

УДК 338.24:004:330.3:351

JEL O33, F52, H56

DOI <https://doi.org/10.32782/2786-765X/2026-14-26>**Фісуненко Н.О.**

кандидат економічних наук,

в.о. завідувача кафедри девелопменту нерухомості, фінансів, обліку та маркетингу,

Український державний університет науки і технологій

ORCID: <https://orcid.org/0000-0003-3985-7813>

ЦИФРОВА СТРАТЕГІЧНА НАВІГАЦІЯ ЯК ОСНОВА ЗАХИСТУ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

У статті досліджено теоретичні засади цифрової стратегічної навігації економіки як основи захисту національної економіки в умовах цифрової трансформації. Обґрунтовано, що посилення цифрової залежності держави, гібридні загрози, кібератаки та вразливість критичної інфраструктури потребують переходу від фрагментарної цифровізації до стратегічно скоординованої моделі управління. Уточнено зміст поняття цифрової стратегічної навігації економіки, розмежовано його з близькими категоріями цифрового розвитку та систематизовано ключові контури її реалізації. Визначено роль IT-сектору як критичної інфраструктурної основи економічної безперервності держави. Окреслено можливості використання запропонованого підходу для формування цифрової політики, оцінювання вразливостей і стратегічного планування в умовах воєнних та поствоєнних викликів.

Ключові слова: цифрова трансформація, цифрова стратегічна навігація, стратегія, захист економіки, економічна стійкість, національна економіка, IT-сектор, цифровий суверенітет.

Постановка проблеми. У сучасних умовах глобальної нестабільності цифрова трансформація перестала бути виключно технологічною категорією та набула ознак системного чинника економічної, політичної й безпекової стійкості держави. Війна, геоекономічне суперництво, посилення кіберзагроз, вразливість платформної інфраструктури та залежність критичних функцій управління від цифрових сервісів істотно змінили характер економічних ризиків. Якщо раніше цифровізація розглядалася переважно як засіб підвищення ефективності, то нині вона безпосередньо пов'язується з питаннями безперервності управління, захисту критичної інфраструктури, збереження економічного суверенітету та стійкості фінансових і логістичних систем.

Повномасштабна війна проти України продемонструвала, що цифрове середовище є не тільки простором розвитку, а й ареною багаторівневого протистояння. За оцінками OECD, цифровізація здатна підвищувати стійкість українських підприємств, але рівень використання цифрових інструментів залишається нерівномірним: близько 70 % великих підприємств мають вебсайт, тоді як серед середніх цей показник становить 47 %, а серед малих – лише 30 % [7].

Паралельно дослідження Світового банку засвідчує критичну важливість кібербезпеки

для економічної результативності в цифрову добу, що особливо актуалізується в умовах воєнного тиску на фінансові, комунікаційні та державні системи [9].

Особливої актуальності це набуває у зв'язку з тим, що сучасний цифровий простір дедалі більше функціонує як середовище стратегічного суперництва. Цифрові платформи, дані, канали зв'язку та сервіси стають інструментами економічного тиску, системної дестабілізації та геополітичного впливу. У такому контексті цифровізація виступає одночасно ресурсом модернізації, сферою ризиків і полем стратегічного маневру, що зумовлює потребу в осмисленні цифрової трансформації економіки як процесу, який має власну логіку пріоритезації, захисту та адаптивного управління [8; 11].

Аналіз останніх досліджень і публікацій. У сучасній науковій літературі цифрова трансформація економіки здебільшого аналізується через категорії цифрової стратегії, технологічного впровадження, платформної взаємодії, управління змінами та формування цифрових екосистем. У документах OECD, присвячених цифровій трансформації бізнесу в Україні, підкреслено, що цифрове середовище потребує не лише технічної модернізації, а й стратегічного бачення, яке поєднує аналітику даних, організаційну адаптивність, міжплатформну взаємодію

та цілеспрямоване інституційне супроводження [7; 8]. Фактично йдеться про необхідність переходу від ситуативної цифровізації до системного цифрового орієнтування.

В своїх дослідженнях М. D'Cruz, G. Timbrell, J. Watson, розглядають цифрову стратегію як динамічний процес, що змінює класичне розуміння стратегічного планування. На думку авторів, цифрова стратегія повинна бути гнучкою, адаптивною та експериментальною, оскільки цифрове середовище є несталим і вимагає постійного коригування рішень [3].

Це положення є важливим, однак зазначені автори зосереджуються переважно на рівні організації, залишаючи поза достатньою увагою макроекономічний вимір цифрового орієнтування.

Разом з тим науковці J. Díaz-Arancibia, J. Hochstetter-Diez, A. Bustamante-Mora, S. Sepúlveda-Cuevas, I. Albayay, J. Arango-López, стверджують, що цифрова трансформація розглядається крізь призму малих і середніх підприємств у країнах, що розвиваються. Дослідники доводять, що її результативність визначається не лише технологічними рішеннями, а й станом підприємницької екосистеми, соціокультурними умовами, доступом до інфраструктури, рівнем цифрової грамотності та ресурсними обмеженнями [4].

Такий висновок важливий для макrorівневого аналізу, адже підкреслює необхідність контекстуалізації цифрової політики.

Важливим також є розробки М. Egodawele, D. Sedera, V. Bui, які було здійснено науковцями узагальнюючи літературу 2013–2021 рр., котрі запропонували номологічну модель RC3O, яка пояснює цифрову трансформацію через взаємозв'язок ресурсів, конфігурацій, компетентностей і результатів [5]. Вони звертають увагу на такі обмеження, як нестача цифрових ресурсів, інфраструктурні вузькі місця, кадровий дефіцит та низька адаптивність організацій. Ці положення також важливі, оскільки дають підстави трактувати цифрову навігацію не лише як вибір маршруту, а і як управління обмеженнями маршруту.

Сучасники C. Chen, L. Zhang, Y. Li, T. Liao, S. Zhao, Z. Zheng, H. Huang, J. Wu у праці присвяченій цифровій економіці через програми Web3.0 і виклики наголошують на значенні децентралізації, цифрової ідентичності, захищених транзакцій і блокчейн-рішень для підвищення безпеки, конфіденційності та довіри до цифрового середовища [2, с. 233–239]. Вони фактично

показують, що технологічна архітектура цифрової економіки прямо впливає на її стратегічну стійкість.

Праця R. Baggio та G. Del Chiappa, присвячена туристичним DESTINACIЯM як цифровим бізнес-екосистемам, підтверджує, що цифрова взаємодія є повноцінною структурною складовою економічної системи, а управління інформаційними потоками стає не менш важливим, ніж управління фізичними активами [1, с. 4–7]. Ця ідея має універсальне значення, оскільки дозволяє поширити логіку цифрових екосистем на рівень національної економіки.

Окремий напрям сучасних досліджень формують підходи, що зосереджені на деструктивному та геоeкономічному вимірі цифровізації. Матеріали OECD і Світового банку показують, що цифрові інциденти здатні породжувати не тільки технічні, а й економічні, соціальні та репутаційні втрати, підривати довіру до цифрових сервісів і стримувати інновації [8; 9].

Водночас аналітика World Economic Forum засвідчує, що технологічні зрушення та геоeкономічна фрагментація дедалі сильніше впливають на регуляторні рамки, ланцюги постачання, інвестиційні рішення й конкурентоспроможність економік [11].

Отже, у сучасних дослідженнях достатньо глибоко опрацьовано питання цифрової стратегії, впровадження технологій та розвитку цифрових екосистем, але недостатньо висвітлено макроекономічний і безпековий вимір цифрового управління. Невирішеною залишається проблема інтеграції цих підходів у єдину теоретичну рамку, яка б описувала процес цілеспрямованого стратегічного орієнтування національної економіки у цифровому середовищі.

Метою статті є теоретичне обґрунтування поняття цифрової стратегічної навігації економіки, розмежування його зі спорідненими поняттями, а також розроблення структурно-логічної моделі використання цифрової стратегічної навігації як інструменту забезпечення стійкості держави в умовах гібридних загроз, війни та зростаючої залежності економіки від критичної цифрової інфраструктури.

Виклад основного матеріалу дослідження. Цифрова трансформація в сучасній економіці має розглядатися щонайменше у трьох взаємопов'язаних площинах: технологічній, інституційній та безпековій. Технологічна площа охоплює запровадження нових платформ, цифрових сервісів, хмарних архітектур, засобів аналітики

даних, автоматизації та штучного інтелекту. Інституційна площина стосується зміни правил, ролей і механізмів координації між державою, бізнесом, громадянами та транснаціональними платформами. Безпекова площина пов'язана з уразливістю цифрової інфраструктури, ризиками втрати даних, технологічної залежності, порушення безперервності управління та асиметричними формами тиску, що реалізуються через кіберпростір [3; 8, с. 5–6; 9, с. 1].

Саме поєднання цих трьох площин формує нову парадигму цифрової епохи. Цифровізація більше не може тлумачитися як суто технічне оновлення. Вона визначає характер економічної взаємодії, структуру ринків, типи вразливостей і моделі стратегічного реагування. У цифрову добу держава змушена управляти не тільки традиційними матеріальними ресурсами, а й цифровими потоками, платформними зв'язками, архітектурою даних, цифровою довірою та стійкістю до кібератак. Отже, економічна політика набуває нової координати – цифрово-безпекової.

Отже, одним із найбільш вживаних у науковому та стратегічному дискурсі останніх років є поняття цифрова економічна війна, особливо вона актуальна в період активних військових дій, доцільно трактувати як форму системного використання цифрових технологій, інфраструктурних залежностей і платформних вразливостей для отримання економічної переваги або завдання економічної шкоди супротивнику. Йдеться не про поодинокі кіберінциденти, а про включення цифрових засобів у ширшу геоекономічну логіку тиску, коли порушення роботи логістики, фінансових сервісів, державних реєстрів чи каналів оброблення даних спричиняє ефект, співставний із наслідками класичних економічних обмежень [8, с. 37–38; 11, с. 4–7].

Іншим ключовим терміном є поняття кіберзагрози, що спричиняють економічним збиткам (кіберекономічні порушення), які концентрують увагу на порушеннях економічного функціонування внаслідок цифрових втручань, а отже є потреба у створенні відповідної стратегії захисту національної економіки. Значення полягає в тому, що загрози дозволяє розглядати кіберподію не тільки як технічний інцидент, а як економічний шок.

Такий шок проявляється у розриві ланцюгів постачання, блокуванні розрахунків, зупинці державних послуг, зниженні довіри до цифрових сервісів, відпливі інвестицій та погіршенні очікувань економічних агентів. Дослідження Світового банку підтверджує,

що кібербезпека безпосередньо пов'язана з економічною результативністю і продуктивністю, а OECD наголошує на мультисекторальному характері цифрових інцидентів та їх здатності підривати інновації і стійкість [8, с. 37–38; 9, с. 1].

Наступним важливим компонентом є поняття цифрова геополітична стратегія, варто розуміти як використання цифрових даних, інфраструктури, регуляторних рішень та аналітики для досягнення довгострокових геополітичних і геоекономічних цілей.

Отже, йдеться про здатність держави або наддержавного утворення контролювати цифрові платформи, аналізувати ресурсні та інформаційні потоки, прогнозувати дефіцити та кризи, а також використовувати цифрові інструменти для впливу на зовнішнє середовище. У результаті дані й цифрові сервіси стають елементом геополітичної могутності, а цифрова політика – інструментом стратегічного позиціонування [2; 11].

Синтез наведених понять дає змогу констатувати: цифрова реальність перестає бути нейтральною. Вона перетворюється на арену протистояння, де одночасно взаємодіють технологічні (цифрові), економічні, політичні та безпекові чинники. Саме тому необхідна категорія, яка об'єднала б стратегічність, адаптивність, аналітичність і ризик-орієнтованість.

Такою категорією у межах цього дослідження є цифрова стратегічна навігація економіки.

На відміну від поняття «навігація в цифровій економіці», яке описує орієнтування суб'єктів у вже сформованому цифровому середовищі, поняття «цифрова стратегічна навігація економіки» має інший фокус. Воно концентрується на економіці як об'єкті управління. У цьому випадку ключовим стає не пристосування до цифрових змін, а формування стратегічної траєкторії цифрового розвитку з урахуванням вразливостей, ресурсних обмежень, інституційних умов та довгострокових цілей держави [3, с. 4–7; 7, с. 13].

Під цифровою стратегічною навігацією економіки доцільно розуміти безперервний процес стратегічного орієнтування, координації, пріоритезації та коригування цифрових рішень у національній економіці з урахуванням ризиків, гібридних загроз, стану критичної інфраструктури, обмеженості ресурсів і довгострокових цілей розвитку. Таке трактування дозволяє охопити як технологічний, так і інституційно-безпековий вимір цифрових процесів.

Концептуальна цінність авторського підходу полягає у відмові від лінійного бачення цифровізації. У більшості практик цифрова трансформація розглядається як послідовність проєктів: цифровізація послуг, автоматизація процесів, створення платформ, інтеграція баз даних. Однак в умовах війни та гібридних загроз така логіка є недостатньою, оскільки не відповідає на питання про пріоритети захисту, порядок перерозподілу ресурсів, способи швидкої зміни траєкторії дій у разі шоку. Цифрова стратегічна навігація, навпаки, виходить із того, що стратегія повинна бути адаптивною і постійно уточнюваною.

Структурно-логічна модель цифрової стратегічної навігації економіки містить шість взаємопов'язаних контурів: цільовий, аналітичний, інфраструктурний, інституційний, ризик-орієнтований та адаптивний. Цільовий контур задає систему стратегічних цілей: безперервність управління, збереження цифрового суверенітету, підвищення економічної стійкості, захист критичної інфраструктури, підтримка інновацій та інтеграція до європейського цифрового простору. Саме цей контур відповідає на питання, заради чого здійснюється цифрова трансформація в умовах високого ризику.

Аналітичний контур забезпечує збирання, інтеграцію, верифікацію та інтерпретацію даних, необхідних для підтримки рішень. Його змістом є ситуаційні центри, інструменти моніторингу цифрових ризиків, системи прогнозування, механізми сценарного аналізу та використання великих даних.

Як показують в своїх дослідженнях А. Jabbar, Р. Akhtar, та S. Dani, оперативна аналітика істотно змінює здатність управлінців приймати рішення в умовах високої динаміки [6]. Для держави це означає можливість своєчасно виявляти цифрові вразливості, логістичні збої, зміни платіжної поведінки чи аномалії у функціонуванні сервісів.

Інфраструктурний контур охоплює технічну основу цифрової стійкості: дата-центри, хмарні рішення, телекомунікаційну мережу, канали зв'язку, державні реєстри, системи резервного копіювання, інструменти електронної ідентифікації, захищені шлюзи транзакцій. Він визначає, чи здатна економіка працювати в режимі стресу, часткової втрати активів або кібератак. Власне інфраструктурна незрілість часто стає причиною того, що навіть раціональні цифрові стратегії не можуть бути реалізовані на практиці.

Інституційний контур пов'язаний із нормативною базою, процедурами координації,

компетенціями органів влади, формами державно-приватного партнерства, правилами обміну даними, відповідальністю за захист критичних цифрових систем. Інституційна слабкість призводить до фрагментації цифрової політики, дублювання функцій, конфліктів повноважень та відсутності спільної картини цифрових ризиків. Отже, без інституційного контуру цифрова стратегічна навігація перетворюється на сукупність несинхронізованих ініціатив.

Ризик-орієнтований контур виконує функцію постійного виявлення, ранжування та переоцінювання цифрових загроз. До них належать кібератаки, відмова критичних вузлів, втрати або спотворення даних, репутаційні шоки, платформна монополізація, залежність від зовнішніх провайдерів, алгоритмічні викривлення та технологічні «сліпі зони». У цьому контурі мають формуватися карти стратегічної вразливості, які слугують основою для пріоритезації захисту та сценарного планування.

Адаптивний контур забезпечує здатність системи швидко змінювати режими роботи, перерозподіляти ресурси, коригувати цифрові маршрути, запускати резервні сценарії та інтегрувати нові рішення. Саме адаптивність відрізняє цифрову стратегічну навігацію від статичного цифрового планування. В умовах війни, коли зовнішні умови змінюються раптово, цифрова політика повинна бути спроможною працювати не в логіці «раз і назавжди ухваленого плану», а в логіці неперервного коригування курсу.

Особливе місце у моделі цифрової стратегічної навігації посідає ІТ-сектор. У сучасних умовах він є не лише галуззю економіки, а й критичною інфраструктурою. Закон України «Про критичну інфраструктуру» закріплює підхід, відповідно до якого об'єкти, порушення функціонування яких може спричинити загрозу національній безпеці, економічній стабільності чи життю населення, підлягають спеціальному режиму захисту [10].

ІТ-інфраструктура цілком відповідає цим ознакам, оскільки саме через неї здійснюються державне управління, бюджетні й банківські операції, соціальні виплати, електронний документообіг, логістична координація та численні сервіси взаємодії держави з громадянами.

Вразливість ІТ-сектору автоматично перетворюється на вразливість усієї економічної системи. Атаки на сервери державних установ, телекомунікації, хмарні сервіси, фінансові платформи чи реєстри мають наслідки,

що виходять далеко за межі технічних збоїв: вони здатні блокувати бюджетні процеси, порушувати розрахунки, гальмувати логістику, дезорганізовувати соціальну підтримку та послаблювати довіру до держави. OECD акцентує, що зростання залежності від цифрових технологій підвищує ризики вздовж усього ланцюга створення вартості і може призводити до масштабних збоїв у критичних послугах [8, с. 37–38].

В умовах війни ІТ-сектор виконує дві функції одночасно. З одного боку, він забезпечує операційне функціонування системи – від документообігу до платіжної інфраструктури. З іншого боку, він генерує інноваційні рішення для адаптації: системи резервного розміщення даних, платформи аналітики, цифрові сервіси для громадян, рішення для відстеження ресурсів, логістики та військово-цивільної координації. Водночас дані OECD свідчать, що подальше підвищення стійкості потребує розширення цифрової зрілості бізнесу та ширшого впровадження інструментів цифрової трансформації в українській економіці [7, с. 13].

Цифрова стратегічна навігація економіки у воєнний період виконує щонайменше три функції. Перша – функція безперервності: забезпечення роботи ключових сервісів навіть в умовах атаки або руйнування окремих вузлів. Друга – функція випереджального реагування: виявлення зон стратегічної вразливості до того, як вони спричинять системні наслідки. Третя – функція підготовки до відновлення: накопичення даних, інструментів і управлінських механізмів, необхідних для прозорості та координованої повоєнної відбудови.

У повоєнному вимірі цифрова стратегічна навігація економіки набуває ще більшої ваги. Відновлення інфраструктури, модернізація виробничої бази, інтеграція до європейського цифрового простору, нарощення інституційної спроможності та відновлення довіри до державних сервісів потребують цілісної цифрової політики. При цьому відбудова має не відтворювати попередні вразливості, а закладати нову архітектуру стійкості: децентралізовані вузли, сумісні системи, хмарні рішення, високий рівень резервування та прозорі механізми контролю.

Важливим елементом прикладного використання концепції є формування системи індикаторів цифрової стратегічної навігації. До кількісних показників доцільно віднести частку ІТ-сектору у ВВП та експорті послуг, частку електронних транзакцій, кількість критичних цифрових сервісів із резервним

контуром, середній час відновлення після інциденту, частку державних систем, перенесених у хмарні середовища, рівень проникнення цифрових сервісів у публічне управління. До якісних показників слід віднести рівень готовності до кіберінцидентів, ступінь міжвідомчої координації, довіру населення до цифрових сервісів, сумісність державних платформ, адаптивність нормативного середовища та швидкість ухвалення цифрових рішень у кризі.

Особливе значення має те, що система індикаторів не повинна бути суто статистичною. Її призначення полягає в підтримці стратегічного орієнтування. Це означає, що показники мають використовуватися у механізмах раннього попередження, сценарного моделювання та пріоритезації ресурсів. Наприклад, падіння доступності конкретного цифрового сервісу має трактуватися не лише як технічний збій, а як сигнал інституційної та економічної вразливості. А висока залежність від одного зовнішнього провайдера повинна оцінюватися як потенційний суверенний ризик.

Практична реалізація цифрової стратегічної навігації економіки потребує низки політичних та управлінських кроків.

По-перше, необхідно інституціоналізувати функцію стратегічного управління цифровими ризиками в системі економічної безпеки.

По-друге, доцільно сформувати національні та галузеві карти стратегічної вразливості цифрової інфраструктури.

По-третє, слід розробити сценарії багаторівневого резервування цифрових сервісів, включаючи хмарні майданчики, автономні канали зв'язку та протоколи швидкого відновлення.

По-четверте, необхідно поглибити інтеграцію ІТ-сектору в архітектуру економічної стійкості через спеціальні режими підтримки кіберзахисту, розвиток критично важливих цифрових сервісів, стимулювання створення вітчизняних платформних рішень та підвищення цифрової грамотності управлінських кадрів.

По-п'яте, державна політика має бути сумісною з європейськими стандартами цифрового ринку, захисту даних і кібербезпеки, але водночас враховувати специфіку країни, що перебуває у стані війни й має підвищений рівень гібридних загроз.

У цілому цифрова стратегічна навігація економіки є не статичною стратегією, а динамічним адаптивним механізмом. Вона дозволяє державі та її інституціям швидко

змінювати вектори цифрових рішень, орієнтуючись на ризики, обмежені ресурси, потребу безперервності управління та довгострокові цілі розвитку. Саме в такому трактуванні цифрова трансформація постає не як опція модернізації, а як обов'язкова умова економічної стійкості й виживання держави у XXI столітті.

Висновки. У статті доведено, що цифрова трансформація сучасної економіки повинна розглядатися не лише як технологічне оновлення, а як безпековий і стратегічний процес, який визначає стійкість держави в умовах гібридних загроз. Систематизація понять Digital Economy Warfare, Cyber Economic Disruption та Digital Geopolitical Strategy підтвердила, що цифрове середовище перетворюється на простір стратегічного протистояння, у якому дані, платформи, інфраструктура та цифрові сервіси набувають значення критичних ресурсів розвитку, влади й захисту.

Обґрунтовано доцільність використання авторського поняття «цифрова стратегічна навігація економіки», яке описує безперервний процес стратегічного орієнтування, координації, пріоритезації та адаптивного коригування цифрових рішень у національній економіці. Запропонована структурно-логічна модель цифрової стратегічної навігації охоплює цільовий, аналітичний,

інфраструктурний, інституційний, ризик-орієнтований та адаптивний контури, що в сукупності утворюють основу державної економічної стійкості у цифрову епоху.

Доведено, що в умовах повномасштабної війни ІТ-сектор має розглядатися як об'єкт критичної інфраструктури та як операційна основа цифрового державного управління. Його захищеність прямо впливає на безперервність бюджетних, банківських, соціальних, логістичних та оборонних процесів. Саме тому резервування цифрових сервісів, розвиток хмарної архітектури, платформна сумісність і готовність до кіберінцидентів повинні бути інтегровані у загальну стратегію економічної політики.

Практична значущість дослідження полягає у можливості використання запропонованого підходу для формування державної цифрової політики, побудови карт стратегічної вразливості, вибору пріоритетів захисту критичної інфраструктури та розроблення антикризових сценаріїв у воєнний і повоєнний періоди. Перспективи подальших досліджень доцільно пов'язати з побудовою формалізованої системи індикаторів цифрової стратегічної навігації економіки, її галузевою та регіональною апробацією, а також із розробленням інструментів сценарного моделювання цифрових ризиків у системі економічної безпеки держави.

Бібліографічний список

1. Baggio R., Del Chiappa G. Tourism destinations as digital business ecosystems. *arXiv*. 2012. URL: <https://arxiv.org/abs/1210.3943> (дата звернення: 14.06.2026).
2. Chen C., Zhang L., Li Y., Liao T., Zhao S., Zheng Z., Huang H., Wu J. When Digital Economy Meets Web3.0: Applications and Challenges. *IEEE Open Journal of the Computer Society*. 2022. Vol. 3. P. 233–245. DOI: <https://doi.org/10.1109/OJCS.2022.3217565>
3. D'Cruz M., Timbrell G., Watson J. Strategy in a digital world. *arXiv*. 2016. URL: <https://arxiv.org/abs/1606.03530> (дата звернення: 12.06.2026).
4. Díaz-Arancibia J., Hochstetter-Diez J., Bustamante-Mora A., Sepúlveda-Cuevas S., Albayay I., Arango-López J. Navigating digital transformation and technology adoption: A literature review from small and medium-sized enterprises in developing countries. *Sustainability*. 2024. Vol. 16 (6). Art. 5946. DOI: <https://doi.org/10.3390/su160605946>
5. Egodawe M., Sedera D., Bui V. A systematic review of digital transformation literature (2013–2021) and the development of an overarching a-priori model to guide future research. *Australasian Conference on Information Systems*. 2022. URL: <https://arxiv.org/pdf/2212.03867> (дата звернення: 01.07.2026).
6. Jabbar A., Akhtar P., Dani S. Real-time big data processing for instantaneous marketing decisions: A problematization approach. *Industrial Marketing Management*. 2019. DOI: <https://doi.org/10.1016/j.indmarman.2019.09.001>
7. Organisation for Economic Co-operation and Development. Enhancing resilience by boosting digital business transformation in Ukraine. Paris : OECD Publishing, 2024. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/05/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_c2e06e50/4b13b0bb-en.pdf (дата звернення: 29.06.2026).
8. Organisation for Economic Co-operation and Development. Digital security and resilience in critical infrastructure and essential services. Paris : OECD Publishing, 2019. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/04/digital-security-and-resilience-in-critical-infrastructure-and-essential-services_5593c149/a7097901-en.pdf (дата звернення: 30.06.2026).
9. Закон України № 1882-IX від 16.12.2021 р. «Про критичну інфраструктуру» URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (дата звернення: 02.07.2026).

10. Vergara Cobos, Estefania; Cakir, Selcen; Mei-Zahav, Hagai; Barakcin Berkay, Baran. 2024. *The Role of Cybersecurity in Economic Performance*. Washington, DC: World Bank. URL: <https://documents1.worldbank.org/curated/en/099092324164526526/pdf/P178769189c7360111ac1f1185e04824dec.pdf> (дата звернення: 20.06.2026).
11. World Economic Forum. Four futures for the new economy: Geoeconomics and technology in 2030. Geneva : World Economic Forum, 2025. URL: https://reports.weforum.org/docs/WEF_Four_Futures_for_the_New_Economy_Geoeconomics_and_Technology_in_2030_2025.pdf (дата звернення: 12.06.2026).

References

1. Baggio, R., & Del Chiappa, G. (2012). *Tourism destinations as digital business ecosystems*. arXiv. Available at: <https://arxiv.org/abs/1210.3943> (accessed June 14, 2026).
2. Chen, C., Zhang, L., Li, Y., Liao, T., Zhao, S., Zheng, Z., Huang, H., & Wu, J. (2022). When Digital Economy Meets Web3.0: Applications and Challenges. *IEEE Open Journal of the Computer Society*, no 3, pp. 233–245. DOI: <https://doi.org/10.1109/OJCS.2022.3217565>
3. D'Cruz, M., Timbrell, G., & Watson, J. (2016). *Strategy in a digital world*. arXiv. Available at: <https://arxiv.org/abs/1606.03530> (accessed June 12, 2026).
4. Díaz-Arancibia, J., Hochstetter-Diez, J., Bustamante-Mora, A., Sepúlveda-Cuevas, S., Albayay, I., & Arango-López, J. (2024). Navigating digital transformation and technology adoption: A literature review from small and medium-sized enterprises in developing countries. *Sustainability*, no 16 (6), Article 5946. DOI: <https://doi.org/10.3390/su160605946>
5. Egodawele, M., Sedera, D., & Bui, V. (2022). A systematic review of digital transformation literature (2013–2021) and the development of an overarching a-priori model to guide future research. *Australasian Conference on Information Systems*. Available at: <https://arxiv.org/pdf/2212.03867> (accessed July 1, 2026).
6. Jabbar, A., Akhtar, P., & Dani, S. (2019). Real-time big data processing for instantaneous marketing decisions: A problematization approach. *Industrial Marketing Management*. DOI: <https://doi.org/10.1016/j.indmarman.2019.09.001>
7. Organisation for Economic Co-operation and Development. (2024). *Enhancing resilience by boosting digital business transformation in Ukraine*. Paris: OECD Publishing. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/05/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_c2e06e50/4b13b0bb-en.pdf (accessed June 29, 2026).
8. Organisation for Economic Co-operation and Development. (2019). *Digital security and resilience in critical infrastructure and essential services*. Paris: OECD Publishing. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/04/digital-security-and-resilience-in-critical-infrastructure-and-essential-services_5593c149/a7097901-en.pdf (accessed June 30, 2026).
9. Verkhovna Rada Ukrainy. (2021). *Pro krytychnu infrastrukturu: Zakon Ukrainy vid 16 lystopada 2021 roku No. 1882-IX* [On critical infrastructure: Law of Ukraine of November 16, 2021 No. 1882-IX]. Available at: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (accessed July 2, 2026).
10. Vergara Cobos, E., Cakir, S., Mei-Zahav, H., & Barakcin Berkay, B. (2024). *The role of cybersecurity in economic performance*. Washington, DC: World Bank. Available at: <https://documents1.worldbank.org/curated/en/099092324164526526/pdf/P178769189c7360111ac1f1185e04824dec.pdf> (accessed June 20, 2026).
11. World Economic Forum. (2025). *Four futures for the new economy: Geoeconomics and technology in 2030*. Geneva: World Economic Forum. Available at: https://reports.weforum.org/docs/WEF_Four_Futures_for_the_New_Economy_Geoeconomics_and_Technology_in_2030_2025.pdf (accessed June 12, 2026).

Nadiia Fisunenکو

Candidate of Economic Sciences,

Chair of the Department of Real Estate Development, Finance, Accounting, and Marketing,

Ukrainian State University of Science and Technology

ORCID: <https://orcid.org/0000-0003-3985-7813>

DIGITAL STRATEGIC NAVIGATION AS THE FOUNDATION FOR PROTECTING THE NATIONAL ECONOMY IN THE CONTEXT OF DIGITAL TRANSFORMATION

This article examines the theoretical foundations of digital strategic navigation of the economy as the basis for protecting the national economy in the context of digital transformation. It is argued that the growing digital dependence of the state, the proliferation of hybrid threats, cyberattacks, information pressure, and the vulnerability of critical infrastructure necessitate a transition from fragmented digitalization to a strategically coordinated model of digital governance. The concept of digital strategic navigation of the economy is clarified and defined as a continuous process of strategic orientation in the digital environment, aimed at ensuring economic security,

maintaining the continuity of the state's functioning, and adapting to dynamic challenges. The categories of digital transformation, navigation in the digital economy, and digital strategic navigation of the economy have been distinguished, which made it possible to specify the theoretical scope of the study and reveal the specifics of its application in the field of national economic security. The key aspects of implementing digital strategic navigation have been systematized, including institutional, infrastructural, security, analytical, technological, and managerial aspects. The role of the IT sector as a critical infrastructure foundation for the state's economic continuity has been identified; this sector ensures the functioning of digital platforms, public services, financial flows, management decisions, and interaction between the state, business, and citizens. The scientific novelty lies in the deepening of the theoretical approach to understanding digital strategic navigation as a component of the national economic security system. The practical significance of the results lies in their potential application to shaping digital policy, assessing vulnerabilities, protecting critical infrastructure, developing digital resilience tools, and strategic planning in the context of wartime and post-war challenges. It is concluded that digital resilience is a necessary condition for a state's economic continuity, adaptability, and security.

Keywords: digital transformation, digital strategic navigation, strategy, economic protection, economic resilience, national economy, IT sector, digital sovereignty.

Дата надходження статті: 15.07.2026

Дата прийняття статті: 04.08.2026

Дата публікації статті: 02.09.2026