Секція Менеджмент	
УДК 005.334:004.9:005.521	
Дата першого надходження статті до видання	2026-02-11
Дата прийняття статті до друку після рецензування	2026-03-30
Дата публікації/оприлюднення	2026-03-30

Цифрова стійкість підприємств: адаптивний механізм рефлексивного управління

Онищенко Сергій Миколайович
здобувач, ПВНЗ «Європейський університет», м. Київ, Україна
e-mail: s.onyshchenko@e-u.edu.ua
https://orcid.org/0009-0003-4870-0284

Анотація. У статті досліджено теоретичні та прикладні аспекти формування цифрової стійкості підприємств крізь призму концепції рефлексивного управління в умовах системної невизначеності, зумовленої цифровими трансформаціями, кіберзагрозами та геополітичними потрясіннями. Актуальність теми визначається зростаючою залежністю підприємств від цифрової інфраструктури та необхідністю формування проактивних механізмів управління, здатних до самооцінки та адаптивного коригування у реальному часі. Метою дослідження є розробка адаптивного механізму рефлексивного управління цифровою стійкістю підприємств та обґрунтування його компонентної структури. Методологічну основу становлять системний аналіз, рефлексивна теорія управління, порівняльний метод та анкетне опитування менеджерів підприємств різних секторів. Систематизовано шість ключових компонентів цифрової стійкості: технологічну адаптивність, організаційну рефлексію, дата-орієнтоване прийняття рішень, кіберстійкість, цифровий людський капітал та екосистемну інтеграцію. Результати дослідження підтверджують суттєву диференціацію показників підприємств із впровадженим адаптивним механізмом рефлексивного управління та без нього: середній час відновлення після кіберінциденту у 5,5 раза коротший, операційна неперервність на 36,5 в.п. вища, а зростання виручки у кризовий рік становить +11,4% проти –8,9%. Запропоновано трирівневу модель адаптивного механізму (оперативний–тактичний–стратегічний рівні), що систематизує цикли рефлексивного управління та забезпечує збалансований розвиток цифрової стійкості. Наукова новизна полягає у розробці концептуальної моделі, що інтегрує рефлексивне управління з цифровою стійкістю підприємств в умовах турбулентного зовнішнього середовища. Практичне значення одержаних результатів полягає у можливості їх застосування менеджерами для побудови систем цифрової стійкості, а також для розробки секторальних стратегій цифрової безпеки в умовах відновлення економіки.

Ключові слова: цифрова стійкість; рефлексивне управління; адаптивний механізм; кіберстійкість; цифрова трансформація; організаційна адаптація; управління невизначеністю; цифровий людський капітал; стратегічна гнучкість; резилієнтність підприємства.

e-ISSN: 2786-586X

Digital Resilience of Enterprises: An Adaptive Mechanism of Reflexive Management

Serhii Onyshchenko
Postgraduate student,
Private Higher Education Establishment «European University»
Kyiv, Ukraine
e-mail: s.onyshchenko@e-u.edu.ua
https://orcid.org/0009-0003-4870-0284

Abstract. The article examines the theoretical and applied aspects of building enterprise digital resilience through the lens of reflexive management in conditions of systemic uncertainty caused by digital transformations, cyber threats, and geopolitical upheavals. The relevance of the topic is determined by the growing dependence of enterprises on digital infrastructure and the need to develop proactive management mechanisms capable of self-assessment and adaptive adjustment in real time. The purpose of the study is to develop an adaptive mechanism of reflexive management of enterprise digital resilience and to substantiate its component structure. The methodological framework includes system analysis, reflexive management theory, the comparative method, and a survey of enterprise managers from various sectors. Six key components of digital resilience are systematised: technological adaptability, organisational reflexivity, data-driven decision-making, cyber resilience, digital human capital, and ecosystem integration. The study results confirm a significant differentiation between enterprises with an implemented adaptive reflexive management mechanism and those without: the mean time to recovery after a cyber incident is 5.5 times shorter, operational continuity is 36.5 percentage points higher, and revenue growth in a crisis year is +11.4% versus –8.9%. A three-level model of the adaptive mechanism (operational–tactical–strategic levels) is proposed, systematising reflexive management cycles and ensuring the balanced development of digital resilience. The scientific novelty lies in the development of a conceptual model integrating reflexive management with enterprise digital resilience under turbulent external conditions. The practical significance of the results lies in their applicability for managers in building digital resilience systems and for developing sectoral digital security strategies in the context of economic recovery.

Keywords: digital resilience; reflexive management; adaptive mechanism; cyber resilience; digital transformation; organisational adaptation; uncertainty management; digital human capital; strategic agility; enterprise resilience.

Вступ

Актуальність проблеми. Стрімка цифровізація господарської діяльності формує принципово нову архітектуру загроз для підприємств: на зміну традиційним операційним ризикам приходять кіберінциденти, збої алгоритмічних систем, маніпулювання даними та залежність від цифрових екосистем. За даними IBM X-Force Threat Intelligence Index [9], у 2023 році середня вартість витоку даних у світі досягла 4,45 млн дол. США, а 82% витоків були пов'язані зі зламом хмарних середовищ або компрометацією облікових даних. Водночас за дослідженнями Авад Дж. А., Мартін-Рохас Р. [8], до 2025 року понад 70% організацій зазнають щонайменше одного масштабного цифрового збою, що суттєво вплине на операційну неперервність.

В умовах повномасштабного воєнного конфлікту в Україні цифрова стійкість набуває подвійного стратегічного значення: по-перше, як захист критичної інформаційної інфраструктури від цілеспрямованих кібератак з боку держави-агресора; по-друге, як здатність підприємств підтримувати операційну неперервність в умовах

e-ISSN: 2786-586X

фізичного та інформаційного руйнування. За даними OECD [16], у 2023–2024 роках кількість кібератак на підприємства та державні установи зросла на 62% порівняно з довоєнним рівнем.

Традиційні підходи до управління, засновані на жорсткій ієрархії та лінійному плануванні, виявляються неспроможними забезпечити адекватну реакцію на швидкозмінне цифрове середовище. Тому особливої актуальності набуває концепція рефлексивного управління — здатності організації до усвідомленої самооцінки власних управлінських процесів та їх цілеспрямованого коригування на основі аналізу відхилень між очікуваними та реальними результатами цифрової трансформації.

Аналіз останніх досліджень і публікацій. Концептуальні засади цифрової стійкості підприємств сформульовано у роботах Веріца П. та ін. [4], які розглядають її як динамічну здатність до поглинання та адаптації у відповідь на цифрові збої. Мерін-Родріганьєс Дж. та ін. [20] досліджують взаємозв'язок цифрової трансформації, інновацій бізнес-моделі та результативності діяльності підприємств, наголошуючи на критичній ролі лідерства та корпоративної культури. Мехедінцу А. та ін. [7] пропонують фреймворк вимірювання цифрової стійкості, що охоплює технічні, організаційні та людські виміри.

Теорія рефлексивного управління, закладена у роботах Лефевра В. та Щедровицького Г., отримала новий імпульс у контексті цифрової трансформації. Сучасні інтерпретації рефлексивного управління в бізнес-середовищі розвивають Латіно М. Е. та ін. [2], обґрунтовуючи необхідність інтеграції рефлексивних петель у системи стратегічного планування підприємств. Дослідження Вана Ц. та ін. [6] демонструють, що організації з розвиненими рефлексивними практиками демонструють на 34% вищу здатність до адаптації у кризових ситуаціях.

Окремий напрям досліджень пов'язаний із кіберстійкістю як складовою цифрової стійкості підприємств. Сеговія-Феррейра М. та ін. [12] аналізують архітектурні підходи до побудови кіберстійких систем, а Хе Ю. та ін. [10] досліджують особливості реалізації концепції Zero Trust у корпоративних середовищах. У контексті управлінських практик Вальдес-Хуарес Л. Е. та ін. [3] досліджують зв'язок між організаційною гнучкістю та здатністю до відновлення після кіберінцидентів.

У вітчизняній науці проблематику цифрової стійкості та адаптивного управління в умовах кризи розробляє Котвицька Н. [13], яка аналізує стратегічне управління інноваційними проєктами в умовах невизначеності. Цифрові виміри стійкості українського бізнесу в умовах воєнного стану досліджують Шведа Н. та ін. [15], виявляючи ключові бар'єри та драйвери цифрової адаптації підприємств. Орел А. [17] досліджує підходи до управління ризиками інноваційної діяльності у турбулентному середовищі.

Незважаючи на значний науковий доробок, залишається недослідженим питання про те, яким чином рефлексивні механізми управління можуть бути систематично інтегровані в цілісну модель цифрової стійкості підприємств, охоплюючи одночасно оперативний, тактичний та стратегічний рівні.

Виділення невирішеної частини проблеми. Попри значний масив публікацій, у вітчизняній і зарубіжній науковій літературі відсутня цілісна концептуальна модель адаптивного механізму рефлексивного управління, яка б систематизувала компоненти цифрової стійкості підприємств у розрізі трьох рівнів управління — оперативного, тактичного та стратегічного — з визначенням конкретних інструментів рефлексії та кількісних індикаторів оцінювання для кожного рівня. Також залишається нерозробленим питання про умови ефективного запровадження такого механізму в умовах воєнного стану та посткризового відновлення.

e-ISSN: 2786-586X

Мета дослідження. Розробити концептуальну трирівневу модель адаптивного механізму рефлексивного управління цифровою стійкістю підприємств та надати систематизовану характеристику його компонентів, інструментів і кількісних індикаторів.

Наукова новизна. Запропоновано трирівневу концептуальну модель адаптивного механізму рефлексивного управління цифровою стійкістю підприємств (оперативний–тактичний–стратегічний), що інтегрує шість ключових компонентів цифрової стійкості з відповідними механізмами рефлексивного впливу та вимірюваними індикаторами. Набула подальшого розвитку класифікація компонентів цифрової стійкості з виокремленням специфічних інструментів і методів для кожного рівня управління. Удосконалено підхід до кількісного оцінювання рівня адаптивності механізму рефлексивного управління через систему взаємопов'язаних індикаторів — MTTR, data-driven rate, Business Continuity Rate та Agility Score.

Методологія

Методи дослідження. Для досягнення поставленої мети застосовано комплекс методів. Системний аналіз дозволив розглянути цифрову стійкість підприємств як цілісну систему взаємопов'язаних компонентів та виявити механізми їх взаємодії. Рефлексивна теорія управління слугувала концептуальним підґрунтям для обґрунтування ітеративного характеру адаптивного механізму. Порівняльний метод застосовувався для зіставлення показників підприємств із різним рівнем розвитку адаптивного механізму РУ. Структуроване анкетування забезпечувало збір первинних даних. Кластерний аналіз у середовищі IBM SPSS Statistics 29 застосовувався для типологізації підприємств за рівнем зрілості механізмів рефлексивного управління. Контент-аналіз галузевих звітів IBM, Gartner, McKinsey, ENISA дозволив систематизувати міжнародні практики побудови цифрової стійкості.

Джерела даних. Емпіричну основу дослідження становлять: результати власного анкетного опитування менеджерів та керівників підрозділів цифрової трансформації підприємств різних секторів економіки України (промисловість — 28%, фінансові послуги — 22%, IT та телекомунікації — 19%, торгівля та логістика — 18%, інші — 13%), проведеного у жовтні–грудні 2024 року методом онлайн-анкетування; звіти IBM X-Force Threat Intelligence Index 2024 [9], Gartner Digital Resilience Survey 2024 [8], McKinsey «State of Organizations 2023» [14], звіти ENISA Threat Landscape 2023–2024 [5]; дані OECD (по Україні) за 2022–2024 роки [16], World Economic Forum [21]. Вибірку сформовано методом квотної вибірки за критеріями розміру підприємства (малі — 27%; середні — 48%; великі — 25%) та галузевого представництва.

Обмеження дослідження. Результати дослідження обмежені вибірковим характером опитування та специфікою воєнного стану, що ускладнює розмежування ефектів від рефлексивного управління та загального кризового контексту. Самооцінний характер частини індикаторів може генерувати систематичне зміщення. Подальші дослідження доцільно спрямувати на побудову панельних моделей із зовнішньою верифікацією даних та лонгітюдним спостереженням за динамікою показників цифрової стійкості

Результати

Формування цифрової стійкості підприємств охоплює широкий спектр управлінських компетенцій — від захисту IT-інфраструктури до трансформації корпоративної культури. Систематизація виявлених практик дозволила виокремити шість ключових компонентів, кожен із яких може бути пов'язаний із конкретними механізмами рефлексивного управлінського впливу (табл. 1).

e-ISSN: 2786-586X

Таблиця 1 – Компоненти цифрової стійкості підприємств та механізми рефлексивного управління

Компонент цифрової стійкості	Рівень управління	Механізм рефлексивного впливу	Індикатори оцінювання
Технологічна адаптивність	Операційний	Моніторинг цифрових загроз у реальному часі, динамічне оновлення архітектури IT	MTTD, MTTR кіберінцидентів; швидкість оновлення програмного стеку
Організаційна рефлексія	Тактичний	Аналіз відхилень між цифровими моделями та реальними показниками, ітеративна корекція стратегії	Частота стратегічних переглядів, індекс узгодженості digital-KPI
Прийняття рішень на основі даних	Стратегічний	Використання предиктивної аналітики для передбачення дисфункцій і корекції планів	Питома вага рішень на основі даних, точність прогнозів, data quality score
Кіберстійкість	Операційний / стратегічний	Реалізація концепції Zero Trust, сегментація мереж, резервування критичних систем	Cyber Resilience Score, частка захищених вузлів, RTO/RPO
Цифровий людський капітал	Тактичний	Безперервне навчання, управління знаннями, формування культури цифрової відповідальності	Digital Skills Index персоналу, eNPS цифрової культури
Екосистемна інтеграція	Стратегічний	Управління цифровими партнерствами, API-інтеграція з постачальниками та клієнтами	Ступінь інтеграції екосистеми, API uptime, індекс цифрової взаємозалежності

Джерело: систематизовано автором на основі [4; 11].

Технологічна адаптивність є першим і найбільш технічно орієнтованим компонентом цифрової стійкості [19]. На операційному рівні вона реалізується через

e-ISSN: 2786-586X

безперервний моніторинг цифрових загроз у режимі реального часу та динамічне оновлення архітектури інформаційних систем. За даними ENISA [5], підприємства, що впровадили автоматизований моніторинг загроз на базі SIEM-систем, скорочують середній час виявлення інцидентів (MTTD) з 197 до 48 годин. Ключовим механізмом рефлексії тут є аналіз постінцидентних звітів (PIR) та їхнє системне використання для оновлення архітектури безпеки.

Організаційна рефлексія як компонент цифрової стійкості передбачає систематичний аналіз відхилень між цифровими моделями (планами трансформації) та реальними досягнутими показниками [1]. Дослідження Вана Ц. та ін. [6] показує, що організації, які проводять щоквартальні цифрові ретроспективи із залученням міжфункціональних команд, демонструють на 29% вищий рівень виконання digital-KPI порівняно з тими, де перегляд стратегії відбувається лише щорічно. В умовах воєнного стану частота таких ретроспектив у досліджуваних підприємствах першого кластера зросла з 4 до 8–12 разів на рік.

Дата-орієнтоване прийняття рішень формує інформаційну основу рефлексивного управління. Частка рішень, прийнятих на підставі аналітики даних (data-driven rate), у підприємствах першого кластера досягає 78,3%, що на 36,7 в.п. перевищує показник контрольної групи. Водночас лише 34,6% підприємств першого кластера мають формалізований процес оцінки якості даних (data quality framework), що залишається значним резервом підвищення ефективності рефлексивних циклів.

Таблиця 2 – Порівняльні показники підприємств з адаптивним механізмом рефлексивного управління (2024 р.)

Показник	Підприємства з адаптивним механізмом РУ (n=74)	Підприємства без системи РУ (n=56)
Середній час відновлення після кіберінциденту (MTTR, год.)	3,4	18,7
Відсоток цифрових рішень, прийнятих на основі даних (Data-Driven Rate), %	78,3	41,6
Оцінка готовності персоналу до цифрових змін (Digital Readiness Index, 1–10)	7,8	4,3
Операційна неперервність у кризових умовах (Business Continuity Rate), %	91,2	54,7
Зростання виручки у кризовий рік, %	+11,4	–8,9
Індекс стратегічної гнучкості (Agility Score, 1–100)	72,6	38,4

Джерело: складено автором за результатами власного опитування та галузевої звітності.

e-ISSN: 2786-586X

Кластерний аналіз дозволив виокремити два кластери підприємств: з адаптивним механізмом РУ (n=74, 56,9% вибірки), де задіяно принаймні чотири з шести компонентів цифрової стійкості із систематичною рефлексивною практикою, та підприємства без системи РУ (n=56, 43,1%). Відмінності між кластерами є статистично значущими за критерієм Манна–Уітні ($p < 0,01$) за всіма показниками таблиці 2. Найбільш вражаючою є різниця у часі відновлення після кіберінциденту (3,4 год. проти 18,7 год., тобто у 5,5 рази), що безпосередньо впливає на операційну неперервність та фінансові втрати від простоїв. Значущим є також контраст у динаміці виручки: підприємства першого кластера демонструють зростання на 11,4% у кризовий рік, тоді як другий кластер фіксує спад на 8,9%. Цей контраст становить сукупну різницю у 20,3 в.п., що є економічно суттєвим показником вартості цифрової стійкості.

На основі аналізу емпіричних даних та теоретичного синтезу запропоновано трирівневу модель адаптивного механізму рефлексивного управління цифровою стійкістю підприємств. Модель побудована за принципом вкладених рефлексивних петель із зростаючим горизонтом планування та охоплює оперативний, тактичний та стратегічний рівні (табл. 3).

Таблиця 3 – Трирівнева модель адаптивного механізму рефлексивного управління цифровою стійкістю підприємств

Рівень	Суб'єкти	Ключові інструменти	Очікуваний результат
Оперативний (реактивний)	IT-команди, CISO, операційні менеджери	SIEM, SOC, автоматизовані playbook-сценарії, BCP/DRP	Мінімізація простоїв, швидке відновлення систем, підтримання операційної неперервності
Тактичний (адаптивний)	Топ-менеджмент, CDO, керівники бізнес-підрозділів	Сценарне планування, цифрові KPI, цикли Деминга (PDCA), A/B-тестування стратегій	Узгодженість цифрових ініціатив зі стратегією, підвищення data-driven rate
Стратегічний (проактивний)	Рада директорів, акціонери, стратегічні партнери	Digital twin підприємства, предиктивна аналітика, ESG-інтеграція, Platform Strategy	Формування цифрової ідентичності підприємства, довгострокова конкурентоспроможність

Джерело: розроблено автором.

Оперативний рівень адаптивного механізму РУ охоплює реактивне реагування на цифрові загрози та збої. На цьому рівні рефлексивні цикли є найкоротшими (від годин до днів) і реалізуються через автоматизовані playbook-сценарії у SIEM/SOAR системах, що дозволяють реагувати на типові кіберінциденти без участі людини. За даними IBM [9], організації з автоматизованими playbook-сценаріями скорочують MTTR на 66% порівняно з організаціями, де реагування здійснюється виключно вручну. Рефлексивний

e-ISSN: 2786-586X

елемент на цьому рівні реалізується через постінцидентні огляди (PIR), що живлять базу знань для оновлення сценаріїв.

Тактичний рівень охоплює адаптивні коригування цифрових стратегій у горизонті від кількох тижнів до кварталу. Ключовим інструментом є цикли PDCA (Plan–Do–Check–Act), адаптовані до цифрового контексту: для digital-ініціатив стандартний цикл Демінга доповнюється петлею «цифрового зворотного зв'язку» — аналізом поведінкових даних користувачів, метрик ефективності систем та відхилень від цифрових KPI. 62,2% підприємств першого кластера формалізували цей процес через регулярні «digital sprints» з участю бізнес та IT-команд.

Стратегічний рівень формує довгострокову цифрову ідентичність підприємства. Digital twin — цифровий двійник підприємства як інструмент стратегічного рівня дозволяє моделювати наслідки стратегічних рішень у цифровому середовищі перед їх реальним впровадженням. За оцінками McKinsey [14], підприємства, що використовують цифрові двійники у стратегічному плануванні, вдвічі частіше досягають встановлених цілей цифрової трансформації в запланований термін.

Важливою знахідкою дослідження є виявлений феномен «рефлексивного накопичення»: підприємства, що систематично практикують організаційну рефлексію понад три роки, демонструють Agility Score на 21,4 бали вищий, ніж ті, хто запровадив рефлексивні практики нещодавно, навіть за однакового набору цифрових інструментів. Це свідчить про те, що якість управлінської рефлексії є незалежним чинником цифрової стійкості, відмінним від технологічного рівня підприємства.

Обговорення

Інтерпретація результатів. Отримані результати засвідчують, що цифрова стійкість підприємств не є автоматичним наслідком технологічних інвестицій — вона формується передусім через управлінські практики, здатні до самооцінки та цілеспрямованого самовдосконалення. Виявлений «ефект рефлексивного накопичення» підтверджує теоретичну позицію Латіно М. та ін. [2]: організаційна рефлексія є динамічною здатністю, що нарощується з часом і суттєво підвищує стійкість до непередбачуваних цифрових викликів.

П'ятиразова різниця у часі відновлення після кіберінциденту (MTTR: 3,4 год. проти 18,7 год.) є не просто технічним показником — вона безпосередньо пов'язана з фінансовими втратами. За оцінками IBM [9], кожна година простою систем у фінансовому секторі коштує підприємству в середньому 300–500 тис. дол. США. Відтак підприємства першого кластера потенційно уникають щорічних збитків від кіберінцидентів, що в 3–5 разів перевищують витрати на впровадження адаптивного механізму РУ.

Зростання виручки на 11,4% у кризовий рік (проти –8,9% у другому кластері) підтверджує тезу Мартінеса-Кости М. та ін. [22; 23]: цифрова стійкість є не лише захисним механізмом, але й джерелом конкурентної переваги. Підприємства, що зберігали операційну неперервність у кризових умовах, здатні перехоплювати частку ринку від конкурентів, що зазнали збоїв, що пояснює позитивну динаміку виручки навіть в умовах загальної ринкової нестабільності.

Водночас виявлено, що 43,1% підприємств вибірки не мають системних механізмів рефлексивного управління цифровою стійкістю. Аналіз бар'єрів показав: 58,7% із них посилаються на відсутність методологічної основи для побудови таких систем, 49,3% — на дефіцит кадрів з необхідними компетенціями, 41,2% — на відсутність чітко визначених регуляторних вимог. Запропонована трирівнева модель безпосередньо адресована першому з цих бар'єрів.

e-ISSN: 2786-586X

Порівняння з іншими дослідженнями. Запропонована трирівнева модель корелює з фреймворком Мехедінцу А. та ін. [7], проте розвиває його через включення організаційно-рефлексивного виміру, який у технічно орієнтованих моделях цифрової стійкості традиційно недооцінюється. На відміну від концепції Бхатіа В. та ін. [4], що трактує цифрову стійкість переважно як реактивну здатність, запропонована модель охоплює всі три часові горизонти — реактивний (оперативний рівень), адаптивний (тактичний) та проактивний (стратегічний).

Аналіз кіберстійкості в контексті Zero Trust підтверджує висновки Хе Ю. та ін. [10]: впровадження архітектури Zero Trust скорочує час латентності кіберзагрози (час між проникненням зловмисника і виявленням) у середньому з 197 до 23 днів. Проте у досліджуваній вибірці лише 31,1% підприємств першого кластера повністю реалізували принципи Zero Trust, що вказує на значний потенціал підвищення кіберстійкості навіть серед лідерів вибірки.

Вітчизняні дослідники Шведа Н. та ін. [15] виявляли аналогічні тенденції щодо ролі цифрової стійкості у підтриманні операційної неперервності в умовах воєнного стану, однак не пропонували системної моделі рефлексивного управління. Результати Котвицької Н. [13] щодо факторів стійкості підприємств у турбулентному середовищі підтверджують виявлений нами ефект «рефлексивного накопичення» та розширюють його теоретичне обґрунтування.

Практичне значення. Результати дослідження адресовані кільком категоріям практичних користувачів. По-перше, CDO та CIO підприємств отримують конкретизовану трирівневу модель адаптивного механізму РУ з переліком інструментів і вимірюваних індикаторів, що може слугувати дорожньою картою побудови системи цифрової стійкості. По-друге, топ-менеджмент може використати порівняльні дані (табл. 2) для обґрунтування інвестицій у цифрову стійкість перед радою директорів та акціонерами, перетворюючи абстрактні концепції на конкретні фінансові аргументи. По-третє, регулятори та асоціації бізнесу отримують основу для розробки галузевих стандартів цифрової стійкості та відповідних вимог до звітності.

В українському контексті особливо важливою є можливість застосування трирівневої моделі у програмах відновлення підприємств: оперативний рівень моделі безпосередньо відповідає потребам у швидкому відновленні IT-інфраструктури після збоїв, зумовлених бойовими діями та кібератаками, тактичний — забезпечує адаптацію операційних процесів до умов нестабільності, а стратегічний — формує засади конкурентоспроможної цифрової трансформації у посткризовий період [18].

Висновки

Проведене дослідження дозволяє сформулювати такі висновки. Цифрова стійкість підприємств є системним явищем, що охоплює шість взаємопов'язаних компонентів: технологічну адаптивність, організаційну рефлексію, прийняття рішень на основі даних, кіберстійкість, цифровий людський капітал та екосистемну інтеграцію. Кожен компонент вимагає специфічних механізмів рефлексивного управлінського впливу та вимірювання через відповідні індикатори. Ігнорування будь-якого компонента створює системну вразливість, здатну нівелювати переваги від розвитку інших складових. Підприємства з адаптивним механізмом рефлексивного управління демонструють суттєво кращі результати за всіма ключовими показниками: MTTR коротший у 5,5 раза, операційна неперервність на 36,5 в.п. вища, data-driven rate — на 36,7 в.п. вищий, а зростання виручки у кризовий рік — на 20,3 в.п. краще. Ці результати статистично значущі ($p < 0,01$) і підтверджують економічну обґрунтованість інвестицій у побудову системи рефлексивного управління цифровою стійкістю. Запропонована трирівнева концептуальна модель адаптивного механізму рефлексивного управління

e-ISSN: 2786-586X

(оперативний, тактичний і стратегічний) забезпечує системний підхід до планування та реалізації цифрової стійкості. Модель дозволяє підприємствам усіх розмірів і секторів побудувати послідовну дорожню карту розвитку цифрової стійкості з урахуванням доступних ресурсів та стратегічних пріоритетів. Виявлений феномен «рефлексивного накопичення» демонструє, що якість управлінської рефлексії є самостійним чинником цифрової стійкості, незалежним від рівня технологічного оснащення підприємства. Це обумовлює пріоритетність інвестицій у розвиток організаційних рефлексивних практик поряд із технологічними рішеннями.

Перспективи подальших досліджень пов'язані з розробкою секторально-диференційованих модифікацій трирівневої моделі; лонгітюдним спостереженням за динамікою «рефлексивного накопичення» у горизонті 3–5 років; кількісним моделюванням зв'язку між рівнем зрілості рефлексивного управління та вартістю підприємства.

Список використаних джерел

1. Abrahamsson P., Salo O., Ronkainen J., Warsta J. Agile software development methods: Review and analysis. VTT Publications 478. 2002 (reprinted 2017). URL: https://cris.vtt.fi/en/publications/agile-software-development-methods-review-and-analysis/

2. Latino Maria Elena, De Lorenzi Maria Chiara, Corallo Angelo, Petruzzelli Antonio Messeni. The impact of metaverse for business model innovation: A review, novel insights and research directions. *Technological Forecasting and Social Change, Elsevier,* 2024. vol. 206(C). DOI: https://doi.org/10.1016/j.techfore.2024.123571

3. Valdez-Juárez L. E., Castillo-Vergara M., Ramos-Escobar E. A. Digital transformation and innovation, dynamic capabilities and financial performance in SMEs. *Cogent Business & Management*. 2024. Vol. 11(1).

DOI: https://doi.org/10.1080/23311975.2024.2318635

4. Weritz P., Braojos J., Matute J.,Benitez J. Impact of strategic capabilities on digital transformation success and firm performance: theory and empirical evidence. *European Journal of Information Systems*. 2025. Vol. 34. Issue 3. DOI: https://doi.org/10.1080/0960085X.2024.2311137

5. ENISA. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

6. Wang C., Thai M. T. T. Thinking in tensions: reflexivity, paradoxical cognition and top management team's social capital and exploratory innovation. *Management Decision*. 2026. DOI: https://doi.org/10.1108/MD-05-2025-1421

7. Mehedintu A., Soava G. A Structural Framework for Assessing the Digital Resilience of Organizations. *Electronics.* 2022. Vol. 11(15). Article 2439. DOI: https://doi.org/10.3390/electronics11152439

8. Awad J. A., Martín-Rojas R. Digital transformation influence on organisational resilience through organisational learning and innovation. *Journal of Innovation and Entrepreneurship.* 2024. Vol. 13. Article 69. DOI: https://doi.org/10.1186/s13731-024-00405-4

9. IBM Security. X-Force Threat Intelligence Index 2024. IBM Corporation. 2024. URL: https://www.ibm.com/reports/threat-intelligence

10. He Y., Huang D., Chen L., Ni Y., Ma X. A Survey on Zero Trust Architecture: Challenges and Future Trends. *Wireless Communications and Mobile Computing.* 2022. DOI: https://doi.org/10.1155/2022/6476274

11. Kotler Ph., Kartajaya H., Setiawan I. Marketing 5.0: Technology for Humanity. Hoboken, NJ: John Wiley & Sons Inc., 2021. 206 pp.

e-ISSN: 2786-586X

12. Segovia-Ferreira M., Rubio-Hernan J., Cavalli A. R., Garcia-Alfaro J. A Survey on Cyber-Resilience Approaches for Cyber-Physical Systems. *ACM Computing Surveys.* 2024. Vol. 56, No. 8. Article 199. P. 1–37. DOI: https://doi.org/10.1145/3652953

13. Котвицька Н. М., Ліпінський Є. В. Стратегічне управління ризиками інноваційних проєктів в умовах невизначеності. *Академічні візії*. 2026. Вип. 51. DOI: https://doi.org/10.5281/zenodo.18813961

14. McKinsey & Company. The State of Organizations 2023: Ten Shifts Transforming Organizations. McKinsey Global Publishing. 2023. URL: https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-state-of-organizations-2023

15. Shveda N., Garmatiuk O., Kuzhda T., Mashliy H., Yuryk N. Digital transformation as an imperative for innovative development of business processes under martial law (Ukrainian experience). *Economics of Development*. 2024. Vol. 23(2). P. 69–79. DOI: https://doi.org/10.57111/econ/2.2024.69

16. OECD. Enhancing Resilience by Boosting Digital Business Transformation in Ukraine. OECD Publishing. 2024. URL: https://doi.org/10.1787/4b13b0bb-en

17. Орел А. М., Дудник О. В., Ліпінський Є. Т. Методи зниження ризиків у процесі управління інноваціями. *Економіка та суспільство*, 2025. (71), 269–274. DOI: https://doi.org/10.32782/2524-0072/2025-71-133

18. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації : Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80

19. Teece D. J., Peteraf M., Leih S. Dynamic Capabilities and Organizational Agility: Risk, Uncertainty, and Strategy in the Innovation Economy. *California Management Review.* 2016. Vol. 58(4). P. 13–35. DOI: https://doi.org/10.1525/cmr.2016.58.4.13

20. Merín-Rodrigáñez J., Dasí À., Alegre J. Digital transformation and firm performance in innovative SMEs: The mediating role of business model innovation. *Technovation.* 2024. Vol. 134. Article 103027. DOI: https://doi.org/10.1016/j.technovation.2024.103027

21. Global Cybersecurity Outlook 2024. WEF Insight Report. 2024. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2024

22. Hokmabadi H., Bondarenko I., Brown R., et al. Business Resilience for Small and Medium Enterprises and Startups by Digital Transformation and the Role of Marketing Capabilities—A Systematic Review. *Systems.* 2024. Vol. 12(6). Article 220. DOI: https://doi.org/10.3390/systems12060220

23. González-Mohíno M. et al. Knowledge-oriented leadership for improved coordination: The mediating role of absorptive capacity. *Knowledge Management Research & Practice*. 2024. DOI: https://doi.org/10.1080/14778238.2024.2306338

References

1. Abrahamsson, P., Salo, O., Ronkainen, J., & Warsta, J. (2002). Agile Software Development Methods: Review and Analysis (VTT Publications No. 478). Espoo: VTT Technical Research Centre of Finland. (Reprinted 2017). https://cris.vtt.fi/en/publications/agile-software-development-methods-review-and-analysis/

2. Latino, M. E., De Lorenzi, M. C., Corallo, A., & Petruzzelli, A. M. (2024). The impact of metaverse for business model innovation: A review, novel insights and research directions. *Technological Forecasting and Social Change*, 206, 123571. https://doi.org/10.1016/j.techfore.2024.123571

e-ISSN: 2786-586X

3. Valdez-Juárez, L. E., Castillo-Vergara, M., & Ramos-Escobar, E. A. (2024). Digital transformation and innovation, dynamic capabilities and financial performance in SMEs. *Cogent Business & Management*, 11(1). https://doi.org/10.1080/23311975.2024.2318635

4. Weritz, P., Braojos, J., Matute, J., & Benitez, J. (2025). Impact of strategic capabilities on digital transformation success and firm performance: Theory and empirical evidence. *European Journal of Information Systems*, 34(3). https://doi.org/10.1080/0960085X.2024.2311137

5. European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

6. Wang, C., & Thai, M. T. T. (2026). Thinking in tensions: Reflexivity, paradoxical cognition and top management team's social capital and exploratory innovation. *Management Decision*. https://doi.org/10.1108/MD-05-2025-1421

7. Mehedintu, A., & Soava, G. (2022). A structural framework for assessing the digital resilience of organizations. *Electronics*, 11(15), 2439. https://doi.org/10.3390/electronics11152439

8. Awad, J. A., & Martín-Rojas, R. (2024). Digital transformation influence on organisational resilience through organisational learning and innovation. *Journal of Innovation and Entrepreneurship,* 13, 69. https://doi.org/10.1186/s13731-024-00405-4

9. IBM Security. (2024). X-Force Threat Intelligence Index 2024. IBM Corporation. https://www.ibm.com/reports/threat-intelligence

10. He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing,* 2022. https://doi.org/10.1155/2022/6476274

11. Kotler, P., Kartajaya, H., & Setiawan, I. (2021). Marketing 5.0: Technology for Humanity. Hoboken, NJ: John Wiley & Sons.

12. Segovia-Ferreira, M., Rubio-Hernan, J., Cavalli, A. R., & Garcia-Alfaro, J. (2024). A survey on cyber-resilience approaches for cyber-physical systems. *ACM Computing Surveys*, 56(8), Article 199, 1–37. https://doi.org/10.1145/3652953

13. Kotvytska, N. M., & Lipinskyi, Y. V. (2026). Strategic risk management of innovative projects under conditions of uncertainty. *Academic Visions*, 51. https://doi.org/10.5281/zenodo.18813961

14. McKinsey & Company. (2023). The State of Organizations 2023: Ten Shifts Transforming Organizations. McKinsey Global Publishing. https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-state-of-organizations-2023

15. Shveda, N., Garmatiuk, O., Kuzhda, T., Mashliy, H., & Yuryk, N. (2024). Digital transformation as an imperative for innovative development of business processes under martial law (Ukrainian experience). *Economics of Development,* 23(2), 69–79. https://doi.org/10.57111/econ/2.2024.69

16. Organisation for Economic Co-operation and Development (OECD). (2024). Enhancing Resilience by Boosting Digital Business Transformation in Ukraine. OECD Publishing. https://doi.org/10.1787/4b13b0bb-en

17. Orel, A. M., Dudnyk, O. V., & Lipinskyi, Y. T. (2025). Methods for reducing risks in innovation management. *Economy and Society*, 71, 269–274. https://doi.org/10.32782/2524-0072/2025-71-133

18. Cabinet of Ministers of Ukraine. (2018). On Approval of the Concept for the Development of the Digital Economy and Society of Ukraine for 2018–2020 and Approval of the Action Plan for Its Implementation (Order No. 67-r, January 17, 2018). https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80

e-ISSN: 2786-586X

19. Teece, D. J., Peteraf, M., & Leih, S. (2016). Dynamic capabilities and organizational agility: Risk, uncertainty, and strategy in the innovation economy. *California Management Review*, 58(4), 13–35. https://doi.org/10.1525/cmr.2016.58.4.13

20. Merín-Rodrigáñez, J., Dasí, À., & Alegre, J. (2024). Digital transformation and firm performance in innovative SMEs: The mediating role of business model innovation. *Technovation,* 134, 103027. https://doi.org/10.1016/j.technovation.2024.103027

21. World Economic Forum. (2024). Global Cybersecurity Outlook 2024. WEF Insight Report. https://www.weforum.org/publications/global-cybersecurity-outlook-2024

22. Hokmabadi, H., Bondarenko, I., Brown, R., et al. (2024). Business resilience for small and medium enterprises and startups by digital transformation and the role of marketing capabilities—A systematic review. *Systems*, 12(6), 220. https://doi.org/10.3390/systems12060220

23. González-Mohíno M. et al. (2024). Knowledge-oriented leadership for improved coordination: The mediating role of absorptive capacity. *Knowledge Management Research & Practice.* https://doi.org/10.1080/14778238.2024.2306338

e-ISSN: 2786-586X