

А. О. Сидорчук,
докторант кафедри економіки та менеджменту,
Український державний університет науки і технологій
ORCID ID: <https://orcid.org/0000-0002-7420-7405>

DOI: 10.32702/2306-6814.2026.10.529

СТРАТЕГІЧНЕ УПРАВЛІННЯ СТІЙКІСТЮ СМАРТ-ІНФРАСТРУКТУРИ ТРАНСПОРТУ УКРАЇНИ НА ЗАСАДАХ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА ТА СОЦІАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ БІЗНЕСУ

A. Sydorчук,
Doctoral candidate of the Department of Economics and Management,
Ukrainian State University of Science and Technologies

STRATEGIC MANAGEMENT OF THE RESILIENCE OF UKRAINE'S SMART
TRANSPORT INFRASTRUCTURE BASED ON PUBLIC-PRIVATE
PARTNERSHIP AND CORPORATE SOCIAL RESPONSIBILITY

Актуальність дослідження зумовлена потребою розробки стратегій управління транспортною смарт-інфраструктурою України в умовах війни, цифровізації, ресурсних обмежень та європейської інтеграції. Наукова новизна полягає в обґрунтуванні концептуального підходу, у межах якого стійкість розглядається не як характеристика окремих об'єктів, а як здатність критичних транспортних послуг зберігати функціональність і відновлюватися після фізичних, цифрових, енергетичних та інституційних збоїв. Методологічну основу становлять теорія інфраструктурної стійкості, підходи до державно-приватного партнерства, соціальної відповідальності бізнесу, кіберфізичної безпеки та стратегічного управління. Запропоновано систему принципів і показників договірного управління стійкістю, що поєднує доступність послуг, відновлюваність, цифрову надійність, фінансову забезпеченість і соціальну прийнятність. Практична цінність полягає у можливості використання результатів для підготовки проєктів ДПП, удосконалення контрактів, контролю ризиків і формування політики післявоєнного відновлення транспорту.

The relevance of this research is determined by the need to rethink the strategic management of Ukraine's smart transport infrastructure under pressure from war, digital transformation, resource scarcity and European integration. Destruction of transport assets, the vulnerability of logistics corridors, the dependence of control systems on energy and data networks, and the growth of cyber risks require a shift from object-centred reconstruction to the management of critical transport services. Scientific novelty lies in the development of a conceptual approach in which resilience is interpreted as the capacity of transport services, corridors and nodes to maintain core functions, recover in an acceptable period and operate under repeated physical, digital, financial, institutional and social disruptions. The methodology combines infrastructure resilience theory, strategic management, public-private partnership, corporate social responsibility, cyberphysical security and responsible business conduct. Article substantiates the role of public-private partnership not merely as a mechanism for attracting capital, but as a contractual framework for allocating responsibility

for service availability, recovery speed, cyber security, transparency and social acceptability. Corporate social responsibility is considered not as a reputational supplement, but as an operational component of resilience, covering labour safety, human rights, accessibility, stakeholder engagement, data protection and grievance mechanisms. A system of principles and indicators for contractual resilience management is proposed. It integrates service continuity, recoverability, digital reliability, life-cycle financial sustainability, accountability and social compliance. The practical significance lies in its use for preparing partnership projects, designing resilience-oriented contracts, monitoring risks and forming Ukraine recovery policy. The proposed approach may support authorities, operators, private partners and donors in prioritising investments, strengthening institutional capacity and aligning recovery with European requirements. Future research should test the indicators in transport corridors and develop model contractual provisions for smart transport infrastructure.

Ключові слова: Смарт-інфраструктура, транспорт, стійкість, державно-приватне партнерство, соціальна відповідальність бізнесу, кібербезпека, воєнний стан, європейська інтеграція.

Key words: smart infrastructure, transport, resilience, public-private partnership, corporate social responsibility, cybersecurity, martial law, European integration.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Війна зробила транспортну інфраструктуру України полем не лише інженерної, а й управлінської кризи: під ураженням опинилися фізичні активи (колії, мости, дороги, порти, термінали), інфраструктурні вузли та цифрові контури, що забезпечують планування, диспетчеризацію, моніторинг і платіжні сервіси.

Практичне завдання держави полягає не в абстрактній "модернізації", а в утриманні здатності країни до переміщення людей і вантажів у режимі постійних обмежень; це означає підтримання мінімально прийнятних сервісів за умов повторюваних руйнувань, дефіциту ресурсів, кадрових втрат, обмежень експорту/імпорту через зміну логістичних маршрутів і зростання кіберризиків.

На цьому фоні оновлена Національна транспортна стратегія визначає потребу адаптації сектору та посилення інституційної спроможності управління, включно з цифровими рішеннями, у зв'язку з воєнними впливами та орієнтацією на європейську інтеграцію [1].

Якщо розглядати смарт-інфраструктура транспорту, то можливо зазначити, що це кіберфізична система, де цифровий контур (дані, сенсори, зв'язок, алгоритми, цифрові платформи управління проєктами та активами) впливає на фізичну функцію мережі. Європейські рамки ITS прямо трактують інтелектуальні транспортні системи як сферу, де координація і сумісність послуг є предметом регуляторної політики і оновлення ITS-рамки 2023 року підтверджує курс на масштабованість, інтероперабельність та якість даних [2].

Для України цифрова модернізація транспортної інфраструктури пов'язана з істотним ускладненням управлінських рішень. Упровадження цифрових сервісів, з одного боку, розширює можливості оперативного контролю, координації, аналітичного супроводу та підвищення прозорості управлінських процесів, а з іншого — посилює залежність функціонування інфраструктурних

об'єктів від стабільності енергозабезпечення, телекомунікаційних мереж і систем оброблення даних.

За умов порушення роботи хоча б одного з названих компонентів виникає ризик послідовного поширення збоїв на суміжні підсистеми, що може спричиняти зниження якості управління, підвищення імовірності технічних відмов, погіршення безпеки перевезень і скорочення пропускної спроможності транспортної мережі.

У такому контексті відбудова транспортної інфраструктури без попереднього закладення принципів стійкості, надійності та захищеності не лише знижує її довгострокову ефективність, а й створює додаткові інституційні та фінансові труднощі в процесі узгодження з європейськими правилами та стандартами.

У цих умовах механізми державно-приватного партнерства, включно з концесіями, набувають системного значення як інструменти мобілізації ресурсів і компетенцій на довгому горизонті.

Закон № 4510-ІХ не лише оновлює рамку ДПП, а й вводить визначення "гранту для проєктів ДПП" як безоплатного, безпроцентного і безповоротного фінансування, наданого донорами, та передбачає можливість залучення донорів до аналізу ефективності проєктів, якщо планується грантове фінансування [3].

Однак ДПП, створене для того, щоб просто "залучити гроші", не гарантує стійкості. Воєнна специфіка підштовхує до переосмислення ролі бізнесу, коли приватний партнер у транспортній смарт-інфраструктурі несе операційні обов'язки, без яких мережа не здатна підтримувати критичні послуги, а отже соціальна відповідальність бізнесу повинна розглядатися як функціональна підсистема стійкості, що формує дисципліну безпеки, підзвітності, захисту праці та цифрової відповідальності, а не як репутаційна "надбудова".

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Теоретичне поле стійкості інфраструктури історично будується на напрузі між двома школами. Екологіч-

на інтерпретація стійкості наголошує на здатності системи зберігати функції, адаптуючись до збурень, і допускає множинність можливих "стабільних" режимів, що знімає ілюзію про єдину траєкторію повернення до попереднього стану [4].

Інженерно-управлінська школа прагне операціоналізувати стійкість через вимірювані параметри. Робота М. Bruneau та співавт. запропонувала рамку кількісного оцінювання стійкості (зокрема через робастність/швидкість відновлення та "зменшення ймовірності відмов", "наслідків відмов", "часу до відновлення"), що вплинуло на формування практик KPI для критичної інфраструктури [5].

У транспортній проблематиці останніх років суттєвим є зміщення від "актив-центричного" бачення до розуміння стійкості як управлінської спроможності держави і операторів. Н. J. Liu та співавт. показали, що дефіцит критичних досліджень щодо організаційних спроможностей уряду погіршує здатність формувати дієву стратегію транспортної стійкості, автори акцентують взаємодію управлінських спроможностей і необхідність їхнього керованого розвитку [6].

Систематичний огляд Yang Yang та співавт. щодо стійкості інтегрованих міських транспортних мереж встановлює такі методичні прогалини, як нерівномірність показників, обмежену здатність моделей відображати динамічні взаємодії попиту і пропозиції, слабе врахування каскадних відмов і міжвидових зчеплень [7].

Перехід до смарт-інфраструктури стимулює інтерес до інструментів штучного інтелекту та цифрових моделей. О. О. Ажауї та співавт. досліджують потенціал AI для підсилення інфраструктурної стійкості на прикладі транспортних систем і окреслюють типові обмеження — дефіцит даних, обмежену валідацію моделей у реальних умовах та інституційні бар'єри масштабування [8].

У площині державно-приватного партнерства в українському науковому дискурсі значущими є праці, що розглядають ДПП як один із практичних механізмів повоєнного відновлення і наголошують на інституційному забезпеченні та прозорості як умовах залучення приватного капіталу. Зокрема Є. Матвіїшин і Ю. Вершигора підкреслюють роль ДПП у післявоєнній відбудові та необхідність розвитку інституційного супроводу [9].

Також проблематика стійкості транспортної інфраструктури розробляється переважно в межах досліджень залізничного транспорту, де увага поступово зміщується від опису окремих організаційно-технічних змін до питань антикризового та інституційного управління. Особливо показовими в цьому сенсі є праці Т. Ю. Чаркіної, у яких дослідження конкурентоспроможності пасажирських перевезень послідовно переростає в ширшу концепцію антикризового управління пасажирським комплексом залізничного транспорту. Їх наукове значення полягає в поєднанні проблем організації перевезень, структурної перебудови пасажирського господарства, інвестиційного забезпечення та управління розвитком галузі [10].

У працях В. О. Задой центр аналізу зміщується до цифровізації як чинника розвитку залізничного транспорту та підвищення конкурентоспроможності пасажирських перевезень. Принциповим є те, що цифрові зміни розглядаються ним не як локальне технічне онов-

лення, а як складова маркетингового управління розвитком галузі, пов'язана з якістю послуг, ринковими позиціями перевізника та обґрунтуванням управлінських рішень [11].

Такий підхід розширює український науковий дискурс і наближає його до розуміння цифрово оснащеної транспортної інфраструктури як об'єкта довгострокового управління.

Спільні праці Т. Ю. Чаркіної та В. О. Задой зі співавторами показують подальше зближення антикризової, інноваційної та цифрової проблематики. У цих дослідженнях розглядаються цифровий менеджмент як інструментарій антикризового управління розвитком підприємства, а також трансформація інноваційного управління підприємствами залізничного транспорту в умовах цифрової конвергенції та корпоративного партнерства [12].

У наявних дослідженнях виразно видно кілька розривів, які в умовах війни набувають особливої гостроти. Інженерні підходи дають змогу оцінювати відмови, їх наслідки та час відновлення, але значно слабше пояснюють, як на стійкість впливають управлінські спроможності, організаційне навчання, міжвидові зв'язки та каскадні збої в транспортній системі.

Не менш помітним є розрив між цифровим оновленням транспорту і готовністю керувати цифровими та кіберфізичними ризиками. Попри наявність підходів до захисту інтелектуального транспорту, у договорах державно-приватного партнерства ці питання часто залишаються другорядними. Водночас спрощення процедур відновлення та залучення донорських ресурсів скорочує час підготовки проєктів, але загострює питання якості обґрунтування, доброчесності та контролю.

Окремий розрив пов'язаний із соціальною відповідальністю бізнесу. У науковій літературі її розглядають як чинник суспільної прийнятності та надійності інфраструктурних проєктів, проте в вітчизняній практиці вона рідко переходить у систему показників, процедур контролю та зобов'язань на всьому життєвому циклі об'єкта.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Метою даної статті є розроблення концептуальних положень стратегічного управління розвитком і стійкістю інтелектуалізованої транспортної інфраструктури України з урахуванням механізмів державно-приватного партнерства, соціальної відповідальності бізнесу, умов воєнного стану та європейської інтеграції.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

У центрі дослідження перебуває не інфраструктура як сукупність окремих об'єктів, а система критичних транспортних послуг, що забезпечується взаємодією матеріальних елементів і цифрових засобів управління.

За такого підходу стійкість пов'язується не з фізичним збереженням активу як таким, а зі здатністю транспортної послуги зберігати своє призначення або відновлюватися у прийнятний строк без надмірних ризиків для життя людей, їхніх прав, довкілля та господарської діяльності.

У такій системі соціальну відповідальність бізнесу доцільно розглядати не як додатковий репутаційний елемент, а як складову забезпечення стійкості. Передусім вона зменшує операційну крихкість через належні умови праці, підтримання професійної спроможності персоналу, безпекове навчання, внутрішні механізми повідомлення про порушення та недопущення дискримінації.

За воєнних умов це має особливу вагу, оскільки зростання аварійності пов'язане не лише з руйнуваннями, а й з виснаженням працівників, браком підготовки та психологічним напруженням.

У міжнародних підходах відповідальність бізнесу трактується не як благодійність, а як обов'язок поважати права людини й забезпечувати дієві механізми реагування на порушення. Не менш важливою є її роль у зниженні суспільної напруги навколо інфраструктурних проєктів.

Для транспортної сфери прийнятність тарифів, рішень щодо пріоритетності відновлення та умов доступності для різних груп населення безпосередньо впливає на конфліктність реалізації, ризик судових спорів, затримки та перегляд уже ухвалених рішень. Дослідження у сфері державно-приватного партнерства показують, що соціальна відповідальність охоплює не абстрактний "соціальний блок", а сукупність чинників, від яких залежить стабільність проєкту в політичному й суспільному середовищі [13].

Для цифрово оснащеної транспортної інфраструктури ця відповідальність охоплює також роботу з даними, кіберризики, захистом користувачів та реагуванням на інциденти.

Європейські рекомендації у сфері кібербезпеки транспорту підкреслюють, що такі системи потребують узгоджених організаційних і технічних рішень між органами влади, операторами, виробниками та регуляторами [14]. В вітчизняних умовах це узгоджується з чинними вимогами у сфері кібербезпеки та кіберзахисту критичної інфраструктури.

Водночас відповідальність бізнесу має практичну цінність лише тоді, коли вона переходить у вимірювані зобов'язання, процедури контролю, перевірки результатів і механізми відповідальності. Подібний підхід уже закріплюється у європейських вимогах до корпоративної звітності та належної обачності, що створює підстави для включення таких норм до договорів державно-приватного партнерства.

Транспортна інфраструктура України нині перебуває під впливом кількох взаємопов'язаних груп загроз.

Йдеться про фізичне ураження транспортних вузлів і коридорів, енергетичні обмеження, від яких критично

залежить цифровий контур управління, кіберризиків й компрометацію даних, нестачу інвестиційних ресурсів та високу вартість капіталу, а також інституційні ризики, що виникають унаслідок прискорених процедур і дефіциту довіри.

Гострота цих викликів посилюється тим, що транспорт належить до секторів, які зазнали найбільших втрат і потребують значних ресурсів для відновлення.

У таких умовах розвиток транспортної інфраструктури має спиратися не на фрагментарне відновлення окремих об'єктів, а на цілісне управління стійкістю послуг, безпекою, цифровою надійністю та суспільною прийнятністю.

Такий підхід дає змогу розглядати фізичні, енергетичні, цифрові, фінансові, інституційні та соціальні загрози не відокремлено, а як сукупність чинників, що спільно визначають здатність транспортної мережі зберігати функціональність і відновлюватися в умовах воєнного часу (Табл. 1).

Таблиця 1. Основні елементи цифрової моделі інноваційного менеджменту структурних підрозділів залізничного транспорту

Клас ризику	Прояв у транспортній системі	Управлінські рішення в межах ДПП та СВБ	Показники оцінювання
<i>Фізичне ураження ключових вузлів</i>	Пошкодження мостів, станцій, терміналів і колійних дільниць зменшує пропускну спроможність мережі та переводить потоки на обхідні напрямки	Завчасне визначення резервних маршрутів, поетапне відновлення, створення запасів матеріалів, вимоги до технічної готовності і безпеки робіт	Час відновлення, частка вузлів із резервною схемою роботи, відновлення пропускну спроможності у встановлений строк
<i>Енергетична залежність цифрових систем</i>	Перебої з електроживленням порушують зв'язок, спостереження та диспетчерське керування	Резервне й автономне живлення критичних систем, дублювання каналів зв'язку, забезпечення безперервності послуг	Рівень доступності цифрових сервісів, час переходу на резервне живлення, кількість випадків роботи в ав. режимі
<i>Кіберризик та втрата достовірності даних</i>	Втручання в системи керування, оплати та обліку може зупинити роботу або спотворювати управлінські рішення	Постійне оцінювання кіберризику, перевірка постачальників, план реагування на інциденти, закріплення вимог щодо захисту даних у договорі	Час виявлення інциденту, час усунення наслідків, кількість критичних інцидентів
<i>Інвестиційний дефіцит</i>	Нестача коштів на утримання і відновлення пришвидшує зношення та подовжує період повернення до нормальної роботи	Поєднання приватних коштів, бюджетного фінансування і донорської підтримки, чіткий розподіл ризиків, прозорий контроль витрат	Забезпеченість витрат на утримання та відновлення, зміна вартості протягом життєвого циклу
<i>Інституційна крихкість</i>	Спрощення процедур може знижувати якість підготовки проєктів, послаблювати контроль і підвищувати недовіру	Оприлюднення ключових показників, незалежний аудит, дієвий розгляд скарг, перевірка дотримання договірних і етичних вимог	Частка проєктів із відкритими показниками результативності, кількість обгрунтованих скарг
<i>Соціальна неприйнятність</i>	Незгода щодо тарифів, пріоритетів відновлення чи доступності послуг ускладнює реалізацію проєктів і може зупинити роботи	Системна взаємодія із заінтересованими сторонами, врахування потреб маломобільних груп, прозоре обгрунтування тарифів і сервісних рішень	Рівень задоволеності користувачів, доступність послуг для маломобільних груп, кількість спорів, що призвели до зупинення робіт

Джерело: сформовано на основі [1, 3, 5, 14].

Поданий розподіл ризиків дає підстави для важливого висновку. У воєнних умовах загрози для транспортної інфраструктури не є разовими. Вони повертаються, змінюють форму і спрямовуються на найуразливіші елементи системи.

За таких обставин пріоритетом стає не лише відновлення пошкодженого, а й завчасне управління ремонтпридатністю, резервними схемами роботи та інформаційним забезпеченням. Без цього кошти на відбудову швидко втрачають результативність, оскільки система знову потребує відновлення, а витрати протягом усього строку її функціонування зростають, що знижує інвестиційну привабливість проєктів державно-приватного партнерства.

Запропонована концепція розвитку інтелектуалізованої транспортної інфраструктури ґрунтується на кількох положеннях:

- стійкість доцільно пов'язувати не з окремим об'єктом, а з мережею транспортних послуг, тому в центрі управління мають бути сервіси й коридори, а не перелік будівель чи споруд;
- джерело стійкості полягає у спроможності державних органів і операторів діяти узгоджено, накопичувати досвід, навчатися на збоях і підтримувати інституційну впорядкованість;
- у період воєнного відновлення державно-приватне партнерство має спиратися на змішане фінансування і прозорі процедури. Чинне законодавство передбачає використання грантових ресурсів і участь донорів у підготовці та оцінюванні таких проєктів, а концесійні норми скорочують часові бар'єри для відновлення, але посилюють вимоги до якості, доброчесності та контролю;
- соціальна відповідальність бізнесу набуває реального змісту лише тоді, коли вона вбудована у

систему показників результативності, процедур належної обачності та механізмів контролю і узгодження з міжнародними підходами у сфері прав людини, відповідального ведення бізнесу та корпоративної звітності.

Концепцію інтеграції інституційних, цифрових і соціально-відповідальних елементів подано на рис. 1.

Поданий рисунок показує, що соціальна відповідальність бізнесу не може існувати окремо від цифрового нагляду і договірних показників результативності. Для транспортної інфраструктури воєнного часу це не другорядне питання, а одна з умов дієздатності всієї системи.

Коли економічна частина договору існує сама по собі, а соціальні зобов'язання залишаються поза основним контуром управління, виникають дві проблеми — приватний партнер не несе належної відповідальності за безпеку, доступність і безперервність послуг, а держава, своєю чергою, не має достатньо чіткої основи для контролю, звітування та захисту суспільного інтересу. Наслідком стають втрата довіри, затягування рішень, зростання конфліктності й додаткові витрати на узгодження та виправлення помилок.

Положення, на яких ґрунтується запропонований підхід, мають прикладне значення і їхня цінність полягає не в проголошенні загальних орієнтирів, а в тому, що вони задають спосіб побудови договорів, процедур контролю та системи показників (Табл. 2).

Таблиця показує, що кожен із принципів має значення лише тоді, коли його можна перевести у процедури, обов'язки сторін і показники оцінювання.

Принцип партнерства нічого не змінює, якщо за ним не стоять чіткі вимоги до доступності послуг, роз-

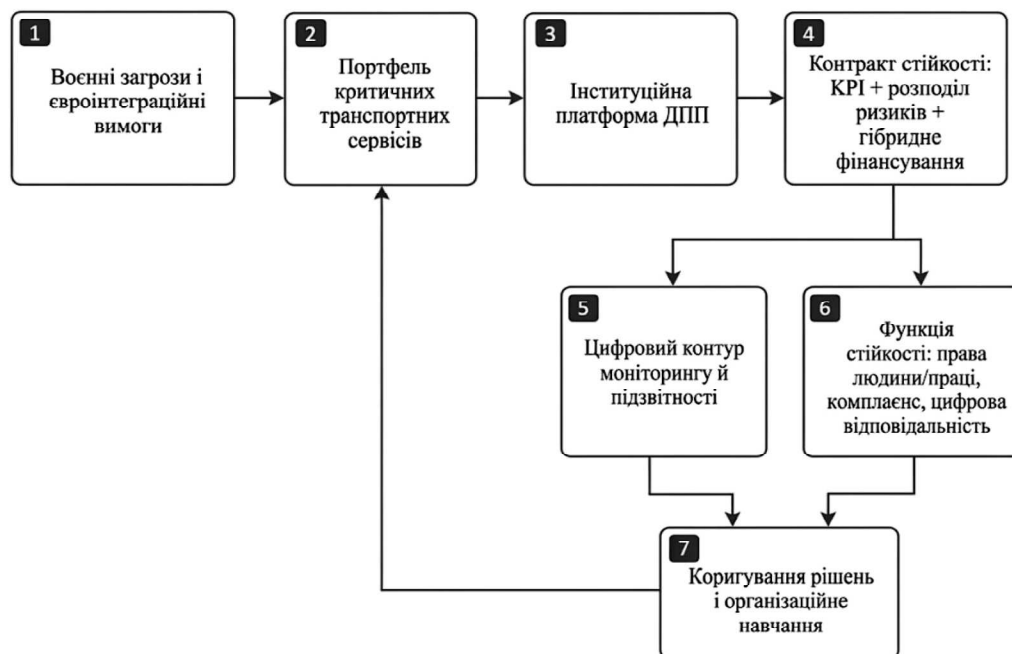


Рис. 1. Концепція стратегічного управління розвитком смарт-інфраструктури транспортної системи України

Джерело: сформовано на основі [14, 15, 16].

**Таблиця 2. Принципи стратегічного управління
стійкістю інтелектуалізованої транспортної інфраструктури
України**

Принцип	Зміст у вогнищному та відновлювальному контексті	Практичне втілення через ДПП і СВБ	Приклад показника
<i>Адаптивність</i>	Регулярне оновлення рішень відповідно до змін ризикового середовища, а не орієнтація на незмінний план	Сценарне планування, періодичний перегляд ризиків, можливість змінювати договір	Періодичність перегляду ризиків, час погодження змін
<i>Стійкість послуг</i>	Пріоритет збереження критичних перевезень і транспортних функцій, а не формального збереження об'єктів	Показники доступності та відновлення для коридорів, вузлів і сервісів	Рівень доступності послуги, час відновлення функцій
<i>Інтегрованість</i>	Урахування залежностей між енергозабезпеченням, зв'язком, транспортом і даними	Міжвідомчі протоколи, сумісність цифрових даних, спільні плани реагування	Кількість узгоджених протоколів, частота каскадних збоїв
<i>Партнерство</i>	Розподіл відповідальності між державою, бізнесом і громадами за результат, а не лише за окремі дії	Договір, зорієнтований на результат, співфінансування, система заохочень і санкцій	Виконання показників результативності, частка приватного та донорського фінансування
<i>Технологічна сумісність</i>	Узгодження рішень із європейськими вимогами, щоб не накопичувати регуляторних розривів	Дотримання вимог до інтелектуальних транспортних систем, цифрової безпеки та стійкості інфраструктури	Рівень відповідності стандартам, кількість суттєвих невідповідностей
<i>Соціальна відповідальність</i>	Захист прав людини, безпека праці, інклюзивність, робота зі зверненнями та довірою користувачів	Процедури належної обачності, розгляд звернень, забезпечення доступності послуг	Кількість і строки розгляду скарг, виробничий травматизм, рівень доступності
<i>Безпекова орієнтованість</i>	Фізична та цифрова безпека як обов'язкова умова експлуатації	Дотримання вимог кіберзахисту, перевірки захищеності, навчання персоналу	Середній час виявлення інциденту, середній час усунення наслідків, результати перевірок
<i>Підзвітність</i>	Зменшення корупційних і репутаційних ризиків, особливо за спрощених процедур	Відкриті дані щодо результативності, незалежні перевірки, цифровий нагляд	Частка відкритих показників, кількість порушень і зауважень за результатами аудиту

Джерело: сформовано на основі [16, 17, 18].

поділу відповідальності, системи стимулів і відповідальності за порушення. Так само соціальна відповідальність бізнесу не працює, якщо не пов'язана із захистом користувачів, належними умовами праці, реагуванням на скарги та перевіркою дотримання встановлених вимог.

Для транспортної інфраструктури воєнного часу це питання не морального значення, а якості управління та здатності системи працювати в умовах постійної загрози. Щоб такий підхід був придатним до практичного застосування, потрібна система показників, яка охоплює не лише технічний стан об'єктів.

Якщо оцінювання зводиться до інженерних характеристик, поза увагою залишаються питання цифрової безпеки, організаційної спроможності та суспільної довіри. Якщо ж оцінювання будується лише на соціальних характеристиках, втрачається розуміння реальної здатності мережі підтримувати перевезення і відновлювати функції після уражень.

З цієї причини доцільно поєднати показники доступності послуг, відновлення функцій, цифрової стійкості,

фінансової забезпеченості життєвого циклу та соціальної прийнятності (Табл. 3).

Ця система показників працює лише тоді, коли її можна незалежно перевірити і коли вона пов'язана з договірними стимулами. Інакше показники перетворюються на звітність, яка не впливає на поведінку сторін і не змінює якість рішень.

Європейські вимоги до корпоративної звітності та належної обачності можуть дати корисну основу для впорядкування даних і процедур контролю, але вони не замінюють показників, що характеризують доступність транспортних послуг, швидкість відновлення й роботу системи після уражень [16—17]. Для державно-приватного партнерства вирішальним залишається зв'язок між показником, перевіркою, винагородою та відповідальністю.

Запропонований підхід має свої межі і якщо немає незалежного аудиту, професійних конкурсних комісій, стабільних правил й довіри до процедур, довгострокові договори державно-приватного партнерства втрачають зміст та перетворюються на формальну оболонку без реального управління результатом.

Таблиця 3. Орієнтовна система показників для договірної управління стійкістю інтелектуалізованої транспортної інфраструктури в режимі державно-приватного партнерства

Блок показників	Зміст	Можливі показники	Коментар щодо обмежень
<i>Доступність послуг</i>	Здатність мережі забезпечувати критичні перевезення	Рівень безперервності критичних сервісів, частка виконаних графіків, доступність коридорів	Потребує чіткого визначення переліку критичних послуг
<i>Відновлюваність</i>	Швидкість і якість повернення функції після уражень	Час відновлення функції, частка відновленої пропускної спроможності у визначений строк	За повторюваних уражень потрібна постійно оновлювана база інцидентів
<i>Цифрова стійкість</i>	Здатність виявляти, локалізувати й відновлювати цифрові контури управління	Середній час виявлення інциденту, середній час усунення наслідків, частка систем із оновленням захистом, результати тестування захищеності, ступінь сегментації мережі	Залежить від якості ресстрації інцидентів і незалежності перевірок
<i>Фінансова стійкість життєвого циклу</i>	Забезпеченість поточних і капітальних витрат для ремонту, утримання та резервування	Виконання планів поточних і капітальних витрат, зміна вартості протягом життєвого циклу, частка грантових і донорських ресурсів	Потребує прозорого обліку витрат і єдиної методики розрахунку
<i>Соціальна прийнятність і дотримання вимог</i>	Довіра користувачів, доступність послуг, права праці й людини, робота зі зверненнями	Виробничий травматизм, доступність для маломобільних груп, час розгляду скарг, кількість підтверджених порушень установлених вимог	Існує ризик формального звітування без реального впливу, тому потрібна незалежна перевірка

Джерело: сформовано на основі [19—21].

У підходах до належного врядування стійкості критичної інфраструктури наголошується, що випереджальні інвестиції в надійність можливі лише за наявності довіри, партнерської взаємодії та постійного обміну інформацією. Без цього інвестор орієнтується не на довгий горизонт, а на мінімізацію власних втрат у короткому проміжку часу.

Інша межа стосується фінансування і воєнного ризику і загальне правило державно-приватного партнерства полягає в тому, що ризик передається тій стороні, яка здатна ним управляти. У воєнних умовах цей підхід діє лише частково.

Частину загроз приватний сектор не може оцінити в прийнятний спосіб без державних гарантій, компенсаційних механізмів або донорської участі. Законодавчі норми, які передбачають використання грантів і залучення донорів до проєктів державно-приватного партнерства, створюють для цього правову основу, але сама по собі наявність такої норми не розв'язує проблему. Потрібні зрозумілі правила оцінювання воєнного ризику, підходи до його ціноутворення та прозорі механізми державної підтримки.

Окремої уваги потребує питання даних адже цифровий нагляд не дає результату, якщо дані неповні, несвоєчасні або недостовірні.

Платформи цифрового контролю, які забезпечують відкритість і простежуваність інфраструктурних проєктів, можуть істотно підвищити якість управління, але їхня користь залежить від повноти внесення інформації, однакових правил її перевірки та дисципліни всіх учасників. Якщо цього немає, створюється лише видимість керованості, а помилки й перекручення накопичуються на кожному наступному етапі.

Ще одна межа пов'язана з природою інтелектуалізованої інфраструктури. У такій системі збій у цифровому контурі управління може мати наслідки, порівнянні з фізичним пошкодженням об'єкта.

Дослідження кіберфізичної стійкості показують, що надійність таких систем залежить від одночасного розвитку показників оцінювання, правових вимог і досвіду захисту. Рекомендації щодо цифрової безпеки транспорту також наголошують, що критичні елементи інтелектуалізованих транспортних систем потребують узгоджених організаційних і технічних рішень.

Законодавство України у сфері кібербезпеки та кіберзахисту критичної інфраструктури задає лише загальні обов'язкові вимоги [19—20]. Для реальної роботи державно-приватного партнерства їх потрібно переводити у договірні умови, показники перевірки та процедури контролю на рівні конкретного проєкту.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Стійкість інтелектуалізованої транспортної інфраструктури України в умовах війни визначається не кількістю впроваджених технологій, а здатністю держави, бізнесу й операторів діяти узгоджено в межах спільної системи управління. Критичним стає не стільки відновлення окремих об'єктів, скільки збереження та швидке поновлення транспортних послуг, від яких залежить безперервність перевезень, безпека людей і функціонування економіки. Масштаб втрат і потреб у транспортному секторі підтверджує, що для України

вже недостатньо підходу, зосередженого лише на відбудові активів. Потрібен перехід до управління стійкістю послуг, коридорів і вузлів у межах довгострокової системи рішень.

У цьому контексті державно-приватне партнерство слід розглядати не лише як канал залучення коштів, а як форму розподілу відповідальності за доступність послуг, швидкість відновлення, цифрову безпеку та суспільну прийнятність інфраструктурних рішень.

Соціальна відповідальність бізнесу в такій системі має значення лише тоді, коли вона переходить у площину конкретних зобов'язань, контрольованих процедур і показників оцінювання. Йдеться про захист прав людини і праці, цифрову безпеку, антикорупційні запобіжники, розгляд скарг і відшкодування завданої шкоди. За такого підходу вона перестав бути додатковим репутаційним компонентом і стає частиною механізму зниження ризиків та підтримання довіри до інфраструктурних проєктів.

Подальші дослідження доцільно зосередити на перевірці запропонованої системи показників у реальних транспортних коридорах і вузлах, на вивченні взаємопов'язаних цифрових і фізичних збоїв у транспортних мережах, а також на розробленні типових договорів державно-приватного партнерства для різних видів транспортної інфраструктури з урахуванням вимог до цифрової безпеки, підзвітності та належної обачності

Література:

1. Кабінет Міністрів України. Про схвалення Національної транспортної стратегії України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025—2027 роках: постанова від 27.12.2024 № 1550. URL: <https://zakon.rada.gov.ua/go/1550-2024-%D0%BF>.
2. European Parliament, Council of the European Union. Directive (EU) 2023/2661 of 22 November 2023 amending Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023L2661>.
3. Закон України. Про публічно-приватне партнерство: Закон України від 19.06.2025 № 4510-IX. URL: <https://zakon.rada.gov.ua/go/4510-20>.
4. Holling C. S. Resilience and Stability of Ecological Systems. Annual Review of Ecology and Systematics. 1973. Vol. 4. P. 1—23. DOI: <https://doi.org/10.1146/annurev.es.04.110173.000245>.
5. Bruneau M., Chang S. E., Eguchi R. T., Lee G. C., O'Rourke T. D., Reinhorn A. M., Shinozuka M., Tierney K., Wallace W. A., von Winterfeldt D. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. Earthquake Spectra. 2003. Vol. 19, № 4. P. 733—752. DOI: <https://doi.org/10.1193/1.1623497>.
6. Liu H. J., Love P. E. D., Zhao J., Lemckert C., Muldoon-Smith K. Transport infrastructure asset resilience: Managing government capabilities. Transportation Research Part D: Transport and Environment. 2021. Vol. 100. Article 103072. DOI: <https://doi.org/10.1016/j.trd.2021.103072>.
7. Yang Y., Huang H., Li G., Han B., Ma H. A systematic review of resilience assessment and enhancement of urban integrated transportation networks. Journal of Transport Geography. 2025. Vol. 126. Article 104420. DOI: <https://doi.org/10.1016/j.jtrangeo.2025.104420>.
8. Ajayi O. O., Kurien A., Djouani K., Dieng L. Artificial Intelligence for Infrastructure Resilience: Transportation Systems as a Strategic Case for Policy and Practice. Sustainability. 2025. Vol. 17, № 20. Article 8992. DOI: <https://doi.org/10.3390/su17208992>.
9. Matviishyn Y., Vershyhora Y. Prospects of using public and private partnership for the reconstruction of Ukraine in the post-war period. Democratic Governance. 2022. Vol. 30, № 2. P. 29—43. DOI: <https://doi.org/10.23939/dg2022.02.029>.
10. Чаркіна Т. Ю. Механізми та напрямки антикризового управління пасажирським комплексом залізничного транспорту. Вісник Хмельницького національного університету. Економічні науки. 2020. № 4, т. 2. С. 67—71. DOI: [https://doi.org/10.31891/2307-5740-2020-284-4\(2\)-11](https://doi.org/10.31891/2307-5740-2020-284-4(2)-11).
11. Задоя В. О., Купцов Ю. В. Вплив цифровізації на конкурентоспроможність пасажирських залізничних перевезень. Review of Transport Economics and Management. 2024. Вип. 10 (26). С. 142—149. DOI: <https://doi.org/10.15802/rtem2023/300529>.
12. Чаркіна Т. Ю., Задоя В. О., Купцов Ю. В. Трансформація інноваційного менеджменту промислових підприємств залізничного транспорту в умовах цифрової конвергенції та корпоративного партнерства. Інвестиції: практика та досвід. 2026. № 3. С. 132—137. DOI: <https://doi.org/10.32702/2306-6814.2026.3.132>.
13. Osei-Kyei R., Chan A. P. C., Yu Y., Chen C., Ke Y., Tijani B. Social Responsibility Initiatives for Public-Private Partnership Projects: A Comparative Study between China and Ghana. Sustainability. 2019. Vol. 11, № 5. Article 1338. DOI: <https://doi.org/10.3390/su11051338>.
14. ENISA. Cyber Security and Resilience of Intelligent Public Transport: Good practices and recommendations. 2016. URL: <https://www.enisa.europa.eu/publications/good-practices-recommendations>.
15. OHCHR. Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework. New York; Geneva, 2011. URL: https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.
16. European Parliament, Council of the European Union. Directive (EU) 2022/2464 of 14 December 2022 as regards corporate sustainability reporting. URL: <https://eur-lex.europa.eu/eli/dir/2022/2464/oj/eng>.
17. European Parliament, Council of the European Union. Directive (EU) 2024/1760 of 13 June 2024 on corporate sustainability due diligence. URL: <https://eur-lex.europa.eu/eli/dir/2024/1760/oj/eng>.
18. Longo A., Aghazadeh Ardebili A., Lazari A., Ficarella A. Cyber-Physical Resilience: Evolution of Concept, Indicators, and Legal Frameworks. Electronics. 2025. Vol. 14, № 8. Article 1684. DOI: <https://doi.org/10.3390/electronics14081684>.
19. Закон України. Про концесію: Закон України від 03.10.2019 № 155-IX. URL: <https://zakon.rada.gov.ua/laws/show/155-20/print>.
20. Закон України. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL: <https://zakon.rada.gov.ua/go/1882-20>.

21. OECD. OECD Guidelines for Multinational Enterprises on Responsible Business Conduct. Paris: OECD Publishing, 2023. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/06/oecd-guidelines-for-multinational-enterprises-on-responsible-business-conduct_a0b49990/81f92357-en.pdf (дата звернення: 04.05.2026).

References:

1. Cabinet of Ministers of Ukraine (2024), Resolution "On approval of the National Transport Strategy of Ukraine for the period until 2030 and approval of the operational action plan for its implementation in 2025-2027", available at: <https://zakon.rada.gov.ua/go/1550-2024-%D0%BF> (Accessed 01 May 2026).
2. European Parliament, Council of the European Union. (2023), "Directive (EU) 2023/2661 of 22 November 2023 amending Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport", available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023L2661> (Accessed 01 May 2026).
3. Verkhovna Rada of Ukraine (2025), "On Public-Private Partnership: Law of Ukraine", Available at: <https://zakon.rada.gov.ua/go/4510-20> (Accessed 01 May 2026).
4. Holling, C.S. (1973), "Resilience and Stability of Ecological Systems", Annual Review of Ecology and Systematics, vol. 4, pp. 1—23. DOI: <https://doi.org/10.1146/annurev.es.04.110173.000245>.
5. Bruneau, M. et al. (2003), "A framework to quantitatively assess and enhance the seismic resilience of communities", Earthquake Spectra, vol. 19 (4), pp. 733—752. DOI: <https://doi.org/10.1193/1.1623497>.
6. Liu, H. J., Love, P. E. D., Zhao, J., Lemckert, C. and Muldoon-Smith, K. (2021), "Transport infrastructure asset resilience: Managing government capabilities", Transportation Research Part D: Transport and Environment, Vol. 100, Article 103072. DOI: <https://doi.org/10.1016/j.trd.2021.103072>.
7. Yang, Y., Huang, H., Li G., Han, B. and Ma, H. (2025), "A systematic review of resilience assessment and enhancement of urban integrated transportation networks", Journal of Transport Geography, Vol. 126, Article 104420. DOI: <https://doi.org/10.1016/j.jtrangeo.2025.104420>.
8. Ajayi, O. O., Kurien, A., Djouani, K. and Dieng, L. (2025), "Artificial Intelligence for Infrastructure Resilience: Transportation Systems as a Strategic Case for Policy and Practice", Sustainability, Vol. 17, no. 20. Article 8992. DOI: <https://doi.org/10.3390/su17208992>.
9. Matviishyn, Y. and Vershyhora, Y. (2022), "Prospects of using public and private partnership for the reconstruction of Ukraine in the post-war period", Democratic Governance. Vol. 30, no. 2, pp. 29—43. DOI: <https://doi.org/10.23939/dg2022.02.029>.
10. Charkina, T. Yu. (2020), "Mechanisms and directions of anti-crisis management of the passenger complex of railway transport", Visnyk Khmel'nyts'koho natsional'noho universytetu. Seriya: Ekonomichni nauky, vol. 4, no. 2, pp. 67—71. DOI: [https://doi.org/10.31891/2307-5740-2020-284-4\(2\)-11](https://doi.org/10.31891/2307-5740-2020-284-4(2)-11).
11. Zadoia, V.O. and Kuptsov, Yu.V. (2022), "The impact of digitalization on the competitiveness of passenger rail transport", Review of Transport Economics and Management, vol. 10 (26), pp. 142—149. DOI: <https://doi.org/10.15802/rtem2023/300529>.
12. Charkina, T. Yu., Zadoia, V. O. and Kuptsov, Yu. V. (2026), "Transformation of Innovation Management in Industrial Railway Enterprises under Conditions of Digital Convergence and Corporate Partnership", Investysii: praktyka ta dosvid, vol. 3, pp. 132—137. DOI: <https://doi.org/10.32702/2306-6814.2026.-3.132>.
13. Osei-Kyei, R., Chan, A. P. C., Yu, Y., Chen, C., Ke, Y. and Tijani, B. (2019), "Social Responsibility Initiatives for Public-Private Partnership Projects: A Comparative Study between China and Ghana", Sustainability, Vol. 11, no. 5. Article 1338. DOI: <https://doi.org/10.3390/su11051338>.
14. ENISA. (2016), "Cyber Security and Resilience of Intelligent Public Transport: Good practices and recommendations.", available at: <https://www.enisa.europa.eu/publications/good-practices-recommendations> (Accessed 01 May 2026).
15. OHCHR (2011), "Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework", available at: https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf (Accessed 01 May 2026).
16. European Parliament, Council of the European Union. (2022), "Directive (EU) 2022/2464 of 14 December 2022 as regards corporate sustainability reporting", available at: <https://eur-lex.europa.eu/eli/dir/2022/2464/oj/eng> (Accessed 01 May 2026).
17. European Parliament, Council of the European Union. (2024), "Directive (EU) 2024/1760 of 13 June 2024 on corporate sustainability due diligence", available at: <https://eur-lex.europa.eu/eli/dir/2024/1760/oj/eng> (Accessed 01 May 2026).
18. Longo, A., Aghazadeh Ardebili, A., Lazari, A. and Ficarella, A. (2025), "Cyber-Physical Resilience: Evolution of Concept, Indicators, and Legal Frameworks", Electronics.. Vol. 14, no. 8. Article 1684. DOI: <https://doi.org/10.3390/electronics14081684>.
19. Verkhovna Rada of Ukraine (2019), The Law Ukraine "About concessions", available at: <https://zakon.rada.gov.ua/laws/show/155-20/print> (Accessed 01 May 2026).
20. Verkhovna Rada of Ukraine (2021), The Law of Ukraine "On critical infrastructure", available at: <https://zakon.rada.gov.ua/go/1882-20>. (Accessed 01 May 2026).
21. OECD (2023), "OECD guidelines for multinational enterprises on responsible business conduct", OECD Publishing, available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/06/oecd-guidelines-for-multinational-enterprises-on-responsible-business-conduct_a0b49990/81f92357-en.pdf (Accessed 04.05.2026).

Отримано редакцією журналу / Received: 09. 05.26

Професійно / Revised: 19. 05.26

Дата публікації / Published: 21.05.26