

Ukraini" [Challenges of Reforming the Healthcare System in Modern Ukraine]. *Transformatsiia ukrain-skoho suspilstva v tsyfrovu eru*. 2023. <https://dspace.onua.edu.ua/server/api/core/bitstreams/f6614de1-d2a4-4ace-8070-8379e83d2253/content>

Wang, F., and Preininger, A. "AI in Health: State of the Art, Challenges, and Future Directions". Yearbook of

Medical Informatics, vol. 28, no. 1 (2019): 16-26. DOI: <https://doi.org/10.1055/s-0039-1677908>

**Науковий керівник – Сергієнко О. А.**, доктор економічних наук, професор, професор кафедри підприємництва, торгівлі і логістики НТУ «ХПІ» (Харків)

УДК 005.93: 334.72:005.21(477)

JEL: D83; L21; M15; O33

DOI: <https://doi.org/10.32983/2222-4459-2025-7-89-98>

## ТЕНДЕНЦІЇ ІНФОРМАТИЗАЦІЇ В ДІЯЛЬНОСТІ СУЧАСНИХ КОРПОРАЦІЙ В УКРАЇНІ: АНАЛІЗ ПІДХОДІВ ТА ПРИЙНЯТТЯ РІШЕНЬ

©2025 СЕМЕНЧА І. Є.

УДК 005.93: 334.72:005.21(477)

JEL: D83; L21; M15; O33

### Семенча І. Є. Тенденції інформатизації в діяльності сучасних корпорацій в Україні: аналіз підходів та прийняття рішень

Метою статті є дослідження сучасних підходів до інформатизації корпоративного управління в умовах цифрової трансформації економіки України та розроблення індексу цифрової управлінської стійкості (ІЦУС) як аналітичного інструменту оцінювання здатності корпорацій підтримувати стабільність і ефективність управлінських процесів в умовах постійних викликів. У статті за допомогою методів порівняльного аналізу, структурно-логічного моделювання, експертного оцінювання та індексного підходу проведено систематизацію основних цифрових чинників, які визначають управлінську спроможність великих корпоративних структур до функціонування в умовах економічної турбулентності. Обґрунтована актуальність дослідження з огляду на виклики, що постали перед українським бізнесом у зв'язку з війною, цифровою нерівністю, розривом технологічного циклу та потребою в підвищенні операційної стійкості. У результаті роботи запропоновано авторську концепцію цифрової управлінської стійкості корпорації, що включає шість взаємопов'язаних блоків: загальна цифрова інфраструктура, корпоративна система збору й аналітики даних, цифрова гнучкість, цифрова компетентність персоналу, інформаційні системи підтримки рішень та інформаційна безпека. Запропоновано методику кількісного оцінювання кожного блоку та комплексної оцінки ІЦУС з формалізованими шкалами, ваговими коефіцієнтами та процедурою інтерпретації результатів. Доведено наукову та прикладну значущість методики для впровадження практик цифрового менеджменту, аудиту інформаційної архітектури та стратегічного планування розвитку корпорацій в Україні. На відміну від загальних моделей цифрової трансформації, які орієнтовані переважно на загальнодержавні або міжгалузеві порівняння, ІЦУС дозволяє здійснювати внутрішньокорпоративний аудит цифрової інфраструктури саме з позиції управлінської стабільності. Упровадження цієї методики забезпечить керівництво корпорацій аналітичним інструментом для виявлення вразливих зон у цифровій архітектурі управління, оптимізації інвестицій у інформаційно-комунікаційні технології, планування цифрових реформ із урахуванням специфіки великої корпоративної структури. Таким чином, ІЦУС може бути використаний як у стратегічному плануванні, так і в щорічному моніторингу ефективності цифрового управління, що значно підвищує адаптивність і конкурентоспроможність корпорації в умовах турбулентного середовища.

**Ключові слова:** обґрунтування вибору, фактори, інформаційно-комунікаційні технології, персонал, готовність до змін, корпоративний менеджмент, методи управління, управлінська стійкість.

**Табл.:** 9. **Формул.:** 1. **Бібл.:** 16.

**Семенча Ілона Євгенівна** – доктор економічних наук, професор, професор кафедри економіки, підприємництва та управління підприємствами, Дніпровський національний університет імені Олеся Гончара (просп. Науки, 72, Дніпро, 49010, Україна)

**E-mail:** [semilon@ua.fm](mailto:semilon@ua.fm)

**ORCID:** <https://orcid.org/0000-0002-8736-3992>

**Researcher ID:** <https://www.webofscience.com/wos/author/record/S-4143-2017>

**Scopus Author ID:** <https://www.scopus.com/authid/detail.uri?authorid=57209535827>

UDC 005.93: 334.72:005.21(477)

JEL: D83; L21; M15; O33

### Semencha I. Ye. Trends in Informatization in the Activities of Modern Corporations in Ukraine: Analyzing the Approaches and Decision-Making

The aim of the article is to study contemporary approaches to the informatization of corporate governance in the context of the digital transformation of Ukraine's economy and to develop a Digital Managerial Resilience Index (DMRI) as an analytical tool for assessing the ability of corporations to maintain stability and efficiency in managerial processes amidst constant challenges. The article uses methods of comparative analysis, structural-logical modeling, expert evaluation, and an index approach to systematize the main digital factors that determine the managerial capability of large corporate structures to function in conditions of economic turbulence. The relevance of the research is substantiated in light of the challenges facing Ukrainian businesses due to the ongoing war, digital inequality, technological cycle disruption, and the need to enhance operational resilience. As a result of the study, an author's conception of digital managerial resilience for corporations has been proposed, which includes six interconnected blocks: overall digital infrastructure, corporate data collection and analytics system, digital flexibility, digital competence of staff, decision support information systems, and information security. A methodology for the

quantitative assessment of each block and a comprehensive assessment of digital managerial resilience has been proposed, with formalized scales, weighting coefficients, and a procedure for interpreting the results. The scientific and practical significance of the methodology for implementing digital management practices, auditing information architecture, and strategic planning for the development of corporations in Ukraine has been established. Unlike general models of digital transformation that primarily focus on national or inter-industry comparisons, digital managerial resilience enables internal corporate auditing of the digital infrastructure from the perspective of managerial stability. The implementation of this methodology will provide corporate leaders with an analytical tool to identify vulnerable areas in the digital management architecture, optimize investments in information and communication technologies, and plan digital reforms considering the specifics of large corporate structures. Thus, DMRI can be used both in strategic planning and in the annual monitoring of the efficiency of digital management, significantly enhancing the adaptability and competitiveness of the corporation in a turbulent environment.

**Keywords:** substantiation of choice, factors, information and communication technologies, staff, readiness for change, corporate management, management methods, managerial resilience.

**Tabl.:** 9. **Formulae:** 1. **Bibl.:** 16.

**Semencha Ilona Ye.** – Doctor of Sciences (Economics), Professor, Professor of the Department of Economics, Entrepreneurship and Enterprise Management, Oles Honchar Dnipro National University (72 Nauky Ave., Dnipro, 49010, Ukraine)

**E-mail:** semilon@ua.fm

**ORCID:** <https://orcid.org/0000-0002-8736-3992>

**Researcher ID:** <https://www.webofscience.com/wos/author/record/S-4143-2017>

**Scopus Author ID:** <https://www.scopus.com/authid/detail.uri?authorId=57209535827>

У сучасних умовах ведення бізнесу інформатизація перетворилася на системоутворювальний чинник функціонування та розвитку корпорацій. Особливої ваги ця тенденція набуває для українських компаній, які діють в умовах високої стратегічної невизначеності, військової загрози, порушеної логістики, зниженого попиту та обмеженого доступу до ресурсів. З огляду на ці обставини, саме цифрова трансформація та впровадження інструментів інформатизації розглядаються як ключові напрями збереження операційної стійкості, конкурентоспроможності та здатності до стратегічної адаптації.

Аналіз світових і вітчизняних практик свідчить, що корпорації, які своєчасно інтегрують інформаційно-аналітичні платформи, системи підтримки управлінських рішень, CRM, ERP і BI-технології, демонструють вищу здатність до швидкої перебудови внутрішніх процесів, зниження транзакційних витрат, персоналізації клієнтського досвіду та формування відкритих інноваційних моделей. Водночас в Україні системна інформатизація корпоративного управління все ще відстає за низкою ключових параметрів – від відсутності єдиної цифрової стратегії до недостатньої синергії між IT-підрозділами та менеджментом.

Відсутність належного наукового супроводу процесів інформатизації, а також фрагментарність наявних підходів до аналізу цифрових стратегій корпорацій вимагає комплексного теоретико-методологічного переосмислення даного питання. Потреба в нових дослідженнях зумовлена також швидкими темпами еволюції комп'ютерних технологій, необхідністю адаптації до міжнародних стандартів цифрового управління, інтеграцією українського бізнесу в європейські цифрові ринки та переходом до нових форматів прийняття рішень

на основі великих даних, штучного інтелекту та автоматизованої аналітики.

У цьому контексті актуальним є виявлення та систематизація сучасних тенденцій інформатизації в корпоративному секторі України, аналіз провідних підходів до її впровадження, а також визначення ролі інформатизації в трансформації системи прийняття стратегічних, тактичних та оперативних рішень на рівні корпорацій.

Сучасна наукова думка визнає інформатизацію як критичний фактор організаційної еволюції корпорацій у нестабільному та складному середовищі. У зарубіжній літературі цю проблематику розкривають у широкому міждисциплінарному контексті. Так, відома базова праця Е. Brynjolfsson, А. McAfee [1], в якій покладено основи інформатизації бізнес-структур, де автори підкреслюють, що корпорації, які впроваджують алгоритми прийняття рішень, побудовані на аналітиці великих даних, виявляють вищу адаптивність до цифрових викликів. Наголос робиться не лише на впровадженні IT, а на стратегічній реконфігурації управлінських практик.

Сучасні трансформаційні моделі, як-от Business Model Transformation 4.0, яка, наприклад, розглянута у [2], або концепція «антикрихких» організацій [3], набувають значущості як концептуальні платформи для інтеграції цифрових технологій у бізнес-рішення. Вагоме місце займають дослідження гнучких підходів до цифрової архітектури [4], які пропонують інструменти та фреймворки для переосмислення ролі даних у стратегічному управлінні.

На українському академічному горизонті цифрова трансформація корпоративного сектора розглядається дуже широко, але переважно у зв'язку із загальними тенденціями часу та викликами,

з якими стикаються підприємства в Україні. Наприклад, у дослідженнях: М. Мащенко та Є. Іпполітов, О. Нога, В. Титаренко, В. Зянка та Т. Нечипоренко [5–8]. У праці Н. Домбровської та В. Фаріон [9] розглянуто вплив інноваційних технологій на адаптацію управлінських функцій. Н. Євтушенко та Д. Стеценко [10] акцентують увагу на необхідності переосмислення підходів до ризик-менеджменту в цифровому середовищі. М. Гвоздь із колегами [11] досліджують можливості використання гнучких методологій типу Agile для покращення керованості в умовах динамічного середовища.

Втім, попри зростання наукового інтересу до теми, все ще бракує емпірично обґрунтованих інструментів оцінки рівня інформатизації вітчизняних корпорацій. Обмежено представлені адаптивні моделі впровадження цифрових рішень із урахуванням галузевої специфіки, ресурсного потенціалу та технологічної зрілості компаній, а питання управління корпораціями в епоху цифровізації економіки взагалі майже не розглядається. Також відсутня чітка класифікація цифрових підходів, релевантна для управлінських задач в умовах українського післякризового бізнес-середовища.

*Метою* статті є обґрунтування теоретико-методологічних засад і розробка прикладного підходу до вимірювання цифрової управлінської стійкості сучасних корпорацій в Україні шляхом побудови комплексного індексу, який враховує специфіку функціонування корпоративних структур в умовах кризової економіки та цифрової трансформації.

*Методологія* даного дослідження базується на міждисциплінарному підході, що інтегрує концепції корпоративного менеджменту, цифрової трансформації та управлінської стійкості. У ході дослідження було застосовано поєднання якісних і кількісних методів, зокрема: структурно-логічний аналіз – для побудови концептуальної моделі цифрової управлінської стійкості корпорації; метод експертних оцінок – для визначення релевантних складових Індексу цифрової управлінської стійкості; аналітичне групування – для систематизації показників у межах кожного блоку; нормалізація даних і побудова інтегрального індексу з використанням адитивної агрегатної моделі.

Історія розвитку економічної діяльності у 21 ст. засвідчує непоодинокі випадки, коли великі корпорації зазнавали суттєвих збитків через прогалини в управлінні цифровими технологіями. У 2008–2013 рр. «BBC» намагалася автоматизувати архівування відео, проте проект DMI (*Digital Media Initiative*) провалився, що спричинило втрату близько £100 млн і £27 млн судового врегулювання із «Siemens». PwC виявила слабкий менедж-

мент змін і відсутність цифрового контролю за проектом [12]. Після некоректного оновлення програмного забезпечення компанія «Delta Air Lines» у липні 2024 р. втратила близько \$500 млн загального доходу через масові скасування рейсів, компенсації та логістичні витрати [13]. Хакерська атака у 2017 р. у програмі М.Е.Дос спричинила хвилю зараження вже українських підприємств вірусом Petya. Унаслідок цього багато компаній були змушені фактично переконфігурувати всі комп'ютери та сервери, замінити обладнання, відновлювати дані – витрати складали десятки мільйонів гривень, бо цілі регіони залишалися без обліку, логістики, звітності [14; 15]. Відома також кібер-атака на «Київстар» у грудні 2023 р., яка вивела з ладу ядро мережі оператора [16]. Подекуди без зв'язку залишилися 24 млн абонентів. Загальні прямі та вторинні втрати компанія оцінила у \$100 млн, інфраструктурні та репутаційні наслідки серйозно підірвали довіру клієнтів і партнерів.

Отже, ці приклади чітко демонструють: інвестування в цифрову стійкість – це не опція, а необхідність, інакше ймовірність масштабних збитків дуже висока.

Крім запобігання ризикам, у період війни та перебудови ринкових зв'язків цифрова стійкість корпорацій визначає їхню здатність забезпечити безперервність управління, координацію бізнес-одиниць та оперативне ухвалення рішень. Крім того, такий підхід сприяє зниженню внутрішніх, управлінських ризиків, пов'язаних з розривами в комунікаціях, кіберзагрозами, людським фактором і неузгодженістю ІТ-систем, які є типовими для великих корпоративних структур в Україні. Корпорації, які мають чітко визначений рівень цифрової управлінської стійкості, зможуть ефективніше взаємодіяти з міжнародними партнерами, залучати інвесторів, проходити аудит, брати участь у міжнародних програмах відбудови. Для держави – це можливість моніторингу цифрового потенціалу ключових корпоративних гравців, формування політик розвитку галузей і стимулювання цифрових інвестицій на макрорівні.

Таким чином, вважаємо необхідним визначити поняття «цифрова управлінська стійкість корпорації» та розробити методологічну основу для її забезпечення в українських реаліях.

Отже, пропонуємо під *цифровою управлінською стійкістю корпорації* розуміти здатність корпоративної системи забезпечувати безперервність, адаптивність і результативність управлінських рішень в умовах внутрішніх і зовнішніх викликів шляхом інтегрального використання цифрових технологій, систем підтримки прийняття

рішень, даних і цифрових компетентностей персоналу в стратегічному управлінні корпорацією.

Слід зазначити, що поняття «цифрова управлінська стійкість корпорації» (ЦУСК) суттєво відрізняється від суміжних понять (табл. 1).

Таблиця 1

Порівняння змісту поняття ЦУСК і суміжних понять

| Суміжні поняття         | Змістовна різниця                                                          |
|-------------------------|----------------------------------------------------------------------------|
| Цифрова трансформація   | Це процес, а ЦУСК – характеристика результату трансформації                |
| Інформатизація          | Стосується лише впровадження ІТ, а ЦУСК – також про управлінські механізми |
| Кіберстійкість          | Зосереджена на захисті, а ЦУСК – на прийнятті ефективних рішень            |
| ІТ-стійкість            | Зосереджена лише на технологічній інфраструктурі                           |
| Антикрихіткість бізнесу | Більш загальна категорія, не фокусується на управлінських процесах         |

Джерело: розроблено автором.

Визначення цифрової управлінської стійкості корпорації базується на оцінюванні Індексу цифрової управлінської стійкості (ІЦУС).

ІЦУС – це інтегральний показник, що відображає рівень здатності корпорації забезпечувати ефективне цифрове управління, адаптивність і безперервність діяльності на основі цифрових рішень у динамічному середовищі.

ІЦУС складається з 6 блоків (компонентів):

**Б1.** Загальна цифрова інфраструктура діяльності корпорації.

**Б2.** Корпоративна система збору, обробки та аналітики даних.

**Б3.** Цифрова гнучкість корпорації.

**Б4.** Цифрова компетентність персоналу.

**Б5.** Цифрові системи підтримки управлінських рішень.

**Б6.** Інформаційна корпоративна безпека та операційна стабільність.

Методика оцінювання ІЦУС корпорації передбачає системний, кількісний і якісний підходи до вимірювання цифрової стійкості з урахуванням масштабів, складності та багаторівневої структури корпоративного управління.

У методику закладено принципи *системності* (оцінюється не лише наявність, але й інтеграція компонентів ІЦУС), *ієрархічності* (кожен блок ІЦУС поділено на підкритерії), *принципу оцінки на основі доказів* (проведення аудитів, аналіз звітів, цифрових метрик), *гнучкості* (можливість адаптувати шкали оцінювання до типу корпорації),

*суб'єктності* (оцінювання здійснюється як внутрішніми, так і зовнішніми аудиторамі).

Загальний розрахунок ІЦУС проводиться за формулою:

$$ІЦУС = \sum_{i=1}^6 W_i \times S_i, \quad (1)$$

де  $W_i$  – ваговий коефіцієнт  $i$ -го блоку (розподіляється залежно від стратегії компанії);

$S_i$  – оцінка за бальною шкалою для  $i$ -го блоку (1–5).

Рекомендовані ваги ( $W_i$ ) для кожного блоку ІЦУС: **Б1:** 0,20; **Б2:** 0,15; **Б3:** 0,15; **Б4:** 0,15; **Б5:** 0,15; **Б6:** 0,20.

Оцінка ( $S_i$ ) по кожного блоку від 1 до 5 балів (табл. 2).

Таблиця 2

Шкала оцінювання загального ІЦУС

| Оцінка, бал | Пояснення                                                                           |
|-------------|-------------------------------------------------------------------------------------|
| 5           | Високий рівень розвитку (інтеграція, автоматизація, відповідність кращим практикам) |
| 4           | Добрий рівень (є вбудовані рішення, часткова інтеграція, автоматизовані функції)    |
| 3           | Середній рівень (роз'єднані рішення, обмежене охоплення)                            |
| 2           | Низький рівень (локальні рішення, слабка координація)                               |
| 1           | Дуже низький рівень або відсутність рішення                                         |

Джерело: розроблено автором.

Для забезпечення можливостей порівняння показників ІЦУС різних корпорацій або різних періодів, для визначення стану ЦУСК пропонуються такі рівні цифрової управлінської стійкості (табл. 3).

Далі коротко розглянемо зміст і методику оцінювання блоків ІЦУС.

**Б1. Загальна цифрова інфраструктура діяльності корпорації.** Оцінюється сукупність інтегрованих цифрових платформ і технологічних рішень, які забезпечують наскрізне управління ключовими ресурсами та процесами.

До елементів, що підлягають оцінюванню в Б1, входять: *загальна ERP-платформа корпорації* (єдиний контур для управління фінансами, виробництвом, персоналом, логістикою); *CRM-системи корпоративного рівня* (управління взаємовідносинами з клієнтами на основі даних усіх бізнес-одиниць); *BI-рішення* (Business Intelligence – системи візуалізації, звітності, дашбордів); *SCM* (Supply Chain Management – цифрова логістика та управління ланцюгами постачання); *хмарні середовища* (інфраструктура для зберігання та обробки даних

## Рівні ІЦУС та їх інтерпретація

| Рівень ІЦУС                  | Показник ІЦУС | Інтерпретація                                                                 |
|------------------------------|---------------|-------------------------------------------------------------------------------|
| Висока цифрова стійкість     | 4,2–5,0       | Цифрова архітектура повністю інтегрована, керована даними, захищена           |
| Задовільна цифрова стійкість | 3,5–4,1       | Наявні ефективні цифрові рішення, є потенціал для посилення інтеграції        |
| Помірна стійкість            | 2,5–3,4       | Рішення часткові, потребують стратегічної трансформації                       |
| Критична зона                | 1,0–2,4       | Відсутність цифрової координації, серйозні ризики в корпоративному управлінні |

Джерело: розроблено автором.

з гарантованою масштабованістю та доступом); *API-шлюзи та платформи інтеграції* (об'єднання внутрішніх і зовнішніх цифрових рішень).

Ознаки та методи оцінювання елементів у Б1 визначені та систематизовані в табл. 4.

Таблиця 4

## Ознаки та методи оцінювання, закладені в Б1

| Ознаки оцінювання в Б1           | Методи оцінки                             |
|----------------------------------|-------------------------------------------|
| Структура та інтеграція платформ | ІТ-аудит, експертне опитування            |
| Рівень централізації управління  | Контент-аналіз документації               |
| Масштаб хмарної інфраструктури   | Кількісне опитування, порівняльний аналіз |
| Відмовостійкість                 | Тестування, інтерв'ювання ІТ-фахівців     |
| API-сумісність                   | Технічний аудит                           |

Джерело: розроблено автором.

**Б2. Корпоративна система збору, обробки та аналітики даних.** Оцінюється структурована багаторівнева ІТ-архітектура, що забезпечує наскрізний потік інформації: від збору первинних даних у підрозділах до їхньої обробки, візуалізації та аналітичної інтерпретації на рівні центрального управління корпорації.

До елементів, що підлягають оцінюванню в Б2, входять: *DWH* (Data Warehouse) – корпоративне сховище структурованих даних; *ETL-процеси* для інтеграції даних з різних джерел (Extract, Transform, Load); *BI-інструменти* як платформи для побудови дашбордів, OLAP-запитів, автоматизованої звітності; аналітичні модулі прогнозування, виявлення відхилень, сценарний аналіз; системи управління метаданими для контролю якості та уніфікації даних.

Ознаки та методи оцінювання елементів у Б2 визначені та систематизовані в табл. 5.

Таблиця 5

## Ознаки та методи оцінювання, закладені в Б2

| Ознаки оцінювання в Б2 | Методи оцінки                            |
|------------------------|------------------------------------------|
| Покриття даними        | Контент-аналіз інформаційних потоків     |
| Автоматизація ETL      | Спостереження, технічний аудит           |
| Стандартизація         | Аналіз корпоративних регламентів         |
| BI-аналітика           | Експертна оцінка, тестування функціоналу |
| Предикативність        | Огляд проєктів, пілотів                  |
| Доступність            | Аналіз систем контролю доступу           |

Джерело: розроблено автором.

**Б3. Цифрова гнучкість корпорації.** Оцінюється здатність багаторівневої корпоративної структури адаптувати свою управлінську модель, внутрішні процеси, організаційну конфігурацію та систему ухвалення рішень під впливом змін зовнішнього та внутрішнього середовища. Вона передбачає: цифрову підтримку делегування повноважень; автоматизоване переналаштування процесів управління; динамічну зміну ролей, маршрутів інформаційних потоків і координації між підрозділами; можливість швидкої реструктуризації підконтрольних компаній та бізнес-одиниць.

Цифрова гнучкість втілюється через використання low-code/no-code платформ, BPMS, інструментів сценарного планування, адаптивних CRM/ERP-середовищ.

До елементів, що підлягають оцінюванню в Б3, входять: швидкість внесення змін до внутрішніх управлінських регламентів через цифрові інструменти; наявність цифрових моделей бізнес-процесів, які можуть бути адаптовані без втручання розробників; ступінь автоматизації перерозподілу

ролей і доступів у разі змін організаційної структури; використання симуляційних або сценарних інструментів для прогнозування управлінських змін; гнучкість взаємодії між підрозділами через спільні цифрові платформи; інституційна здатність до реструктуризації на рівні корпоративного управління.

Ознаки та методи оцінювання елементів у Б3 визначені та систематизовані в *табл. 6*.

Таблиця 6

Ознаки та методи оцінювання, закладені в Б3

| Ознаки оцінювання в Б3      | Методи оцінки                     |
|-----------------------------|-----------------------------------|
| Регламентна гнучкість       | Аналіз змін до внутрішніх політик |
| Гнучкість процесів          | Оцінка параметрів BPMS/CRM        |
| Перерозподіл ролей          | Аналіз журналів IAM/SSO           |
| Сценарне планування         | Експертна оцінка                  |
| Кросфункціональна взаємодія | Спостереження, аналіз інтерфейсів |
| Адаптація оргструктур       | Аналіз кейсів змін                |

Джерело: розроблено автором.

**Б4. Цифрова компетентність персоналу.** Оцінюється як інтегральна характеристика управлінських і функціональних кадрів корпорації, що визначає їхню здатність ефективно застосовувати цифрові інструменти, адаптуватися до нових технологічних рішень, підтримувати цифрові трансформації та діяти в умовах постійних технологічних змін.

До елементів, що підлягають оцінюванню в Б4, входять: оцінювання цифрових навичок керівного складу та ключових співробітників; система внутрішнього навчання, сертифікації та розвитку цифрової компетентності; цифрові платформи для самоосвіти, контролю прогресу, дашборди ІТ-ефективності; стимулювання участі в цифрових ініціативах через інструменти гейміфікації та KPI.

Ознаки та методи оцінювання елементів у Б4 визначені та систематизовані в *табл. 7*.

**Б5. Цифрові системи підтримки управлінських рішень.** Цей блок оцінює спроможність корпорації впроваджувати, адаптувати й ефективно використовувати цифрові інструменти, що допомагають управлінцям приймати стратегічні та оперативні рішення на базі достовірних, своєчасних і релевантних даних.

До елементів, що підлягають оцінюванню в Б5, входять: цифрові дашборди, інтегровані з даними всієї корпорації; модулі сценарного планування, симуляції та прогнозування; алгоритмічні системи прийняття рішень (rule-based, ML/AI); інтелектуальні агрегатори даних з різних систем (ERP, CRM, SCM); корпоративні центри аналітики (CoE).

Таблиця 7

Ознаки та методи оцінювання, закладені в Б4

| Ознаки оцінювання в Б4  | Методи оцінки                             |
|-------------------------|-------------------------------------------|
| Рівень цифрових навичок | Тестування, самооцінювання, аудит навичок |
| Освітні програми        | Аналіз контенту, опитування               |
| Сертифікація            | Верифікація сертифікатів, аналіз участі   |
| Доступність знань       | Аналіз баз знань, FAQ, гайдлайнів         |
| Цифрова ініціативність  | Оцінка участі в цифрових проєктах         |
| ІТ-аналітика активності | Моніторинг системного використання        |

Джерело: розроблено автором.

Ознаки та методи оцінювання елементів у Б5 визначені та систематизовані в *табл. 8*.

Таблиця 8

Ознаки та методи оцінювання, закладені в Б5

| Ознаки оцінювання в Б5        | Методи оцінки                |
|-------------------------------|------------------------------|
| Доступність рішень            | Аудит систем                 |
| Автоматизація                 | Аналіз процесів              |
| Сценарне планування           | Тестування функцій           |
| Дашборди                      | Експертна оцінка інтерфейсів |
| Алгоритмічне ухвалення рішень | Верифікація логіки           |
| Агрегація даних               | Перевірка потоків            |

Джерело: розроблено автором.

**Б6. Інформаційна корпоративна безпека та операційна стабільність.** Цей блок оцінює рівень захищеності цифрових активів корпорації, здатність підтримувати безперервність цифрових процесів і стійкість до кіберзагроз. Особливу увагу має бути приділено оцінці: централізованим політикам кіберзахисту, резервному відновленню систем (*disaster recovery*), аудиту та моніторингу інформаційних потоків, стабільності інформаційної взаємодії між підрозділами.

Ознаки та методи оцінювання елементів у Б6 визначені та систематизовані в *табл. 9*.

Основною відповідальною особою за стан ЦУСК повинен бути директор з інформаційної безпеки. Посада директора (керівника служби) з інформаційної безпеки, за нашим переконанням, є керівною на стратегічному рівні, обов'язковою в

Таблиця 9

## Ознаки та методи оцінювання, закладені в Б6

| Ознаки оцінювання в Б6  | Методи оцінки               |
|-------------------------|-----------------------------|
| Політика інфобезпеки    | Аналіз документації         |
| Кібермоніторинг         | Аудит SOC                   |
| Стійкість до атак       | Пентест, симуляції          |
| Відновлення             | Оцінка BCP, DRP             |
| Контроль доступу        | Перевірка прав доступу      |
| Операційна стабільність | Перевірка логістичних збоїв |

Джерело: розроблено автором.

структурі сучасної цифроорієнтованої корпорації, особливо якщо компанія працює з великими обсягами даних, критичною інфраструктурою або є частиною міжнародного ланцюга постачання. Такий керівник повинен відповідати за розробку стратегії кібербезпеки компанії (політик, стандартів, процедур), за управління ризиками інформаційної безпеки, їх ідентифікацію, оцінку, мінімізацію, за контроль відповідності до законодавства та міжнародних стандартів ISO/IEC 27001, NIST, GDPR тощо, за організацію моніторингу кіберзагроз і реагування на інциденти, за забезпечення безпеки цифрової інфраструктури корпорації (включно з ERP, CRM, базами даних, серверами), за побудову корпоративної культури кібербезпеки, проведення тренінгів для персоналу. Він повинен здійснювати керівництво окремим підрозділом або департаментом інформаційної безпеки, що для великих корпорацій має бути обов'язковим. Щодо належності до корпоративної структури, то він має бути підзвітним напряду генеральному директору, бути членом Правління та мати вето на впровадження цифрових рішень, які порушують політику інформаційної безпеки корпорації.

Таким чином, сформований підхід, на нашу думку, забезпечуватиме корпораціям багатоаспектний ефект:

1. *Адаптивність* через забезпечення гнучкого реагування на зміни через цифрові інструменти.
2. *Інтеграційність* шляхом охоплення всього управлінського циклу (планування, аналіз, ухвалення рішень, моніторинг).
3. *Кіберзахищеність*, оскільки забезпечена стійкість до ІТ-загроз і технічних збоїв.
4. *Системний рівень*, що стосується не лише ІТ-інфраструктури, а всієї інформаційно-аналітичної моделі управління.

5. *Орієнтація як на процес, так і на результат*, адже включає цифрову адаптивність у процесах прийняття рішень та реагування на загрози.

6. *Прогнозність* – через спроможність розробляти різні сценарії та системи для аналізу ризиків і трендів розвитку.

7. *Масштабованість і фактор часу*, що дозволить корпорації швидко поширювати результати та трансформувати бізнес-процеси, безперервно функціонувати під час криз, кіберзагроз і турбулентностей.

8. *Компетентнісний підхід*, який формується як необхідність набуття управлінської цифрової компетентності, як необхідна умова ефективного корпоративного менеджменту.

9. *Інформаційна автономія* шляхом набуття незалежності від нестабільних зовнішніх цифрових середовищ.

10. *Антикрихкість*, що спиратиметься на здатність корпорації посилювати загальну управлінську ефективність під тиском різноманітних викликів.

Слід також зазначити, що впровадження методики оцінювання ІЦУС у корпорації, як і будь-який захід, передбачає витрати. Але, за нашим аналізом, вони не є надмірними порівняно з потенційними втратами від неефективного цифрового управління, особливо в умовах українських кризових реалій. Оцінка витратності цього підходу має бути багатовимірною:

1. *Початкові витрати на впровадження методики*. Передбачається аналітична фаза (1–2 місяці): залучення внутрішніх експертів або зовнішніх консультантів для аналізу цифрових систем, що показує низький або середній рівень витрат (до 1% від річного бюджету ІТ-підрозділу).

*Адаптація шкал і критеріїв ІЦУС під специфіку корпорації*: вимагає одноразового ресурсного залучення (оцінюється в межах 5–10 тис. дол. США при зовнішньому консалтингу або до 1–2 тис. внутрішнім ресурсом).

2. *Інструментальне забезпечення впровадження*. ERP, CRM, BI, аналітичні платформи вже є в багатьох корпораціях. Методика ІЦУС лише структурує їхнє використання та оцінку. Тобто, немає потреби в нових платформах, лише в підвищенні ефективності їх використання.

*Інструменти оцінювання*: таблиці, матриці, шаблони можуть бути реалізовані в Power BI, Excel, Notion, Google Data Studio без додаткових фінансових витрат.

3. *Кадрові витрати щодо впровадження методики*. Для формування внутрішньої групи оцінки ІЦУС: зазвичай достатньо 3–5 ключових

фахівців із функціональних департаментів. Додаткового персоналу не потребує.

Навчання для роботи з критеріями ІЦУС можна реалізувати за рахунок внутрішніх семінарів або короткотермінового онлайн-курсу, а це мінімальні витрати. А переваги даного підходу є очевидними, адже ІЦУС дозволяє виявити та зміцнити слабкі місця, що стосуються централізованої кібербезпеки, disaster recovery та управління інцидентами.

Інтегрована цифрова інфраструктура відповідно до методики може мінімізувати зони вразливості, де утворюються «входи» для атак (наприклад, непідготовлені оновлення чи недостатній внутрішній контроль).

Методика дозволяє оцінити вартість потенційних ризиків, а значить – виправдати інвестиції у профілактичне посилення ІТ-стану та цифрових систем, дозволяє мінімізувати втрати корпорації, причому зниження витрат є не одноразовим, а сталим ефектом цифрової управлінської стійкості.

**У** комплексі це говорить про економію на рівні 10–25% операційного бюджету окремих напрямів діяльності корпорації. Це стається за рахунок:

#### **1. Скорочення дублювання функцій і процесів.**

*До впровадження ІЦУС:* у різних підрозділах можуть функціонувати паралельні ІТ-системи, дублюватися операції з обробки даних, управління персоналом, контролю якості тощо.

*Після впровадження:* загальна цифрова інфраструктура об'єднує ERP, CRM, SCM, що дозволяє централізувати управління (очікуваний ефект: зниження адміністративних витрат, зменшення штатів дублюючих посад).

#### **2. Оптимізація логістики та закупівель.**

Завдяки блокам ERP і BI: корпорація краще прогнозує потреби, уникнення надлишкових запасів, зниження витрат на зберігання (очікуваний ефект: до 10–15% економії в логістичних витратах).

#### **3. Автоматизація рутинних операцій.**

Сценарне планування та цифрові дашборди: замінюють щоденну ручну звітність, розрахунки, моніторинг KPI (очікуваний ефект: вивільнення часу висококваліфікованих управлінців, підвищення продуктивності персоналу).

#### **4. Зменшення витрат на помилки та не-ефективні рішення.**

Системи підтримки прийняття рішень мінімізують ризики прийняття хибних управлінських рішень через аналітику в реальному часі (очікуваний ефект: скорочення збитків, викликаних невдалими проектами, неефективними інвестиціями, втраченими угодами).

#### **5. Економія на ІТ-підтримці.**

Перехід на уніфіковану хмарну платформу знижує витрати на підтримку застарілих або ізолюваних систем (очікуваний ефект: зменшення витрат на зовнішніх підрядників, закупівлю ліцензій, технічне обслуговування).

#### **6. Зниження витрат на кіберзагрози.**

Централізований кіберзахист зменшує кількість атак, втрат даних, простоїв (очікуваний ефект: економія на інцидент-менеджменті, аудитах, штрафах і судових витратах).

#### **7. Менше часу на навчання нових працівників.**

Уніфікована цифрова система та внутрішнє навчання скорочує час на адаптацію нових кадрів (очікуваний ефект: до 20–30% зниження витрат на onboarding та тренінги).

### **ВИСНОВКИ**

Запропонована методика побудови та оцінювання Індексу цифрової управлінської стійкості (ІЦУС) корпорацій є інноваційною як у науковому, так і у прикладному вимірах. Наукова цінність дослідження полягає в розробці нової категоріальної основи для системної оцінки цифрової управлінської спроможності корпорацій в умовах високої турбулентності середовища.

Структура ІЦУС охоплює шість взаємопов'язаних блоків (від цифрової інфраструктури до кібербезпеки), що дозволяє не лише виявляти критичні зони цифрової нестійкості, але й формувати цільові управлінські стратегії для їх подолання.

Методика створює умови для кількісного аналізу цифрової трансформації не у вузькотехнологічному вимірі, а в площині управлінських процесів, міжпідроздільної взаємодії, кадрового потенціалу та стійкості цифрових рішень. Такий підхід відкриває нові горизонти у стратегічних дослідженнях корпоративного менеджменту, дозволяючи проводити міжгалузеві та міжкорпоративні порівняння цифрової зрілості.

Практична значущість підходу визначається його відповідністю викликам економіки України, що функціонує в умовах військової загрози, дефіциту ресурсів, технологічної фрагментованості та обмеженої інтеграції з міжнародними ІТ-системами. ІЦУС може служити базою для стратегічного планування цифрової трансформації, внутрішнього аудиту управлінських систем, обґрунтування інвестицій у цифрову інфраструктуру. Для державного сектора та регуляторів методика може стати інструментом моніторингу цифрової спроможності ключових корпоративних гравців, що має важливе значення для побудови національної політики цифрової відбудови.

Таким чином, методика ІЦУС є економічно обґрунтованим і масштабованим рішенням для корпоративного управління в Україні. Її впровадження вимагає помірних інвестицій у підготовчий етап, але дає високий потенціал економії та зниження стратегічних ризиків, особливо в умовах обмежених ресурсів і нестабільності.

ІЦУС може використовуватись як інструмент стратегічного планування цифрових трансформацій, бюджетування ІТ-витрат, кадрового розвитку та кібербезпеки, що особливо актуально в умовах обмежених ресурсів.

Подальші наукові дослідження доцільно спрямувати на розроблення галузевих модифікацій Індексу цифрової управлінської стійкості з урахуванням специфіки цифровізації в різних секторах економіки України (енергетика, логістика, агробізнес тощо), а також на емпіричну перевірку впливу високих значень ІЦУС на показники фінансової стабільності, адаптивності та стратегічної ефективності корпоративного управління в умовах кризових і післякризових трансформацій. ■

#### БІБЛІОГРАФІЯ

1. Brynjolfsson E., McAfee A. The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. W. W. Norton & Company, 2016. 336 p.
2. Akinola S., Telukdarie A. Business Model Transformation 4.0: Unleashing Growth and Innovation through Digitalization. *TWIST*, 2024. Vol. 19. Iss. 1. P. 481–496.  
DOI: <https://doi.org/10.5281/zenodo.10049652#115>
3. Botjes E., Van den Berg M., Van Gils B., H. Mulder. Attributes relevant to antifragile organizations. *IEEE 23rd Conference on Business Informatics (CBI)*. 2021. DOI: <https://doi.org/10.1109/CBI52690.2021.00017>
4. Altafin B. G., Morini C., Capitani D. H. D. Business model revisited: a novel canvas for digital transformation. *Revista de Gestao (REGE)*. 2025. Vol. 32. Iss. 2. P. 81–98. URL: <https://www.emerald.com/rege/article-pdf/32/2/81/9781873/rege-12-2023-0142.pdf>
5. Мащенко М. А., Іпполітов Є. М. Формування стратегії посилення інформаційної безпеки підприємства. *Економіка та суспільство*. 2024. Вип. 70. DOI: <https://doi.org/10.32782/2524-0072/2024-70-147>
6. Нога О. Сутність та значення інформаційно-комунікаційного забезпечення управління зовнішньоекономічною діяльністю підприємств. *Економіка. Фінанси. Право*. 2025. № 5. С. 114–119. DOI: <https://doi.org/10.37634/efp.2025.5.23>
7. Титаренко В. Є. Штучний інтелект як фактор оптимізації стратегічного управління та зміцнення конкурентних позицій підприємства. *Економіка. Фінанси. Право*. 2025. № 2. С. 26–29. DOI: <https://doi.org/10.37634/efp.2025.2.6>
8. Zianko V., Nechyporenko T. Impact of artificial intelligence on business models and competitiveness of

enterprises. *Економіка. Фінанси. Право*. 2025. № 1. С. 10–15.

DOI: <https://doi.org/10.37634/efp.2025.1.2>

9. Домбровська Н., Фаріон В. Цифрова трансформація в менеджменті підприємства: адаптація бізнес-моделей під впливом інноваційних технологій. *Економічний аналіз*. 2024. Т. 34. № 3. С. 40–53. DOI: <https://doi.org/10.35774/econa2024.03.040>
10. Євтушенко Н. М., Стеценко Д. І. Цифрова трансформація бізнесу в умовах війни в Україні: виклики та можливості. *Економічний простір*. 2024. № 191. С. 211–216. DOI: <https://doi.org/10.32782/2224-6282/191-34>
11. Гвоздь М. Я., Морозов М. Я., Олинець А.-М. Я. Цифрова трансформація підприємств: інтеграція AGILE-підходів у систему менеджменту. *Економіка та суспільство*. 2025. Вип. 73. DOI: <https://doi.org/10.32782/2524-0072/2025-73-126>
12. BBC 'took too long to realise DMI project was in trouble'. *The Guardian*. URL: [https://www.theguardian.com/media/2013/dec/18/bbc-dmi-project-pwc-report?utm\\_source=chatgpt.com](https://www.theguardian.com/media/2013/dec/18/bbc-dmi-project-pwc-report?utm_source=chatgpt.com)
13. Delta Air Lines v. CrowdStrike. URL: [https://en.wikipedia.org/wiki/Delta\\_Air\\_Lines\\_v.\\_CrowdStrike?utm\\_source=chatgpt.com](https://en.wikipedia.org/wiki/Delta_Air_Lines_v._CrowdStrike?utm_source=chatgpt.com)
14. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *WIRED*. August 22, 2018. URL: [https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/?utm\\_source=chatgpt.com](https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/?utm_source=chatgpt.com)
15. Хакерські атаки на Україну (2017). URL: <https://surl.li/yihuem>
16. Мельник Т. Телеком-Чорнобиль. Forbes склав детальну реконструкцію хакерської атаки на «Київстар» у грудні 2023-го. Чи здатна компанія відновити зруйноване. *Forbes Ukraine*. 19.03.2024. URL: <https://forbes.ua/company/telekom-chornobil-15032024-19815>

#### REFERENCES

- Akinola, S., and Telukdarie, A. "Business Model Transformation 4.0: Unleashing Growth and Innovation through Digitalization". *TWIST*, vol. 19, no. 1 (2024): 481–496.  
DOI: <https://doi.org/10.5281/zenodo.10049652#115>
- Altafin, B. G., Morini, C., and Capitani, D. H. D. "Business model revisited: a novel canvas for digital transformation". *Revista de Gestao (REGE)*. 2025. <https://www.emerald.com/rege/article-pdf/32/2/81/9781873/rege-12-2023-0142.pdf>
- "BBC 'took too long to realise DMI project was in trouble'". *The Guardian*. [https://www.theguardian.com/media/2013/dec/18/bbc-dmi-project-pwc-report?utm\\_source=chatgpt.com](https://www.theguardian.com/media/2013/dec/18/bbc-dmi-project-pwc-report?utm_source=chatgpt.com)
- Botjes, E. et al. "Attributes relevant to antifragile organizations". *IEEE 23rd Conference on Business Informatics (CBI)*. 2021. DOI: <https://doi.org/10.1109/CBI52690.2021.00017>

- Brynjolfsson, E., and McAfee, A. *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. W. W. Norton & Company, 2016.
- "Delta Air Lines v. CrowdStrike". [https://en.wikipedia.org/wiki/Delta\\_Air\\_Lines\\_v.\\_CrowdStrike?utm\\_source=chatgpt.com](https://en.wikipedia.org/wiki/Delta_Air_Lines_v._CrowdStrike?utm_source=chatgpt.com)
- Dombrovska, N., and Farion, V. "Tsyfrova transformatsiia v menedzhmenti pidpriemstva: adaptatsiia biznes-modelei pid vplyvom innovatsiinykh tekhnolohii" [Digital Transformation in Enterprise Management: Adaptation of Business Models Under the Influence of Innovative Technologies]. *Ekonomichnyi analiz*, vol. 34, no. 3 (2024): 40-53.  
DOI: <https://doi.org/10.35774/econa2024.03.040>
- Hvoz, M. Ya., Morozov, M. Ya., and Olynets, A.-M. Ya. "Tsyfrova transformatsiia pidpriemstv: intehratsiia AGILE-pidkhodiv u systemu menedzhmentu" [Digital Transformation of Enterprises: Integration of AGILE Approaches into the Management System]. *Ekonomika ta suspilstvo*, no. 73 (2025).  
DOI: <https://doi.org/10.32782/2524-0072/2025-73-126>
- "Khakerski ataky na Ukrainu (2017)" [Hacker Attacks on Ukraine (2017)]. <https://surl.li/yihuem>
- Mashchenko, M. A., and Ippolitov, Ye. M. "Formuvannia stratehii posylennia informatsiinoi bezpeky pidpriemstva" [Formation of a Strategy to Strengthen the Enterprise's Information Security]. *Ekonomika ta suspilstvo*, no. 70 (2024).  
DOI: <https://doi.org/10.32782/2524-0072/2024-70-147>
- Melnyk, T. "Telekom-Chornobyl. Forbes sklav detalnu rekonstruktsiiu khakerskoi ataky na «Kyivstar» u hrudni 2023-ho. Chy zdatna kompaniia vidnovyty zruinovane" [Telecom-Chernobyl. Forbes Has Compiled a Detailed Reconstruction of the Hacker Attack on Kyivstar in December 2023. Is the Company Able to Restore the Destroyed]. *Forbes Ukraine*. March 19, 2024. <https://forbes.ua/company/telekom-chornobil-15032024-19815>
- Noha, O. "Sutnist ta znachennia informatsiino-komunikatsiinoho zabezpechennia upravlinnia zovnishnoekonomichnoiu diialnistiu pidpriemstv" [The Essence and Importance of Information and Communication Support for Managing Foreign Economic Activities of Enterprises]. *Ekonomika. Finansy. Pravo*, no. 5 (2025): 114-119.  
DOI: <https://doi.org/10.37634/efp.2025.5.23>
- "The Untold Story of NotPetya, the Most Devastating Cyberattack in History". *WIRED*. August 22, 2018. [https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/?utm\\_source=chatgpt.com](https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/?utm_source=chatgpt.com)
- Tytarenko, V. Ye. "Shtuchnyi intelekt yak faktor optymizatsii stratehichnoho upravlinnia ta zmitsnennia konkurentnykh pozytsii pidpriemstva" [Artificial Intelligence as a Factor in Optimizing Strategic Management and Strengthening the Competitive Position of an Enterprise]. *Ekonomika. Finansy. Pravo*, no. 2 (2025): 26-29.  
DOI: <https://doi.org/10.37634/efp.2025.2.6>
- Yevtushenko, N. M., and Stetsenko, D. I. "Tsyfrova transformatsiia biznesu v umovakh viiny v Ukraini: vyklyky ta mozhlyvosti" [Digital Business Transformation in the Context of War in Ukraine: Challenges and Opportunities]. *Ekonomichnyi prostir*, no. 191 (2024): 211-216.  
DOI: <https://doi.org/10.32782/2224-6282/191-34>
- Zianko, V., and Nechyporenko, T. "Impact of artificial intelligence on business models and competitiveness of enterprises". *Ekonomika. Finansy. Pravo*, no. 1 (2025): 10-15.  
DOI: <https://doi.org/10.37634/efp.2025.1.2>