ECONOMIES' HORIZONS
Економічні горизонти

DOI: doi.org/10.31499/2616-5236
Homepage: http://eh.udpu.edu.ua

ISSN 2522-9273 (print)
2616-5236 (online)

UDC: 658.15:005.21

JEL Classification G31, G32, M21

DOI: 10.31499/2616-5236.2(35).2026.357282

Received 16.02.2026
Accepted 23.03.2026
Published 10.04.2026

Oleksii Zakharkin, *Sumy State University*
Doctor of Economic Sciences, Professor, Associate Professor of the Department of Financial Technologies and Entrepreneurship

Liudmyla Zakharkina, *Sumy State University*
PhD in Economics, Associate Professor, Associate Professor of the Department of Financial Technologies and Entrepreneurship

Oleksandr Hrytsenko, *Sumy State University*
PhD Student

КАРТА ПОТЕНЦІЙНИХ МОЖЛИВОСТЕЙ ТА РИЗИКІВ ЗАСТОСУВАННЯ ІННОВАЦІЙНО-ЦИФРОВИХ ТЕХНОЛОГІЙ У ПУБЛІЧНО-ПРИВАТНОМУ ПАРТНЕРСТВІ

MAP OF POTENTIAL OPPORTUNITIES AND RISKS OF THE APPLICATION OF INNOVATIVE DIGITAL TECHNOLOGIES IN PUBLIC-PRIVATE PARTNERSHIP

Анотація: *У статті досліджено можливості та ризики застосування інноваційно-цифрових технологій (ІЦТ) у публічно-приватному партнерстві (ППП) в умовах воєнних загроз і післявоєнного відновлення України. У роботі використано методи системного та структурно-функціонального аналізу, порівняння, узагальнення та ризик-орієнтований підхід. Сформовано аналітичну карту потенційних можливостей і ризиків застосування ШІ, IoT, блокчейн-технологій, цифрових платформ та хмарних сервісів у ППП. Отримані результати можуть бути використані для підвищення прозорості, стійкості та безпеки державних інвестиційних рішень.*

Abstract: *The article examines the opportunities and risks associated with the application of innovative digital technologies in public-private partnership (PPP) projects under conditions of military threats and post-war recovery in Ukraine. The purpose of the study is to provide a systematic justification of how digital solutions affect the efficiency, transparency, resilience, and security of PPP project life-cycle management. The research is based on a combination of systemic and structural-functional analysis, comparative analysis, generalization, and a risk-oriented approach to digital governance.*

The paper identifies key groups of innovative digital technologies relevant to PPP implementation, including artificial intelligence and data analytics, distributed ledger technologies, Internet of Things solutions, digital PPP management platforms, cloud services, and electronic identification tools. The study demonstrates that digitalization of PPPs can significantly enhance ex-ante and ex-post control, reduce transaction costs, improve monitoring of contractual obligations, and strengthen the resilience of critical infrastructure projects. At the same time, it reveals that each technological group generates specific risks related to cybersecurity, data protection, regulatory compliance, ethical issues, institutional capacity, and technological dependence.

As a result, an analytical map of potential opportunities and risks of innovative digital technologies in PPPs is developed. This map can serve as a practical analytical tool for public authorities when designing, selecting, implementing, and monitoring PPP projects in the context of wartime challenges and post-war reconstruction. The findings emphasize that the effectiveness of digital PPPs depends on the integration of technological solutions with open data standards, robust platform governance, contractual risk allocation, and the preservation of meaningful human oversight over automated decision-making processes.

Keywords: *public-private partnership, digital transformation, innovative digital technologies, risk management, cybersecurity, transparency, digital platforms, post-war recovery.*

Ключові слова: *публічно-приватне партнерство, цифровізація, інноваційні технології, управління ризиками, кібербезпека, прозорість, цифрові платформи, відбудова України*

Постановка проблеми. Воєнні дії та ракетно-дронові атаки по критичній інфраструктурі створюють нові виклики для виробничих, логістичних, енергетичних і фінансових контурів економіки, що ускладнює як поточне функціонування держави, так і реалізацію великомасштабних програм відновлення. Системний характер загроз підсилює потребу у технологічних рішеннях, які одночасно забезпечують швидкість (оперативність), прозорість (доброчесність), стійкість (resilience) і безпеку (cyber/physical) у державних інвестиціях і партнерствах.

Публічно-приватне партнерство розглядається як інструмент, що дозволяє залучати приватні інвестиції, компетенції та інновації до реалізації суспільно значущих послуг/інфраструктури, передаючи частину ризиків приватному партнеру та структуруючи відносини через довгостроковий договір. Новий Закон України «Про публічно-приватне партнерство» концептуально закріплює ці ознаки та розширює/нормує застосування ППП у цифровій сфері (електронні комунікації, цифрова інфраструктура, ІТ та кібербезпека). [1]

Разом із тим, «цифрове ППП» формує новий клас системних ризиків: кіберризики, ризики захисту персональних даних і прав людини, технологічні та регуляторні ризики (включно з відповідністю нормам ЄС у контексті євроінтеграції), ризики корупційних/непрозорих рішень, ризики залежності від постачальників (vendor lock-in), а для технологій подвійного призначення – додаткові безпекові та етичні дилеми. [2].

Отже, в умовах воєнних загроз і післявоєнної відбудови актуалізується потреба у науково обґрунтованому визначенні можливостей та ризиків застосування інноваційно-цифрових технологій у публічно-приватному партнерстві як інструменту підвищення прозорості, стійкості та безпеки державних інвестиційних рішень.

Аналіз останніх досліджень і публікацій. ППП у міжнародних підходах розглядається як довгостроковий контрактний механізм надання суспільно значущих послуг/інфраструктури з розподілом ризиків між публічним і приватним партнерами, що потребує чіткої політико-правової та інституційної рамки. У «PPP Reference Guide 3.0» акцентовано, що «PPP framework» має охоплювати ідентифікацію, оцінювання, відбір, бюджетування, закупівлю, моніторинг і облік зобов'язань, а також запобігати надмірним фіскальним ризикам через прозорість та підзвітність [3]

Паралельно в літературі з цифрового врядування ключовими є принципи «government as a platform», «data-driven public sector», «open by default» і ризик-орієнтований підхід до безпеки й приватності. В публікаціях OECP (OECD) підкреслюється, що реалізація цифрових стратегій пов'язана не лише з технологіями, а насамперед із моделями координації, лідерством, вимірюванням результатів та управлінням ризиками безпеки/приватності. [4].

Окремий блок джерел стосується прозорості публічних контрактів через стандарти відкритих даних. Open Contracting Partnership підтримує Open Contracting Data Standard (OCDS), який описує публікацію даних і документів на всіх стадіях закупівельного/контрактного циклу та покликаний посилити прозорість і аналітику контрактування [5]. Для інфраструктури та проєктного циклу релевантним є OC4IDS (Open Contracting for Infrastructure Data Standard), що поєднує контрактні дані з проєктним рівнем і прямо описує застосування для інфраструктурних проєктів та відповідних контрактів.

Український контекст цифрової держави демонструє готовність до «платформенного підходу». У звіті OECP (OECD) (2024) описано екосистему Дія (портал, застосунок, Diia.Business, Diia.Engine тощо) як один із міжнародно визнаних результатів цифровізації; застосунок запущено у 2020 р. і він «будується на» інтероперабельній децентралізованій системі обміну даними «Trembita» [6]. Це важливо

для ППП, оскільки цифровізація ППП потребує інтеграції даних реєстрів, контрактів і проєктних реєстрів для належної підготовки, конкурсного відбору та подальшого моніторингу.

У сфері закупівель українська система ProZorro позиціонується як електронна платформа, що з'єднує десятки тисяч замовників і сотні тисяч постачальників на базі електронних процедур та аукціону [7]. Для ППП це є «готовою інфраструктурою доброчесності» для етапів конкурентного відбору приватного партнера й закупівель у межах контрактів (з урахуванням правового режиму конкретного ППП).

У наукових українських публікаціях, релевантних для теми, підкреслюються необхідність адаптації правового регулювання ППП до нових сфер (наука/інновації) у контексті закону №4510-IX, формування державно-приватних партнерств у кібербезпеці та роль цифровізації/ІКТ у таких взаєминах, застосування інноваційних технологій у моделях ДПП/ППП за досвідом ЄС, постановка ППП як механізму повоєнного відновлення [8].

Разом з тим, попри наявність напрацювань щодо інституційної рамки ППП, принципів цифрового врядування та стандартів відкритих даних, у науковій літературі залишається недостатньо систематизованим комплексний підхід до одночасної оцінки можливостей і ризиків застосування інноваційно-цифрових технологій у ППП, особливо в умовах воєнних загроз та післявоєнного відновлення, що й зумовлює потребу подальших досліджень у цьому напрямі.

Формулювання мети статті. Метою статті є системне обґрунтування потенційних можливостей і ризиків застосування інноваційно-цифрових технологій у публічно-приватному партнерстві в умовах воєнних загроз та повоєнного відновлення України, а також формування аналітичної карти їх впливу на ефективність управління життєвим циклом ППП-проєктів.

Для досягнення поставленої мети в статті передбачено вирішення таких завдань:

– узагальнити сучасні теоретичні підходи та міжнародні практики використання цифрових технологій у публічно-приватному партнерстві;

– ідентифікувати ключові групи інноваційно-цифрових технологій, релевантних для підготовки, реалізації та моніторингу ППП-проєктів;

– визначити основні можливості цифровізації ППП з позицій підвищення прозорості, ефективності, стійкості та безпеки інфраструктурних і сервісних проєктів;

– систематизувати технологічні, кібербезпекові, регуляторні та інституційні ризики цифрового ППП, актуальні для воєнного й повоєнного періодів;

– сформувати аналітичну карту взаємозв'язку можливостей і ризиків застосування інноваційно-цифрових технологій у ППП як інструмент підтримки

управлінських рішень у сфері державних інвестицій та відбудови.

Виклад основного матеріалу. Станом на 01.01.2026 в Україні було укладено 201 договір на умовах ППП, але реалізовувалося лише 19; 171 договір не реалізовувався, а 11 – призупинено у зв'язку зі збройною агресією рф. Це одночасно вказує на значний «портфельний потенціал» і системні інституційні бар'єри, які у воєнний/повоєнний періоди мають бути подолані, зокрема через цифрові інструменти життєвого циклу ППП та управління ризиками. [9].

Нижче наведено аналітичну порівняльну таблицю – карту потенційних можливостей та ризиків застосування інноваційно-цифрових технологій у публічно-приватному партнерстві (орієнтовні рівні готовності/вартості є сценарними й залежать від масштабу проєкту, кількості реєстрів/інтеграцій, вимог до кіберзахисту та критичності інфраструктури; для точного бюджетування потрібна TCO-оцінка на рівні конкретного проєкту ППП). Підхід до класифікації базується на принципах цифрового врядування та управління кібер/AI-ризиками. [10]

Таблиця 1

Карта потенційних можливостей та ризиків застосування інноваційно-цифрових технологій у публічно-приватному партнерстві

Технологія	Потенційні можливості в ППП	Ключові ризики
ШІ / аналітика даних (вкл. GenAI)	Прогноз попиту/доходів; виявлення аномалій у контрактах/кошторисах; оптимізація техобслуговування; прискорення підготовки документів і «data room» (за умов контролю).	Упередженість/помилки моделей; непрозорість рішень; витоки даних; ризик «автоматизованого» ухвалення рішень без належного людського контролю; регуляторні обмеження (особливо для high-risk).
Блокчейн / DLT	Незаперечність записів (аудит-трейл); потенційно – відстеження критичних поставок/матеріалів; смарт-контракти для окремих тригерів/платежів (обережно).	Юридична невизначеність смарт-контрактів; складність масштабування; помилки коду; ілюзія «антикорупційності» без інституцій; ризики ключів/ідентифікації.
IoT / edge-сенсори	Моніторинг інфраструктури в реальному часі (мости, мережі, водоканали, енергетика); зменшення аварійності; доказова база виконання KPI; підсилення стійкості критичної інфраструктури.	Кібервразливості пристроїв; фізичне знищення/перехоплення; помилки даних; залежність від зв'язку/електрики (воєнні умови).
Цифрові платформи управління ППП (портфелі/проєктні реєстри)	Єдиний «ринок проєктів» для інвесторів; прозорі стадії підготовки; контроль виконання; зниження транзакційних витрат; координація донорів/грантів (що прямо передбачено як джерело фінансування ППП).	«Захоплення платформи» (governance capture); неякісні дані; фрагментація (різні реєстри); кіберризики; vendor lock-in
Кібербезпека (CSF 2.0, SOC, Zero Trust)	Захист критичних даних ППП; зменшення простоїв; захист ланцюгів постачання; виконання вимог до критичної інфраструктури.	Висока вартість і кадрові дефіцити; складність інтеграції вимог у контракти; ризик формального комплаєнсу
Хмарні сервіси (cloud)	Масштабованість під пікові навантаження; швидкість запуску сервісів; резервування; можливість швидкого відновлення після інцидентів	Залежність від провайдера; питання суверенітету даних; вимоги до безпеки/ідентифікації; ризики конфігурацій
Електронна ідентифікація та довірчі послуги (eID/e-підпис)	Юридично значимі електронні документи; дистанційні конкурси/підписання; зменшення людського фактора; прискорення процедур	Компрометація ключів; шахрайство; нерівний доступ; потреба управління доступом до реєстрів

Джерело: сформовано авторами на основі джерел [1, 2, 10, 11].

Використання інструментів штучного інтелекту (ШІ), включно з аналітикою великих даних та генеративними моделями, відкриває можливості для підвищення якості підготовки та супроводу ППП-проєктів. Зокрема, ШІ може застосовуватися для прогнозування попиту на інфраструктурні послуги, моделювання грошових потоків, оцінки фіскальних ризиків, а також виявлення аномалій у кошторисах і контрактах. У поєднанні з відкритими даними (наприклад, закупівель або проєктних реєстрів) аналітичні алгоритми здатні посилити ex-ante та ex-post контроль за реалізацією ППП.

Водночас надмірна автоматизація управлінських рішень породжує ризики алгоритмічної упередженості, непрозорості моделей («black box effect») та потенційного порушення принципу людського контролю. Особливо чутливими є ризики витоку даних і невідповідності регуляторним вимогам щодо високоризикових систем ШІ, що актуально в контексті гармонізації з нормами ЄС та рекомендаціями NIST щодо управління AI-ризиками

Технології розподіленого реєстру можуть використовуватися в ППП як інструмент забезпечення незаперечності та простежуваності транзакцій, формуючи захищений аудит-трейл для ключових рішень і фінансових операцій. У межах інфраструктурних проєктів блокчейн потенційно дозволяє відстежувати походження матеріалів, виконання контрактних умов або тригерні платежі за смарт-контрактами.

Однак практична цінність DLT у ППП значною мірою залежить від інституційного середовища. Без належної правової визначеності смарт-контрактів та інтеграції з традиційними правовими механізмами блокчейн може створювати лише ілюзію антикорупційності. Додаткові ризики пов'язані з масштабованістю рішень, помилками програмного коду та управлінням криптографічними ключами, що є критичним для проєктів із високою суспільною значущістю.

Інтернет речей (IoT) та edge-сенсори відіграють ключову роль у моніторингу фізичного стану інфраструктури, що є особливо актуальним для ППП у сферах транспорту, енергетики, водопостачання та критичної інфраструктури. Реальний час збору даних дозволяє зменшувати аварійність, оптимізувати технічне обслуговування та формувати доказову базу виконання KPI приватним партнером.

Водночас у воєнних і повоєнних умовах суттєво зростають ризики кібер- і фізичної вразливості сенсорних мереж: пошкодження обладнання, перехоплення сигналів, спотворення даних або залежність від нестабільного електропостачання й зв'язку. Це потребує інтеграції вимог кіберстійкості безпосередньо в контракти ППП та застосування підходів Zero Trust.

Платформні рішення (портфелі ППП, проєктні реєстри, цифрові «data rooms») формують основу для системного управління портфелем ППП та взаємодії з

інвесторами й донорами. Єдиний цифровий простір дозволяє зменшити транзакційні витрати, підвищити прозорість стадій підготовки та реалізації проєктів, а також координувати різні джерела фінансування, включно з грантовими й донорськими коштами, що прямо передбачено чинним законодавством.

Ключовими ризиками є захоплення платформи (governance capture), фрагментація даних між різними реєстрами, низька якість первинної інформації та технологічна залежність від постачальників (vendor lock-in). Це вимагає чітких правил управління платформами, відкритих стандартів даних і прозорих механізмів доступу.

Кібербезпека, хмарні технології та електронна ідентифікація формують базовий інфраструктурний рівень цифрового ППП. Хмарні сервіси забезпечують масштабованість і швидке відновлення, а eID та електронний підпис – юридичну значущість дистанційних процедур і контрактів. Водночас висока вартість кіберзахисту, кадровий дефіцит і ризики формального комплаєнсу без реальної стійкості залишаються суттєвими обмеженнями.

Висновки

Впровадження інноваційно-цифрових технологій у публічно-приватне партнерство формує якісно нову модель управління життєвим циклом ППП-проєктів в умовах воєнних загроз і повоєнного відновлення. Доведено, що цифровізація ППП не зводиться до окремих ІТ-рішень, а виступає системною трансформацією інституційної, контрактної та технологічної архітектури взаємодії держави й бізнесу.

Результати дослідження свідчать, що застосування штучного інтелекту, аналітики даних, IoT, блокчейн-технологій, хмарних сервісів, електронної ідентифікації та платформних рішень здатне підвищити прозорість, ефективність і стійкість ППП-проєктів, знизити транзакційні витрати, посилити контроль за виконанням контрактних зобов'язань і управління ризиками. Водночас встановлено, що кожна з технологічних груп генерує специфічні ризики – кібербезпекові, регуляторні, етичні, інституційні та ризики технологічної залежності, які без належного врегулювання можуть нівелювати потенційні переваги цифровізації.

Запропонована в статті карта можливостей і ризиків інноваційно-цифрових технологій у ППП дозволяє систематизувати ці ефекти та може бути використана як аналітичний інструмент для ухвалення управлінських рішень на етапах підготовки, відбору, реалізації й моніторингу ППП-проєктів. Особливо підкреслено, що ефективність цифрового ППП залежить від поєднання технологічних рішень із відкритими стандартами даних, чіткими правилами управління платформами, контрактним закріпленням вимог до кіберстійкості та збереження людського контролю над автоматизованими рішеннями.

Перспективи подальших наукових розвідок пов'язані з розробленням кількісних методик оцінювання цифрової зрілості ППП-проєктів, моделей інтеграції AI- та data-driven інструментів у фіскальний і ризик-менеджмент ППП, а також із дослідженням практик гармонізації українського регулювання цифрового ППП з нормами ЄС. Окремим напрямом є емпіричний аналіз ефективності конкретних цифрових рішень у ППП-проєктах критичної інфраструктури в умовах війни та післявоєнного відновлення, що дозволить поглибити наукові висновки та підвищити прикладну цінність результатів дослідження.

Стаття підготовлена за результатами дослідження, що фінансується за рахунок бюджетних коштів МОН України «Цифровізація системи публічно-приватного партнерства як драйвер економічної безпеки держави у воєнний і повоєнний періоди» (реєстраційний номер: 0126U000543).

References

Pro publichno-pryvatne partnerstvo: Zakon Ukrainy vid 19 chervnia 2025 roku № 4510-IX. URL: https://zakon.rada.gov.ua/laws/show/4510-20#Text [in Ukrainian].

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper No. NIST CSWP 29). U.S. Department of Commerce. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

World Bank. (2017). PPP Reference Guide – PPP Framework. World Bank Group. URL: https://ppp.worldbank.org/library/ppp-reference-guide-ppp-framework

OECD. (2019). The path to becoming a data-driven public sector (OECD Digital Government Studies). OECD Publishing. URL: https://doi.org/10.1787/059814a7-en

Open Contracting Partnership. (2026). Open Contracting Data Standard (OCDS). Retrieved February 15, 2026. URL: https://standard.open-contracting.org/latest/en/

OECD. (2024). Enhancing resilience by boosting digital business transformation in Ukraine (OECD Publishing). OECD. URL: https://doi.org/10.1787/4b13b0bb-en

Prozorro. (n.d.). About (English home page). Retrieved February 15, 2026. URL: https://prozorro.gov.ua/en

Chaltseva, O. M., & Loboda, D. O. (2024). Derzhavno-pryvatne partnerstvo yak perspektyvnyi mekhanizm povoiennoho vidnovlennia Ukrainy. Public networks and communications, (2), 11–18. URL: https://doi.org/10.31558/3083-5895.2024.2.2

Stan zdiisnennia DPP v Ukraini. Ministerstvo ekonomiky, dovkillia ta silskoho hospodarstva Ukrainy. Vebsait. URL: https://me.gov.ua/Documents/Detail/9fc90c5e-2f7b-44b2-8bf1-1ffb7ee1be26?lang=uk-UA&title=StanZdiisnenniaDppVUkraini

OECD. (2021). The E-Leaders Handbook on the Governance of Digital Government (OECD Digital Government Studies). OECD Publishing. https://doi.org/10.1787/ac7f2531-en

Tabassi, E. (2023). AI Risk Management Framework. National Institute of Standards and Technology. https://doi.org/10.6028/nist.ai.100-1