

Увесь контент ліцензовано за умовами [Creative Commons BY 4.0 International license](https://creativecommons.org/licenses/by/4.0/)

РЕГІОНАЛЬНА ПОЛІТИКА
REGIONAL POLICY

УДК 332.1:004.9:338.24:005.334

doi: <https://doi.org/10.15330/apred.1.22.313-324>

Кльоба В. Л.¹, Павліха Н. В.²

ЦИФРОВА РЕЗИЛЬЄНТНІСТЬ РЕГІОНІВ ЯК ОБ'ЄКТ ІНСТИТУЦІЙНО-ЕКОНОМІЧНОГО ЗАБЕЗПЕЧЕННЯ В УМОВАХ КРИЗОВИХ І ПОСТКРИЗОВИХ ТРАНСФОРМАЦІЙ

¹Луцький національний технічний університет,
Лабораторія проєктів та інновацій,
вул. Львівська, 75, м. Луцьк,
43018, Україна,
тел.: +380 93 767 29 49,
e-mail: victor.klioba@gmail.com
ORCID: <https://orcid.org/0009-0009-1327-2594>

²Луцький національний технічний університет,
кафедра публічного та проєктного управління,
вул. Львівська, 75, м. Луцьк,
43018, Україна,
тел.: +380 50 378 51 43,
e-mail: nataliia.pavlikha@gmail.com
ORCID: <https://orcid.org/0000-0001-5191-242X>

Анотація. У статті обґрунтовано цифрову резильєнтність регіонів як самостійну мезорівневу категорію регіональної економіки та як об'єкт інституційно-економічного забезпечення в умовах кризових і посткризових трансформацій. Актуальність теми зумовлена тим, що під впливом воєнних, інфраструктурних, соціально-економічних і кібернетичних шоків цифрова підсистема регіону перестала бути допоміжним інструментом сервісної модернізації й перетворилася на критичну умову життєзабезпечення територій, безперервності публічних і приватних послуг та збереження інституційної керованості. Метою дослідження є теоретико-концептуальне обґрунтування цифрової резильєнтності регіонів, розкриття її змісту та визначення місця в системі інституційно-економічних механізмів регіонального розвитку. Методологічну основу становлять положення регіональної економіки та інституційної економічної теорії, еволюційна концепція економічної резильєнтності, підхід адаптивного циклу, а також методи наукової абстракції, порівняльного категоріального аналізу, систематизації та структурно-функціонального моделювання; емпіричною базою слугували офіційні оцінки збитків і потреб у відновленні, статистика кіберінцидентів, дані вимірювання цифрової трансформації регіонів і громад та нормативно-правові акти України і Європейського Союзу. За результатами дослідження запропоновано авторське визначення цифрової резильєнтності регіону через найближчий рід і видову відмінність, здійснено її розмежування з цифровою трансформацією, цифровою зрілістю, кіберстійкістю, цифровою операційною резильєнтністю та національною стійкістю, побудовано двовимірну структурну модель, що поєднує чотири функціональні фази резильєнтності – опірність, відновлюваність, переорієнтацію та оновлення – з п'ятьма компонентами цифрової підсистеми регіону, і окреслено сім підсистем інституційно-економічного забезпечення. Наукова новизна полягає у виокремленні цифрової резильєнтності регіону як самостійної мезорівневої категорії, відмінної від суміжних понять за масштабом аналізу, часовою логікою та ключовим дослідницьким питанням, а також в обґрунтуванні її матричної операціоналізації. Теоретичне значення роботи

полягає в розширенні понятійного апарату регіональної економіки цифровим виміром резильєнтності, практичне – у формуванні основи для розроблення системи показників та інтегрального індексу цифрової резильєнтності регіонів, придатного для підтримки регіональної політики, кризового управління та планування посткризового відновлення.

Ключові слова: цифрова резильєнтність регіону; регіональна економіка; інституційно-економічне забезпечення; цифрова трансформація; цифрова зрілість; кіберстійкість; національна стійкість; кризові трансформації; посткризове відновлення.

Kloba V. L.¹, Pavlikha N. V.²

**REGIONAL DIGITAL RESILIENCE AS AN OBJECT OF INSTITUTIONAL
AND ECONOMIC SUPPORT UNDER CRISIS AND POST-CRISIS
TRANSFORMATIONS**

¹Lutsk National Technical University,
Project and Innovation Laboratory,
Lvivska Str., 75, Lutsk,
43018, Ukraine,
tel.: +380 93 767 29 49,
e-mail: victor.klioba@gmail.com
ORCID: <https://orcid.org/0009-0009-1327-2594>

²Lutsk National Technical University,
Department of Public and Project Management,
Lvivska Str., 75, Lutsk,
43018, Ukraine,
tel.: +380 50 378 51 43,
e-mail: nataliia.pavlikha@gmail.com
ORCID: <https://orcid.org/0000-0001-5191-242X>

Abstract. The article substantiates regional digital resilience as an autonomous meso-level category of regional economics and as an object of institutional and economic support under crisis and post-crisis transformations. The relevance of the topic stems from the fact that, under the impact of wartime, infrastructural, socio-economic and cyber shocks, the digital subsystem of a region has ceased to be an auxiliary instrument of service modernisation and has become a critical precondition for territorial life support, for the continuity of public and private services and for the preservation of institutional governability. The purpose of the study is to provide a theoretical and conceptual substantiation of regional digital resilience, to disclose its content and to determine its place within the system of institutional and economic mechanisms of regional development. The methodological basis comprises the propositions of regional economics and institutional economic theory, the evolutionary concept of economic resilience, the adaptive cycle approach, as well as the methods of scientific abstraction, comparative categorical analysis, systematisation and structural-functional modelling; the empirical basis includes official assessments of damage and recovery needs, cyber incident statistics, measurement data on the digital transformation of regions and communities, and the regulatory acts of Ukraine and the European Union. The study results in an original definition of regional digital resilience formulated through the proximate genus and the specific difference, in its differentiation from digital transformation, digital maturity, cyber resilience, digital operational resilience and national resilience, in a two-dimensional structural model that combines four functional phases of resilience – resistance, recovery, re-orientation and renewal – with five components of the regional digital subsystem, and in the identification of seven subsystems of institutional and economic support. The scientific novelty consists in singling out regional digital resilience as an autonomous meso-level category that differs from adjacent concepts in the scale of analysis, the temporal logic and the key research question, and in substantiating its matrix-based operationalisation. The theoretical significance of the work lies in extending the conceptual apparatus of regional economics with the digital dimension of resilience; the practical significance lies in creating the basis for developing a

system of indicators and an integral index of regional digital resilience suitable for supporting regional policy, crisis management and post-crisis recovery planning.

Keywords: regional digital resilience; regional economy; institutional and economic support; digital transformation; digital maturity; cyber resilience; national resilience; crisis transformations; post-crisis recovery.

Вступ. Повномасштабна війна змінила функціональне призначення цифрової підсистеми регіонів України: з допоміжного інструменту сервісної модернізації вона перетворилася на критичну умову життєзабезпечення територій, збереження інституційної керованості та підтримання соціально-економічної взаємодії в умовах системних шоків. Масштаб цих шоків фіксують офіційні оцінки: станом на 31 грудня 2025 р. прямі збитки України становили 195,1 млрд дол. США, соціально-економічні втрати – 666,7 млрд дол. США, а десятирічна потреба у відновленні та реконструкції – 587,7 млрд дол. США, причому сектор телекомунікацій і цифрової інфраструктури зазнав 2,5 млрд дол. США прямих збитків і потребує 7,1 млрд дол. США на відновлення [1, с. 24-31]. Паралельно зростає інтенсивність кібернетичного тиску: у 2025 р. CERT-UA опрацювала 5927 кіберінцидентів, що на 37,4 % більше, ніж роком раніше [2].

Наукова проблема породжена методологічним розривом між тим, що вимірюють наявні інструменти оцінювання цифрового розвитку, і тим, що фактично визначає життєздатність території в момент шоку. Регіональна політика цифровізації побудована на логіці нарощування спроможностей, а саме – кількості переведених в електронну форму послуг, рівня покриття, ступеня цифровізації адміністративних процедур. Тоді як здатність цифрового контуру регіону витримувати руйнування інфраструктури, кібератаки, дефіцит ресурсів і міграційні зміни залишається поза вимірюванням. Понад те, поглиблення цифровізації без резервування, дублювання критичних функцій, захищеності даних та інституційної координації продукує нові вразливості. Чим вищою є залежність території від цифрових сервісів, тим масштабнішими є наслідки їх відмови. Відтак високоцифровізований регіон може виявитися функціонально крихким, а помірно цифровізований відносно стійким за наявності механізмів резервування, адаптації та швидкого відновлення. Цифровий розвиток і цифрова резильєнтність не є тотожними категоріями, а їх ототожнення унеможливорює коректне вимірювання цієї властивості, обмежує міжрегіональне порівняння та ускладнює формування адресної регіональної політики.

Проблематика дослідження формується на перетині чотирьох наукових напрямів. Перший напрям – це теорія резильєнтності соціально-економічних і регіональних систем. Витоки сучасного розуміння категорії сягають праці К. Холлінга, який розмежував інженерне трактування стійкості як повернення системи до попереднього стану рівноваги та екологічне трактування як здатність поглинати збурення, зберігаючи базові функції, структуру й ідентичність [3, с. 1-23]. Еволюційний розвиток цього підходу в регіональній економіці здійснено Р. Мартіном і П. Санлі, які трактують регіональну резильєнтність не як статичну характеристику, а як динамічну здатність регіональної економіки протистояти шокам, відновлюватися після них, адаптувати структуру та інституційні механізми й за потреби переходити на нову траєкторію розвитку, виокремлюючи чотири функціональні фази – опірність, відновлюваність, переорієнтацію та оновлення [4, с. 1-42].

Другий науковий напрям репрезентує українська наукова школа регіонального розвитку та просторового управління. У попередніх дослідженнях обґрунтовано теоретико-методологічні засади управління сталим розвитком просторових систем та інноваційні моделі відновлення конкурентоспроможності регіонів і територіальних громад у воєнний і повоєнний періоди [5, с. 179-193]. У працях науковців Інституту

регіональних досліджень імені М. І. Долішнього НАН України резильєнтність ендогенного розвитку регіонів розглядається як здатність територіальних соціально-економічних систем зберігати функціональність, адаптуватися до глобальних і внутрішніх викликів та формувати власні джерела відновлення [6]. Водночас цифровий вимір у цих працях постає переважно як один із чинників розвитку, а не як окрема підсистема, що потребує спеціального інституційно-економічного забезпечення.

Третій напрям охоплює дослідження цифрової трансформації та цифрової зрілості територіальних систем. І. Іртишева та О. Сенкевич розглядають цифрову трансформацію регіонів України як об'єктивну необхідність модернізації економіки, підвищення якості управління та доступності публічних послуг [7, с. 14-21]. Прикладним відображенням цього напрямку є Індекс цифрової трансформації регіонів та громад, що охоплює систему субіндексів і показників рівня цифрового розвитку територій, стану цифрової інфраструктури, доступності е-послуг та інституційної спроможності [8]. Однак цей інструментарій за своєю логікою оцінює досягнутий рівень цифрової трансформації й не дає відповіді на питання про глибину падіння функціональності цифрових сервісів під час шоку, тривалість відновлення та наявність резервних контурів.

Четвертий науковий напрям пов'язаний із цифровою операційною резильєнтністю та національною стійкістю. На рівні Європейського Союзу цей напрям набув нормативної інституціалізації: Регламент DORA визначає цифрову операційну стійкість через здатність суб'єктів підтримувати ІКТ-спроможності, необхідні для безперервного надання послуг під час збоїв [9]; Директива NIS2 встановлює високий спільний рівень кібербезпеки для критичних і важливих секторів [10]; рамка NIST Cybersecurity Framework 2.0 структурує управління кіберризиками за функціями Govern, Identify, Protect, Detect, Respond, Recover [11, с. 5-12]. В українському контексті формування системи національної стійкості інституційно пов'язане з Концепцією забезпечення національної системи стійкості [12]. Ці підходи, однак, зорієнтовані або на організаційно-галузевий, або на макрорівень держави й не враховують територіальної, публічно-сервісної та інституційно-економічної природи регіону як мезорівневої системи.

Кожен із розглянутих напрямів формує важливі теоретико-методологічні передумови, проте жоден із них не забезпечує цілісного пояснення цифрової резильєнтності саме на мезорівні. Теорія регіональної резильєнтності дає загальну рамку аналізу шоків, відновлення й адаптації, але не виокремлює цифрову підсистему як самостійний об'єкт; дослідження цифрової трансформації пояснюють технологічне оновлення територій поза контекстом шоку; підходи до цифрової операційної стійкості акцентують на безперервності ІКТ-функцій окремих суб'єктів; концепція національної стійкості окреслює макрорівневу спроможність держави. Унаслідок цього цифрова резильєнтність регіону залишається недостатньо визначеною науковою категорією, яка змішується із суміжними поняттями. Невирішеною є проблема інтеграції зазначених підходів на рівні регіону та концептуалізації цифрової резильєнтності як об'єкта інституційно-економічного забезпечення, чому й присвячено цю статтю.

Постановка завдання. Метою статті є теоретико-концептуальне обґрунтування цифрової резильєнтності регіонів як самостійної мезорівневої категорії регіональної економіки та як об'єкта інституційно-економічного забезпечення в умовах кризових і посткризових трансформацій. Досягнення мети передбачає розв'язання чотирьох взаємопов'язаних завдань: обґрунтувати правомірність перенесення концепту резильєнтності на цифрову підсистему регіону; сформулювати визначення цифрової резильєнтності регіону через найближчий рід і видову відмінність; розмежувати запропоновану категорію із суміжними поняттями за масштабом, часовою логікою та

об'єктом аналізу; побудувати структурну модель, придатну для подальшої операціоналізації.

Теоретико-методологічним підґрунтям слугують положення регіональної економіки, інституційної економічної теорії, еволюційна концепція економічної резильєнтності та підхід адаптивного циклу. Відповідно до логіки дослідницьких завдань застосовано: метод наукової абстракції та сходження від абстрактного до конкретного – для формулювання дефініції; порівняльний категоріальний аналіз – для розмежування досліджуваної категорії із суміжними поняттями за критеріями предмета опису, масштабу аналізу, часової логіки та ключового дослідницького питання; систематизацію та узагальнення – для виокремлення підсистем інституційно-економічного забезпечення; логіко-семантичний аналіз наукових і нормативних джерел – для верифікації понятійного апарату.

Емпіричним підґрунтям дослідження є офіційні оцінки прямих збитків, втрат і потреб у відновленні України [1], статистика опрацьованих кіберінцидентів [2], дані вимірювання цифрової трансформації регіонів і громад [8], а також нормативно-правові акти Європейського Союзу та України у сфері цифрової операційної стійкості, кібербезпеки й національної стійкості [9-12]. Дослідження має концептуальний характер. Запропонована категоріальна конструкція і структурна модель формують теоретичну основу для подальшого визначення системи індикаторів, розроблення методичного інструментарію оцінювання та обґрунтування механізмів інституційно-економічного забезпечення цифрової резильєнтності регіонів.

Результати. Цифровізація регіональної економіки супроводжується перетворенням цифрової інфраструктури, даних, платформ, електронних сервісів і цифрових компетентностей на системоутворювальні чинники територіального розвитку. Від їхньої надійності та доступності залежать безперервність надання адміністративних і соціальних послуг, функціонування підприємницького сектору, міжвідомча взаємодія, комунікація органів влади з населенням, організація освітніх і медичних процесів, а також здатність регіонів координувати дії під час кризових ситуацій. Відповідно, порушення роботи цифрової підсистеми перестає бути вузькотехнологічною проблемою та набуває ознак комплексного соціально-економічного ризику.

В умовах воєнних дій, руйнування інфраструктури, кібератак, вимушеного переміщення населення, нестабільності енергопостачання та інституційної невизначеності цифрові системи регіонів зазнають одночасного впливу різномірних шоків. Такі впливи можуть спричиняти фізичне пошкодження телекомунікаційних мереж, втрату або недоступність даних, припинення роботи електронних сервісів, порушення каналів зв'язку, дефіцит фахівців та посилення цифрової нерівності.

Наявність розвиненої цифрової інфраструктури або високий рівень цифрової трансформації самі по собі не гарантують здатності регіону протистояти кризовим впливам. Цифрово розвинена система може залишатися вразливою внаслідок надмірної централізації, технологічної залежності, відсутності резервних каналів, недостатньої сумісності інформаційних систем, низької якості управління даними або нерівномірного доступу населення до цифрових послуг. Тому рівень цифровізації відображає переважно досягнутий стан цифрового розвитку, тоді як цифрова резильєнтність характеризує поведінку регіональної цифрової підсистеми під час порушень, її здатність реагувати на них і змінюватися внаслідок набутого досвіду.

Категорія резильєнтності сформувалася на перетині природничих, технічних і соціально-економічних наук, послідовно еволюціонувавши від уявлення про механічне повернення системи до попереднього стану рівноваги до розуміння її адаптивної здатності зберігати, відновлювати й трансформувати власну функціональність під

впливом шоків. В інженерному трактуванні резильєнтність пов'язується зі швидкістю повернення системи до вихідного стану, а ключовою метрикою є час відновлення. В екологічному трактуванні акцент зміщується на обсяг збурення, який система здатна поглинути без втрати базових функцій, структури та ідентичності [3, с. 1-23]. В еволюційному трактуванні, найбільш придатному для аналізу соціально-економічних систем, резильєнтність розглядається як здатність системи не лише відновлюватися, а й адаптувати структуру, функції та інституційні механізми, переходячи за потреби на нову, стійкішу траєкторію розвитку [4, с. 1-42].

Для регіональної економіки саме еволюційне трактування є методологічно продуктивним, оскільки регіон не є механічною системою з єдиним станом рівноваги, а функціонує як складна відкрита соціально-економічна система, у якій інфраструктурні, інституційні, виробничі, людські, інформаційні та управлінські компоненти перебувають у постійній взаємодії [6]. Перенесення цієї рамки на цифрову підсистему регіону є методологічно правомірним з огляду на чотири аргументи. По-перше, цифрова підсистема має системний характер, оскільки охоплює телекомунікаційну та енергозалежну інфраструктуру, реєстри й бази даних, публічні та приватні цифрові послуги, платформи, організаційні регламенти, людські компетентності й інститути їх підтримання. По-друге, вона є шокозалежною: її функціонування порушується внаслідок руйнування інфраструктури, кібератак, перебоїв електропостачання, міграційних змін і кадрового дефіциту [1, с. 24-31; 2]. По-третє, вона має критичне функціональне значення, забезпечуючи доступ населення, бізнесу й органів влади до адміністративних, соціальних, фінансових, освітніх і медичних сервісів. По-четверте, вона здатна до адаптивної реконфігурації через перехід на резервні канали зв'язку, альтернативні платформи, зміну процедур надання послуг і оновлення архітектури даних.

З урахуванням еволюційного підходу до регіональної резильєнтності, положень інституційної економічної теорії та специфіки цифрової підсистеми території пропонується таке визначення: цифрова резильєнтність регіону – це здатність цифрової підсистеми регіону, що охоплює цифрову інфраструктуру, дані, цифрові публічні й приватні послуги, людські компетентності та інститути їх забезпечення, протистояти кризовим шокам, підтримувати критичну функціональність, відновлювати її у прийнятні строки, адаптивно реконфігуруватися та оновлювати інституційно-економічні механізми цифрового розвитку задля збереження життєздатності території й переходу на стійкішу траєкторію функціонування. Найближчим родом у цій дефініції є здатність соціотехнічної підсистеми регіону, а видовою відмінністю – спрямованість на збереження, відновлення й оновлення критичної функціональності саме в часовому вікні до, під час і після шоку, а не на нарощування рівня цифровізації. Цифрова резильєнтність регіону є, отже, динамічною властивістю, яка проявляється не в нормальному режимі функціонування, а в ситуації порушення, дефіциту ресурсів та інституційної напруги.

Запропоноване визначення дає змогу кваліфікувати цифрову резильєнтність регіонів як самостійну мезорівневу категорію регіональної економіки. Її мезорівневий характер зумовлений тим, що вона не зводиться до стійкості окремої організації, інформаційної системи чи домогосподарства, але й не тотожна макрорівневій національній стійкості держави [12]. Регіональний рівень є проміжним, однак функціонально критичним, оскільки саме на ньому відбувається просторове поєднання цифрової інфраструктури, органів влади, громад, бізнесу, населення, провайдерів послуг і локальних механізмів кризового реагування.

Для наукової коректності запропонованої категорії необхідно розмежувати її із суміжними поняттями, які функціонують в одному смисловому полі, але різняться

Цифрова резильєнтність регіонів як об'єкт інституційно-економічного...

природою, масштабом, часовою логікою та об'єктом аналізу. Результати такого розмежування, здійсненого за чотирма критеріями, наведено в табл. 1.

Таблиця 1

Розмежування цифрової резильєнтності регіону із суміжними категоріями

Table 1

Differentiation of a Region's Digital Resilience into Adjacent Categories

Категорія	Що описує	Масштаб аналізу	Часова логіка	Ключове питання
Цифрова трансформація	Процес упровадження цифрових технологій, платформ, сервісів і нових моделей управління	Організація, громада, регіон, держава	Траєкторія розвитку	Наскільки і як швидко система цифровізується?
Цифрова зрілість	Досягнутий стан цифрових спроможностей, інфраструктури та компетентностей	Організація, громада, регіон	Статичний (порівняльний) стан	Наскільки розвиненими є цифрові спроможності на певний момент?
Кіберстійкість	Здатність інформаційних систем протидіяти кіберзагрозам і відновлюватися після інцидентів	ІТ-система, організація, сектор	Реагування на кіберінцидент	Чи захищеними та відновлюваними є інформаційні системи?
Цифрова операційна резильєнтність	Здатність суб'єктів забезпечувати безперервність ІКТ-функцій під час технологічних збоїв	Організаційний і галузевий рівень	Безперервність операцій	Чи здатна організація підтримувати критичні цифрові операції?
Національна стійкість	Здатність держави й суспільства протистояти екзистенційним загрозам, реагувати на них і відновлюватися	Макрорівень держави	Стійкість державної системи	Чи здатна держава загалом витримати системну загрозу?
Цифрова резильєнтність регіону (авторська категорія)	Здатність цифрової підсистеми регіону підтримувати, відновлювати, адаптувати й оновлювати критичну функціональність під впливом шоку	Мезорівень регіону	Динаміка до, під час і після шоку	Чи здатний цифровий контур регіону витримати шок і відновити критичні функції?

Джерело: складено авторами на основі [3; 4; 6; 9-12].

Основна відмінність між розглянутими поняттями полягає в тому, що вони характеризують різні аспекти цифрового розвитку. Цифрова трансформація та цифрова зрілість відображають рівень упровадження цифрових технологій і накопичення відповідних ресурсів, компетентностей та управлінських практик. Водночас ці поняття переважно описують стан системи без урахування впливу кризових подій.

Кіберстійкість і цифрова операційна резильєнтність мають вужче значення. Вони зосереджені насамперед на захисті інформаційних систем, забезпеченні безперервності ІКТ-процесів та відновленні діяльності окремих організацій після кібератак або технічних збоїв [9-11]. Національна стійкість стосується вищого рівня аналізу та характеризує здатність держави протистояти масштабним загрозам і забезпечувати виконання основних функцій [12].

Цифрова резильєнтність регіону, натомість, характеризує поведінку територіальної цифрової системи до, під час і після кризового впливу. Вона дає змогу оцінити, наскільки знижується функціональність цифрової підсистеми регіону внаслідок шоку, як швидко та повно вона відновлюється, а також чи здатна система адаптуватися й оновитися з урахуванням отриманого кризового досвіду. Звідси випливає ключовий методологічний висновок: рівень цифрової трансформації та цифрова резильєнтність не є взаємозамінними характеристиками й можуть розходитися, що обґрунтовує потребу в окремому вимірювальному інструменті, відмінному від наявних індексів цифрового розвитку [8].

Для операціоналізації запропонованої категорії доцільно сформувати двовимірну структурну модель. Перший вимір становлять функціональні фази резильєнтності, перенесені з еволюційної рамки [4, с. 1-42] на цифровий контур регіону: опірність – це здатність цифрової підсистеми зберігати критичну функціональність під час дії шоку; відновлюваність – це здатність відновлювати цифрові сервіси, дані, канали зв'язку та управлінські функції у прийнятні строки; переорієнтація – це здатність змінювати канали, процедури, організаційні ролі й технологічні рішення відповідно до нових умов; оновлення – це здатність після шоку переходити на якісно стійкішу цифрову архітектуру та вдосконалювати механізми забезпечення.

Другий вимір утворюють компоненти цифрової підсистеми регіону, у межах яких реалізуються зазначені фази: інфраструктурний (зв'язок, енергоживлення, центри обробки даних, хмарні рішення, резервні канали); інституційний (нормативні правила, регламенти, повноваження, відповідальність, механізми координації та кризового управління); економіко-ресурсний (фінансове забезпечення, інвестиції, бюджетні й донорські ресурси, економічні стимули); людський (цифрові компетентності, кадрова спроможність, кризова готовність персоналу); компонент даних і послуг (доступність реєстрів, резервування даних, безперервність критичних сервісів, альтернативні канали надання послуг). Перетин чотирьох фаз і п'яти компонентів утворює аналітичну матрицю, у вузлах якої визначаються конкретні показники (табл. 2).

Таблиця 2

Матриця цифрової резильєнтності регіону як основа її операціоналізації

Table 2

Matrix of a Region's Digital Resilience as the Basis for Its Operationalization

Компонент	Опірність	Відновлюваність	Переорієнтація	Оновлення
Інфраструктурний	Частка критичних цифрових сервісів, доступних під час шоку; наявність резервного електроживлення та каналів зв'язку	Середній час відновлення зв'язку, доступу до платформ і каналів передачі даних	Перехід на резервні канали, хмарні рішення та альтернативні майданчики	Модернізація архітектури резервування, підвищення надійності інфраструктури
Інституційний	Наявність кризових регламентів, визначених повноважень і відповідальних суб'єктів	Швидкість ухвалення управлінських рішень і запуску процедур відновлення	Міжвідомча, міжрівнева та міжсекторна координація	Оновлення регламентів, процедур і моделей управління за підсумками шоку

Продовження табл.2

Економіко-ресурсний	Наявність фінансових резервів і джерел ресурсного забезпечення цифрових функцій	Швидкість мобілізації коштів на відновлення цифрових сервісів	Перерозподіл ресурсів між критичними сервісами та інфраструктурними вузлами	Формування сталих фінансових механізмів підтримки цифрової резильєнтності
Людський	Готовність персоналу діяти в умовах цифрових порушень; рівень цифрових компетентностей	Здатність команд швидко відновити роботу критичних сервісів	Перерозподіл ролей, дистанційна робота, залучення альтернативних команд	Навчання, підвищення кваліфікації, формування культури кризової цифрової готовності
Дані й послуги	Доступність реєстрів, платформ і критичних цифрових послуг під час шоку	Показники RTO/RPO для даних, швидкість відновлення сервісів	Альтернативні канали надання адміністративних, соціальних і фінансових послуг	Удосконалення архітектури даних, інтеграція резервних сервісів, підвищення інтероперабельності

Джерело: розроблено авторами.

Запропонована матриця має не лише описове, а й методологічне значення. Вона дає змогу перейти від загального поняття до системи показників, які фіксують не просто наявність цифрових сервісів, а їхню здатність функціонувати в умовах шоку, відновлюватися після порушень, адаптуватися до нових умов і ставати стійкішими внаслідок пережитих криз. У цьому полягає принципова відмінність майбутнього індексу цифрової резильєнтності регіонів від наявних індексів цифрової трансформації, які вимірюють рівень цифрового розвитку, але не оцінюють часову динаміку падіння та відновлення критичних функцій [8].

Резильєнтність цифрового контуру регіону не виникає автоматично з технічного оснащення. Вона є результатом дії інституційно-економічних механізмів – правил, стимулів, повноважень, ресурсів і координаційних практик, які забезпечують резервування, швидке прийняття рішень і мобілізацію ресурсів під час шоку. Відповідно до компонентної структури моделі інституційно-економічне забезпечення охоплює сім взаємопов'язаних підсистем:

- нормативно-регуляторна підсистема, що визначає правила функціонування критичних цифрових сервісів, вимоги до захисту даних, резервування, кібербезпеки, безперервності послуг і відповідальності суб'єктів [9-11];
- організаційно-координаційна підсистема, що забезпечує взаємодію органів державної влади, органів місцевого самоврядування, громад, бізнесу, операторів інфраструктури та провайдерів цифрових послуг [12];

- фінансово-ресурсна підсистема, що передбачає мобілізацію коштів на резервування інфраструктури, модернізацію сервісів, кіберзахист, навчання персоналу та відновлення після інцидентів [1, с. 24-31];
- інфраструктурно-технологічна підсистема, що пов'язана з розвитком резервних каналів зв'язку, альтернативного енергоживлення, центрів обробки даних, хмарних рішень, захищених реєстрів і платформ;
- кадрово-компетентнісна підсистема, що охоплює цифрові навички населення, професійні компетентності управлінців і технічного персоналу, готовність команд діяти в умовах кризових порушень [7, с. 14-21];
- інформаційно-аналітична підсистема, що забезпечує моніторинг цифрових ризиків, оцінювання вразливостей, аналіз інцидентів і формування доказової основи для управлінських рішень [2; 8];
- адаптаційно-навчальна підсистема, що передбачає оновлення процедур, інституційних правил і технологічних рішень за результатами пережитих шоків [5, с. 179-193].

У такій логіці цифрова резильєнтність регіонів постає результатом не лише технологічної модернізації, а й узгодженої дії інституцій, економічних ресурсів, управлінських процедур, людського капіталу та механізмів міжсекторної взаємодії. Це відповідає положенням регіональної та інституційної економіки, згідно з якими стійкість просторових систем визначається не тільки наявністю ресурсів, а й якістю правил, координації та здатністю суб'єктів до спільної дії [4, с. 1-42; 6]. Дослідницький фокус тим самим зміщується із суто технологічного на інституційно-економічний, що й дає підстави розглядати цифрову резильєнтність регіонів як самостійний об'єкт інституційно-економічного забезпечення.

Висновки. За результатами дослідження цифрову резильєнтність регіону визначено як самостійну категорію регіональної економіки мезорівня. Вона характеризує здатність цифрової підсистеми регіону зберігати критично важливі функції під час кризового впливу, відновлювати їх у прийнятні строки, адаптуватися до нових умов і вдосконалювати інституційно-економічні механізми цифрового розвитку.

Запропоноване визначення розкриває цифрову резильєнтність через загальну ознаку – здатність соціотехнічної підсистеми регіону реагувати на кризові впливи – та специфічну ознаку, яка полягає в оцінюванні її функціонування до, під час і після шоку. Отже, цифрова резильєнтність характеризує не загальний рівень цифровізації регіону, а його здатність зберігати, відновлювати й оновлювати цифрові функції в умовах кризи.

Обґрунтовано, що запропонована категорія не є тотожною цифровій трансформації, цифровій зрілості, кіберстійкості, цифровій операційній резильєнтності чи національній стійкості: перші дві описують рівень і траєкторію цифрового розвитку, третя і четверта – технічний захист та безперервність ІКТ-операцій окремих суб'єктів, п'ята – макрорівневу спроможність держави. Розмежування здійснено за чотирма критеріями: предметом опису, масштабом аналізу, часовою логікою та ключовим дослідницьким питанням.

Запропоновано розглядати модель цифрової резильєнтності регіону, яка показує, як різні складові його цифрової системи реагують на кризу. Модель охоплює чотири етапи: здатність витримати негативний вплив, відновити роботу, пристосуватися до нових умов і вдосконалити систему після кризи. Ці етапи розглядаються за п'ятьма основними складовими: цифровою інфраструктурою, інституціями, ресурсним забезпеченням, людським потенціалом, даними та цифровими послугами. На цій основі визначаються напрями інституційно-економічного забезпечення цифрової резильєнтності.

Модель цифрової резильєнтності регіону може стати основою для розроблення інтегрального індексу цифрової резильєнтності регіонів. На нашу думку, на відміну від індексів цифрової трансформації, він має оцінювати не кількість упроваджених цифрових технологій, а здатність регіональної цифрової системи зберігати працездатність, швидко відновлюватися та змінюватися після кризових впливів.

Теоретичне значення отриманих результатів полягає в розширенні понятійного апарату регіональної економіки цифровим виміром резильєнтності, практичне – у створенні підґрунтя для проектування інституційно-економічних механізмів забезпечення цифрової резильєнтності регіонів та для інформаційно-аналітичної підтримки регіональної політики, кризового управління й планування посткризового відновлення. Перспективи подальших досліджень пов'язані з операціоналізацією запропонованої матриці в систему вимірюваних показників, розробленням методики нормалізації та агрегування субіндексів і апробацією індексу на даних регіонів України в умовах воєнних і посткризових трансформацій.

1. Ukraine Fifth Rapid Damage and Needs Assessment (RDNA5), February 2022 – December 2025 / World Bank, Government of Ukraine, European Union, United Nations. Washington, DC : World Bank, 2026. 156 p. DOI: <https://doi.org/10.1596/44369>.
2. Державна служба спеціального зв'язку та захисту інформації України. CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів: кількість ворожих атак зросла на 37 %. 2026. URL: <https://cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracuyvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zroslo-na-37> (дата звернення: 30.06.2026).
3. 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>.
4. Martin R., Sunley P. On the notion of regional economic resilience: conceptualization and explanation. *Journal of Economic Geography*. 2015. Vol. 15, No. 1. P. 1-42. DOI: <https://doi.org/10.1093/jeg/lbu015>.
5. Павліха Н. В., Корнелюк О. А. Циркулярна модель як інноваційна система відновлення конкурентоспроможності регіонів і територіальних громад в Україні у воєнний і повоєнний періоди. *Вісник Національного університету водного господарства та природокористування. Серія «Економічні науки»*. 2023. Вип. 3(103). С. 179-193. DOI: <https://doi.org/10.31713/ve3202315>.
6. Резильєнтність ендегенного розвитку регіонів в умовах глобальних викликів та шоків : монографія / наук. ред. М. І. Мельник. Львів : ДУ «Інститут регіональних досліджень імені М. І. Долишнього НАН України», 2024. 307 с. URL: <https://ird.gov.ua/irdp/p20240001.pdf> (дата звернення: 30.06.2026).
7. Іртищева І. О., Сенкевич О. Ф. Цифрова трансформація регіонів України: об'єктивна необхідність, принципи цифрового розвитку та особливості регулювання. *Регіональна економіка*. 2020. № 1. С. 14-21. DOI: <https://doi.org/10.36818/1562-0905-2020-1-2>.
8. Індекс цифрової трансформації регіонів та громад / Міністерство цифрової трансформації України ; платформа «Дія.Цифрова громада». URL: <https://hromada.gov.ua/> (дата звернення: 30.06.2026).
9. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA). *Official Journal of the European Union*. 2022. L 333. P. 1-79. URL: <https://eur-lex.europa.eu/eli/reg/2022/2554/oj> (дата звернення: 30.06.2026).
10. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2). *Official Journal of the European Union*. 2022. L 333. P. 80-152. URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> (дата звернення: 30.06.2026).
11. The NIST Cybersecurity Framework (CSF) 2.0 : NIST CSWP 29. Gaithersburg, MD : National Institute of Standards and Technology, 2024. 32 p. DOI: <https://doi.org/10.6028/NIST.CSWP.29>.
12. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості» : Указ Президента України від 27.09.2021 № 479/2021. URL: <https://zakon.rada.gov.ua/laws/show/479/2021> (дата звернення: 30.06.2026).

References

1. World Bank, et al. *Ukraine Fifth Rapid Damage and Needs Assessment (RDNA5)*, February 2022 – December 2025. World Bank, 2026, <https://doi.org/10.1596/44369>.
2. State Service of Special Communications and Information Protection of Ukraine. “In 2025 CERT-UA Processed Almost 6,000 Cyber Incidents: The Number of Hostile Attacks Increased by 37 %.” *Cip.gov.ua*, 2026, cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracuyvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zroslo-na-37. Accessed 30 June 2026.

3. Holling, C. S. "Resilience and Stability of Ecological Systems." *Annual Review of Ecology and Systematics*, vol. 4, 1973, pp. 1-23, <https://doi.org/10.1146/annurev.es.04.110173.000245>.
4. Martin, Ron, and Peter Sunley. "On the Notion of Regional Economic Resilience: Conceptualization and Explanation." *Journal of Economic Geography*, vol. 15, no. 1, 2015, pp. 1-42, <https://doi.org/10.1093/jeg/lbu015>.
5. Pavlikha, N. V., and O. A. Korneliuk. "Circular Model as an Innovative System for Restoring the Competitiveness of Regions and Territorial Communities in Ukraine during the War and Post-War Periods." *Bulletin of the National University of Water and Environmental Engineering. Economic Sciences*, no. 3(103), 2023, pp. 179-93, <https://doi.org/10.31713/ve3202315>.
6. Melnyk, M. I., editor. *Resilience of Endogenous Regional Development under Global Challenges and Shocks*. Dolishnyi Institute of Regional Research of the NAS of Ukraine, 2024, ird.gov.ua/irdp/p20240001.pdf. Accessed 30 June 2026.
7. Irtysheva, I. O., and O. F. Senkevych. "Digital Transformation of the Regions of Ukraine: Objective Necessity, Principles of Digital Development and Regulatory Features." *Regional Economy*, no. 1, 2020, pp. 14-21, <https://doi.org/10.36818/1562-0905-2020-1-2>.
8. "Index of Digital Transformation of Regions and Communities." Diia. Digital Community, Ministry of Digital Transformation of Ukraine, hromada.gov.ua/. Accessed 30 June 2026.
9. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector (DORA). *Official Journal of the European Union*, L 333, 2022, pp. 1-79, eur-lex.europa.eu/eli/reg/2022/2554/oj. Accessed 30 June 2026.
10. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union (NIS2). *Official Journal of the European Union*, L 333, 2022, pp. 80-152, eur-lex.europa.eu/eli/dir/2022/2555/oj. Accessed 30 June 2026.
11. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, NIST, 2024, <https://doi.org/10.6028/NIST.CSWP.29>. Accessed 30 June 2026.
12. President of Ukraine. On the Decision of the National Security and Defence Council of Ukraine of 20 August 2021 "On the Introduction of the National Resilience System". Decree no. 479/2021, 27 Sept. 2021, zakon.rada.gov.ua/laws/show/479/2021. Accessed 30 June 2026.

Дата подання: 02.08.2026

Дата прийняття до друку: 19.08.2026