного досвіду користування електронними державними сервісами з довірою до уряду [9]. Проблему цифрового розриву розкривають D. Mesa [10], H. Liu, Q. Zhou та S. Liang [11], R. Peeters, S. M. Miller та M. Schuilenburg [12]. Чинники прийняття електронного уряду, зокрема користь, простоту використання, якість системи, прозорість і безпеку, досліджують A. Sabani, V. Thai та M. A. Hossain [13].

Наявні праці створюють теоретичну основу для аналізу цифрового врядування як інституційного, сервісного та соціального явища. Поглиблення потребує зв'язок між цифровим врядуванням і конкурентоспроможністю держави через ризики, що зменшують практичний ефект цифровізації, зокрема кіберстійкість, рівний доступ, цифрові навички, довіру до цифрових процедур і відповідальність органів влади за помилки, які виникають у цифровому середовищі.

Мета статті полягає в обґрунтуванні ролі цифрового врядування у підвищенні конкурентоспроможності держави з урахуванням ризиків кібербезпеки, нерівного доступу до цифрових сервісів і цифрового розриву.

Виклад основного матеріалу дослідження. Цифрове врядування впливає на конкурентоспроможність держави через сукупність каналів, пов'язаних із витратами взаємодії, якістю процедур, довірою до публічних інституцій, роботою з даними, участю громадян, стійкістю сервісів і доступністю цифрових послуг для різних груп населення та територій. У практичному вимірі ці канали проявляються через скорочення адміністративних витрат для громадян і бізнесу, підвищення прозорості інституційної взаємодії, зміцнення довіри до державних сервісів, розвиток спроможності органів влади працювати з даними, розширення електронної участі, підтримання сервісної стійкості під час криз і забезпечення цифрової включеності.

Скорочення адміністративних витрат проявляється у зменшенні часу, зусиль і супровідних дій, потрібних для отримання державної послуги.

Онлайн-доступ дає змогу пройти значну частину процедури без особистого звернення до установи та очікування в чергах. Зрозумілий порядок подання заяви, використання даних із цифрових реєстрів і відмова від повторного подання документів спрощують контакт з органами влади та знижують імовірність помилок. У підприємницькій діяльності такий ефект помітний у реєстраційних, дозвільних, податкових і звітних процедурах, де затримки безпосередньо впливають на витрати бізнесу. У повсякденному житті громадян цифровий формат полегшує доступ до соціальних, освітніх, медичних і адміністративних сервісів, зокрема за умов територіальної віддаленості або обмеженого доступу до установ.

Підвищення якості інституційної взаємодії пов'язане з тим, що цифрові сервіси роблять управлінські дії більш видимими для аналізу й контролю. У якісному цифровому сервісі користувач бачить вимоги до процедури, строки розгляду, статус звернення, причину відмови та порядок оскарження, що зменшує простір для довільного трактування правил і затягування рішень. Якщо паперова процедура з надмірними погодженнями, дублюванням документів і нечіткими підставами для відмови переноситься в онлайн без перегляду її змісту, користувач отримує новий інтерфейс, зберігаючи старе джерело адміністративної складності.

Довіра до державних сервісів і публічних інституцій формується через досвід конкретної взаємодії. Стабільна робота сервісу, зрозумілі повідомлення, захист персональних даних і відсутність зайвих дій поступово створюють відчуття передбачуваності, а збій, витік даних або відмова сервісу швидко послаблюють накопичену довіру, особливо за умов слабкого інформування користувачів. У цифровому врядуванні довіра є практичним ресурсом, від якого залежить готовність людей користуватися новими сервісами без побоювань за результат процедури та безпеку власних даних.

Розвиток спроможності держави працювати з даними охоплює якість реєстрів, сумісність інформаційних систем, актуальність записів і швидкість обміну між органами влади. Завдяки цьому держава точніше бачить потреби населення, швидше реагує на кризи й обґрунтованіше планує публічні рішення. Цифрова публічна інфраструктура, описана OECD, створює основу для повторного використання спільних компонентів, запуску нових послуг і взаємодії між публічними та приватними сервісами [6]. У контексті конкурентоспроможності це означає вищу швидкість управлінської реакції та прозоріші правила роботи цифрової економіки.

Розширення участі громадян у публічних рішеннях забезпечують електронні петиції, консультації, опитування, відкриті бюджети, цифрові кабінети та сервіси зворотного зв'язку. У 2024 році Україна отримала максимальне

значення E-Participation Index 1,0000 і перше місце у світі, що засвідчує потенціал електронної участі за умови її впливу на реальні рішення [3].

Підвищення стійкості державних сервісів до кризових і безпекових ризиків охоплює здатність електронних сервісів зберігати працездатність під час кібератак, технічних збоїв, воєнних загроз і різкого зростання навантаження. Реєстри, системи ідентифікації, портали, цифрові платежі та канали повідомлень мають спиратися на резервування, захист даних і зрозумілі сценарії відновлення. У разі збою важливими стають: швидка реакція органу влади, повне інформування користувачів і альтернативний спосіб отримання послуги, оскільки кібербезпека в такому вимірі підтримує безперервність базових адміністративних процесів. Стійкість цифрових сервісів посилює конкурентоспроможність держави через менші втрати часу, стабільнішу роботу інституцій і вищу готовність суспільства користуватися цифровими рішеннями.

Забезпечення рівного доступу до цифрових послуг пов'язане з цифровою інклюзією. Обмежена якість інтернету, брак навичок, незрозумілий дизайн інтерфейсу, складна мова сервісу або відсутність консультаційної підтримки перетворюють формально доступний інструмент на бар'єр. Територіальні громади з пошкодженою інфраструктурою, люди старшого віку, внутрішньо переміщені особи та користувачі з низькою цифровою впевненістю потребують простих інтерфейсів, зрозумілих інструкцій і допоміжних каналів звернення.

Окреслені канали показують, за рахунок чого цифрове врядування здатне підсилювати конкурентоспроможність держави. Одночасно кожен із них має ризиковий вимір, пов'язаний із безпекою даних, фактичною доступністю сервісів, довірою користувачів і здатністю органів влади працювати з помилками. З огляду на це, подальший аналіз доцільно спрямувати на ризики, які зменшують управлінський ефект цифровізації навіть за наявності розвиненої цифрової інфраструктури.

Для систематизації ризиків цифрового врядування доцільно виокремити чотири ризикові площини, через які цифровізація публічного управління впливає на конкурентоспроможність держави. Безпекова площина охоплює: кібератаки, витоки даних, збої сервісів, залежність від сторонніх постачальників і здатність держави відновлювати роботу після інцидентів. Інклюзивна площина пов'язана з доступом до інтернету, пристроїв, цифрових навичок, консультаційної підтримки та адаптованих каналів звернення. Інституційно-довірча площина стосується прозорості цифрових рішень, відповідальності за помилки, якості комунікації, пояснюваності алгоритмічних перевірок і можливості користувача захистити свої права.

Координаційна площина відображає узгодженість реєстрів, стандартів даних, сервісних процедур та міжвідомчої взаємодії.

Безпекова площина ризиків є вагомою для держави, яка поступово переводить адміністративні процедури у цифровий формат. У паперовій або змішаній моделі збій окремої установи, як правило, обмежується локальними наслідками. У цифровому середовищі ситуація помітно складніша. Один уражений компонент може порушити роботу цілої групи послуг, оскільки центральний реєстр, система ідентифікації чи канал обміну даними безпосередньо обслуговують різні процедури й формують спільну точку вразливості для громадян, бізнесу та органів влади. Кіберстійкість, у свою чергу, охоплює: запобігання інцидентам, моніторинг, реагування, резервування даних і відновлення сервісів. Зокрема, аудит коду, контроль доступу, сегментація систем, шифрування й перевірка постачальників знижують імовірність порушень. Після інциденту актуальності набувають швидкість виявлення проблеми, зрозуміле інформування користувачів, координація органів влади та альтернативний порядок отримання послуги. Правова визначеність також підтримує довіру, адже користувач має розуміти, які дані збираються, хто отримує доступ і як виправляється помилка [8].

Інклюзивна площина показує, що цифровий сервіс має оцінюватися з позиції різних груп користувачів. Людина може мати смартфон, однак не завжди вміє розібратися у складній формі, нестабільному з'єднанні, незрозумілій мові сервісу, страху помилитися або відсутності консультації. За таких умов наявність онлайн-послуги фіксує технічний рівень цифровізації та потребує перевірки її реальної доступності для користувача. Дослідження D. Mesa доводить вплив рівня освіти на використання цифрових публічних послуг і довіру до публічного адміністрування [10]. Системний огляд H. Liu, Q. Zhou та S. Liang також підтверджує, що цифрова інклюзія має рівні дії, пов'язані з політикою, організаціями та безпосереднім досвідом користувача [11].

Інституційно-довірча площина пов'язана з тим, як держава пояснює цифрові рішення, виправляє помилки та здійснює нагляд за алгоритмічними процедурами. У дата-платформному середовищі органи влади дедалі частіше використовують алгоритмічні інструменти для опрацювання звернень, перевірки даних, розподілу навантаження й прогнозування потреб. Такі інструменти пришвидшують роботу, але за відсутності належного контролю, можуть погіршити становище осіб, чиї життєві ситуації виходять за типові параметри системи. R. Peeters, S. M. Miller та M. Schuilenburg наголошують, що інклюзивність автоматизації врядування потребує аналізу того, як цифрові системи визначають норму, виняток і право на допомогу [12].

Координаційна площина стосується узгодженості цифрових рішень, реєстрів і процедур. Найбільший ризик для користувача виникає тоді, коли цифрова система подається як нейтральна, хоча в її основі лежать правила, припущення, формати даних і технічні обмеження. Вимога підтвердити інформацію через реєстр може бути простою для більшості громадян і майже недосяжною для людини, яка втратила документи через війну, переїзд або знищення архівів. За відсутності людського перегляду, пояснення причини відмови й зрозумілого порядку коригування даних цифрова процедура здатна відтворювати адміністративну несправедливість у новій технічній формі.

Для поєднання зазначених ризиків із завданням підвищення конкурентоспроможності держави запропоновано ризик-орієнтовану матрицю цифрового врядування (табл. 1).

Таблиця 1. Ризик-орієнтована матриця цифрового врядування для підвищення конкурентоспроможності держави

Ризикова площина	Прояв у публічному управлінні	Механізм впливу на конкурентоспроможність держави	Індикатори моніторингу	Управлінські дії
Безпекова	кібератаки на реєстри, витоки персональних даних, відмова сервісів, фішинг, залежність від сторонніх цифрових компонентів	порушення безперервності послуг, зниження довіри, зростання витрат на відновлення, репутаційні втрати держави	кількість інцидентів, час відновлення, частка сервісів із резервуванням, кількість повідомлень про витоки, оцінка безпеки користувачами	аудит безпеки, резервування, сегментація систем, плани реагування, перевірка постачальників, кризова комунікація
Інклюзивна	різна якість інтернету, нестача пристроїв, слабкі цифрові навички, складні для доступу інтерфейси, відсутність консультацій	звуження фактичного охоплення електронних послуг, перенесення витрат на користувача, нерівний доступ до адміністративних і соціальних прав	частка користувачів за віком і територією, кількість звернень до підтримки, частка заяв без результату, результати тестування доступності, звернення в офлайн-каналах	пункти цифрової підтримки, змішані канали обслуговування, прості інструкції, навчання користувачів, тестування сервісів із різними групами населення

Закінчення таблиці 1

Ризикова площина	Прояв у публічному управлінні	Механізм впливу на конкурентоспроможність держави	Індикатори моніторингу	Управлінські дії
Інституційно-довірча	низька прозорість відмов, помилки в реєстрах, складне оскарження, алгоритмічні перевірки без пояснення, слабка відповідальність за якість даних	зростання скарг, відчуття несправедливості, нижча легітимність цифрових рішень, зменшення готовності користуватися сервісами	частка скарг, строки виправлення даних, кількість відмов через реєстрові невідповідності, частка рішень із поясненням, кількість випадків людського перегляду	пояснення причин рішення, процедура людського перегляду, аудит алгоритмів, контроль якості даних, публічні звіти про роботу сервісів
Координаційна	слабка сумісність реєстрів, дублювання даних, різні стандарти сервісів, слабка взаємодія між органами влади	повільне масштабування цифрових рішень, вищі витрати, непередбачуваний сервісний досвід, дублювання адміністративних дій	кількість інтегрованих реєстрів, частота повторного запиту документів, час міжвідомчого обміну, кількість процедур із дублюванням даних	єдині стандарти даних, міжвідомчі команди, цифрова публічна інфраструктура, регулярний моніторинг сервісного маршруту

Джерело: складено авторами

Матриця ризиків дає змогу побачити, що вплив цифрового врядування на конкурентоспроможність держави формується через кілька взаємопов'язаних управлінських ліній. Кіберінцидент, передусім, порушує безперервність надання послуги, зачіпає питання захисту даних і досить швидко знижує довіру до органу влади. Нерівний доступ, своєю чергою, звужує коло користувачів електронних сервісів, унаслідок чого частина громадян знову звертається до повільніших і дорожчих офлайн-процедур. Коли помилки в реєстрах поєднуються з алгоритмічними перевірками зі слабкою прозорістю, зростає кількість скарг, подовжується строк проходження процедури й посилюється відчуття правової непевності. Окремо слід враховувати слабку сумісність інформаційних систем, адже вона гальмує поширення цифрових рішень між органами влади, ускладнює обмін даними та погіршує сервісний досвід користувача.

Оцінювання цифрового врядування доцільно пов'язувати з тим, як послуга фактично проходиться користувачем. Наявність порталу або

застосунку засвідчує технічний доступ, залишаючи поза увагою якість адміністративної процедури, її зрозумілість і здатність довести звернення до результату. Для прояву управлінських впливів важливими факторами є: середній час проходження процедури, частка завершених заяв, кількість повторних звернень, відмови через помилки даних, строки виправлення записів, кількість скарг, час відновлення після інцидентів, доступність інтерфейсу та охоплення користувачів із нижчою цифровою впевненістю. Такі показники дають змогу оцінити реальну результативність електронного сервісу, виявити місця виникнення помилок і зрозуміти, чи отримує громадянин або бізнес очікуваний результат.

Український досвід свідчить, що висока цифрова динаміка може розвиватися поруч із підвищеним рівнем ризику. Сильні позиції в електронній участі та онлайн-послугах дають державі репутаційний ресурс, підтримують контакт громадян із публічними сервісами під час війни і підвищують видимість України в міжнародному цифровому просторі. Одночасно така залежність від цифрових каналів посилює вимоги до кіберзахисту, резервування, кризової комунікації та альтернативних процедур. У разі атаки на реєстри або тимчасового припинення роботи сервісу орган влади має оперативно пояснити, які послуги залишаються доступними, які канали можна використати, чи існує ризик для даних, коли очікується відновлення і що повинен зробити користувач.

Цифровий інцидент потребує узгодженої технічної й комунікаційної реакції, що охоплює відновлення роботи сервісу, пояснення причин збою, захист даних і зрозумілі інструкції для користувачів. Нечіткі повідомлення породжують чутки, переводять користувачів у неофіційні джерела інформації та посилюють недовіру. Громадянину потрібні конкретні відомості про стан сервісу, ризики для персональних даних, доступні альтернативи та час наступного оновлення. Регулярні повідомлення з практичними інструкціями зменшують напругу, повертаючи ситуацію в кероване інформаційне поле.

Цифрову інклюзію варто закладати ще під час проєктування сервісу, коли визначаються логіка процедури, мова інструкцій і спосіб підтримки користувача. До запуску доцільно перевіряти сервіс за участю людей старшого віку, осіб з особливими потребами, мешканців малих громад, внутрішньо переміщених осіб і підприємців із різним рівнем цифрової підготовки. Окремої уваги потребують кількість кроків, зрозумілість ідентифікації, доступність консультації та порядок виправлення помилки. Після запуску сервісу орган влади має аналізувати скарги, рахувати процедури без результату, фіксувати повторні звернення і, спираючись на ці дані, коригувати сервісний маршрут відповідно до фактичних труднощів користувачів.

Публічні службовці в цифровій державі потребують компетентностей, пов'язаних із даними, кіберризиками, сервісною комунікацією та роботою зі скаргами. Йдеться також про здатність пояснювати цифрову процедуру, бачити бар'єри доступу, розуміти межі алгоритмічної перевірки і своєчасно передавати проблему тим, хто може її виправити. Без зміни адміністративної культури електронний інструмент часто відтворює стару процедуру в новому інтерфейсі. У результаті користувач бачить цифрову оболонку й стикається із затримками, повторним поданням документів і нечіткими підставами для відмови.

З позиції публічного управління цифрове врядування потрібно оцінювати через відповідальність конкретних суб'єктів. У практичному вимірі мають бути визначені ті, хто виправляє помилку в реєстрі, якщо вона блокує послугу; пояснює причину відмови після алгоритмічної перевірки; інформує громадян під час збою; контролює сторонніх постачальників цифрових компонентів. За відсутності таких відповідей цифрова держава може мати розвинену технологічну інфраструктуру, зберігаючи слабкість з погляду адміністративної справедливості.

Для підвищення конкурентоспроможності держави цифрове врядування має працювати на публічну цінність. До її змісту належать: доступність, безпека, швидкість, прозорість, передбачуваність, участь громадян і повага до прав користувача. Якщо один із цих елементів системно випадає, соціальний ефект цифровізації звужується, а висока якість сервісу для цифрово впевнених громадян може співіснувати з бар'єрами для тих, хто має слабший доступ до інтернету, нижчі навички або складнішу життєву ситуацію. У такому разі держава втрачає частину управлінського результату, навіть за умов подальшого розширення цифрової інфраструктури.

Цифрове врядування як чинник конкурентоспроможності держави потребує управління ризиками протягом усього життєвого циклу послуги. На етапі проєктування варто оцінювати функціональність, зрозумілість процедури, можливі бар'єри та потреби груп користувачів, для яких цифровий формат може бути складним. Під час запуску значення мають: тестування, навчання персоналу, підготовка інструкцій і створення каналів підтримки. У процесі експлуатації, своєю чергою, потрібні моніторинг інцидентів, аналіз скарг, перевірка якості даних, аудит алгоритмічних рішень і регулярне оновлення правил безпеки.

Висновки та пропозиції. Проведене дослідження дає підстави стверджувати, що цифрове врядування підвищує конкурентоспроможність держави через скорочення адміністративних витрат, прискорення

процедур, розвиток роботи з даними, більшу прозорість, підтримку електронної участі та зміцнення довіри до публічних інституцій. Зазначений ефект залежить від якості сервісного маршруту, стійкості цифрової інфраструктури, захисту персональних даних, доступності для різних груп населення та здатності органів влади швидко виправляти помилки. Тому запуск онлайн-сервісу має супроводжуватися переглядом цифрової процедури, її спрощенням, поясненням користувачу та перевіркою стійкості до збоїв.

Кібербезпека у цифровому врядуванні має розглядатися як частина управлінської спроможності держави. Вона охоплює захищену архітектуру сервісів, контроль доступу, резервування, підготовку до інцидентів, зрозумілу кризову комунікацію та відновлення послуг у прийнятні строки. Для громадян і бізнесу цифровий канал має бути надійним, передбачуваним і правово зрозумілим, адже ці характеристики переводять зручність сервісу у сталу довіру до держави.

Нерівний доступ і цифровий розрив зменшують фактичне охоплення цифрового врядування. Їх причинами стають слабкий інтернет, нестача пристроїв, низький рівень навичок, складні форми, складні для доступу інтерфейси, обмежена консультаційна підтримка та відсутність змішаних каналів обслуговування. З огляду на це цифрову інклюзію доцільно включати в проєктування послуг на ранньому етапі, враховуючи потреби людей старшого віку, осіб з особливими потребами, внутрішньо переміщених осіб, мешканців малих громад і користувачів із нижчою цифровою впевненістю.

Науковий результат статті полягає в розробленні ризик-орієнтованої рамки аналізу цифрового врядування, яка поєднує безпекову, інклюзивну, інституційно-довірчу та координаційну площини. Вона пов'язує цифрові реформи з якістю користування сервісами, стійкістю інфраструктури, доступністю процедур, прозорістю цифрових рішень і відповідальністю органів влади перед користувачем. Практична цінність матриці полягає в її використанні для аудиту електронних послуг, підготовки стратегій цифрового розвитку, програм цифрової грамотності та оцінювання сервісної якості публічного управління.

Подальші дослідження варто спрямувати на систему індикаторів, за допомогою яких можна кількісно оцінити зв'язок між цифровим врядуванням і конкурентоспроможністю держави. Окремого аналізу потребують моделі кіберстійкості публічних сервісів, механізми підтримки вразливих груп, правове регулювання алгоритмічних рішень і вплив цифрових послуг на довіру громадян до публічної влади.

ЛІТЕРАТУРА

1. OECD. The OECD Digital Government Policy Framework: Six dimensions of a Digital Government. *OECD Public Governance Policy Papers*. 2020. № 02. Paris: OECD Publishing. DOI: https://doi.org/10.1787/f64fed2a-en.

2. OECD. 2023 OECD Digital Government Index: Results and key findings. *OECD Public Governance Policy Papers*. 2024. Paris: OECD Publishing. DOI: https://doi.org/10.1787/1a89ed5e-en.

3. United Nations. United Nations E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development. New York: United Nations, 2024. DOI: https://doi.org/10.18356/9789211067286.

4. Sagarik D. Enhancing Digital Competitiveness Through the Lens of Digital Government Among Asian Economies. *International Journal of Public Administration in the Digital Age*. 2023. Vol. 10. No 1. Pp. 1 – 11. DOI: https://doi.org/10.4018/IJPADA.326122.

5. Mettler T., Miscione G., Jacobs C. D., Guenduez A. A. Same same but different: How policies frame societal-level digital transformation. *Government Information Quarterly*. 2024. Vol. 41. No 2. Article 101932. DOI: https://doi.org/10.1016/j.giq.2024.101932.

6. OECD. Digital public infrastructure for digital governments. *OECD Public Governance Policy Papers*. 2024. № 68. Paris: OECD Publishing. DOI: https://doi.org/10.1787/ff525dc8-en.

7. Haug N., Dan S., Mergel I. Digitally-induced change in the public sector: a systematic review and research agenda. Public Management Review. 2024. Vol. 26. No 7. Pp. 1963 – 1987. DOI: https://doi.org/10.1080/14719037.2023.2234917.

8. Gupta P., Hooda A., Jeyaraj A., Seddon J. J. M., Dwivedi Y. K. Trust, Risk, Privacy and Security in e-Government Use: Insights from a MASEM Analysis. *Information Systems Frontiers*. 2025. Vol. 27. Pp. 1089 – 1105. DOI: https://doi.org/10.1007/s10796-024-10497-8.

9. Li Y., Shang H. How does e-government use affect citizens' trust in government? Empirical evidence from China. *Information and Management*. 2023. Vol. 60. No 7. Article 103844. DOI: https://doi.org/10.1016/j.im.2023.103844.

10. Mesa D. Digital divide, e-government and trust in public service: The key role of education. *Frontiers in Sociology*. 2023. Vol. 8. Article 1140416. DOI: https://doi.org/10.3389/fsoc.2023.1140416.

11. Liu H., Zhou Q., Liang S. Digital inclusion in public services for vulnerable groups: A systematic review for research themes and goal-action framework from the lens of public service ecosystem theory. *Government Information Quarterly*. 2025. Vol. 42. No 2. Article 102019. DOI: https://doi.org/10.1016/j.giq.2025.102019.

12. Peeters R., Miller S. M., Schuilenburg M. Digital government inclusion: Exploring strategies for inclusive government automation. *Government Information Quarterly*. 2025. Vol. 42. No 2. Article 102028. DOI: https://doi.org/10.1016/j.giq.2025.102028.

13. Sabani A., Thai V., Hossain M. A. Factors Affecting Citizen Adoption of E-Government in Developing Countries. *Journal of Global Information Management*. 2023. Vol. 31. No 1. Pp. 1 – 27. DOI: https://doi.org/10.4018/JGIM.318131.

REFERENCES

1. OECD. (2020). The OECD Digital Government Policy Framework: Six dimensions of a Digital Government. *OECD Public Governance Policy Papers,* No 02. OECD Publishing. https://doi.org/10.1787/f64fed2a-en.

2. OECD. (2024). 2023 OECD Digital Government Index: Results and key findings. *OECD Public Governance Policy Papers*. OECD Publishing. https://doi.org/10.1787/1a89ed5e-en.

3. United Nations. (2024). United Nations E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development. United Nations. https://doi.org/10.18356/9789211067286.

4. Sagarik, D. (2023). Enhancing digital competitiveness through the lens of digital government among Asian economies. *International Journal of Public Administration in the Digital Age,* 10(1), 1 – 11. https://doi.org/10.4018/IJPADA.326122.

5. Mettler, T., Miscione, G., Jacobs, C. D., & Guenduez, A. A. (2024). Same same but different: How policies frame societal-level digital transformation. *Government Information Quarterly,* 41(2), 101932. https://doi.org/10.1016/j.giq.2024.101932.

6. OECD. (2024). Digital public infrastructure for digital governments. *OECD Public Governance Policy Papers,* No 68. OECD Publishing. https://doi.org/10.1787/ff525dc8-en.

7. Haug, N., Dan, S., & Mergel, I. (2024). Digitally-induced change in the public sector: a systematic review and research agenda. *Public Management Review,* 26(7), 1963 – 1987. https://doi.org/10.1080/14719037.2023.2234917.

8. Gupta, P., Hooda, A., Jeyaraj, A., Seddon, J. J. M., & Dwivedi, Y. K. (2025). Trust, risk, privacy and security in e-government use: Insights from a MASEM analysis. *Information Systems Frontiers,* 27, 1089 – 1105. https://doi.org/10.1007/s10796-024-10497-8.

9. Li, Y., & Shang, H. (2023). How does e-government use affect citizens' trust in government? Empirical evidence from China. *Information and Management*, 60(7), 103844. https://doi.org/10.1016/j.im.2023.103844.

10. Mesa, D. (2023). Digital divide, e-government and trust in public service: The key role of education. *Frontiers in Sociology,* 8, 1140416. https://doi.org/10.3389/fsoc.2023.1140416.11.

11. Liu, H., Zhou, Q., & Liang, S. (2025). Digital inclusion in public services for vulnerable groups: A systematic review for research themes and goal-action framework from the lens of public service ecosystem theory. *Government Information Quarterly,* 42(2), 102019. https://doi.org/10.1016/j.giq.2025.102019.

12. Peeters, R., Miller, S. M., & Schuilenburg, M. (2025). Digital government inclusion: Exploring strategies for inclusive government automation. *Government Information Quarterly,* 42(2), 102028. https://doi.org/10.1016/j.giq.2025.102028.

13. Sabani, A., Thai, V., & Hossain, M. A. (2023). Factors affecting citizen adoption of e-government in developing countries. *Journal of Global Information Management,* 31(1), 1 – 27. https://doi.org/10.4018/JGIM.318131.