Національний університет «Одеська політехніка»
Міністерство освіти і науки України
Національний університет «Одеська політехніка»
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

АЛІ РАШИД ХАЛІФА БУМЕКАЙР АЛЬМАНСУРІ

УДК 005.35:004.032.2:330.342.3(043.3/.5)

ДИСЕРТАЦІЯ
«ЦИФРОВІ ІНФОКОМУНІКАЦІЙНІ РЕСУРСИ ЗАБЕЗПЕЧЕННЯ РОЗВИТКУ ПІДПРИЄМСТВА В УМОВАХ КРИЗ»

073 – Менеджмент
07 – Управління та адміністрування

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Алі Рашид Халіфа Бумекайр Альмансурі.

Науковий керівник: Ткач Костянтин Іванович, доктор економічних наук, доцент.

Одеса – 2025

АНОТАЦІЯ

Алі Рашид Халіфа Бумекайр Альмансурі. *Цифрові інфокомунікаційні ресурси забезпечення розвитку підприємства в умовах криз*. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеню доктора філософії за спеціальністю 073 – Менеджмент галузі знань 07 – Управління та адміністрування. – Національний університет «Одеська політехніка» МОН України, Одеса, 2025.

Дисертацію присвячено вирішенню важливого наукового завдання, яке полягає в удосконаленні управління підприємствами шляхом системного управління цифровими інфокомунікаційними ресурсами в умовах криз. Його вирішено за рахунок розроблення та обґрунтування теоретичних і науково-методичних підходів до використання цифрових інфокомунікаційних ресурсів забезпечення розвитку підприємства в умовах криз на засадах системного підходу, що забезпечує підвищення цифрової стійкості та ефективності розвитку підприємства.

У розділі 1 «Теоретичні засади формування цифрових інфокомунікаційних ресурсів підприємства» висвітлено теоретичні засади формування цифрових інфокомунікаційних ресурсів підприємства. Досліджено їх сутність, класифікацію та еволюцію, обґрунтовано роль цифрових інфокомунікаційних ресурсів як інтегрованої соціотехнічної системи, що забезпечує функціонування підприємства в умовах цифрової трансформації. Систематизовано класифікаційні ознаки цифрових інфокомунікаційних ресурсів, виділено п'ять ключових груп ресурсів та проаналізовано їхню еволюцію від локальних інформаційних систем до інтегрованих цифрових екосистем.

Обґрунтовано, що цифрові інфокомунікаційні ресурси є стратегічним активом, який забезпечує підприємству не лише технологічне оновлення, а й формування цифрової стійкості та стійких конкурентних переваг. Розкрито

теоретичні підходи та моделі впливу цифрових ресурсів на розвиток підприємства, зокрема через впровадження діджиталізаційних та смарт-моделей управління. Доведено, що впровадження цих моделей є ключовим каталізатором для переходу до даних-орієнтованого та проактивного управління.

Проаналізовано особливості формування інфокомунікаційної інфраструктури підприємства в умовах кризових викликів. Визначено та класифіковано багатовимірні ризики і вразливості (технологічні, кібернетичні, організаційні), які постають перед підприємством у періоди нестабільності. Розкрито стратегічний функціональний потенціал цифрових інфокомунікаційних ресурсів, що забезпечує моніторинг загроз, координацію дій та аналітичну підтримку антикризового управління.

Сформульовано таку робочу гіпотезу дослідження: підвищення рівня цифрової стійкості (Digital Resilience) та інфокомунікаційне забезпечення розвитку підприємства в умовах кризових викликів може бути досягнуте шляхом впровадження інтегрованої системи управління цифровими інфокомунікаційними ресурсами, яка базується на принципах проактивного ризик-менеджменту, адаптивності цифрової архітектури та синергії технологічних, комунікаційних та кібербезпекових елементів.

В розділі 2 «Аналітична оцінка стану та ефективності використання інфокомунікаційних цифрових ресурсів на підприємствах» здійснено поглиблений аналітичний аналіз стану цифрової зрілості підприємств як ключової передумови формування ефективного інфокомунікаційного забезпечення розвитку в умовах кризових викликів. Основна увага зосереджена на виявленні структурних особливостей цифрової трансформації підприємств, визначенні сильних і слабких сторін їх цифрового розвитку, а також на обґрунтуванні ролі цифрових інфокомунікаційних ресурсів у забезпеченні стійкості, безперервності та адаптивності діяльності. У розділі систематизовано сучасні наукові та прикладні підходи до оцінювання цифрової зрілості, що дозволило сформувати цілісне бачення даного

феномену як багатовимірної управлінської категорії.

Визначено п’ять ключових вимірів цифрової зрілості підприємства – процеси, технології, дані, персонал та управління, які розглядаються як взаємопов’язані елементи єдиної цифрової екосистеми. Розкрито зміст кожного виміру, окреслено їх вплив на формування цифрової стійкості та доведено, що домінування окремих технологічних рішень без належної інтеграції з управлінськими та організаційними механізмами не забезпечує сталого ефекту цифрової трансформації. Особливий акцент зроблено на ролі управління даними та цифрових компетенцій персоналу, які в умовах криз набувають визначального значення для прийняття обґрунтованих управлінських рішень.

Розроблено та обґрунтовано методику оцінювання цифрової зрілості підприємств, що базується на використанні системи субіндикаторів та розрахунку інтегрального індексу цифрової зрілості. Запропонована методика забезпечує можливість кількісного вимірювання рівня цифрового розвитку підприємств, порівняння результатів між різними галузями та країнами, а також ідентифікації критичних зон цифрової вразливості. На основі цієї методики проведено оцінювання цифрової зрілості вибірки підприємств IT-сфери, фінтех-сектору та виробничої сфери, що дозволило виявити суттєві галузеві відмінності у рівні цифрової інтеграції та управління інфокомунікаційними ресурсами.

Окрему увагу приділено порівняльному аналізу цифрової зрілості підприємств України та ОАЕ, який засвідчив наявність істотного розриву між рівнем технологічного розвитку та рівнем цифрового управління й використання даних. Установлено, що в Україні цифровізація часто має фрагментарний та реактивний характер, орієнтований на подолання кризових наслідків, тоді як у країнах з більш стабільним інституційним середовищем цифрова трансформація реалізується як стратегічний інструмент довгострокового розвитку.

Доведено, що саме інтегроване управління цифровими

інфокомунікаційними ресурсами є ключовою умовою підвищення цифрової стійкості підприємств в умовах кризових викликів. Отримані аналітичні висновки підтвердили робочу гіпотезу дослідження та сформували методичну і практичну основу для розробки концептуальних моделей і управлінських рішень, представлених у третьому розділі роботи.

В розділі 3 «Системне цифрове інфокомунікаційне забезпечення розвитку підприємства в умовах криз» наведене авторське бачення цифрового інфокомунікаційного забезпечення розвитку підприємства в умовах криз на системній основі. Запропоновано: концептуальну модель фокусного цифрового інфокомунікаційного забезпечення розвитку підприємства, науково-методичні засади формування цифрової інфокомунікаційної стратегії підприємства з урахуванням кризових умов; інструменти та рекомендації щодо оцінювання цифрових рішень підприємства.

Розроблено й обґрунтовано концептуальні та прикладні рішення щодо впровадження інтегрованої системи управління цифровими інфокомунікаційними ресурсами підприємства як інструменту підвищення цифрової стійкості та забезпечення розвитку в умовах кризових викликів, які спрямовані на трансформацію виявлених проблем і диспропорцій цифрової зрілості у практичні управлінські механізми.

Сформовано архітектуру цифрового інфокомунікаційного забезпечення розвитку підприємства, яка інтегрує технологічні, комунікаційні, аналітичні та кібербезпекові компоненти в єдину керовану систему. Обґрунтовано доцільність використання фокусного підходу до управління цифровими інфокомунікаційними ресурсами, що дозволяє узгодити стратегічні цілі розвитку підприємства з операційними цифровими рішеннями та антикризовими пріоритетами.

Особливу увагу приділено розробці механізмів антикризового управління на основі цифрових даних, зокрема інструментів моніторингу, оцінювання та прогнозування стану цифрової інфраструктури. Запропоновано систему KPI та індикаторів, орієнтованих на вимірювання цифрової стійкості,

безперервності та адаптивності діяльності підприємства. Показано, що застосування таких інструментів забезпечує своєчасне виявлення цифрових ризиків та підвищує обґрунтованість управлінських рішень у кризових ситуаціях.

Розроблено алгоритм проєктування і впровадження інфокомунікаційної системи підприємства, який охоплює етапи фокусного вибору цифрових платформ, побудови внутрішніх комунікацій і захисту даних, а також інтеграції аналітики, штучного інтелекту та хмарних сервісів. Запропонований алгоритм має універсальний характер і може бути адаптований до підприємств різних галузей з урахуванням рівня їх цифрової зрілості та ресурсних обмежень. Доведено, що інтеграція KPI розвитку цифрової інфраструктури з KPI принципів екосистеми створює синергетичний ефект і сприяє підвищенню цифрової стійкості.

Розроблені методичні підходи та аналітичний інструментарій оцінювання оцінювання результативності та цифрової стійкості інфокомунікаційних цифрових рішень містять: а) критеріально-орієнтований добір інструментів, застосовних для формування організаційних (скорочення часу, автоматизація, безпека) та антикризових (стійкість, безперервність, адаптивність) ефектів; б) рекомендації щодо оцінювання цифрових ресурсів підприємства у складі політики оцінювання цифрових ресурсів, механізмів моніторингу й оцінювання інфокомунікаційних цифрових рішень, компетентностей персоналу; в) інтеграції критеріїв стійкості, безперервності та адаптивності з аналітичними інструментами, що охоплюють часову ефективність, автоматизацію, кіберзахист, операційну стабільність та ризики; г) методичний підхід і методика паспортизації цифрових решень та інструментів для методів оцінювання інфокомунікаційних цифрових рішень.

Ключові слова: інфокомунікаційне забезпечення, криза, модель, оцінювання, розвиток підприємства, системний підхід, технології, фокусне управління, цифрова архітектура, цифрова зрілість, цифрова стійкість, цифрова інфокомунікаційна стратегія, цифрові інфокомунікаційні ресурси.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Статті у фахових виданнях України

1. Алі Рашид Халіфа Бумекайр Альмансурі. Формування інфокомунікаційної інфраструктури підприємства в умовах криз. *Економічний журнал Одеського політехнічного університету*. 2025. №1(31). С. 136-145. URL: https://economics.net.ua/ejopu/2025/No1/136.pdf (Дата звернення 05.10.2025). DOI: 10.15276/EJ.01.2025.14, DOI: 10.5281/zenodo.18025510 *(Кат. Б., Index Copernicus, Google Scholar) (1,15 д.а.).*

2. Ткач К.І., Алі Рашид Халіфа Бумекайр Альмансурі. Оцінювання стану та ефективності використання інфокомунікаційних цифрових ресурсів на підприємствах. *Економіка: реалії часу. Науковий журнал.* 2025. № 1 (77). С. 129-139. URL: https://economics.net.ua/files/archive/2025/No1/129.pdf (Дата звернення 05.10.2025). DOI: 10.15276/ETR.01.2025.15. DOI: 10.5281/ zenodo.18036081 *(Кат. Б., Index Copernicus, Ulrich's Periodicals Directory, EBSCO Publishing, Google Scholar) (1,1 д.а., особистий внесок: розроблено рекомендації, методику оцінювання цифрових ресурсів підприємства, систему для формування організаційних і антикризових ефектів. 0,6 д.а.).*

3. Алі Рашид Халіфа Бумекайр Альмансурі. Діагностика цифрової зрілості у котнексті інфокомунікаційніих ресурсів підприємства. *Економічний журнал Одеського політехнічного університету.* 2025. № 2 (32). С. 141-151. URL: https://economics.net.ua/ejopu/2025/No2/141.pdf (Дата звернення 05.09.2025). DOI: 10.15276/EJ.02.2025.16, DOI: 10.5281/zenodo.18025967 *(Кат. Б., Index Copernicus, Google Scholar). (1,05 д.а.)*

4. Ткач К.І., Алі Рашид Халіфа Бумекайр Альмансурі. Системне цифрове інфокомунікаційне забезпечення розвитку підприємства: фокусування в умовах криз. *Економіка: реалії часу. Науковий журнал.* 2025. № 2 (78). С. 150-161. URL: https://economics.net.ua/files/archive/2025/No2/150.pdf. (Дата звернення 05.10.2025). DOI: 10.15276/ETR.02.2025.16, DOI:

10.5281/zenodo.18039087 *(Index Copernicus, Google Scholar). (1,2 д.а., особистий внесок: обґрунтувано концептуальні засади системного цифрового інфокомунікаційного забезпечення розвитку підприємства, напрями його фокусування в умовах криз: структурно-логічну модель, принципи побудови інфокомунікаційної екосистеми, архітектуру, ключові елементи і KPI) (0,7 д.а.)*

Опубліковані праці апробаційного характеру

5. Алі Рашид Халіфа Бумекайр Альмансурі. Принципи побудови інфокомунікаційної екосистеми в умовах криз. *Актуальні проблеми теорії та практики менеджменту*: Матеріали XII міжнар. наук.-практ. конф. 26 травня 2023, Україна, м. Одеса. С. 201-203. URL: https://economics.net.ua/files/science/men/2023/s7.pdf. (Дата звернення 20.10.2022). (*0,15 д.а.*).

6. Алі Рашид Халіфа Бумекайр Альмансурі. Структура інфокомунікаційних цифрових ресурсів підприємства. *Економічна кібернетика: теорія, практика та напрямки розвитку* : Матеріали міжнар. наук.-практ. конф. 29-30 листопада 2022, Україна, м. Одеса, С.148-150. URL: https://economics.net.ua/files/science/ek_kiber/2022/tezy.pdf. (Дата звернення 20.01.2023) *(0,1 д.а.)*.

7. Ткач К.І., Алі Рашид Халіфа Бумекайр Альмансурі. Концептуальна структурно-логічна модель фокусного цифрового інфокомунікаційного забезпечення розвитку та діяльності підприємства. *Сучасні управлінські та соціально-економічні аспекти розвитку держави, регіонів та суб'єктів господарювання в умовах трансформації публічного управління*. Матеріали міжнар. наук. конф. 14 листопада 2024, Україна, м. Одеса. С.110-112. URL: https://economics.net.ua/files/science/admin_men/2024/tezy24.pdf. (Дата звернення 15.12.2024) *(0,15 д.а., особистий внесок: опис переваг фокусного цифрового інфокомунікаційного забезпечення розвитку підприємства в умовах криз – 0,1 д.а.)*.

8. Алі Рашид Халіфа Бумекайр Альмансурі. Зовнішні кризові фактори та їх вплив на цифрову інфраструктуру підприємств. *Обліково-аналітичне забезпечення інноваційної трансформації економіки України (в умовах воєнного стану та поствоєнний період)* : Матеріали всеукраїнської наук.-практ. конф. 24 листопада 2024, Україна, м. Одеса, С.170-172. URL: https://economics.net.ua/files/science/oblik/2024/Tezy.pdf. (Дата звернення: 15.01.2025) (*0,15 д.а.*).

9. Алі Рашид Халіфа Бумекайр Альмансурі. Архітектура та ключові елементи цифрового інфокомунікаційного забезпечення розвитку підприємства. *Сучасні управлінські та соціально-економічні аспекти розвитку держави, регіонів та суб'єктів господарювання в умовах трансформації публічного управління.* Матеріали міжнар. наук. конф. 14 листопада 2025, Україна, м. Одеса. С.55-57. URL: https://economics.net.ua/publ. (Дата звернення 17.11.2025) (*0,15 д.а.*).

10. Ткач К.І., Алі Рашид Халіфа Бумекайр Альмансурі. Міжнародна практика реагування на зовнішні кризові впливи щодо формування пріоритетів інвестування у цифрові технології та модернізацію цифрової інфраструктури: кейси ОАЕ. *Обліково-аналітичне забезпечення інноваційної трансформації економіки України (в умовах воєнного стану та поствоєнний період)* : Матеріали всеукраїнської наук.-практ. конф. 24 листопада 2025, Україна, м. Одеса, С.72-74. URL: https://economics.net.ua/oaz. (Дата звернення: 15.01.2025) *(0,15 д.а., особистий внесок: систематизація інвестиційних кейсів ОАЕ у сфері цифрових технологій (0,1 д.а.).*

11. Алі Рашид Халіфа Бумекайр Альмансурі. Управлінські виклики і трансформацій у системі менеджменту для ефективного впровадження цифрових інструментів. *Економічна кібернетика: теорія, практика та напрямки розвитку* : Матеріали міжнар. наук.-практ. конф. 27-28 листопада 2025, Україна, м. Одеса. С.280-286. URL: https://economics.net.ua/files/science/ek_kiber/2025/tezy25.pdf (Дата звернення 01.12.2025) *(0,1 д.а.).*

SUMMARY

Ali Rashed Khalifa Bumeqairaa Almansoori. *Digital information and communication resources for ensuring enterprise development in crisis conditions*. – Qualifying scientific work as a manuscript.

Thesis for the Philosophy Doctor degree in specialty 073 – Management. – Odesa Polytechnic National University of the Ministry of Education and Science of Ukraine, Odesa, 2025.

The dissertation is devoted to solving an important scientific problem, which consists in improving enterprise management through systematic management of digital information and communication resources in crisis conditions. This task is solved by developing and substantiating theoretical and scientific-methodological approaches to the use of digital information and communication resources to ensure the development of enterprises in crisis conditions based on a systematic approach that ensures increased digital resilience and efficiency of enterprise development

Chapter 1 «Theoretical Foundations of the Formation of Digital Information and Communication Resources of an Enterprise» highlights the theoretical foundations of the formation of digital information and communication resources of an enterprise. Their essence, classification and evolution are investigated, and the role of digital information and communication resources as an integrated socio-technical system that ensures the functioning of an enterprise in conditions of digital transformation is substantiated. The classification characteristics of digital information and communication resources are systematised, five key resource groups are identified, and their evolution from local information systems to integrated digital ecosystems is analysed.

It is substantiated that digital information and communication resources are a strategic asset that provides an enterprise not only with technological innovation, but also with the formation of digital resilience and sustainable competitive advantages. Theoretical approaches and models of the impact of digital resources on the development of an enterprise are revealed, in particular through the implementation

of digitalisation and smart management models. It is proven that the implementation of these models is a key catalyst for the transition to data-driven and proactive management.

The peculiarities of the formation of an enterprise's information and communication infrastructure in conditions of crisis challenges are analysed. Multidimensional risks and vulnerabilities (technological, cybernetic, organisational) that enterprises face in periods of instability are identified and classified. The strategic functional potential of digital information and communication resources, which provides threat monitoring, coordination of actions and analytical support for crisis management, is revealed.

The following working hypothesis of the study has been formulated: increasing the level of digital resilience and ensuring the development of enterprises in terms of information and communication in crisis conditions can be achieved by implementing an integrated system for managing digital information and communication resources based on the principles of proactive risk management, adaptability of digital architecture, and synergy between technological, communication, and cybersecurity elements.

Chapter 2 «Analytical assessment of the state and effectiveness of the use of information and communication digital resources in enterprises» provides an in-depth analytical analysis of the state of digital maturity of enterprises as a key prerequisite for the formation of effective information and communication support for development in conditions of crisis challenges. The main focus is on identifying the structural features of the digital transformation of enterprises, determining the strengths and weaknesses of their digital development, and substantiating the role of digital information and communication resources in ensuring the sustainability, continuity and adaptability of activities. The chapter systematises modern scientific and applied approaches to assessing digital maturity, which has made it possible to form a holistic view of this phenomenon as a multidimensional management category.

Five key dimensions of digital maturity of an enterprise have been identified – processes, technologies, data, personnel and management, which are considered as interrelated elements of a single digital ecosystem. The content of each dimension is revealed, their impact on the formation of digital sustainability is outlined, and it is proven that the dominance of individual technological solutions without proper integration with management and organisational mechanisms does not ensure a sustainable effect of digital transformation. Particular emphasis is placed on the role of data management and digital competencies of personnel, which in times of crisis become crucial for making informed management decisions.

A methodology for assessing the digital maturity of enterprises has been developed and substantiated, based on the use of a system of sub-indicators and the calculation of an integral index of digital maturity. The proposed methodology provides the ability to quantitatively measure the level of digital development of enterprises, compare results between different industries and countries, and identify critical areas of digital vulnerability. Based on this methodology, the digital maturity of a sample of enterprises in the IT sphere, fintech sector and manufacturing sphere was assessed, which made it possible to identify significant industry differences in the level of digital integration and management of information and communication resources.

Special attention is paid to a comparative analysis of the digital maturity of enterprises in Ukraine and the UAE, which revealed a significant gap between the level of technological development and the level of digital management and data usage. It has been established that in Ukraine, digitalisation is often fragmented and reactive in nature, focused on overcoming the consequences of crises, while in countries with a more stable institutional environment, digital transformation is implemented as a strategic tool for long-term development.

It has been proven that integrated management of digital information and communication resources is a key condition for increasing the digital resilience of enterprises in the face of crisis challenges. The analytical conclusions obtained confirmed the working hypothesis of the study and formed a methodological and

practical basis for the development of conceptual models and management decisions presented in the third chapter of the work.

Chapter 3 «Systemic Digital Information and Communication Support for Enterprise Development in Crisis Conditions» presents the author's vision of systemic digital information and communication support for enterprise development in crisis conditions. The following are proposed: a conceptual model of focused digital information and communication support for enterprise development, scientific and methodological foundations for the formation of an enterprise's digital information and communication strategy, taking into account crisis conditions; tools and recommendations for evaluating an enterprise's digital solutions.

Conceptual and applied solutions have been developed and substantiated for the implementation of an integrated system for managing the digital information and communication resources of an enterprise as a tool for increasing digital resilience and ensuring development in crisis conditions, aimed at transforming the identified problems and imbalances of digital maturity into practical management mechanisms.

The architecture of digital information and communication support for enterprise development has been formed, integrating technological, communication, analytical and cybersecurity components into a single managed system. The feasibility of using a focused approach to managing digital information and communication resources has been substantiated, allowing the strategic development goals of the enterprise to be aligned with operational digital solutions and anti-crisis priorities.

Particular attention has been paid to the development of anti-crisis management mechanisms based on digital data, in particular tools for monitoring, assessing and forecasting the state of digital infrastructure. A system of KPIs and indicators focused on measuring the digital resilience, continuity and adaptability of an enterprise's activities is proposed. It is shown that the use of such tools ensures the timely identification of digital risks and increases the soundness of management decisions in crisis situations.

An algorithm for designing and implementing an enterprise information and communication system has been developed, covering the stages of focused selection of digital platforms, building internal communications and data protection, as well as integrating analytics, artificial intelligence and cloud services. The proposed algorithm is universal and can be adapted to enterprises in various industries, taking into account their level of digital maturity and resource constraints. It has been proven that the integration of digital infrastructure development KPIs with ecosystem principle KPIs creates a synergistic effect and contributes to increasing the digital sustainability of an enterprise.

The developed methodological approaches and analytical tools for assessing the effectiveness and digital resilience of information and communication digital solutions include: a) criteria-oriented selection of tools applicable for the formation of organisational (time reduction, automation, security) and anti-crisis (resilience, continuity, adaptability) effects; b) recommendations for assessing the digital resources of an enterprise as part of a digital resource assessment policy, mechanisms for monitoring and evaluating ICT digital solutions, and staff competencies; c) integration of sustainability, continuity and adaptability criteria with analytical tools covering time efficiency, automation, cyber security, operational stability and risks; d) a methodological approach and methodology for certifying digital solutions and tools for assessing ICT digital solutions.

A separate section is devoted to the formation of a policy for the assessment and regulatory use of digital infrastructure KPIs, which ensures consistency between the principles of building an information and communication ecosystem and the practice of digital resource management. The findings are of practical importance and can be used as a basis for developing digital transformation programmes for enterprises in today's turbulent environment.

Keywords: digital architecture, digital maturity, digital resilience, digital information and communication strategy, digital information and communication resources, information and communication support, crisis, enterprise development, systematic approach, focus management, technologies, assessment, model.

LIST OF THE APPLICANT'S PUBLICATIONS

Articles in Professional Journals of Ukraine

1. Ali Rashed Khalifa Bumeqairaa Almansoori. Formation of an enterprise's information and communication infrastructure in crisis conditions. *Economic Journal of Odessa Polytechnic University*. 2025. №1(31). P. 136-145. URL: https://economics.net.ua/ejopu/2025/No1/136.pdf (Date of access: 05.10.2025). DOI: 10.15276/EJ.01.2025.14, DOI: 10.5281/zenodo.18025510 (*Category B, Index Copernicus, Google Scholar*) (*1,15 printed sheet*).

2. Tkach K.I., Ali Rashed Khalifa Bumeqairaa Almansoori. Assessment of the state and effectiveness of the use of information and communication digital resources in enterprises. Economics: Realities of the Times. Scientific journal. 2025. № 1 (77). P. 129-139. URL: https://economics.net.ua/files/archive/2025/No1/129.pdf (Date of access: 05.10.2025). DOI: 10.15276/ETR.01.2025.15, DOI: 10.5281/zenodo.18036081 (*Category B, Index Copernicus, Ulrich's Periodicals Directory, EBSCO Publishing, Google Scholar*) (*1,1 printed sheet, personal contribution: recommendations, methodology for evaluating digital resources of the enterprise, and a system for forming organisational and anti-crisis effects have been developed. 0,6 printed sheet*).

3. Ali Rashed Khalifa Bumeqairaa Almansoori. Diagnosis of digital maturity in the context of enterprise information and communication resources. Economic Journal of Odessa Polytechnic University. 2025. № 2 (32). P. 141-151. URL: https://economics.net.ua/ejopu/2025/No2/141.pdf (Date of access: 05.09.2025). DOI: 10.15276/EJ.02.2025.16, DOI: 10.5281/zenodo.18025967 (*Category B, Index Copernicus, Google Scholar*). (*1,05 printed sheet*).

4. Tkach K.I., Ali Rashed Khalifa Bumeqairaa Almansoori. Systematic digital information and communication support for enterprise development: focusing in times of crisis. Economics: Realities of the Times. Scientific journal. 2025. № 2 (78). P. 150-161. URL: https://economics.net.ua/files/archive/2025/

No2/150.pdf (Date of access: 05.10.2025). DOI: 10.15276/ETR.02.2025.16, DOI: 10.5281/zenodo.18039087 (*Index Copernicus, Google Scholar*). (*1,2 printed sheet, personal contribution: substantiated conceptual foundations of systematic digital information and communication support for enterprise development, areas of focus in crisis conditions: structural and logical model, principles of building an information and communication ecosystem, architecture, key elements and KPIs*) (*0,7 printed sheet*).

Publications of an Approbatory Nature

5. Ali Rashed Khalifa Bumeqairaa Almansoori. Principles of building an information and communication ecosystem in times of crisis. *Current Issues in Management Theory and Practice :* Proceedings of the XII International Scientific and Practical Conference. 26 May 2023. Odesa. Ukraine. P. 201-203. URL: https://economics.net.ua/files/science/men/2023/s7.pdf (Date of access: 20.10.2022). (*0,15 printed sheet*).

6. Ali Rashed Khalifa Bumeqairaa Almansoori. Structure of the enterprise's information and communication digital resources. *Economic cybernetics: theory, practice and directions of development :* Materials of the international scientific and practical conference. 29-30 November 2022, Odesa, Ukraine. P. 148-150. URL: https://economics.net.ua/files/science/ek_kiber/2022/tezy.pdf. (Date of access: 20.01.2023) *(0,1 printed sheet)*.

7. Tkach K.I., Ali Rashed Khalifa Bumeqairaa Almansoori. Conceptual structural-logical model of focal digital information and communication support for enterprise development and operations. *Contemporary managerial and socio-economic aspects of the development of the state, regions and economic entities in the context of public administration transformation :* Proceedings of the International Scientific Conference, 14 November 2024, Odesa, Ukraine. P. 110-112. URL: https://economics.net.ua/files/science/admin_men/2024/tezy24.pdf. (Date of access: 15.12.2024) *(0,15 printed sheet, personal contribution: description of the advantages of focused digital information and communication support for*

enterprise development in crisis conditions – 0,1 printed sheet).

8. Ali Rashed Khalifa Bumeqairaa Almansoori. External crisis factors and their impact on the digital infrastructure of enterprises. *Accounting and analytical support for the innovative transformation of Ukraine's economy (under martial law and in the post-war period))* : Materials of the All-Ukrainian Scientific and Practical Conference. 24 November 2024, Odesa, Ukraine. P. 170-172. URL: https://economics.net.ua/files/science/oblik/2024/Tezy.pdf. (Date of access: 15.01.2025) (*0,15 printed sheet*).

9. Ali Rashed Khalifa Bumeqairaa Almansoori. Architecture and key elements of digital information and communication support for enterprise development. *Contemporary managerial and socio-economic aspects of the development of the state, regions and economic entities in the context of public administration transformation :* Proceedings of the International Scientific Conference, 14 November 2025, Odesa, Ukraine. P. 55-57. URL: https://economics.net.ua/publ. (Date of access: 17.11.2025) (*0,15 printed sheet*).

10. Tkach K.I., Ali Rashed Khalifa Bumeqairaa Almansoori. International practice in responding to external crisis impacts on setting priorities for investment in digital technologies and modernisation of digital infrastructure: UAE case studies. *Accounting and analytical support for the innovative transformation of Ukraine's economy (under martial law and in the post-war period)* : Materials of the All-Ukrainian Scientific and Practical Conference, 24 November 2025, Odesa, Ukraine. P. 72-74. URL: https://economics.net.ua/oaz. (Date of access: 15.01.2025) *(0,15 ð.a., personal contribution: systematisation of UAE investment cases in the field of digital technologies (0,1 printed sheet).*

11. Ali Rashed Khalifa Bumeqairaa Almansoori. Management challenges and transformations in the management system for the effective implementation of digital tools. *Economic cybernetics: theory, practice and directions of development* : Materials of the international scientific and practical conference, 27–28 November 2025, Odesa, Ukraine. P. 280-286. URL: https://economics.net.ua/files/science/ek_kiber/2025/tezy25.pdf (Date of access: 01.12.2025) *(0,1 printed sheet)*

ЗМІСТ

ВСТУП

Актуальність теми. Поглиблення кризових процесів у світовій та національних економіках супроводжується зростанням нестабільності ринкового середовища, порушенням ланцюгів створення вартості, підвищенням операційних і кіберризиків, а також необхідністю забезпечення безперервності розвитку і функціонування підприємств. У таких умовах цифрові інфокомунікаційні ресурси перетворюються з допоміжного інструменту на ключовий фактор управління підприємством, що забезпечує швидкість обміну інформацією, координацію управлінських рішень, адаптивність бізнес-процесів та стійкість до зовнішніх шоків. Проте на практиці цифровізація діяльності підприємств часто має фрагментарний і реактивний характер, що знижує її ефективність і не дозволяє повною мірою реалізувати потенціал цифрових інфокомунікаційних рішень у подоланні кризових викликів.

Це обумовлює необхідність переходу від точкових цифрових ініціатив до системного управління цифровими інфокомунікаційними ресурсами як цілісною управлінською підсистемою розвитку підприємства. Саме інтеграція цифрових технологій, комунікаційних платформ, аналітики даних і кібербезпекових механізмів створює передумови для підвищення цифрової стійкості, адаптивності та конкурентоспроможності підприємств у кризових умовах. Водночас недостатня розробленість теоретичних і методичних підходів до оцінювання та управління цифровими інфокомунікаційними ресурсами з позицій системного підходу зумовлює потребу в науковому обґрунтуванні відповідних управлінських моделей і механізмів, що й визначає актуальність обраної теми дослідження.

У наукових працях попередників достатньо ґрунтовно опрацьовано питання цифрової трансформації підприємств, розвитку інформаційно-комунікаційних технологій, цифровізації бізнес-процесів, впливу цифрових

платформ на ефективність управління, проблематику цифрової зрілості та використання даних у прийнятті управлінських рішень. Значна увага приділялася ролі ІКТ у підвищенні продуктивності, конкурентоспроможності та інноваційної активності підприємств, формуванню цифрових компетентностей персоналу, впровадженню хмарних сервісів, аналітики та штучного інтелекту. Окремі дослідження зосереджені на питаннях антикризового управління, ризик-менеджменту, цифрової безпеки та забезпечення безперервності бізнесу в умовах економічної нестабільності.

Водночас низка питань залишається недостатньо опрацьованою. Зокрема, бракує комплексних досліджень, у яких цифрові інфокомунікаційні ресурси розглядалися б не фрагментарно, а як цілісна система управління розвитком підприємства в умовах криз. Недостатньо розробленими залишаються методичні підходи до інтегрованого управління цифровими інфокомунікаційними ресурсами з урахуванням проактивного ризик-менеджменту, адаптивності цифрової архітектури та синергії технологічних, комунікаційних і кібербезпекових компонентів. Обмежено представлено інструментарій оцінювання ефективності використання таких ресурсів з позицій цифрової стійкості, безперервності та адаптивності діяльності підприємства, що зумовлює необхідність подальших наукових розвідок у цьому напрямі. Враховуючи це й було обрано тему, сформульовано мету, завдання, предмет, визначено структуру та напрями дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано у відповідності до планів науково-дослідних робіт Національного університету «Одеська політехніка» у 2021-2024 рр., а саме: № 155-71 «Менеджмент як фактор сталого розвитку в координатах парадигми економічних систем» (номер державної реєстрації 0118U006802, 2018-2022 рр.), де автором досліджено теоретичні підходи та моделі впливу цифрових ресурсів на розвиток і стійкість підприємства; НДР № 233-71 «Стратегічні імперативи менеджменту організацій в умовах глобалізаційних ризиків та кризових явищ» (номер державної реєстрації 0123U101755), 2023-

2026 рр., де автором розроблено концептуальну модель фокусного інфокомунікаційного цифрового забезпечення розвитку підприємства; розроблено рекомендації щодо оцінювання інфокомунікаційних цифрових рішень підприємства, обґрунтовано науково-методичні засади формування інфокомунікаційної цифрової стратегії підприємства з урахуванням кризових умов; госпдоговірній НДР № 1847-81 «Діджитал-трансформація системи управління виробничого бізнесу: проблеми, перспективи, фактори адаптивності» (27.10.2021-27.10.2022 р.), де автором проаналізовано зовнішні кризові фактори та їх вплив на цифрову інфраструктуру підприємства.

Дисертант приймав участь в НДР як співвиконавець (акт впровадження №1950/67-07 від 05.12.2025 р.).

Мета і задачі дослідження. Мета дослідження полягає у розробленні та обґрунтуванні теоретичних і науково-методичних підходів до використання цифрових інфокомунікаційних ресурсів забезпечення розвитку підприємства в умовах криз на засадах системного підходу.

Досягнення мети роботи зумовило вирішення таких *завдань*:

– визначити сутність, класифікацію, еволюцію, а також обґрунтувати теоретичні підходи та моделі впливу цифрових інфокомунікаційних ресурсів на розвиток і стійкість підприємства в умовах кризових викликів;

– дослідити зовнішні кризові фактори та обгрунтувати їхній вплив на функціонування цифрової інфраструктури підприємств;

– здійснити діагностику рівня цифрової зрілості та інфокомунікаційних ресурсів підприємства і оцінити результативність їх застосування для забезпечення розвитку та стійкості в аналітичному розрізі;

– розробити концептуальну модель фокусного цифрового інфокомунікаційного забезпечення;

– сформувати науково-методичні засади побудови цифрової інфокомунікаційної стратегії підприємства з урахуванням кризових умов;

– обґрунтувати методичний підхід та розробити багатовимірну методику оцінювання результативності та цифрової стійкості

інфокомунікаційних цифрових рішень.

Об'єктом дослідження є процес використання цифрових інфокомунікаційних ресурсів забезпечення розвитку підприємства в умовах криз. *Предметом дослідження* є теоретико-методичні та прикладні засади системного інфокомунікаціного цифрового забезпечення розвитку підприємства в умовах криз та його інструментарію.

Методи дослідження. Поставлені завдання у дисертації вирішено за допомогою таких *методів дослідження як*: *систематизації, монографічний, контент-аналіз* – для характеристики сутності інфокомунікаційних цифрових ресурсів, особливості формування інфокомунікаційної інфраструктури підприємства в умовах кризових викликів*; хронологічного аналізу, типологізації* – для класифікації та опису еволюції інфокомунікаційних цифрових ресурсів, моделей їх впливу на розвиток і стійкість підприємства; *структурно-функціонального та системного аналізу* – для виокремлення ключових вимірів цифрової зрілості та дослідження їх взаємодії в системі управління підприємством; *порівняльного аналізу* – для зіставлення рівнів цифрової зрілості підприємств різних галузей і країн; *експертних оцінок та індикаторного аналізу* – для формування системи субіндикаторів і шкал оцінювання цифрових інфокомунікаційних ресурсів; *індексного та багатокритеріального аналізу* – для розрахунку інтегрального показника цифрової зрілості; *групування, типологізації, case study* – для класифікації підприємств за рівнями цифрової зрілості, аналізу практичних прикладів; *матричного та heatmap-аналізу* – для візуалізації результатів оцінювання та виявлення критичних зон цифрової вразливості; *системного підходу, логіко-функціонального та процесного моделювання* – для розробки архітектури та механізмів управління цифровими інфокомунікаційними ресурсами підприємства; *узагальнення та логічної структуризації* – для побудови загальної структури та формування висновків.

Інформаційну базу цього дослідження склали наукові публікації з проблем цифрової трансформації, управління підприємствами та

інфокомунікаційного розвитку, дані підприємств (які не є їх комерційною таємницею), статистичні дані міжнародних і національних організацій, аналітичні звіти міжнародних консалтингових та експертних інституцій, матеріали профільних міністерств і державних органів, результати спеціалізованих галузевих досліджень, результати експертних оцінок, аналітичні матеріали професійних цифрових платформ, звіти щодо цифрової зрілості та цифрової стійкості підприємств, власні розрахунки і узагальнення.

Наукова новизна одержаних результатів полягає у розробленні та обґрунтуванні теоретико-методичних підходів і рекомендацій щодо управління інфокомунікаційними цифровими ресурсами підприємства в умовах криз за рахунок системного інфокомунікаційного забезпечення його розвитку. Найбільш вагомі наукові результати, щовиносяться на захист та становлять наукову новизну, такі:

удосконалено:

– *сутнісне визначення поняття цифрових інфокомунікаційних ресурсів підприємства,* яке, на відміну від існуючих: а) розглядає їх як інтегровану соціотехнічну систему, що функціонально поєднує п'ять ключових елементів (інформаційні, комунікаційні, технологічні, інфраструктурні та кібербезпекові ресурси); б) акцентує на їхній ролі як стратегічного активу та критичного фактора не лише інноваційного розвитку, а й забезпечення цифрової стійкості (Digital Resilience) підприємства в умовах кризових викликів;

– *науково-методичні підвалини побудови цифрової інфокомунікаційної стратегії підприємства з урахуванням кризових умов*, відмінністю яких є: а) визначення стратегічних векторів цифрової трансформації обгрунтування, класифікація і контурне картографування яких виокремлюють комунікаційно-кооперaційний блок як самостійний стратегічний вимір поряд із технологічним та організаційно-управлінським, фокусуються на інфокомунікаційних цифрових ресурсах як інтегрувальному чиннику розвитку підприємства в умовах криз; б) оцінюванням та ризик-профілем цифрових механізмів антикризового управління; в) матрицею пріоритетів

інвестування в інфокомунікаційні цифрові технології для різних рівнів доступності капіталу, розміру підприємств; г) рекомендаціями щодо алгоритмичного проєктування інфокомунікаційної цифрової системи підприємства;

– *концептуальну модель цифрового інфокомунікаційного забезпечення розвитку підприємства,* яка відрізняється від інших фокусністю управління цифровими інфокомунікаційними ресурсами підприємства, що забезпечує їх цільову інтеграцію в систему управління розвитком на засадах цифрової стійкості, адаптивної архітектури та проактивного антикризового реагування;

– *методичні підходи та аналітичний інструментарій оцінювання оцінювання результативності та цифрової стійкості інфокомунікаційних цифрових рішень*, відмінністю яких є: а) *критеріально-орієнтований добір інструментів,* застосовних для формування організаційних (скорочення часу, автоматизація, безпека) та антикризових (стійкість, безперервність, адаптивність) ефектів; б) *рекомендації щодо оцінювання цифрових ресурсів підприємства* у складі політики оцінювання цифрових ресурсів, механізмів моніторингу й оцінювання інфокомунікаційних цифрових рішень, компетентностей персоналу; в) *інтеграції критеріїв стійкості, безперервності та адаптивності з аналітичними інструментами,* що охоплюють часову ефективність, автоматизацію, кіберзахист, операційну стабільність та ризики; г) *методичний підхід і методика паспортизації цифрових решень та інструментів* для методів оцінювання інфокомунікаційних цифрових рішень*;*

дістало подальшого розвитку:

– *теоретичне обґрунтування впливу цифрових ресурсів на стійкість підприємства через систематизацію та конкретизацію смарт-моделей управління та їх антикризових функцій*, відмінністю якого є акцент на формуванні цифрових інфокомунікаціних ресурсів підприємства як системоутворюючого елемента антикризового управління, що забезпечує проактивне виявлення загроз, координацію дій та аналітичну підтримку

рішень, мінімізуючи багатовимірні (технологічні, кібернетичні та організаційні) ризики, характерні для кризових періодів;

– *об'єкти та напрями дослідження цифрових характеристик розвитку підприємства*, які доповнено*: а) зовнішніми кризовими факторами, що формують загальноекономічний, політичний, техногенний, кібернетичний та соціальний тиск* на діяльність підприємств та функціонування їх цифрової інфраструктури; б) *діагностикою на макро- і мікрорівнях рівня цифрової зрілості та інфокомунікаційних ресурсів підприємства за ключовими вимірами* (процеси, технології, дані, персонал, управління); в) *оцінюванням цифрової зрілості* для пошуку критичних зон цифрової вразливості; г) *використанням інтегрального індексу цифрової зрілості* як інструменту аналітичного моніторингу та результативності антикризового управління.

Практичне значення одержаних результатів полягає в розробленні комплексу науково обґрунтованих і методично завершених рекомендацій щодо системного інфокомунікаційного забезпечення розвитку підприємства в умовах криз. Рекомендації щодо проєктування інфокомунікаційної цифрової системи підприємства, методику паспортизації цифрових решень та інструментів для методів оцінювання інфокомунікаційних цифрових рішень впроваджено ТОВ «ФК «Герц»» (довідка № 25/12-23/02 від 23.12.2025 р.), а багатовимірну методику з рекомендаціями щодо оцінювання результативності та цифрової стійкості інфокомунікаційних цифрових рішень, критеріально-орієнтований добір інструментів, застосовних для формування організаційних (скорочення часу, автоматизація, безпека) та антикризових (стійкість, безперервність, адаптивність) ефектів – ТОВ «Герц» (довідка № 25/12-23/02 від 23.12.2025 р.), дозволяючи удосконалити систему управління.

Теоретичні та аналітичні результати дослідження використано в навчальному процесі Національного університету «Одеська політехніка» МОН України при підготовці навчально-методичних матеріалів з дисциплін «Інфокомунікації в освіті, науці і бізнесу» та «Наукові дослідження в сфері менеджменту» (акт впровадження №1951/67-07 від 05.12.2025 р.).

Особистий внесок здобувача. Дисертація є самостійно виконаною науковою працею, де викладено авторський підхід до трансформації інфокомунікаційних цифрових ресурсів у системне інфокомунікаційне забезпечення розвитку підприємства в умовах криз. Всі наукові результати, викладені в дисертації, одержано автором особисто. З наукових публікацій, виданих в співавторстві, у роботі використані лише положення, що складають його індивідуальний внесок, зазначений у переліку публікацій автора.

Апробація результатів дослідження. Основні результати досліджень представлено на 7 міжнародних і всеукраїнських конференціях: Міжнародній науково-практичній конференції «Економічна кібернетика: теорія, практика та напрямки розвитку» (м. Одеса, 2022, 2025), XII Міжнародній науково-практичній конференції «Актуальні проблеми теорії та практики менеджменту» (м. Одеса, 2023), Міжнародній науковій конференції «Сучасні управлінські та соціально-економічні аспекти розвитку держави, регіонів та суб´єктів господарювання в умовах трансформації публічного управління» (м. Одеса, 2024, 2025), XVIII, XIX Всеукраїнській науково-практичній конференції «Обліково-аналітичне забезпечення інноваційної трансформації економіки України (в умовах воєнного стану та поствоєнний період» (м. Одеса, 2024, 2025).

Публікації. За результатами досліджень опубліковано 11 наукових праць: 4 статті у наукових фахових виданнях України, що включені у міжнародні наукометричні бази; 7 тез доповідей на наукових конференціях. Загальний обсяг публікацій складає 5,45 д.а., з яких 4,35 д.а. належать особисто автору.

Структура і обсяг роботи. Дисертація складається з анотації, вступу, трьох розділів і висновків, списку використаних джерел з 171 найменувань – на 19 сторінках, 3 додатків – на 30 сторінках. Повний обсяг дисертації – 264 сторінки, з них 199 сторінки основного тексту. Дисертація містить 34 рисунки, з яких 3 займають повну сторінку, 42 таблиці, з яких 4 займають повну сторінку.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ ЦИФРОВИХ ІНФОКОМУНІКАЦІЙНИХ РЕСУРСІВ ПІДПРИЄМСТВА

1.1 Сутність, класифікація та еволюція інфокомунікаційних цифрових ресурсів

Для розкриття сутності, класифікації та еволюції інфокомунікаційних цифрових ресурсів як сучасного інструментарію забезпечення розвитку підприємств, доцільно виокремити *такі ключові положення:*

– *сутність інфокомунікаційних цифрових ресурсів*, що визначає їх як сукупність технологічних, інформаційних та комунікаційних засобів, які забезпечують створення, оброблення, передавання, зберігання та використання даних для підтримки управлінських, виробничих і сервісних процесів підприємства;

– *класифікація інфокомунікаційних цифрових ресурсів*, яка включає: а) інформаційні ресурси, б) комунікаційні ресурси, в) технологічні ресурси, г) інфраструктурні ресурси, д) кібербезпекові ресурси;

– *еволюція інфокомунікаційних цифрових ресурсів*, яка проявляється у переході від локальних інформаційно-обчислювальних систем до інтегрованих цифрових екосистем.

А. Сутність інфокомунікаційних цифрових ресурсів. У сучасних умовах цифрової трансформації підприємства ключового значення набувають інфокомунікаційні цифрові ресурси, що формують основу функціонування технологічно орієнтованого бізнес-середовища. Вони забезпечують інтеграцію інформаційних потоків, підтримують безперервність управлінських процесів та підвищують ефективність взаємодії між усіма учасниками виробничо-економічної системи. Розвиток економічних систем

характеризується широким впровадженням цифрових технологій, які стали основою побудови нової моделі організації виробничих та управлінських процесів. Інформація, швидкість її обробки та ефективність комунікацій визначають конкурентоспроможність підприємств на глобальних ринках. У таких умовах особливого значення набувають інфокомунікаційні цифрові ресурси, що забезпечують повноцінну взаємодію між підрозділами, партнерами, стейкхолдерами та споживачами. Визначення їхньої сутності є принципово важливим, оскільки саме ці ресурси стають фундаментом для формування конкурентоспроможних бізнес-моделей, удосконалення сервісних операцій та впровадження інноваційних рішень.

Науковцями приділяється досить багато уваги питанню визначення сутності інфокомунікаційних цифрових ресурсів, що пояснюється стрімкою цифровізацією економічних процесів і трансформацією моделей функціонування підприємств. Так, О. Кузьмінова та Д. Ільїн підкреслюють, що ресурсна природа інформації проявляється у її корисності, можливості накопичення, повторного використання та інтеграції у процеси регулювання діяльності підприємства. При цьому автори додають, що «новий формат інформаційного розвитку сучасного суспільства розширив перелік джерел та канали розподілу управлінської інформації, вдосконалив технології її обробки та зберігання даних» [1, с. 61]. Такий підхід акцентує увагу на інструментальній стуності цифрових ресурсів та їх впливі на підвищення якості управлісньких рішень.

У дослідженні В. Мороза інформаційний ресурс розглядається як «системна єдність впорядкованої у межах певного носія (сховища, місця розташування тощо) інформації (знань) з середовищем її формування, накопичення та розвитку, а також засобами та технологіями її зберігання, використання та передачі» [2, с. 7]. Даний підхід актуалізує системний характер цифрових ресурсів, наголошуючи на тому, що їхня цінність формується через поєднання змістової й технологічної складових.

Суттєвий внесок у розуміння інфокомунікаційної складової зробили В. Шукліна та Р. Набока, які відзначають, що «інформаційні технології забезпечують перехід від рутинних до промислових методів і засобів роботи з даними і знаннями, в тому числі, в сфері управлінської діяльності, підвищуючи її раціональність та ефективність» [3, с. 90]. Дійсно, важливим є не лише використання окремих технологічних інструментів, а й створення цілісної системи, здатної забезпечувати безперервний рух інформації, інтеграцію бізнес-процесів та підтримку інноваційної діяльності. Їх системний характер та здатність інтегрувати різні джерела та типи даних визначають ключову роль розвитку суб'єктів господарювання.

Узагальнюючи думки українських науковців, відзначимо, що поєднання змістової складової (інформаційної) та технологічної природи даних являє собою інфокомунікаційні цифрові ресурси. *Інфокомунікаційні цифрові ресурси формують основу цифрової інфраструктури підприємства, забезпечуючи безперервність управлінських, виробничих і сервісних процесів*. *Їх ключова роль* полягає у здатності об'єднувати різнорідні дані, технології та канали комунікації в єдину структуровану систему, яка підтримує інноваційний розвиток, підвищує якість управлінських рішень та сприяє зміцненню конкурентоспроможності суб'єктів господарювання в умовах цифрової економіки.

На відміну від українських вчених, зарубіжні науковці розглядають поняття інформаційних ресурсів, комунікаційних технологій, узагальнюючи їх більш широкою категорією – *інформаційно-комунікаційні технології (далі – ІКТ),* які трактуються як інтегрована система технічних, програмних, мережевих і комунікаційних засобів, що забезпечують створення, оброблення, зберігання, передавання та використання інформації. Так, Al-Debei та Al-Lozi [4] наголошують, що ІКТ є системним ресурсом, здатним трансформувати організаційну структуру та інформаційну інфраструктуру підприємств, створюючи при цьому нові канали взаємодії та форми управління.

Науковцями [5] ІКТ розглядається як комплексний соціотехнічний ресурс, що змінює механізми досягнення економічних, соціальних і екологічних цілей. Автори підкреслюють, що сучасні інформаційні системи не можуть існувати без комунікаційних технологій, які виконують роль інфраструктури для циркуляції даних, що фактично відповідає сучасному розумінню інфокомунікаційних цифрових ресурсів як системи, що об'єднує контент, технології, платформи та канали взаємодії.

В свою чергу A. Bharadwaj [6] наголошує, що цифрові ресурси підприємства – це комбінація технологій, інфраструктури, управлінських компетенцій і організаційних процесів, які у сукупності забезпечують створення стійких конкурентних переваг. На відміну від базових інформаційних ресурсів, інфокомунікаціні ресурси науковець трактує як динамічні та стратегічні, здатні адаптуватися до змін зовнішнього середовища.

M. Porter та J. Heppelmann відзначають, що інформаційно-комунікаційні ресурси формують нову архітектуру підприємства в основі якої лежить інтеграція даних, сенсорних систем, аналітики та платформ обміну інформацією. Автори підкреслюють, що цифрові ресурси не існують окремо від бізнесу – вони створюють нові канали взаємодії та управлінські підходи [7].

P. Weill та J. Ross розглядають цифрові ресурси підприємства як частину ширшої цифрової архітектури, що включає інформаційні потоки, стандартизовані бізнес-процеси, мережеві платформи та механізми комунікації. На думку авторів, інфокомунікаційні ресурси – це основні елементи корпоративних цифрових платформ, які визначають здатність підприємства забезпечувати цілісність, швидкість та адаптивність управлінських рішень [8].

Науковці C. Zott та R. Amit [9] відзначають, що інформаційно-комунікаційні ресурси забезпечують організацію інформаційних потоків, обмін знаннями та синхронізацію операцій між структурними підрозділами, наголошуючи при цьому, що саме цифрові ресурси визначають можливість

підприємства ефективно функціонувати у мережевих екосистемах та впроваджувати інноваційні практики.

Узагальнюючи підходи зарубіжних науковців, відзначимо, що *інфокомунікаційні цифрові ресурси підприємства розглядаються як стратегічна та інтегрована категорія, що охоплює технологічні, комунікаційні та організаційні складові цифрового середовища*.

Інфокомунікаційні цифрові ресурси доцільно трактувати як системну категорію, що поєднує *три взаємозалежні складові*:

– інформаційні ресурси,

– комунікаційні ресурси,

– цифрові технологічні ресурси.

Їх інтеграція створює нову цифрову архітектуру підприємства, яка забезпечує підтримку управлінських, виробничих та інноваційних процесів.

У науковій літературі трапляються *різні підходи до визначення сутності цифрових ресурсів* як*:* цифрових активів, інформаційних систем, технологічних інструментів управління. Проте більшість визначень не враховують саме інфокомунікаційної складової, що забезпечує синергію між даними, комунікаціями та технологіями. Це дає підстави стверджувати, що формування цілісного уявлення про інфокомунікаційні ресурси потребує оновленого наукового підходу.

Тим самим базуючись на їх дослідженнях, *можна трактувати цифрові інфокомунікаційні ресурси підприємства* не як сукупність окремих технологічних інструментів, а як цілісну соціотехнічну систему, яка забезпечує інтеграцію даних, платформ, знань і бізнес-процесів. Їх системний характер, динамічність та здатність формувати нові моделі взаємодії визначають ключову роль у цифровій трансформації підприємств, підвищенні їх адаптивності та зміцненні конкурентоспроможності в умовах глобальної цифрової економіки. Все вище відзначене дає підстави для відображення сутності інфокомунікаційних цифрових ресурсів (рис. 1.1).

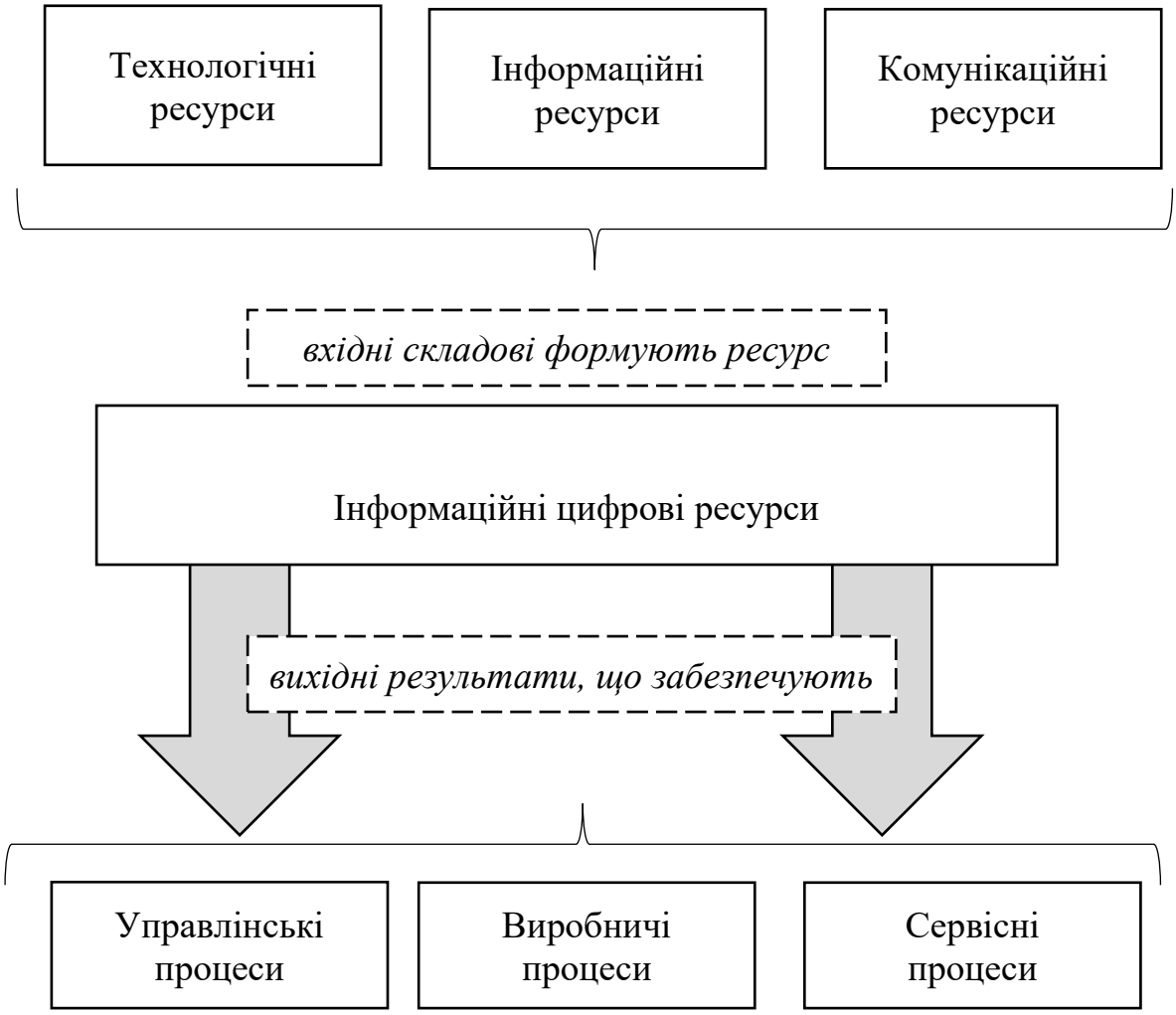


Рисунок 1.1 – Структурно-функціональна модель інфокомунікаційних цифрових ресурсів підприємства (*джерело: авторська розробка*)

Представлена на рис. 1.1 структурно-функціональна модель відображає системний характер інфокомунікаційних цифрових ресурсів підприємства, що формуються на основі взаємодії технологічних, інформаційних та комунікаційних складових. Вхідні елементи – інформаційні дані, технологічні компоненти та комунікаційні платформи – інтегруються в єдине цифрове середовище, яке забезпечує створення, оброблення, передавання та зберігання інформації. У результаті такої інтеграції інфокомунікаційні цифрові ресурси являються основою для підтримки ключових бізнес-процесів, зокрема управлінських, виробничих та сервісних, забезпечуючи їх цілісність, швидкість, адаптивність і ефективність.

Відтак, визначено, що *інфокомунікаційні цифрові ресурси підприємства* визначаються як інтегрований комплекс інформаційних потоків, цифрових даних, інструментів їх обробки, мережевих та комунікаційних платформ, цифрової інфраструктури та систем кіберзахисту, що забезпечують реалізацію управлінських, виробничих і сервісних процесів підприємства та сприяють його інноваційному розвитку.

Б. Класифікація інфокомунікаційних цифрових ресурсів, *яка включає: а) інформаційні ресурси, б) комунікаційні ресурси, в) технологічні ресурси, г) інфраструктурні ресурси, д) кібербезпекові ресурси.* Класифікація інфокомунікаційних цифрових ресурсів є ключовим елементом їх наукового розуміння, оскільки дає змогу структуровано представити різноманіття складових, що забезпечують функціонування цифрового середовища підприємства. Виокремлення основних груп інфокомунікаційних цифрових ресурсів створює підґрунтя для більш глибокого аналізу їх внутрішньої організації та взаємозв'язків. Адже класифікація окреслює складові цього середовища на концептуальному рівні, що дозволить не лише систематизувати ресурси, але й оцінити ступінь їх інтегрованості, збалансованості та впливу на загальну ефективність цифрової інфраструктури. Зарубіжними науковцями структура інфокомунікаційних цифрових ресурсів розглядається *з трьох основних підходів*:

– динамічних цифрових можливостей, в якому науковці [10-14] розглядають інфокомунікаційні цифрові ресурси як здатність підприємства використовувати дані, технології та комунікаційні інструменти для адаптації, інновацій та формування конкурентних переваг;

– стратегічного узгодження та цифрової архітектури підприємства, в якому дослідники [15-19] визначають ключовим узгодженість структури інфокомунікаційних цифрових ресурсів та стратегії і бізнес-процесів підприємства;

– цифрових екосистем та інтегрованої взаємодії, що розглядає структуру інфокомунікаційних цифрових ресурсів як елемент цифрової

екосистеми підприємства, у межах якої дані, платформи, технології, комунікаційні інструменти, алгоритми та зовнішні цифрові сервіси взаємодіють у єдиному середовищі [20-24].

Також варто відзначити, що деякі зарубіжні науковці розглядають структуру інфокомунікаційних цифрових ресурсів підприємств *через архітектурний, інфраструктурний та соціотехнічний підходи,* що дозволяє формувати цілісне уявлення про їх внутрішню організацію.

Так, Т. Iyamu [25] пропонує підхід до розроблення та впровадження технічної архітектури підприємства, у межах якого інфокомунікаційні ресурси постають як система взаємопов'язаних апаратних, програмних і мережевих елементів. Автор підкреслює, що структурованість ІКТ-середовища є передумовою його узгодженості з бізнес-процесами та основою для цифрової модернізації підприємства. Подібного підходу дотримується також A. Widjajarto [26] разом з колективом дослідників, які описують інфокомунікаційні ресурси як інфраструктурні сервіси, згруповані за функціональним призначенням та рівнем підтримки операційної діяльності.

У роботі [27] авторами продемонстровано, що структура інфокомунікаційних ресурсів повинна включати декілька взаємопов'язаних рівнів: інформаційний, технологічний, системний та інфраструктурний, що забезпечує узгодженість між даними, інформаційними потоками, технологіями їх обробки та інструментами комунікації. Емпіричні дослідження, зокрема робоит Van de Wetering R. [28], підтверджують, що структурована та динамічна архітектура цифрових ресурсів зумовлює інноваційність бізнес-процесів і підвищує здатність підприємства адаптуватися до змін зовнішнього середовища.

У контексті цифрової трансформації організації показовим є результати дослідження авторів [29], які розробили модель розподіленої цифрової корпоративної архітектури для освітніх організацій, спираючись на підходи Togaf, Zachman та Federal Enterprise Architecture Framework. Запропонована структура охоплює низку взаємопов'язаних вимірів: бізнес-архітектуру,

архітектуру даних, прикладну, технологічну, інфраструктурну, архітектурну безпеки та людського капіталу, а також блок корпоративного управління, що у сукупності формують цілісну цифрову систему організації. Такий підхід демонструє, що інфокомунікаційні цифрові ресурси доцільно розглядати як багаторівневу архітектуру, у межах якої поєднуються інформаційні потоки, прикладні платформи, технологічна та мережна інфраструктура, механізми кібербезпеки й управлінські та кадрові компоненти, інтегровані в єдиному цифровому середовищі організації.

Відтак, проведений аналіз зарубіжних праць свідчить, що *структура інфокомунікаційних цифрових ресурсів підприємства формується як ієрархічна система,* що складається з інформаційних, технологічних, комунікаційних, інфраструктурних та ресурси цифрової безпеки (рис. 1.2). Їх узгоджена взаємодія забезпечує цілісність цифрового середовища підприємства, підтримує оброблення та рух даних, уможливлює інтеграцію бізнес-процесів і створює підґрунтя для інноваційного розвитку в умовах цифрової економіки.

Представлена структура інфокомунікаційних цифрових ресурсів підприємства містить *п'ять ключових груп,* які відображають їхню функціональне призначення у забезпеченні цифрової діяльності підприємства.

До першої групи віднесено *інформаційні ресурси* (далі – IR), які включають корпоративні бази даних, знань, інформацію про клієнтів, партнерів, постачальників, ринково-аналітичні дані та систему електронного документообігу. Ці ресурси становлять змістову основу цифрового середовища, забезпечуючи наявність структурованих даних для управлінських і операційних процесів. *Інфраструктурні ресурси* (далі – ISR) формують технічну платформу функціонування цифрових систем: хмарні середовища, сервери, дата-центри, мережеве обладнання, канали передавання даних, а також рішення для віртуалізації та контейнеризації. Саме вони визначають продуктивність, масштабованість і стабільність цифрової інфраструктури підприємства.

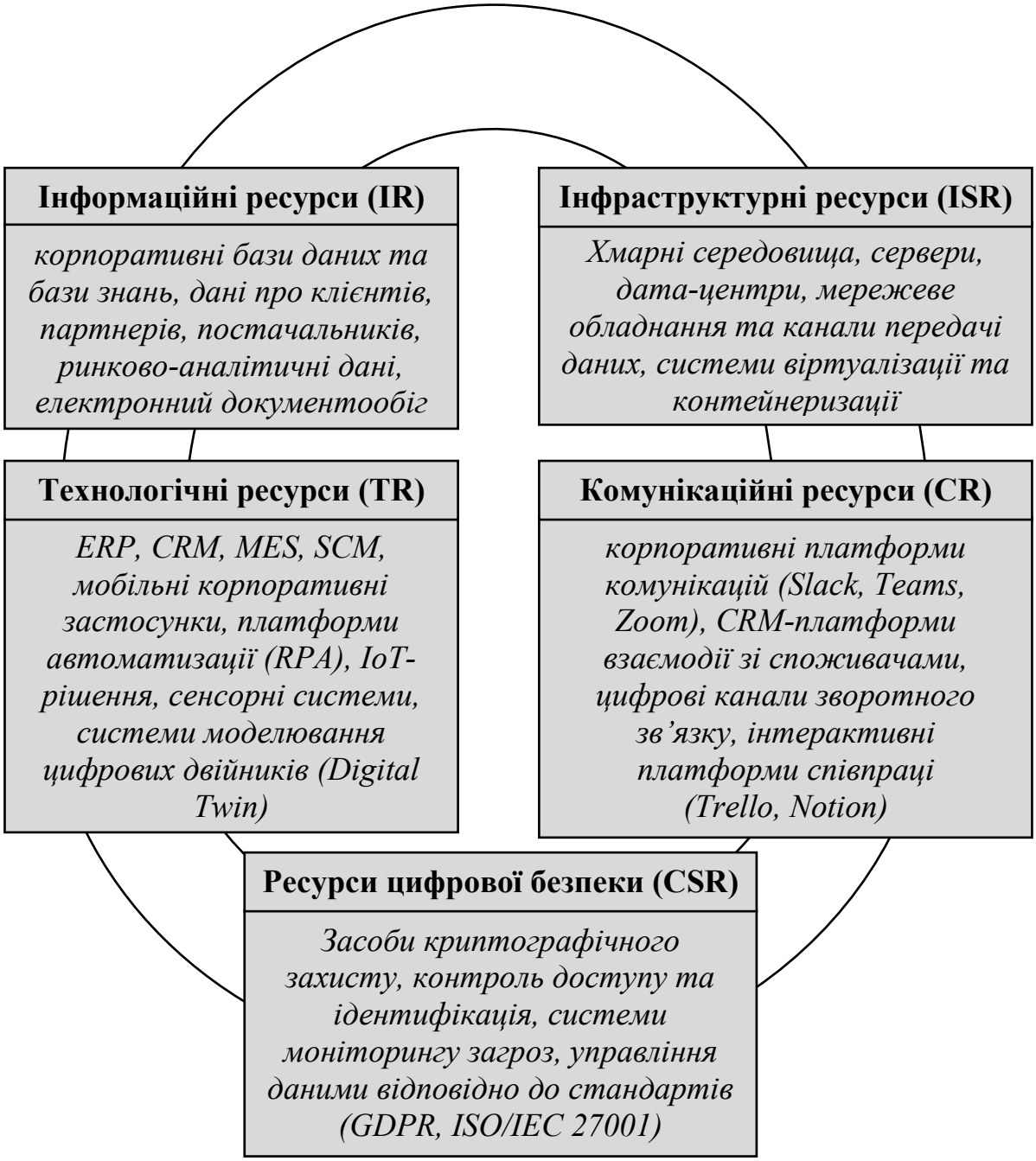


Рисунок 1.2 – Структура інфокомунікаційних цифрових ресурсів

(джерело: авторська розробка)

Технологічні ресурси (далі – TR) охоплюють набір корпоративних інформаційних систем та інструментів автоматизації бізнес-процесів: ERP, CRM, MES, SCM, мобільні застосунки, RPA-рішення, IoT-системи, сенсори, а також технології моделювання цифрових двійників (Digital Twin). Дані ресурси забезпечують операційну цифровізацію, підвищують точність

управління і дозволяють підприємству використовувати дані в режимі реального часу.

Комунікаційні ресурси (далі – CR) об'єднують платформи корпоративної комунікації (Slack, Teams, Zoom), CRM-системи взаємодії зі споживачами, цифрові канали зворотного зв'язку та інтерактивні платформи командної співпраці (Trello, Notion). Вони забезпечують швидку та безперебійну комунікацію між працівниками, клієнтами та партнерами, підтримуючи координацію та прозорість бізнес-процесів. Важливою складовою структури є ресурси цифрової безпеки (CSR), які включають засоби криптографічного захисту, системи контролю доступу й ідентифікації, інструменти моніторингу загроз, системи контролю доступу й ідентифікації, інструменти моніторингу загроз та управління даними відповідно до міжнародних стандартів (GDRP, ISO/IEC 27001). Вони забезпечують захист інформаційних активів підприємства, цілісність даних і надійність функціонування цифрового середовища.

Тим самим *взаємозв'язок всіх п'яти груп ресурсів формує цілісну інфокомунікаційну систему підприємства*, яка забезпечує підтримку управлінських, виробничих та сервісних процесів, сприяючи підвищенню ефективності та інноваційної діяльності. В той же час кожна група ресурсів спрямована на реалізацію певних функцій, що разом формують цілісний механізм підтримки бізнес-процесів (табл. 1.1).

Таблиця 1.1 – Функції інфокомунікаційних цифрових ресурсів підприємства (*джерело: побудовано автором на підставі [32-35]*)

Функція	Зміст функції	Основні ресурси	Приклади інструментів
1	2	3	4
1.Забезпечення ефективності комунікації	Формування внутрішніх та зовнішніх каналів взаємодії, швидкий обмін інформацією	CR, ISR	Slack, Microsoft Teams, Zoom, корпоративна пошта, системи ticketing-сервісів (Jira Service Desk)

Продовження таблиці 1.1

1	2	3	4
2. Підтримка управлінських рішень	Надання актуальних даних, аналітика, цифровий моніторинг діяльності	IR, TR	Power BI, Tableau, SAP BI, CRM-аналітика, корпоративні дашборди, ERP-звіти
3. Оптимізація бізнес-процесів	Автоматизація рутинних операцій, роботизація, цифрові робочі місця	TR, ISR	ERP (SAP, Oracle), RPA (UiPath), MES-системи, SCM-системи, цифрові форми та workflow (Camunda), корпоративні мобільні застосунки
4. Підсилення інноваційної активності	Створення цифрових продуктів, гнучкі сервіси, моделювання цифрових двійників	TR, IR	Digital Twin (Siemens, Dassault), платформи прототипування (Figma), IoT-платформи (Azure IoT), хмарні середовища для розробки (AWS, GCP)
5. Підвищення конкуренто-спроможності	Розширення цифрових каналів збуту, пришвидшення реакції на ринок, покращення взаємодії із клієнтом	CR, TR	CRM (Salesforce, HubSpot), e-commerce платформи (Shopify), чат-боти, Omnichannel-платформи, системи маркетингової автоматизації
6.Забезпечення інформаційної безпеки	Захист інформації, управління доступом, відповідність стандартам, моніторинг загроз	CR, ISR	SIEM-системи (Splunk, IBM, Qradar), системи контролю доступу (Okta), MFA, антивірусні платформи, шифрування, політики GDPR, ISO/IEC 27001

Узагальнення представлених функцій інфокомунікаційних цифрових ресурсів свідчить, що вони охоплюють широке коло завдань: від забезпечення безперебійної комунікації до оптимізації операційної діяльності. Розгляд цих функцій підтверджує, що *цифрові ресурси підприємства є не ізольованими елементами, а цілісною інтегрованою системою,* ефективність якої визначається узгодженою взаємодією інформаційних, технологічних,

комунікаційних, інфраструктурних і безпекових компонентів. Саме комплексне бачення ролі інфокомунікаційних цифрових ресурсів створює необхідне підґрунтя для їх систематизації. Тим самим все вище відзначене є основою побудови їх класифікації (табл. 1.2).

Таблиця 1.2 – Класифікація інфокомунікаційних цифрових ресурсів (*джерело: авторська розробка*)

Група	Характеристики
1	2
1. За функціональним призначенням	
1.1 Інформаційні ресурси	Дані, знання, аналітичні масиви, бази даних
1.2 Комунікаційні ресурси	Платформи взаємодії, канали цифрової комунікації
1.3 Технологічні ресурси	Програмні системи, цифрові інструменти, IoT-модулі
1.4 Інфраструктурні ресурси	Сервери, мережі, хмарні платформи, центри обробки даних
1.5 Кібербезпекові ресурси	Засоби захисту даних, управління доступом, моніторинг загроз
2. За рівнем формування цифрового середовища	
2.1 Рівень даних	Джерела даних, сховища, структуровані/ неструктуровані набори
2.2 Прикладний рівень	ERP, CRM, SCM, MES, BI-системи
2.3 Технологічний рівень	API, middleware, інструменти інтеграції
2.4 Інфраструктурний рівень	Хмарні сервіси, мережеві технології, сервісні системи
2.5 Рівень безпеки	Політики, криптографія, інструменти контролю доступу
2.6 Організаційний рівень	Процеси управління, людський капітал, корпоративні стандарти
3. За джерелом походження	
3.1 Внутрішні ресурси	Сформовані в межах підприємства (внутрішні бази даних, власні IT-системи, внутрішні канали комунікації)
3.2 Зовнішні ресурси	Отримані від зовнішніх контрагентів або платформ (хмарні сервіси, партнерські API, дані маркетингових досліджень, цифрові платформи взаємодії)
4. За ступенем інтегрованості	
4.1 Автономні ресурси	Використовуються окремо (локальні програми, окремі пристрої)

Продовження таблиці 1.2

1	2
4.2 Інтегровані ресурси	Взаємодіють через спільні платформи чи інтерфейси (ERP-модулі, CRM-інтеграції)
4.3 Екосистемні ресурси	Є частиною більш широкої цифрової екосистеми (API-економіка, IoT-мережі, хмарні екосистеми AWS/Azure/Google Cloud)
5. За типом оброблення інформації	
5.1 Ресурси збору інформації	Сенсори, IoT-пристрої, сканери
5.2 Ресурси оброблення інформації	Аналітика, моделі AI/ML, BI-інструменти
5.3 Ресурси зберігання інформації	Бази даних, хмарні сховища
5.4 Ресурси передавання інформації	Мережі, комунікаційні платформи
5.5 Ресурси використання інформації	Інтерфейси користувачів, застосунки, цифрові робочі місця
6. За ступенем критичності для підприємства	
6.1 Стратегічні	Платформи управління, системи даних, кібербезпека
6.2 Операційні	Інструменти виконання щоденних процесів, системи автоматизації
7. За ступенем розміщення	
7.1 Локальні	On-premise
7.2 Хмарні	SaaS, PaaS, IaaS
7.3 Гібридні	Поєднання локальних та хмарних рішень
8. За ступенем стандартизації	
8.1 Стандартизовані	Відповідають міжнародним стандартам, інтегровані з корпоративними політиками
8.2 Гнучкі/ адаптивні	Модульні, кастомізовані
8.3 Інноваційні/ експериментальні	Пілотні рішення на основі AI, IoT, blockchain

Представлена класифікація *(див. табл. 1.2)* дає змогу системно впорядкувати інфокомунікаційні цифрові ресурси та окреслити їх змістове, функціональне й технологічне наповнення. Вона демонструє, що *різні групи ресурсів відрізняються не лише за своїм призначенням чи способом використання, а й за рівнем інтегрованості, критичністю для підприємства, ступенем стандартизації та способом розміщення.* Все вище відзначене свідчить про розгалужений характер інфокомунікаційного забезпечення та

його здатність формувати складне цифрове середовище, яке постійно ускладнюється під впливом технологічних змін, зростання інформаційних потоків та підвищення вимог до безпеки й оперативності оброблення даних.

Відтак, структура і функціональне наповнення цифрових ресурсів не є статичними: вони змінюються разом із трансформацією бізнес-моделей і розвитком цифрових технологій.

В. Еволюція інфокомунікаційних цифрових ресурсів, яка проявляється у переході від локальних інформаційно-обчислювальних систем до інтегрованих цифрових екосистем. Еволюція інфокомунікаційних цифрових ресурсів є ключовим чинником трансформації сучасних підприємств, оскільки визначає характер їхнього інформаційного забезпечення, рівень технологічної зрілості та можливості інноваційного розвитку. Зміна підходів до організації цифрового середовища підприємства відбувалася поступово, відображаючи загальні тенденції розвитку інформаційних технологій, зростання обсягів даних, поширення мережевих комунікацій і потребу в інтеграції бізнес-процесів.

Дослідження науковців [36-38] зосереджені на тому, як підприємства проходять трансформаційний шлях від базового використання ІКТ до формування розвинених цифрових можливостей, що визначають їхню стратегічну гнучкість і здатність до інновацій. Автори підкреслюють, що еволюція цифрових ресурсів тісно пов’язана зі зміною ролі ІТ-підрозділів, посиленням їх функції як центру інновацій та управління даними, а також з розвитком цифрових компетенцій персоналу. Тим самим науковці розглядають цифрові ресурси не як технічні активи, а як стратегічні можливості, що формують нові бізнес-моделі та механізми організаційного оновлення.

В свою чергу вчені [39-41] пояснюють історичну траєкторію розвитку інформаційних систем від локальних інформаційно-обчислювальних рішень до інтегрованих корпоративних систем (ERP, CRM, SCM) та мережевих платформ. Основна увага приділяється тому, як зростання складності бізнес-

процесів і обсягів даних зумовлює потребу у все більш інтегрованих, взаємопов'язаних і масштабованих цифрових рішеннях. Еволюція інформаційних систем розглядається як поетапний процес, у якому відбувається уніфікація даних, стандартизація операцій та поступове впровадження хмарних технологій. Тим самим науковці визначають цифрові ресурси як основу корпоративної архітектури підприємства.

В наукових працях [42-43] автори вивчають перехід від технологічних платформ до комплексних цифрових екосистем та наголошують, що сучасні цифрові ресурси функціонують як комплексна система, яка поєднує інфраструктуру, дані, сервіси, аналітику та учасників взаємодії (споживачів, партнерів, розробників). Екосистемний підхід підкреслює взаємодію між внутрішніми й зовнішніми цифровими ресурсами, важливість відкритості та здатність системи до спільного створення цінності. У даному контексті еволюція цифрових ресурсів розглядається як перехід до мережевих, гнучких і масштабованих структур.

В той же час дослідники [44-46] демонструють, як цифрові технології зумовлюють зміну операційних процесів, моделей управління, сервісної взаємодії та організаційної культури підприємств. Автори доводять, що впровадження цифрових рішень (автоматизація, аналітика, цифрові сервіси) не лише оптимізує операційну діяльність, а й створює умови для переходу підприємства до екосистемної моделі розвитку. Відповідно цифрові ресурси трактуються як ключові каталізатори інновацій, здатні радикально підвищувати ефективність, швидкість та якість бізнес-процесів.

Узагальнення проведених наукових досліджень дає змогу встановити, що *еволюція інфокомунікаційних цифрових ресурсів є закономірним процесом, зумовленим зміною технологічної парадигми, ускладненням інформаційних потоків та зростанням ролі даних у забезпеченні конкурентоспроможності підприємств.* Науковці підкреслюють, що розвиток інфокомунікацій проходив кілька послідовних стадій: від локальних засобів фіксації та передачі інформації до появи електронних технологій, далі – до корпоративних

інформаційних систем і сучасних цифрових платформ, які формують цілісні екосистеми взаємодії.

Тим самим проведений аналіз свідчить, що сучасний стан інфокомунікаційних цифрових ресурсів підприємства варто розглядати в контексті їх історичного розвитку, оскільки саме попередні етапи визначили логіку інтеграції інформаційних технологій, телекомунікацій та цифрових сервісів у єдине середовище (рис. 1.3).

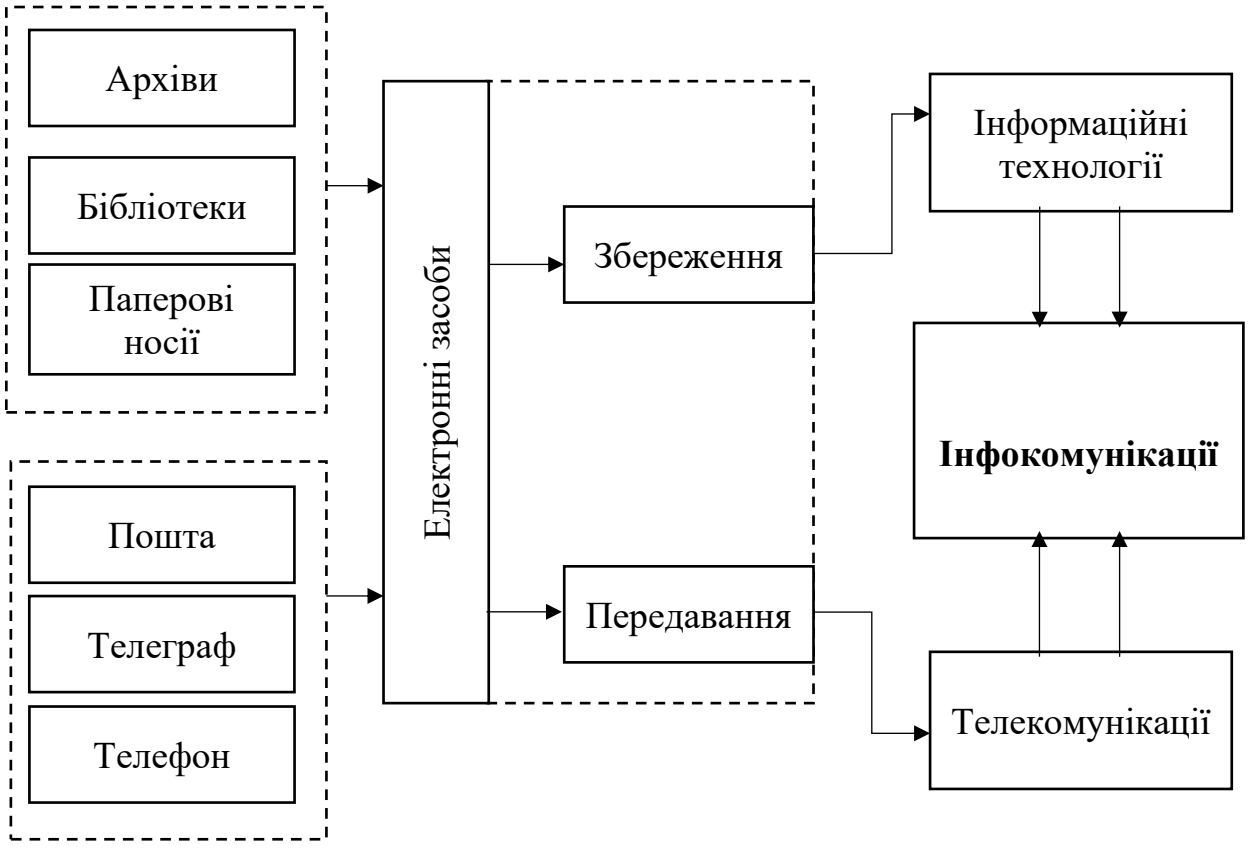


Рисунок 1.3 – Послідовність розвитку інфокомунікацій (*джерело: [47]*)

Відповідно рис. 1.3, відзначимо, що розвиток інфокомунікацій не є фрагментарним процесом, а відбувається за закономірною еволюційною послідовністю, у межах якої наступний етап розширює функціональні можливості попереднього.

Саме тому доцільним є систематизація основних фаз цієї еволюції (табл. 1.3).

Таблиця 1.3 – Еволюція інфокомунікаційних цифрових ресурсів (*джерело: систематизовано автором на підставі* [45-47])

Етап розвитку	Характеристики	Ключові ознаки	Роль для підприємства
1. Локальні інформаційно-обчислювальні системи	Ізольовані системи, які виконують окремі функції без взаємодії між собою	Відсутність інтеграції, обмеженість в обробленні інформації, локальне зберігання інформації	Автоматизація окремих операцій, зменшення ручної праці
2. Корпоративні інформаційні системи (ERP, CRM, SCM)	Базова інтеграція бізнес-процесів в межах підприємства	Спільні бази даних, уніфікація процесів, відносна масштабованість	Підтримка координації та централізованого управління
3. Мережеві та хмарні рішення	Перехід від локальних ресурсів до доступних з будь-якого місця цифрових платформ	Хмарні сховища, дистанційний доступ, гнучкість масштабування	Зростання мобільності та швидкості обміну інформацією
4. Інтегровані цифрові платформи	Об’єднання даних, систем та сервісів у єдиний цифровий простір	Взаємодія систем через API, аналітичні інструменти, підтримка багатьох бізнес-напрямів	Висока узгодженість та прозорість управління
5. Цифрові екосистеми підприємства	Комплексне середовище взаємодії даних, платформ, IoT, AI та інфраструктури	Розподілена архітектура, IoT, сенсорні мережі, аналітика, AI/ML, кіберзахист та інтегровані сервіси	Формування стратегічних компетенцій та інноваційного розвитку
6. Автономні інтелектуальні системи (перспективний етап)	Самонавчальні системи, здатні приймати рішення на основі великомасштабних даних	Штучний інтелект, автоматизоване управління, прогнозні моделі	Створення нових бізнес-моделей, зниження людського фактору

Відтак, можна узагальнити, що розвиток інфокомунікаційних цифрових ресурсів виходить далеко за межі технічного удосконалення інфраструктури. Цифрові ресурси стають міждисциплінарним феноменом, який одночасно охоплює технологічні, організаційні, управлінські та соціальні виміри функціонування підприємства. Ускладнення цифрового середовища, зростання ролі даних, інтелектуалізація процесів та інтеграція в екосистеми визначають нові вимоги до адаптивності, стійкості та здатності підприємства забезпечувати безперервність діяльності в умовах високої мінливості, що потребує визначення теоретичних підходів та моделей, які розкривають напрями впливу цифрових ресурсів на усі його бізнес-процеси.

1.2 Теоретичні підходи та моделі впливу цифрових ресурсів на розвиток і стійкість підприємства

Для розуміння ролі цифрових ресурсів у підвищенні конкурентоспроможності, адаптивності та довгострокової стійкості підприємства важливо розкрити зміст теоретичних підходів та моделей, що визначають механізми їх впливу на розвиток підприємства.

Узагальнення сучасних наукових напрацювань дозволяє *виокремити кілька ключових блоків, які формують основу цифрової трансформації та забезпечують здатність підприємства ефективно функціонувати в умовах турбулентності.* Це:

– діджиталізаційні та смарт-моделі управління, що розглядають цифрові ресурси як каталізатор удосконалення управлінських процесів, оптимізації операцій, підвищення точності управлінських рішень, а також формування інтелектуальних систем підтримки бізнесу (від автоматизації до впровадження штучного інтелекту);

– концепції цифрової стійкості (Digital Resilience), які акцентують увагу на здатності підприємства адаптуватися до криз, зберігати безперервність діяльності та оперативно відновлюватися завдяки наявності цифрових активів, захищених інформаційних систем, даних та інструментів кіберальянсу;

– інфокомунікаційні платформи як елемент антикризового менеджменту, що пояснюють використання корпоративних і міжорганізаційних цифрових середовищ для забезпечення координації, прозорості швидкого обміну даними, комунікації зі стейкхолдерами та підтримки прийняття рішень в умовах кризових ситуацій.

А. Діджиталізаційні та смарт-моделі управління. Для системного розкриття ролі інфокомунікаційних цифрових ресурсів у трансформації управлінських процесів важливо визначити підходи, у межах яких сучасні підприємства здійснюють перехід до технологічно орієнтованих моделей прийняття рішень. Це дасть змогу сформувати нову управлінську логіку, що ґрунтується на використанні даних, інтелектуальних алгоритмів та інтегрованих цифрових платформ, здатних забезпечити синхронізацію інформаційних потоків, автоматизацію рутинних операцій і підвищення точності стратегічного планування. Саме дані елементи визначають змістовну основу перетворень, які дозволяють підприємству діяти швидше, прозоріше й адаптивніше, а також формують умови для проактивного реагування на виклики сучасного ринкового середовища.

У сучасних дослідженнях менеджменту простежується інтенсивне формування теоретико-методичних підходів, які пояснюють вплив цифрових ресурсів на трансформацію моделей управління та підсилення стратегічної стійкості підприємства. Аналіз наукових праць [48-57] зарубіжних авторів дозволяє виокремити *три ключові напрями, що формують методологічну основу діджталізаційних та смарт-моделей управління*:

- концептуальне осмислення цифрової трансформації;
- механізми впливу цифрових ресурсів на розвиток підприємства;

– практичні реалізації смарт-моделей у виробничих і сервісних системах.

Перший напрям пов’язаний із концептуалізацією цифрової трансформації та бізнес-модельних інновацій. У своєму дослідженні науковці [48] розглядають цифровізацію як фундаментальну зміну логіки створення, передачі та привласнення цінності, що потребує перегляду архітектури бізнес-моделі та формування нових динамічних здібностей підприємства. Rachinger разом зі співавторами [49] підкреслюють, що вплив цифрових технологій реалізується через трансформацію ключових елементів бізнес-моделі – від пропозиції цінності до процесів створення результату. У дослідженні Tim і Leidner [50] подано концептуальну рамку цифрової резильєнтності, де цифрові ресурси, IT-архітектура та дані виступають основою організаційної здатності передбачати, витримувати, адаптуватися та відновлюватися по завершенню кризи. Сукупність цих робіт формує теоретичний базис для розуміння діджиталізаційних та смарт-моделей управління як сучасних управлінських конфігурацій, що інтегрують дані, аналітику та цифрову інфраструктуру в систему прийняття стратегічних рішень.

Другий напрям стосується механізмів, через які цифрові ресурси впливають на розвиток і стійкість підприємства. У дослідженні Mehedintu та Soava [52] обґрунтовано структурну модель цифрової стійкості, що формується на основі розвитку цифрового ядра, аналітичних компетенцій та внутрішніх інноваційних процесів. Winarsih, Indriastuti і Fuad [52] наголошують на ролі цифрових платформ, електронної комерції та цифрових компетенцій у забезпеченні життєздатності малого бізнесу за умов зовнішніх обмежень, доводячи, що цифрова трансформація слугує інструментом адаптації бізнес-моделі докризових умов. Емпіричні результати Gun [53] демонструють позитивний зв’язок цифрової трансформації з операційною та фінансовою результативністю підприємств, що зумовлюється розвитком організаційної гнучкості, підвищенням прозорості процесів та інтеграцією цифрових систем у контури управління.

Третій напрям присвячений практичним реалізаціям смарт-моделей управління, які інтегрують інфокомунікаційні цифрові ресурси виробничі та управлінські процеси. Zheng зі співавторами [54] розробляють концептуальну модель Smart manufacturing systems, яка базується на поєднанні IoT, кібер-фізичних систем і аналітики даних для моніторингу, оптимізації та автоматизації виробничих процесів у режимі реального часу. Parhi [55] пропонує модель показників результативності smart-виробництва, що поєднує цифрові технології з комплексною оцінкою продуктивності, гнучкості та інноваційної здатності підприємства. У роботах Badamasi, Xie та Kassem [56] і Kapoor [57] представлено підходи до формування цифрових двійників підприємства (Enterprise Digital Twin), які дозволяють моделювати операційні та стратегічні рішення, інтегруючи дані з різних підсистем у єдине цифрове середовище. Смарт-моделі управління в цих дослідженнях постають як інфокомунікаційні платформи, здатні забезпечити прогнозну аналітику, адаптивність та підвищення стратегічної стійкості підприємства.

Узагальнюючи результати аналізу, визначено, що зарубіжні дослідження демонструють *еволюцію від трактування цифровізації як технологічного інструмента до розуміння її як стратегічної управлінської категорії,* що визначає конфігурацію бізнес-моделі, якість управлінських рішень і рівень організаційної стійкості.

Діджиталізаційні та смарт-моделі управління, які сформувалися в межах сучасної наукової парадигми, демонструють, що цифрові ресурси інтегруються у всі рівні підприємства: від операційної діяльності до стратегічного планування та формування організаційної стійкості. Саме тому перехід до цифрово орієнтованих систем управління пов’язаний з появою нових організаційних тенденцій, що якісно відрізняють цифрові процеси від традиційних підходів. Так, Ю. Нікітін та О. Кульчицький відзначають, що цифровий від традиційних процесів відрізняють три такі тенденції [58] як:

– використання існуючих технологій для скорочення витрат, збору даних та забезпечення кращого досвіду роботи з клієнтами;

– прийняття концепції цифрової трансформації та необхідних культурних зрушень. Управління цифровими послугами може потребувати організаційної перебудови;

– дослідження нових бізнес-моделей, які ставлять досвід клієнтів у центрі цифрової стратегії.

Тим самим сучасні цифрові тенденції формують оновлену управлінську логіку, що поєднує технологічні можливості, аналітичні інструменти та інституційні зміни. Це створює методологічну основу для подальшого розгляду особливостей цифрових процесів та їх впливу на розвиток і стійкість підприємства.

Для системного розуміння трансформаційних процесів, що відбуваються в управлінні сучасними підприємствами, доцільно деталізувати архітектура діджиталізаційних та смарт-моделей управління (рис. 1.4). Їх специфіка полягає у переході від використання окремих цифрових інструментів до розбудови цілісної цифрової інфраструктури, здатної інтегрувати дані, технологічні платформи, інтелектуальні аналітичні моделі та адаптивні управлінські рішення.

Цифрові ресурси в такій моделі відіграють роль ядра, що забезпечує прискорення інформаційних потоків, уніфікацію бізнес-процесів, розширення можливостей аналітики й прогнозування, а також формування інтелектуальних систем підтримки рішень. Саме завдяки комплексному використанню даних, цифрових платформ, інтернету речей, штучного інтелекту та хмарних технологій управлінська система набуває нових властивостей: гнучкості, самонавчання, точності та здатності до безперервної адаптації.

Удосконалення управлінських моделей відбувається шляхом переходу від раціоналізації окремих операцій до створення багаторівневого цифрового середовища. У межах якої взаємодіють інформаційні ресурси, процеси, інструменти та результати. Це забезпечує підвищення якості прийняття

рішень, оптимізацію операційної діяльності, зміцнення стійкості підприємства та формування нової конфігурації стратегічних можливостей.

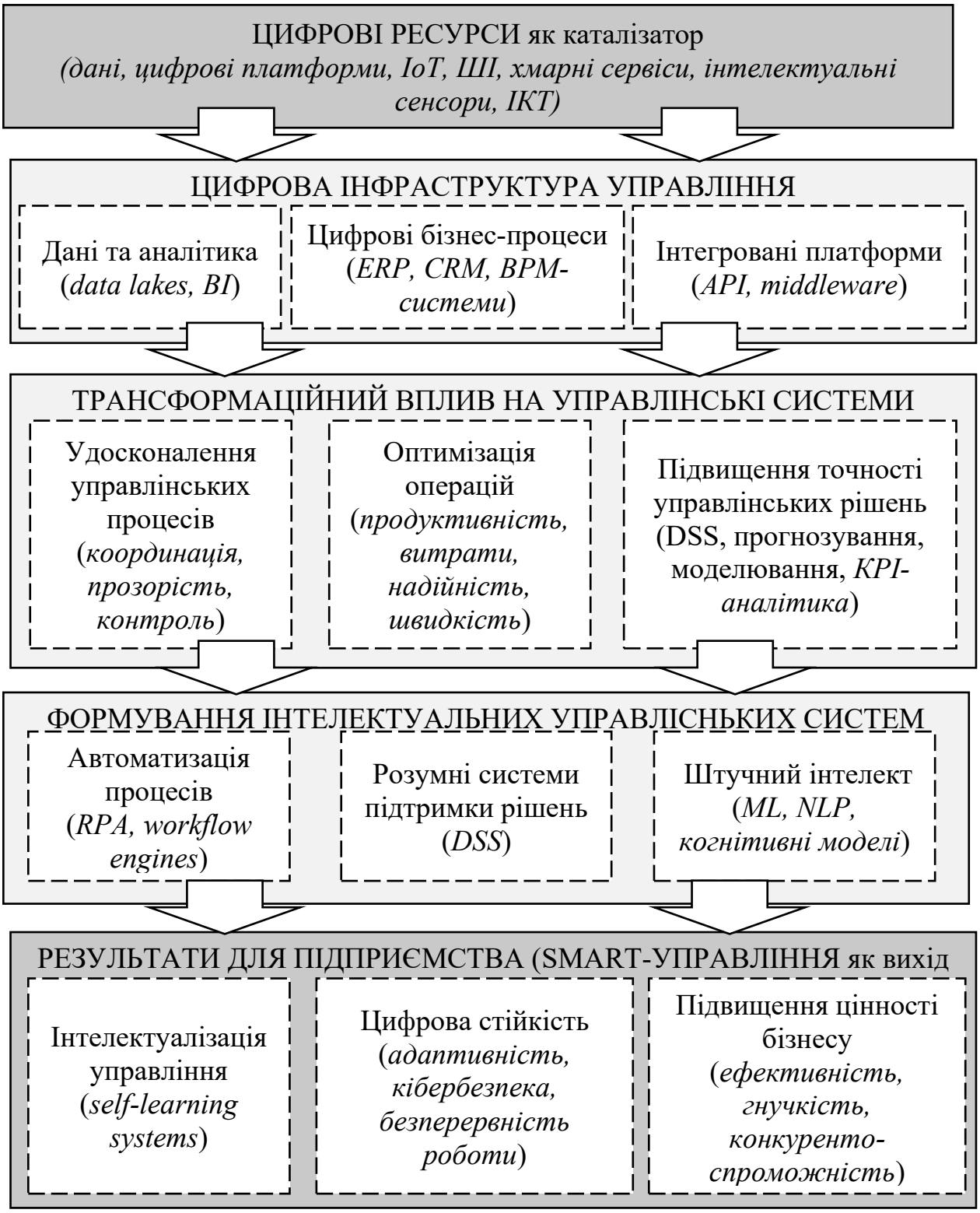


Рисунок 1.4 – Структурно-логічна схема діджиталізаційних та смарт-моделей управління (*джерело: авторська розробка*)

Структурно-логічна схема *(див. рис. 1.4)* демонструє, що цифровізаційні та смарт-підходи до управління формують не лише нову технологічну основу, а й змінюють принципи організації управлінської діяльності. Для підприємства це означає перехід до більш передбачуваного, даних-орієнтованого та адаптивного управління, у якому рішення ґрунтуються на точних показниках, аналітичних моделях та алгоритмах штучного інтелекту.

Впровадження діджиталізаційних та смарт-моделей управління дозволяє досягти *таких результатів* як:

– підвищення точності управлінських рішень завдяки адаптації, моделюванню, прогнозуванню та використанню великих даних (Big data);

– зменшення операційних витрат через автоматизацію рутинних процесів, оптимізацію ресурсів та скорочення часу виконання завдань;

– зростання продуктивності внаслідок використання цифрових інструментів, інтегрованих платформ та інтелектуальних систем підтримки рішень;

– підвищення прозорості та керованості бізнес-процесів через цифрові робочі потоки, моніторинг у реальному часі та швидку реакцію на зміни середовища;

– мінімізацію ризиків через покращення контролю, зменшення залежності від людського фактора та впровадження алгоритмів раннього попередження;

– підвищення якості взаємодії між підрозділами завдяки інтегрованим платформам (ERP, CRM, BPM), що зменшують інформаційні розриви;

– розширення інноваційного потенціалу підприємства через можливість впровадження нових бізнес-моделей, продуктів та цифрових сервісів;

– посилення конкурентоспроможності в умовах цифрової економіки та глобального ринку;

– формування стратегічної гнучкості – здатності підприємства швидко адаптуватися, перебудовувати процеси та приймати проактивні рішення.

Відтак, відповідно вище відзначеним причинам впровадження діджиталізаційних та смарт-моделей управління, визначено, що ефективність цифрових та смарт-моделей управління визначається не лише здатністю підприємства автоматизувати процеси чи підвищувати аналітичну спроможність. Ключовим чинником стає здатність підприємства працювати стабільно, передбачувано та безперервно в умовах зростаючої невизначеності, цифрових ризиків та криз, що потребує інтеграції концепції цифрової стійкості (Digital Resilience), яка визначає механізми забезпечення захищеності, адаптивності та життєздатності підприємства в цифровому середовищі.

Б. Концепції цифрової стійкості (Digital Resilience). Цифрова стійкість у сучасних умовах постає ключовою характеристикою здатності підприємства функціонувати безперервно, надійно та передбачувано в умовах постійних технологічних змін, зростання кіберзагроз та ускладнення інформаційних потоків. На відміну від традиційної стійкості, що зосереджується переважно на структурних та ресурсних аспектах, *цифрова стійкість* охоплює ширший спектр компонентів: технологічну спроможність, захищеність даних, гнучкість цифрової інфраструктури, готовність до швидкого відновлення та здатність до адаптації цифрових процесів. Вона грунтується на принципах проактивності, безперервності та інтелектуальної реакції на зовнішні й внутрішні виклики. Саме цифрова стійкість забезпечує підприємству можливість не лише мінімізувати наслідки технологічних збоїв чи кіберінцидентів, а й використати цифрове середовище як простір для розвитку, інновацій та стратегічного посилення конкурентних позицій.

Для системного розуміння змісту цифрової стійкості та визначення її місця у сучасних управлінських моделях доцільним є проведення аналізу напрацювань вчених (табл. 1.4). Різні наукові школи [59, 62, 63] трактують цифрову та організаційну стійкість співставляючи їх з такими поняттями як інформаційна система, цифрова трансформація, інноваційний розвиток, кібербезпека, адаптивність бізнесу. Попри відмінність контекстів і методологічних підходів, серед науковців [50, 60, 61] простежуються спільні

положення: цифрова стійкість формується на перетині технологічних рішень управлінських практик, організаційних здібностей та компетентностей персоналу.

Таблиця 1.4 – Підходи до трактування поняття «цифрова стійкість» (*джерело: систематизовано автором на підставі* [50, 59-63])

Автори	Трактування поняття	Ключові аспекти
Tim Y., Leidner D.	здатність поглинати цифрові збої, адаптуватися та відновлюватися, забезпечуючи безперервність роботи.	гнучка архітектура ІС, процеси реагування, узгодженість ІТ та управління
Zhang J., Long J., von Schaewen A.M.E.	стійкість як результат цифрової трансформації, що підвищує інноваційність і гнучкість підприємства.	поєднання цифрових інвестицій та інновацій, адаптивність стратегій
Őri D, Szabó I, Kő A, Kovács T.	у малих та середніх підприємств цифровізація посилює стійкість, що дозволяє долати кризові впливи та швидше пристосовуватися.	оцифрування процесів, розвиток компетенцій, гнучкість операцій
Burlacu S., Mocanu V., Platages G., Dobre F.	стійкість як здатність зберігати безперервність діяльності завдяки цифровим процесам.	цифрова модернізація, гнучкі моделі управління, прозорість операцій
Tang C., Dong S., Zhou R.	багатовимірна стійкість, що формується технологіями та внутрішнім здібностям.	технологічні, організаційні та гібридні шляхи посилення стійкості
Dupin J.-J., Pascal A., Godé C.	стійкість як здатність реагувати, відновлюватися та трансформуватися під дією цифрових криз.	культура змін, цифрові компетенції, інтеграція ІТ та управління

Представлені підходи до трактування поняття «цифрова стійкість» зарубіжними науковцями розглядається не як окремий технологічний елемент, а як комплексна характеристика підприємства, що визначає його здатність функціонувати в умовах цифрової турбулентності. Попри різноманітність наукових підходів, спільним є необхідність поєднання технологічних рішень з організаційними змінами, розвитком компетентностей персоналу та

формуванням культури гнучкості й адаптивності. Аналіз представлених праць демонструє, що *цифрова стійкість постає результатом синергії кількох ключових складових*: ефективної цифрової інфраструктури, здатності до швидкого реагування на збої використання даних та аналітики для прийняття рішень, а також стратегічного управління цифровими змінами. Підприємства, які інтегрують ці компоненти, отримують конкурентні переваги, зокрема підвищення операційної безперервності, зменшення ризиків, прискорення інновацій і зміцнення довгострокової стабільності.

Все вище відзначене дає можливість сформулювати *авторське визначення поняття «цифрова стійкість»,* що являє собою інтегральну організаційну здатність забезпечувати безперервність, стабільність і результативність діяльності в умовах цифрової динаміки та ризиків, що формується завдяки синергії ефективної цифрової інфраструктури, здатності оперативно реагувати на цифрові збої, використання даних та аналітики для підтримки управлінських рішень, а також стратегічного управління цифровими змінами, спрямованого на адаптацію, відновлення та розвиток підприємства.

Сформульоване визначення підкреслює багатовимірний характер цифрової стійкості та її залежність від взаємодії технологічних, організаційних, аналітичних і стратегічних чинників, що являє собою *модель структурних елементів цифрової стійкості підприємства* (рис. 1.5). Вона ґрунтується на взаємодії *чотирьох функціональних складових*:

– верхній рівень охоплює *адаптивно-реактивну та технологічну складові*, які забезпечують оперативність реагування на цифрові збої та формують технічну основу функціонування підприємства в цифровому середовищі;

– нижній рівень містить *стратегічно-управлінську та аналітично-інформаційну складові*, відповідальні за підтримку процесів цифрової трансформації, розвиток аналітичних можливостей та підвищення обґрунтованості управлінських рішень.

Рисунок 1.5 – Модель структурних елементів цифрової стійкості підприємства (*джерело: авторська розробка*)

Центральне місце в моделі займає елемент «синергетичний ефект – формування цифрової стійкості», який відображає інтеграційний характер взаємодії складових. Він підкреслює, що цифрова стійкість підприємства формується не окремими функціональними елементами, а їх узгодженим впливом, що забезпечує здатність підприємства підтримувати безперервність діяльності, адаптуватися до цифрових ризиків та забезпечувати довгострокову стратегічну стабільність. Представлена модель *(див. рис. 1.5)* відображає системний характер формування цифрової стійкості підприємства та демонструє, що її результативність забезпечується не окремими елементами, а

їх взаємодією, узгодженістю та взаємним підсиленням. З огляду на це деталізуємо зміст кожної і складових, що формують синергетичну основу цифрової стійкості та визначають напрями розвитку відповідних спроможностей підприємства (табл. 1.5).

Таблиця 1.5 – Характеристика структурних елементів моделі цифрової стійкості підприємства (*джерело: авторська розробка*)

Складова	Зміст та ключові елементи	Роль у формуванні цифрової стійкості
1	2	3
1. Адаптивно-реактивна (*Rapid Response and Adaption Capability*)	– швидкість реагування на цифрові інциденти; – локалізація та мінімізація збоїв; – наявність процедур відновлення; – гнучкість операцій і процесів; – здатність адаптуватися до зовнішніх цифрових криз.	забезпечує підтримання операційної безперервності й мінімізує втрати під час цифрових порушень
2. Технологічна (*Digital Infrastructure Capability*)	– цифрова інфраструктура (ІС, ІКТ, хмарні сервіси, платформи); – інтегрованість і сумісність систем; – кіберзахищеність і надійність; – цифрові активи, інструменти кіберальянсу та механізми спільного кіберзахисту; – можливість масштабування та модернізації.	забезпечує технічний фундамент безперервної діяльності, стійкості до цифрових криз та швидкого відновлення
3. Стратегічно-управлінська (*Digital Change Governance Capability*)	– цифрове лідерство й управління змінами; – цифрова культура; – стратегічне планування цифрового розвитку; –	забезпечує трансформаційну спроможність та розвиток підприємства в цифровому середовищі

Продовження табл. 1.5

1	2	3
	– розвиток цифрових компетенцій персоналу; – управління довгостроковою стійкістю й адаптацією.	
4. Аналітично-інформаційна (*Data and Analytics Capability*)	– збір і оброблення та зберігання даних; – аналітичні моделі, прогнозування та моделювання; – цифрові KPI та метрики стійкості; – data-driven decision making; – використання даних для раннього виявлення цифрових загроз.	формує обґрунтованість рішень і стратегічну передбачуваність, які потрібні для швидкого відновлення

Відзначимо, що одним з ключових елементів технологічної складової є кіберальянс, який займає важливе місце в сучасних підходах до забезпечення цифрової стійкості, оскільки воно відображає тенденцію від ізольованого кіберзахисту до спільних, кооперaційних форм протидії цифровим загрозам. У таких умовах підприємства вже не можуть покладатися виключно на власні ресурси безпеки, а потребують взаємодії в межах ширших цифрових середовищ.

Кіберальянс – це форма організаційної та технологічної взаємодії між підприємствами, інституціями або учасниками цифрового середовища, спрямована на колективне зміцнення кіберзахисту, обмін інформацією про загрози, використання узгоджених інструментів протидії атакам та забезпечення безперервності діяльності в умовах цифрових ризиків. Кіберальянси поєднують цифрові активи, спільні інструменти моніторингу кіберзагроз, координаційні механізми реагування та практики обміну знаннями, що підсилює загальний рівень цифрової стійкості їх учасників. З огляду на це кіберальянс виконує *дві ключові функції*:

– створює додатковий рівень кіберзахищеності, підсилюючи технологічну та організаційну основу розвитку підприємства в умовах цифрових загроз;

– забезпечує ефективний механізм спільного реагування на інциденти, що дозволяє підприємствам швидше відновлюватися після збоїв та адаптуватися до нових типів ризиків, зокрема тих, що мають мережевий або міжорганізаційний характер.

Тим самим залучення інструментів кіберальянсу в систему цифрової стійкості підприємства не лише розширює її технологічну компоненту, але й формує умови для колективної протидії кіберзагрозам, що підвищує готовність підприємства діяти в умовах цифрової турбулентності та глобальної інформаційної взаємозалежності. В світовій практиці нині діють кіберальянси, що об'єднують ресурсні, технологічні та інформаційні можливості організацій (табл. 1.6).

Таблиця 1.6 – Світовий досвід функціонування кіберальянсів або ініціатив співпраці (*джерело: систематизовано автором на підставі* [64-72])

Кіберальянс/ініціатива співпраці	Характеристика
1	2
1. Cyber Threat Alliance (CTA)	Глобальний альянс компаній з кібербезпеки, що обмінюються актуальною інформацією про кіберзагрози в режимі майже реального часу, що дозволяє учасникам спільно реагувати на загрози, поширювати дані про шкідливе програмне забезпечення, вразливості та кібер-атаки.
2. Financial Services Information Sharing and Analysis Center (FS-ISAC)	Галузевий альянс для фінансового сектору, де банки та фінансові установи обмінюються інформацією щодо загроз, атак, вразливостей та рекомендаціями з кіберзахисту, що створює спільну мережу реагування.
3. National Cyber-Forensics and Training Alliance (NCFTA)	Неприбуткова неурядова організація США, яка об'єднує представників приватного сектору, правоохоронних органів, IT-компаній і дослідницьких інституцій для спільної протидії кіберзлочинності.

Продовження табл. 1.6

1	2
4. International Multilateral Partnership Against Cyber Threats (IMPACT)	Міжнародний альянс за підтримки ООН, який об'єднує державні, академічні та приватні інституції для координації заходів щодо запобігання кіберзагрозам, обміну інформацією, розробки політик безпеки та підтримки кіберстійкості на глобальному рівні.

Узагальнення наведених прикладів кіберальянсів *(див. табл. 1.6)* демонструє, що ефективність протидії цифровим загрозам та забезпечення стійкості підприємств значною мірою визначаються не лише внутрішніми можливостями підприємств та організацій, а й здатністю інтегруватися у більш широкі інформаційно-комунікаційні мережі співпраці. Саме такі мережі забезпечують обмін даними про ризики, колективну аналітику, координацію дій та формування превентивних механізмів реагування, що є ключовими чинниками сучасного антикризового управління. У цьому контексті очевидним постає зростання ролі інфокомунікаційних платформ, які виступають не лише технічними інструментами взаємодії, а й інституційними елементами, здатними забезпечувати безперервність комунікацій, підтримувати прийняття управлінських рішень та створювати умови для оперативного реагування на кризові ситуації, зокрема використовуючи інфокомунікаційні платформи.

В. Інфокомунікаційні платформи як елемент антикризового менеджменту. В умовах високої турбулентності, коли кризи мають багатовимірний характер і розвиваються з високою динамікою, саме цифрові середовища корпоративного та міжорганізаційного рівнів формують новий формат управлінської взаємодії. Їх використання забезпечує швидке відстеження змін, оперативний обмін даними, прозорість процесів та ефективну координацію дій між усіма суб'єктами, залученими до антикризових заходів.

Аналіз наукових праць вчених свідчить, що інфокомунікаційні платформи посідають центральне місце в сучасних моделях антикризового

менеджменту, формуючи інформаційне середовище для координації дій, обміну даними та прийняття рішень у режимі реального часу. Перші комплексні підходи до оцінювання ролі цифрових комунікацій у кризових ситуаціях були сформовані у роботі [73], де обґрунтовано перехід від традиційних, односпрямованих каналів інформування до інтерактивних цифрових середовищ, що забезпечують прозорість, двосторонній обмін інформацією та оперативне залучення стейкхолдерів до процесу реагування на кризу. Автори підкреслюють, що цифрові канали формують основу нової моделі кризової комунікації, у якій час реагування та відкритість інформації стають ключовими параметрами ефективності.

Подальший розвиток даного напряму пов’язаний із дослідженням платформ колективної участі та цифрового волонтерства. Так, у роботі [74] розкрито специфіку «мікротаскінгу» (від англ. microtasking) як форми залучення «цифрових волонтерів» до збору, структуризації та перевірки інформації під час надзвичайних ситуацій. Вчені доводять, що інфокомунікаційні платформи такого типу забезпечують швидке формування масивів достовірних даних, що істотно підвищує ситуаційну поінформованість офіційних служб і дає змогу приймати більш зважені оперативні рішення. У цьому контексті цифрові середовища виступають не лише каналами комунікації, а й повноцінними інструментами цифрової комунікації.

Суттєвий внесок у теоретичне узагальнення ролі цифрових платформ зроблено у роботі [75], де проаналізовано понад дві сотні публікацій із проблематики цифрової трансформації в управлінні надзвичайними ситуаціями. Автори систематизують функції інфокомунікаційних платформ у кризових умовах, зокрема інтеграцію даних із сенсорних систем, соціальних мереж, геоінформаційних ресурсів, підтримку прийняття рішень, формування єдиного інформаційного простору для учасників кризового реагування. Це дозволяє трактувати такі платформи як основу цифрового середовища антикризового менеджменту.

У сучасних умовах науковці все частіше підкреслюють те, що цифрові платформи стають інституційним продовженням організаційних структур кризового управління. В статтях, присвячених цифровій трансформації кризового менеджменту [76, 77] відзначається, що цифрові середовища забезпечують синхронізацію управлінських процесів, мінімізують інформаційні розриви між рівнями управління та сприяють формуванню стійких систем реагування. При побудові структури управління менеджери, звісно, намагаються врахувати якомога більше факторів та чинників, що можуть впливати на стабільну їх діяльність [78]. Тим самим відзначається, що більшість критичних подій супроводжуються значним інформаційним резонансом у соціальних мережах та корпоративних платформах, а отже підприємства та організації змушені інтегрувати цифрові інструменти в основу антикризових стратегій.

У дослідженні [79] розглянуто феномен «цифрової неохоти», що притаманний підприємствам із низьким рівнем цифрової зрілості. Автор обґрунтовує, що недостатнє використання інфокомунікаційних платформ під час криз призводить до затримок у поширенні інформації, втрати контролю над внутрішніми й зовнішніми комунікаціями та зниження довіри стейкхолдерів. Натомість системна побудова цифрових каналів комунікації є ключовою передумовою організаційної стійкості.

В свою чергу у дослідженні С. Філиппової та О. Кульчицького [80] запропоновано удосконалену модель розробки інноваційних послуг із застосуванням цифрових технологій, що ґрунтується на ідеях інтеграції та синергії між цифровими компаніями, підприємствами Індустрії 4,0/5.0, державними інституціями та науковим сектором. Модель демонструє, що ефективний розвиток цифрових сервісів можливий лише за умов проникності інформаційних потоків, узгодженості цифрових рішень та функціонування спільних інфокомунікаційних платформ (рис. 1.6).

У контексті антикризового менеджменту така модель є цінною тим, що показує як взаємодія між учасниками цифрового середовища може

підвищувати адаптивність підприємств, підтримувати інформаційну стійкість та забезпечувати швидке узгодження дій у кризових ситуаціях.

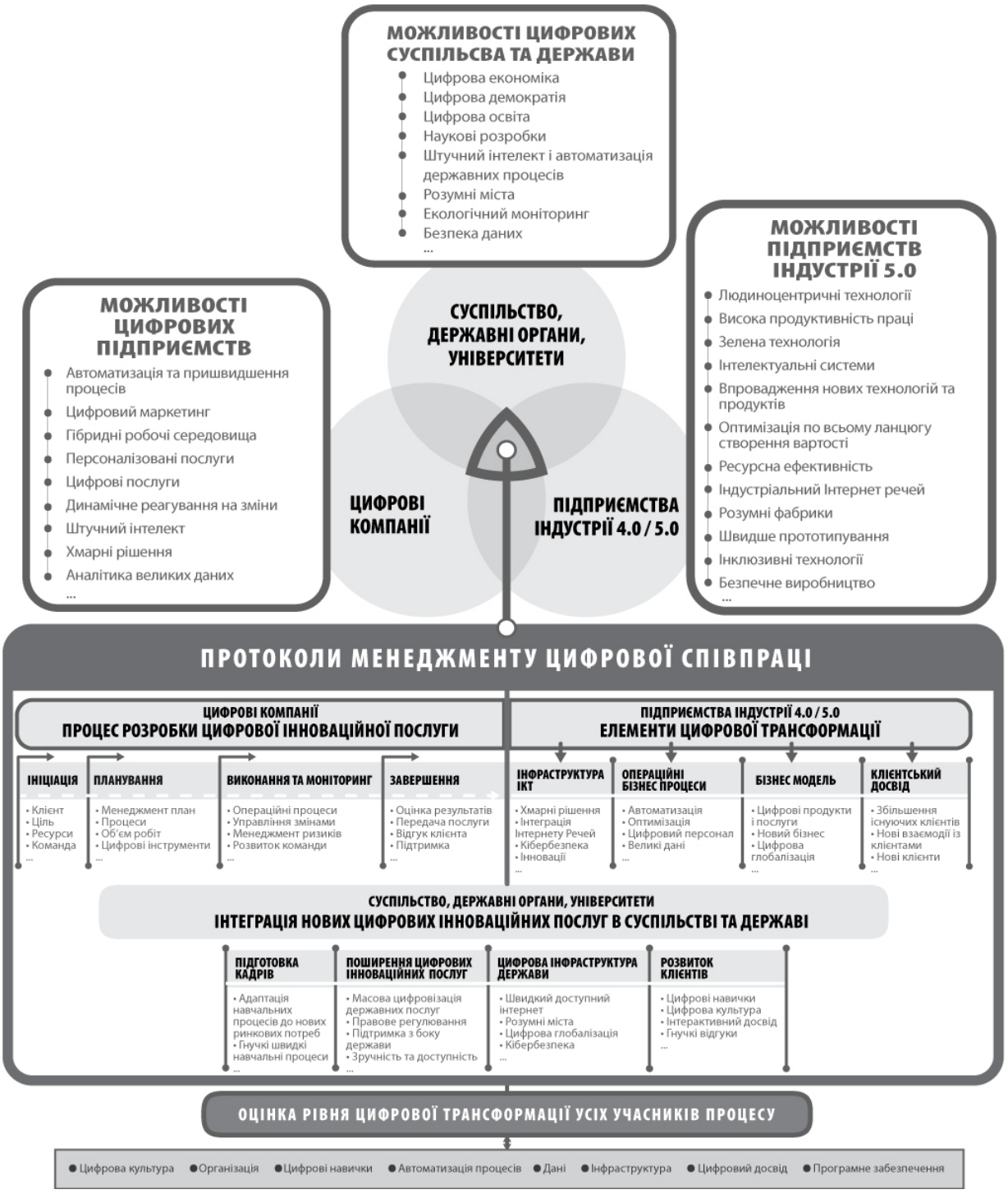


Рисунок 1.6 – Модель розробки інноваційних послуг із застосуванням цифрових технологій *(джерело: [80])*

В цілому проведений аналіз дозволяє виокремити *кілька ключових тенденцій у розвитку інфокомунікаційних платформ*. Це:

– зміщення від традиційних каналів кризових комунікацій до інтерактивних і мережевих цифрових середовищ;

– розширення функцій платформ від інструментів обміну даними до комплексних середовищ управління кризами;

– зростання ролі аналітики, прогнозування та штучного інтелекту в архітектурі цифрових платформ;

– формування нової організаційної логіки, заснованої на прозорості, швидкості та інтеграції інформаційних потоків;

– поява моделей оптимізації інфокомунікаційних платформ на рівні окремого підприємства.

Принципова особливість такого підходу полягає у тому, що цифрові платформи розглядаються не лише як технологічний інструментарій, а як інституційне середовище, у межах якого відбувається координація дій, управління інформаційними потоками та формування колективної відповідальності за результати спільної діяльності.

За рахунок цього інфокомунікаційні платформи здатні виконувати *низку критично важливих функцій*, до яких віднесено:

– забезпечувати оперативний доступ до даних;

– підтримувати безперервність комунікацій між стейкхолдерами;

– інтегрувати внутрішні й зовнішні цифрові сервіси;

– підсилювати можливості моніторингу та прогнозування;

– створювати єдиний простір для прийняття узгоджених управлінських рішень.

Для узагальнення отриманих результатів аналізу та систематизації внеску різних груп учасників цифрової взаємодії доцільним є виділення ключових можливостей і ролі у формуванні інфокомунікаційних платформ антикризового менеджменту (табл. 1.7). Узгодженість дій цифрових компаній, підприємств Індустрії 4.0/5.0, державних структур, наукових установ,

користувачів та стейкхолдерів визначає рівень ефективності інформаційних потоків, оперативність управлінських реакцій і здатність підприємства підтримувати стійкість у кризових умовах.

Таблиця 1.7 – Можливості учасників цифрової взаємодії та стейкхолдерів для формування інфокомунікаційних платформ антикризового менеджменту *(джерело: систематизовано автором на підставі [75-80])*

Учасники	Ключові можливості та внесок	Значення для антикризового менеджменту
1. Цифрові компанії	технологічні рішення, розробка платформ, ШІ, аналітика, кіберзахист	формування технічної бази платформи, швидке масштабування, висока адаптивність
2. Підприємства Індустрії 4.0/5.0	інтеграція IoT, автоматизація та аналітика у виробництво	підвищення операційної стійкості, цифровий моніторинг, зменшення ризиків
3. Держава та регулятори	нормативна підтримка, інфраструктура, політика безпеки, інвестиції	інституційні гарантії, кіберзахист, стабільність у кризових умовах
4. Наукові установи та університети	дослідження, трансфер технологій, підготовка кадрів	підсилення експертної підтримки, розвиток цифрових компетенцій
5. Суспільство/ користувачі	зворотний зв’язок, участь у цифрових сервісах, адаптація до технологій	формування достовірної інформації, соціальна підтримка рішень
6. Стейкхолдери (постачальники, партнери, клієнти)	дані про процеси, інтеграція ланцюгів постачання, сумісність систем	координація в ланцюгах вартості, мінімізація операційних збоїв
7. Інвестори	фінансування цифрових рішень, участь у проєктах, стратегічна підтримка, вимоги до прозорості	підвищення фінансової стійкості, забезпечення ресурсів для розвитку платформ, підсилення вимог до управлінської дисципліни

Відтак, узагальнені результати дозволяють трактувати інфокомунікаційні платформи як ключовий елемент антикризового менеджменту, що забезпечує використання корпоративних і міжорганізаційних цифрових середовищ для координації стейкхолдерів, прозорості процесів, швидкого обміну даними та підтримки прийняття управлінських рішень у режимі реального часу. Їхнє впровадження створює основу для підвищення стійкості підприємства до риз, мінімізації інформаційних ризиків та формування адаптивних механізмів реагування на кризові ситуації. Разом із тим ефективність функціонування таких платформ безпосередньо залежить від якості та цілісності інфокомунікаційної інфраструктури підприємства, рівня її інтегрованості з зовнішніми цифровими середовищами та здатності забезпечувати безперервність інформаційних потоків в умовах турбулентності.

1.3 Особливості формування інфокомунікаційної інфраструктури підприємства в умовах кризових викликів

Для розуміння особливостей формування інфокомунікаційної інфраструктури підприємства в умовах кризових викликів важливо окреслити теоретичні положення, що визначають зміст, функції та функціональну спрямованість інфокомунікаційних ресурсів у забезпечення стійкості бізнесу. Узагальнення сучасних наукових досліджень дозволяє виокремити *три ключові концептуальні блоки, які формують основу побудови інфокомунікаційної інфраструктури, здатної ефективно функціонувати в умовах економічних, військових, технологічних та соціальних криз.* Це:

– структура інфокомунікаційних систем, що включає архітектуру технічних, мережевих, хмарних та програмних рішень, а також інтегрованих цифрових середовищ, які забезпечують безперебійний рух інформаційних

потоків, оперативність взаємодії та доступність даних для управлінських рішень;

– ризики і вразливості цифрової інфраструктури, зумовлені впливом зовнішніх кризових факторів, кібератак, технічних збоїв, дефіциту людського капіталу цифрових компетенцій та зростаючою залежністю підприємства від інформаційно-комунікаційних платформ та провайдерів цифрових послуг;

– функції інфокомунікаційних ресурсів у запобіганні та подоланні кризових явищ, що проявляються у забезпеченні координації між підрозділами, підтримці прозорості процесів, швидкому поширенні даних, підвищенні точності управлінських рішень та посиленні цифрової стійкості підприємства.

А. Структура інфокомунікаційних систем. Роль інфокомунікаційних систем полягає у забезпеченні цілісного інформаційно-комунікаційного простору, який дає змогу підприємству підтримувати узгодженість операцій та стабільність управлінських процесів навіть у ситуаціях криз. Завдяки цій інфраструктурній основі відбувається оперативна передача критично важливих даних, своєчасна координація дій між підрозділами та збереження доступності інформаційних ресурсів, що є ключовими умовами ефективного реагування на кризові впливи. Відповідно до рис. 1.2, структура інфокомунікаційних ресурсів містить *такі структурні елементи*: інформаційні, інфраструктурні, технологічні, комунікаційні ресурси та ресурси цифрової безпеки. Однак для цілісного розуміння їх ролі у забезпеченні стійкого функціонування підприємства недостатньо лише ідентифікувати наявні цифрові активи. Важливо простежити, яким чином ці ресурси інтегруються між собою, взаємодіють у межах єдиного інформаційного простору та утворюють комплексну інфокомунікаційну систему, що забезпечує узгоджені інформаційні потоки, оперативний обмін даними та підтримку управлінських процесів.

У сучасних умовах цифрової трансформації інфокомунікаційні системи підприємства сформувалися як комплексна архітектура, що охоплює

інформаційні, технологічні, комунікаційні та безпекові компоненти, інтегровані в єдиний управлінський простір. Зарубіжні дослідження підтверджують, що ефективність взаємодії цих елементів визначає рівень адаптивності підприємства, його операційну узгодженість та здатність забезпечувати стійкість у мінливих умовах.

Значущу роль інформаційної складової підтверджує дослідження [81], у якому обґрунтовано, що управлінські інформаційні системи забезпечують формування своєчасних, релевантних та аналітично цінних даних, необхідних для прийняття ефективних рішень. Це безпосередньо стосується інформаційного елемента інфокомунікаційної системи, який формує інформаційні потоки, підтримує аналітичну діяльність і забезпечує прозорість бізнес-процесів. Подібні результати отримано у дослідженні [82], де підкреслено, що якість даних, їхня доступність та інтеграція визначають швидкість операцій, гнучкість управління й рівень внутрішньої координації. Це демонструє критичність інформаційних ресурсів як основу функціонування всієї системи. Класичний висновок автора [83], який розробив модель детермінант ефективності організаційних інформаційних систем, також належить до інформаційного елемента інфокомунікаційної системи, оскільки описує залежність організаційних результатів від структури, форми та якості інформації, що циркулює в системі.

Дослідження [84] показує, що ERP-системи підсилюють внутрішню та зовнішню інтеграцію, оптимізують ланцюги постачання та підвищують ефективність операцій. ERP виступає основою технологічного елемента інфокомунікаційної системи, забезпечуючи стандартизацію процесів, централізацію даних та інтеграцію з цифровими системами підприємства. Аналогічно з попереднім дослідженням, результати [85] свідчать про суттєве зростання фінансових результатів підприємств, що впровадили ERP. Це підтверджує, що технологічний елемент інфокомунікаційної системи є ключовим джерелом підвищення ефективності операцій і конкурентоспроможності. Суттєвий інституційний аспект технологічної

складової аналізує [86], доводячи, що цінність корпоративних інформаційних систем залежить від ефективності корпоративного управління. Це стосується стратегічно-управлінського рівня інфокомунікаційного середовища, де технологічні рішення поєднуються з організаційними механізмами.

Комунікаційна складова інфокомунікаційної системи визначає, наскільки ефективно підприємство організовує внутрішню та зовнішню взаємодію. У дослідженнях інформаційних систем NASA, виконаних [87], показано, що інфокомунікаційна система може виконувати функції забезпечення стабільності операцій, узгодження даних та мінімізацію впливів криз у періоди організаційних змін. Це безпосередньо демонструє роль комунікаційних інструментів у підтримці стійкості.

Робота [88] підкреслює тенденцію до переходу від традиційних інформаційних систем до інтелектуальних, що включають експертні модулі, засоби підтримки рішень і знаннєві технології. Цей напрям є ключовим для інтеграційно-аналітичного елемента інфокомунікаційної системи, оскільки демонструє, як системи синхронізують інформацію та забезпечують адаптивність у складних управлінських ситуаціях. В свою чергу модель [89], яка описує еволюцію інформаційних систем від підсистем обліку до стратегічно орієнтованих цифрових платформ, також належить до цього елемента. Вона демонструє, як відбувається поступове нарощування інтеграції, масштабування та розширення функціональності інфокомунікаційної системи відповідно до потреб підприємства.

Науковці [90] досліджують роль ERP у забезпеченні точності, цілісності та доступності облікової інформації. Їх висновки прямо стосуються елемента цифрової безпеки інфокомунікаційної системи, оскільки ERP виступає основою захисту даних, зниження ризиків помилок і забезпечення відповідності регуляторним вимогам. В свою чергу [87] також частково торкається питання операційної стійкості, доводячи, що інфокомунікаційна система здатна виступати «амортизатором криз» у періоди структурних змін,

що є ключовим для розуміння ролі безпекового та стійкісного елементів інфокомунікаційної системи.

В той же час важливим є інтеграційно-аналітичний елемент, який не входить до переліку інфокомунікаційних ресурсів підприємства, оскільки не є окремим видом цифрового активу. Але його інтеграція є важливою, адже на рівні функціонування інфокомунікаційної системи необхідний окремий комплекс механізмів, що забезпечують узгодження, аналітичну обробку даних та синхронізація інформаційних потоків.

Тим самим проведений аналіз зарубіжних джерел підтверджує, що *інфокомунікаційна система підприємства виступає багатовимірною архітектурою*, де:

– інформаційний елемент забезпечує якість, доступність і релевантність даних;

– технологічно-інфраструктурний елемент формує цифровий фундамент операцій;

– комунікаційний елемент забезпечує інтегровану взаємодію і координацію;

– інтеграційно-аналітичний елемент створює можливості для інтелектуалізації та адаптивності;

– елемент цифрової безпеки та стійкості гарантує надійність і захищеність функціонування системи.

Такий підхід дозволяє розглядати інфокомунікаційну систему підприємства не як набір окремих цифрових інструментів, а як цілісну архітектуру, що забезпечує стале функціонування підприємства та його здатність реагувати на кризові виклики. Взаємодія інформаційних, технологічних, комунікаційних та безпекових компонентів формує підґрунтя для безперервності бізнес-процесів і швидкого переналаштування інформаційних потоків у нестабільних умовах. Розглянемо структуру інфокомунікаційної системи підприємства, що функціонує під впливом зовнішніх криз (рис. 1.7).

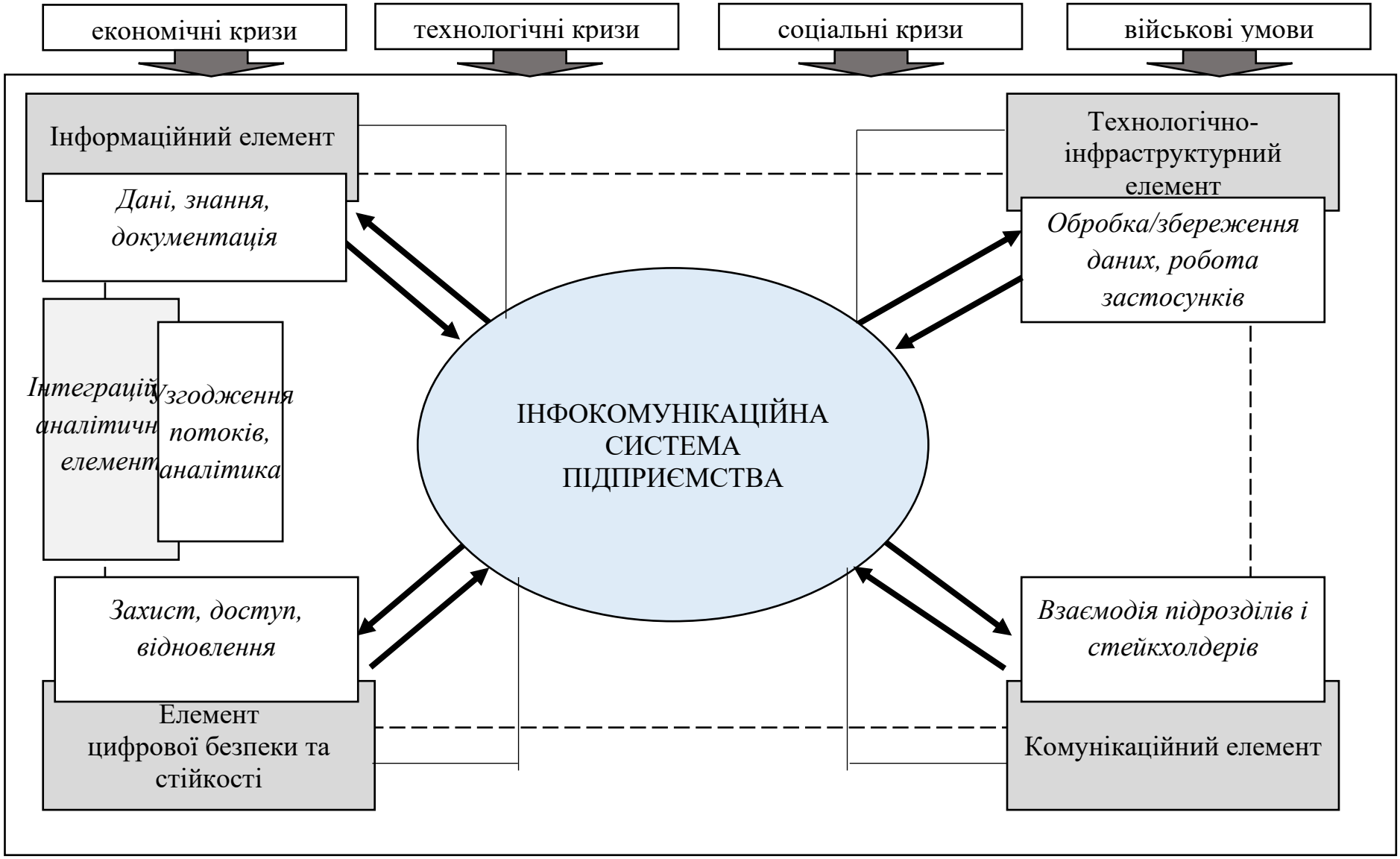


Рисунок 1.7 – Структура інфокомунікаційної системи підприємства (*джерело: авторська розробка*)

Вище відзначена структура інфокомунікаційної системи підприємства *(див. рис. 1.7)* демонструє логіку її формування як узгодженої сукупності функціональних елементів, кожен з яких забезпечує окремий напрям цифрової взаємодії та підтримує стійкість підприємства в умовах зовнішніх викликів. Центральною ланкою виступає безпосередньо інфокомунікаційна система підприємства, яка координує і поєднує інформаційні, технологічні, комунікаційні, аналітичні та безпекові елементи та процеси в єдине управлінське цифрове середовище.

Інформаційний елемент охоплює ключові змістові компоненти цифрової діяльності – дані, знання та документацію – які становлять інформаційну базу для прийняття рішень. Технологічно-інфраструктурний елемент забезпечує технічне підґрунтя функціонування системи: підтримує роботу застосунків, оброблення й збереження даних, мережеву взаємодію та інші технологічні операції. Комунікаційний елемент відповідає за організацію взаємодії між підрозділами та стейкхолдерами, сприяючи своєчасному та узгодженому обміну даними. Елемент цифрової безпеки та стійкості підтримує захищеність інформаційних процесів, контролює доступ, забезпечує відновлення та джерела цифрової надійності. Інтеграційно-аналітичний елемент виконує системоутворювальну роль, синхронізуючи інформаційні потоки, забезпечуючи їх узгодженість та створюючи аналітичну основу для обґрунтованих управлінських рішень.

Важливо підкреслити, що наведені елементи суттєво відрізняються від структури інфокомунікаційних ресурсів підприємства. Якщо ресурси відображають, що саме має підприємство (технології, дані, інфраструктуру, канали комунікації, засоби кіберзахисту), то елементи інфокомунікаційної системи характеризують, як ці ресурси взаємодіють у межах єдиного цифрового середовища. Іншими словами, *ресурсний підхід визначає змістовне наповнення цифрової бази підприємства, тоді як системний підхід формує архітектуру їх функціонування, взаємопов'язаність та ролі у забезпеченні стійкості.* Саме тому такі компоненти, як інтеграційно-аналітичний елемент

або елемент стійкості, не є ресурсами у вузькому розумінні, але виникають як надбудова, коли ресурси об’єднуються в узгоджену схему.

Зовнішній контур рисунка *(див. рис. 1.7)* охоплює чотири кризових викликів: економічні, технологічні, соціальні та військові кризи. Їх включення підкреслює, що інфокомунікаційна система функціонує не ізольовано, а постійно реагує на зовнішні ризики, які визначають вимоги до її гнучкості, надійності та адаптивності.

Відтак, у сукупності представлена модель демонструє, що лише взаємодія всіх елементів дозволяє підприємству використовувати свої цифрові ресурси максимально ефективно та підтримувати стійкість у мінливих умовах.

Б. Ризики і вразливості цифрової інфраструктури. Функціонування цифрової інфраструктури підприємства в сучасних умовах супроводжується зростанням кількості та складності ризиків, що впливають на доступність, цілісність та безперервність інформаційних процесів. На відміну від традиційних технічних загроз, сучасні ризики цифрового середовища мають комплексний характер, поєднуючи технологічні, організаційні, кібернетичні та зовнішні фактори, які здатні порушити роботу інфокомунікаційних систем і знизити загальну стійкість підприємства. В свою чергу вразливості виникають як на рівні технічних компонентів (мережеве обладнання, сервери, хмарні платформи), так і на рівні програмних застосунків, інтеграційних модулів, користувацького доступу та управління даними.

Особливої актуальності ці ризики набувають у контексті кризових ситуацій – економічних, технологічних, соціальних і військових – які посилюють нерівномірність навантажень на цифрові системи, підвищують ймовірність збоїв, перевантаження каналів зв’язку, кібератак чи втрати критично важливої інформації. За таких умов *цифрова інфраструктура стає не лише технічною основою функціонування підприємства, а й потенційним джерелом системних загроз,* здатних вплинути на ключові бізнес-процеси, фінансові результати й здатність підприємства та організації забезпечувати безперервність діяльності (табл. 1.8).

Таблиця 1.8 – Ризики цифрової інфраструктури підприємств (*джерело: систематизовано автором на підставі* [91-94])

Вид ризику	Характеристика	Приклад прояву
1. Технологічні	Виникають внаслідок збоїв у роботі апаратного та програмного забезпечення, порушень функціонування мережевих компонентів або інфраструктурних платформ	вихід з ладу серверів чи комутаторів, збої ERP/CRM, помилки у роботі хмарних рішень
2. Кібернетичні	Пов’язані з навмисним втручанням у цифрове середовище для порушення доступності, цілісності або конфіденційності даних	DDoS-атаки, шкідливе ПЗ, фішинг, використання вразливостей у програмних компонентах
3.Організаційно-управлінські	Зумовлені недосконалістю внутрішніх регламентів, політик безпеки та управлінських процедур	неналежний розподіл прав доступу, відсутність політик резервного копіювання, недостатня цифрова компетентність персоналу
4.Інтеграційні	Виникають під час взаємодії між різними програмними модулям, сервісами або системами	конфлікти модулів ERP, помилки API, несумісність протоколів або даних
5. Зовнішні та кризові	Формуються внаслідок впливу зовнішнього середовища, що може порушувати роботу інфраструктури або збільшувати її навантаження	перебої електропостачання, фізичні руйнування об’єктів інфраструктури, воєнні загрози, регуляторні зміни

Проведена деталізація *(див табл. 1.8)* дає змогу системно окреслити основні напрями ризиків, з якими стикається цифрова інфраструктура підприємства, та показує, що їх природа є багатовимірною й виходить за межі виключно технічних збоїв чи кібератак. Значна частина ризиків формується на стику технологічних, організаційних та інтеграційних процесів, що потребує комплексного підходу до їх виявлення та оцінювання. Важливо підкреслити, що кожна група ризиків по-різному впливає на інфраструктуру: технологічні загрози здебільшого порушують доступність цифрових сервісів, кібернетичні

порушують конфіденційність і цілісність даних, організаційні створюють умовні «внутрішні точки» вразливості, тоді як зовнішні та кризові чинники здатні провокувати системні порушення в роботі інфокомунікаційної системи. Відповідно до багатовекторного характеру цих загроз важливим є не лише класифікувати ризики, але й визначити їх конкретні джерела, можливі наслідки для підприємства та інструменти, що дають змогу мінімізувати вплив кожного з них (табл. 1.9).

Таблиця 1.9 – Заходи мінімізації ризиків цифрової інфраструктури (*джерело: систематизовано автором на підставі* [93-96])

Ризик	Джерело виникнення	Можливі наслідки для підприємства	Основні заходи мінімізації
1	2	3	4
1. Збій у роботі серверів або мережевого обладнання	Технічні помилки, зношеність обладнання, перевантаження інфраструктури	Зупинка бізнес-процесів, порушення доступності сервісів, втрата даних	Резервування серверів, кластеризація, моніторинг навантаження, заміна застарілого обладнання
2. Кібернетична атака (DDoS, шкідливе ПЗ, фішинг)	Зовнішні хакерські дії, відсутність належного захисту, людський фактор	Компрометація даних, порушення конфіденційності, фінансові втрати	Брандмауери, IDS/IPS, багаторівневий доступ, SOC-моніторинг, навчання персоналу
3. Інтеграційний збій між системами	Несумісність протоколів, помилки API, неправильні налаштування інтеграцій	Незбалансованість даних, збій операцій, зупинка критичних процесів	Стандартизація інтеграційних протоколів, тестування, резервні схеми оброблення
4. Помилки користувачів	Недостатня цифрова грамотність, порушення політик безпеки, людські помилки	Витік інформації, зміна або видалення даних, некоректні операції	Навчання персоналу, інструкції, контроль доступу, логування дій

Продовження таблиці 1.9

1	2	3	4
5. Відсутність резервного копіювання або його нерегулярність	Ігнорування політик IT-безпеки, нестача ресурсів, слабке управління	Втрата критично важливої інформації, неможливість відновлення систем	Регламентоване резервне копіювання, зберігання копій у хмарі, періодичне тестування відновлення
6. Залежність від одного провайдера інтернет або хмарних послуг	Монополізація технологічної інфраструктури, відсутність альтернативних каналів	Повна недоступність сервісів у разі аварії провайдера	Мультиканальні схеми доступу, мультихмарна стратегія, SLA-контроль
7. Перебої електро-постачання або фізичні руйнування	Аварії, катастрофи , воєнні загрози	Зупинка IT-сервісів, пошкодження обладнання, простій підприємства	Генератори, переміщення частини інфраструктури у хмару
8. Регуляторні зміни та вимоги відповідності	Оновлення законодавства, нові стандарти захисту даних	Штрафи, обмеження діяльності, необхідність доробок систем	Юридичний моніторинг, аудит відповідності, адаптація політик та протоколів

Представлені заходи *(див. табл. 1.9)* узагальнює ключові ризики цифрової інфраструктури та демонструє, що кожен із них має власну природу виникнення, характер впливу на роботу підприємства й специфічні механізми мінімізації. Відзначені взаємозв’язки між джерелами ризиків, можливими наслідками та відповідними заходами мінімізації дозволяють оцінити їх комплексний характер і сформувати цілісне бачення потенційних загроз для інфокомунікаційної системи. Зокрема технологічні та інтеграційні ризики здатні безпосередньо порушити безперервність роботи цифрових сервісів, тоді як кібернетичні загрози переважно впливають на конфіденційність і цілісність

даних, а організаційні фактори створюють додаткові внутрішні передумови для матеріалізації інших видів ризиків.

Систематизація ризиків у такому форматі є важливою для подальшого визначення критичних вразливих точок цифрової інфраструктури, через які зазначені ризики можуть реалізуватися. Вразливості не лише відкривають шлях до матеріалізації загроз, але й відображають слабкі місця у структурі, процесах або політиках підприємства, що потребують підсилення. Проведемо класифікацію вразливостей цифрової інфраструктури, яка дозволяє точніше визначити, які саме фактори створюють ризикове середовище та яким чином вони впливають на загальний рівень цифрової стійкості підприємства (табл. 1.10).

Таблиця 1.10 – Класифікація вразливостей цифрової інфраструктури підприємства (*джерело: систематизовано автором на підставі* [95-99])

Група вразливостей	Характеристика	Типові прояви
1	2	3
1. Технічні	Порушення або слабкі місця в апаратному забезпеченні, мережевій інфраструктурі та фізичних компонентах системи	Зношене або застаріле обладнання, відмова мережевих вузлів, відсутність резервування критичних компонентів
2. Програмні	Недоліки, помилки чи закриті прогалини у програмному забезпеченні, які можуть бути використанні для порушення роботи системи	Відсутність оновлень ПЗ, вразливості у кодуванні, помилки у конфігурації або патч-менеджменті
3.Користувацькі	Слабкі місця, пов’язані з діями або помилками користувачів, що відкривають можливості для реалізації загроз	Слабкі паролі або повторне використання доступів, фішингова поведінка, нехтування інструкціями безпеки
4. Організаційні	Недостатня регламентація процесів, відсутність політик, процедур або контролю	Відсутність чітких правил доступу, нерегулярне резервне копіювання, низька культура інформаційної безпеки

Продовження таблиці 1.10

1	2	3
5. Інтеграційні	Проблеми, що виникають під час взаємодії між різними системами, сервісами або модулями	Помилки API-інтеграцій, несумісність протоколів, слабкі механізми контролю сторонніх постачальників
6. Інфраструк-турні	Слабкі місця у фізичній або мережевій інфраструктурі, що роблять системи чутливими до збоїв і зовнішніх чинників	Залежність від одного провайдера, інтернету чи хмари, відсутність резервних каналів зв'язку, низька відмовостійкість мереж
7.Процесуальні	Недоліки в організації процесів, що підтримують цифрову інфраструктуру, та в управлінні життєвим циклом ІТ-систем	Слабкий контроль змін, відсутність планів реагування на інциденти, неузгоджені процеси техпідтримки

Проведена класифікація вразливостей цифрової інфраструктури дозволяє виділити ключові слабкі місця, через які різні групи ризиків здатні реалізуватися та завдати суттєвої шкоди функціонуванню підприємства. Вразливості мають різну природу – від технічних недоліків обладнання або програмного забезпечення до організаційних прогалин, недостатньої цифрової грамотності персоналу чи помилок інтеграції між інформаційними системами. Саме поєднання цих чинників визначає загальний рівень стійкості інфокомунікаційної системи та ступінь її чутливості до зовнішніх і внутрішніх загроз.

Відтак, значущість виявлених вразливостей полягає у тому, що вони функціонують як «вхідні точки» для ризиків і визначають реальну ймовірність їх матеріалізації. Навіть за наявності сучасних технологій та розвиненої інфраструктури саме слабкі або недостатньозахищені елементи можуть спричинити масштабні збої, порушення бізнес-процесів та втрату критично важливої інформації. У контексті виявлених ризиків і вразливостей особливої ваги набуває, яким чином інфокомунікаційні ресурси можуть бути задіяні для

посилення стійкості підприємства, зменшення чутливості інфраструктури до загроз і забезпечення її безперервності.

В. Функції інфокомунікаційних ресурсів у запобіганні та подоланні кризових явищ. Ефективне використання інфокомунікаційних ресурсів є ключовим чинником підвищення стійкості підприємства до кризових впливів і забезпечення безперервності його діяльності. У сучасних умовах, коли швидкість поширення інформації, інтенсивність кібернетичних загроз та нестабільність зовнішнього середовища зростають, роль цифрових інструментів у запобіганні, виявленні та подоланні криз набуває особливої ваги. *Інфокомунікаційні ресурси виступають не лише технічним забезпеченням функціонування бізнес-процесів, але й системоутворюючим елементом антикризового управління,* що дає змогу оперативно реагувати на зміни, підтримувати критичні операцій та відновлюватися після деструктивних впливів.

Здатність підприємства протистояти кризам значною мірою залежить від того, наскільки ефективно організовані процеси збору, оброблення, аналізу та передачі інформації. У даному контексті інфокомунікаційні ресурси виконують комплекс функцій, спрямованих на забезпечення інформаційної прозорості, своєчасного виявлення загроз, координації дій між підрозділами, підтримки рішень та захисту критично важливих цифрових активів. Саме їх функціональне наповнення визначає можливості підприємства щодо запобігання негативним наслідкам кризових ситуацій і мінімізації ризиків, пов’язаних з порушенням роботи цифрової інфраструктури.

Така багатовекторність ролей інфокомунікаційних ресурсів зумовлює необхідність їх системного розгляду як цілісного функціонального механізму, що інтегрує інформаційні, технологічні, комунікаційні та безпекові компоненти. У кризових умовах кожен із цих компонентів виконує специфічні завдання: від раннього виявлення відхилень у роботі систем до забезпечення узгодженої взаємодії підрозділів і підтримки обґрунтованих управлінських рішень. У результаті інфокомунікаційні ресурси проявляють себе не лише як

інструменти технічної підтримки, а як ключові елементи адаптивності, гнучкості та стійкості підприємства.

Важливим є і те, що функціональний потенціал цих ресурсів дозволяє підприємству не просто реагувати на кризові явища, а й формувати випереджувальну модель поведінки через аналітику, прогнозування, накопичення знань та створення резервних сценаріїв дій. Це підсилює здатність підприємства швидко відновлювати порушені процеси, мінімізувати втрати та забезпечувати керованість у період підвищеної турбулентності. З огляду на це доцільним є представити ключові функції інфокомунікаційних ресурсів, спрямованих на запобігання та подолання кризових явищ (рис. 1.8).

Рисунок 1.8 – Функції інфокомунікаційних ресурсів у запобіганні та подоланні кризових явищ (*джерело: авторська розробка*)

Представлена схема узагальнює ключові функції інфокомунікаційних ресурсів, що формують основу антикризового механізму підприємства. Кожна з них виконує окрему, але взаємопов’язану роль у забезпеченні стійкості

підприємства до зовнішніх і внутрішніх загроз. Їх сукупна дія створює цілісне цифрове середовище, здатне підтримувати стабільність операцій, забезпечувати безперервність інформаційних потоків та сприяти швидкому відновленню бізнес-процесів після кризових впливів. Узагальнене та змістове наповнення цих функцій дозволяє визначити, яким чином інфокомунікаційні ресурси забезпечують проактивне управління ризиками та підвищують адаптивність підприємства в умовах турбулентності.

Функція моніторингу та раннього виявлення загроз забезпечує безперервний контроль стану цифрової інфраструктури та ідентифікацію відхилень, які можуть свідчити про наближення кризової ситуації. Використання інструментів моніторингу та аналізу дає змогу оперативно фіксувати порушення в роботі систем, підвищену активність у каналах зв’язку або спроби несанкціонованого доступу. Завдяки цьому підприємство здатне зменшити часовий лаг між появою загрози та реакцією на неї, що істотно скорочує масштаби потенційних збитків.

Функція координації та синхронізації дій підрозділів полягає у тому, що кризові явища потребують узгодженості рішень і швидкої взаємодії між структурними підрозділами. В свою чергу інфокомунікаційні ресурси створюють єдине інформаційне середовище, у межах якого здійснюється обмін повідомленнями, постановка завдань, фіксація дій і контролювання їх виконання. Це мінімізує дублювання операцій, зменшує хаотичність поведінки підприємства та дозволяє реалізовувати скоординовані заходи у відповідь на кризові впливи.

Функція відновлення та підтримки стійкості охоплює заходи, спрямовані на мінімізацію простоїв та швидке відновлення роботи цифрової інфраструктури після інцидентів. До її змісту належать резервування ресурсів, використання альтернативних каналів доступу, дублювання інформаційних систем та застосування процедур аварійного відновлення. Завдяки цьому забезпечується безперервність критично важливих функцій підприємства навіть у разі масштабних порушень.

Функція аналітичної підтримки управлінських рішень полягає у такому: аналітичні ресурси забезпечують керівництво підприємства достовірними даними, необхідними для оцінки ймовірності виникнення ризиків, визначення найбільш критичних напрямів впливу та вибору оптимальних дій у кризових умовах. Застосування систем бізнес-аналітики, інструментів машинного навчання та прогнозних моделей дозволяє формувати сценарії реагування, оцінювати їх ефективність та приймати обґрунтовані рішення під тиском часу та невизначеності.

У періоди криз кіберзагрози суттєво зростають, тому ключовим завданням інфокомунікаційних ресурсів є захист даних, інформаційних систем і каналів комунікації. Реалізація функції забезпечення кібербезпеки та захисту критичних активів включає контроль доступу, криптографічний захист, багаторівневу автентифікацію, виявлення загроз і моніторинг критичної активності. Це дозволяє запобігти втручанню, несанкціонованому доступу та пошкодженню цифрових активів підприємства.

Функція забезпечення інформаційної прозорості та безперервності обміну полягає у такому: інформаційна прозорість є критичною у періоди динамічності, коли своєчасність даних визначає ефективність оперативних рішень. Інфокомунікаційні ресурси підтримують стабільність інформаційних потоків, забезпечують доступ до актуальної інформації всім учасникам процесу, незалежно від їх локації чи режиму роботи. Це створює умови для оперативного реагування, зменшує ймовірність інформаційних розривів та забезпечує синхронність дій.

Кожна криза генерує унікальний досвід, який за належної фіксації може підвищити ефективність майбутнього реагування. Інфокомунікаційні ресурси створюють платформу для накопичення знань про інциденти, документування процедур та формування бази найкращих практик. Саме тому функція інституціоналізації знань та накопичення досвіду кризового генерування сприяє розвитку організаційної пам’яті, стандартизації дій у повторюваних ситуаціях та підвищенню узгодженості антикризових процесів.

Відтак, формування інфокомунікаційної структури підприємства в умовах кризових викликів набуває стратегічного значення, оскільки саме вона забезпечує можливість підтримувати стабільність, керованість та адаптивність ключових процесів у періоди підвищеної невизначеності. *Сучасна інфраструктура має розглядатися як цілісний соціотехнічний комплекс, у межах якого поєднуються інформаційні, технологічні, комунікаційні, безпекові та інтеграційно-аналітичні елементи, що взаємодіють між собою для створення єдиного цифрового середовища.* Кризові умови суттєво підсилюють вплив ризиків і вразливостей цифрової інфраструктури, що потребує систематизованого підходу до їх ідентифікації та оцінювання. Виявлені технологічні, кібернетичні, організаційні, інтеграційні та зовнішні ризики демонструють широкий спектр загроз, а класифікація вразливостей підкреслює важливість урахування не лише технічних, але й процесуальних, користувацьких та інфраструктурних аспектів.

Це формує підґрунтя для розроблення дієвих механізмів захисту та підвищення стійкості цифрового середовища підприємства. Тим самим інфокомунікаційна інфраструктура в умовах викликів постає як стратегічний елемент забезпечення цифрової стійкості підприємства. Її ефективне формування та управління дозволяє мінімізувати вразливості, підвищити готовність до зовнішніх впливів та забезпечити безперервність критичних бізнес-процесів у довгостроковій перспективі.

Висновки до розділу 1

Дослідження теоретичних засад формування цифрових інфокомунікаційних ресурсів підприємства в умовах криз дозволило дійти *таких ключових висновків*:

1. *Цифрові інфокомунікаційні ресурси* доцільно трактувати не як сукупність розрізнених технологічних інструментів, а як інтегровану

соціотехнічну систему, яка забезпечує органічне поєднання інформаційних потоків, цифрових даних, інструментів їх обробки, мережевих платформ і систем кіберзахисту. Їхня фундаментальна роль полягає у формуванні цілісної цифрової архітектури підприємства , що забезпечує безперервну реалізацію управлінських, виробничих і сервісних процесів. Цифрові інфокомунікаційні ресурси є динамічною та стратегічною категорією, оскільки їхнє ефективне використання створює стійкі конкурентні переваги та зміцнює здатність суб'єктів господарювання до інноваційного розвитку в умовах глобальної цифрової економіки.

2. Систематизація цифрових інфокомунікаційних ресурсів базується на *багаторівневій класифікаційній структурі, яка за функціональним призначенням виділяє п'ять ключових груп*: інформаційні, комунікаційні, технологічні, інфраструктурні та кібербезпекові ресурси. Ця структура не є статичною, оскільки цифрові інфокомунікаційні ресурси пройшли закономірну еволюційну послідовність: від локальних інформаційно-обчислювальних систем і корпоративних інфомаційнпих систем (ERP, CRM) до сучасних інтегрованих цифрових екосистем. Такий еволюційний перехід свідчить про *зміну парадигми інфокомунікаційного забезпечення діяльності та розвитку підприємств*: від простої автоматизації окремих операцій до глибокої інтеграції даних, IoT, ШІ та мережевих сервісів, що перетворює цифрові інфокомунікаційні ресурси на стратегічну основу організаційного оновлення та підвищення технологічної зрілості підприємства.

3. *Вплив цифрових ресурсів на розвиток підприємства реалізується через впровадження діджиталізаційних та смарт-моделей управління, які якісно трансформують логіку управлінських процесів і стратегічного планування*. У цій архітектурі цифрові ресурси (дані, ШІ, хмарні сервіси, IoT) виступають як каталізатор, що забезпечує інтеграцію даних, інтелектуальну аналітику та синхронізацію інформаційних потоків, сприяючи підвищенню точності й обґрунтованості управлінських рішень. Таким чином, *підприємство переходить до більш передбачуваного, даних-орієнтованого та*

адаптивного управління, формуючи інтелектуальні системи підтримки рішень, здатні до самонавчання та безперервної адаптації.

4. *Ключовим результатом впровадження смарт-моделей є формування цифрової стійкості (Digital Resilience),* що визначається як інтегральна організаційна здатність забезпечувати безперервність діяльності та результативність в умовах цифрових ризиків. Ця стійкість формується завдяки синергії *чотирьох структурних складових*: технологічної, адаптивно-реактивної, аналітично-інформаційної та стратегічно-управлінської. В контексті антикризового менеджменту, інфокомунікаційні платформи набувають інституційної ролі, забезпечуючи прозоре, швидке та узгоджене цифрове середовище для координації стейкхолдерів, оперативного обміну даними та прийняття рішень у режимі реального часу.

5. *Формування інфокомунікаційної інфраструктури в кризових умовах реалізується через складну системну архітектуру, яка функціонально складається з п'яти ключових елементів:* інформаційного, технологічно-інфраструктурного, комунікаційного, інтеграційно-аналітичного та елемента цифрової безпеки й стійкості. Проте її ефективність постійно наражається на ризики, які мають багатовимірний характер (технологічні, кібернетичні, організаційні, зовнішні/кризові), а також на численні вразливості (технічні недоліки, програмні прогалини, помилки користувачів, організаційні прогалини). Ці вразливості функціонують як «вхідні точки» для загроз, що вимагає систематичного підходу до їх ідентифікації та формування комплексних механізмів мінімізації ризиків.

6. Інфокомунікаційні ресурси набувають стратегічного функціонального потенціалу у запобіганні та подоланні кризових явищ, виступаючи системоутворюючим елементом антикризового управління. *Їхні ключові антикризові функції охоплюють:* моніторинг та раннє виявлення загроз , координацію та синхронізацію дій підрозділів , аналітичну підтримку рішень та критично важливу функцію відновлення та підтримки стійкості. Належна реалізація цих функцій через резервування систем, застосування

прогнозної аналітики та посилення кібербезпеки дозволяє підприємству перейти до проактивної моделі поведінки, забезпечуючи керованість та безперервність критичних бізнес-процесів навіть у періоди високої турбулентності.

7. Наведене дозволило сформулювати таку *робочу гіпотезу дослідження:* підвищення рівня цифрової стійкості (Digital Resilience) та інфокомунікаційне забезпечення розвитку підприємства в умовах кризових викликів може бути досягнуте шляхом впровадження інтегрованої системи управління цифровими інфокомунікаційними ресурсами (ЦІКР), яка базується на принципах проактивного ризик-менеджменту, адаптивності цифрової архітектури та синергії технологічних, комунікаційних та кібербезпекових елементів. Перевірка цієї гіпотези здійснюватиметься шляхом дослідження стану та ефективності використання інфокомунікаційних цифрових ресурсів та оцінювання цифрової зрілості підприємств за ключовими вимірами, аналізу інфокомунікаційного забезпечення та порівняння рівнів цифрової стійкості підприємств різних галузей і інституційних середовищ.

Результати розділу 1 висвітлено у працях автора, наведених у Додатку А. Це публікаії: [1, 5, 6].

РОЗДІЛ 2
АНАЛІТИЧНА ОЦІНКА СТАНУ ТА ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ІНФОКОМУНІКАЦІЙНИХ ЦИФРОВИХ РЕСУРСІВ НА ПІДПРИЄМСТВАХ

2.1 Аналіз зовнішніх кризових факторів та їх впливу на цифрову інфраструктуру підприємств

Послідовність аналізу зовнішніх кризових факторів та їх впливу на цифрову інфраструктуру підприємств може бути представлена *такими етапами:*

а) ідентифікація зовнішніх кризових факторів, що формують загальноекономічний, політичний, техногенний, кібернетичний та соціальний тиск на діяльність підприємства;

б) аналіз міжнародних практик реагування на зовнішні кризові впливи, зокрема досвіду Об'єднаних Арабських Еміратів щодо формування пріоритетів інвестування у цифрові технології та модернізацію цифрової інфраструктури.

А. Ідентифікація зовнішніх кризових факторів, що формують загальноекономічний, політичний, техногенний, кібернетичний та соціальний тиск на діяльність підприємства. Процес ідентифікації зовнішніх кризових факторів передбачає системне виявлення та класифікацію тих впливів зовнішнього середовища, які здатні порушувати стабільність функціонування підприємства та створювати підвищений тиск на його цифрову інфраструктуру. У сучасних умовах зростання турбулентності економічних процесів, активізації геополітичних конфліктів та ескалації кібернетичних загроз проведення даного етапу є доволі важливим.

В умовах посилення зовнішніх кризових впливів особливого значення набуває аналіз глобальних тенденцій розвитку цифрових технологій та

визначення пріоритетних напрямів інвестування у провідних країнах світу (рис. 2.1). Це зумовлено тим, що міжнародні практики формують орієнтири для підвищення стійкості цифрової інфраструктури, дають змогу оцінити ефективність різних моделей технологічної модернізації та визначити інструменти, які забезпечують найбільший захист від кризових загроз.

Рисунок 2.1 – Основні пріоритети інвестицій у цифрові технології у світі (*джерело: систематизовано автором на підставі* [100-115])

Одним із ключових стратегічних напрямів глобальних інвестицій у цирфові технології є розвиток *штучного інтелекту* (далі – ШІ) та пов’язаної з ним інфраструктури. Впродовж останніх років ШІ трансформувався з інноваційного інструмента в основу технологічної конкурентоспроможності

держав і корпорацій, що обумовлює різке зростання капіталовкладень у відповідні технологічні рішення. Найбільші світові технологічні компанії, зокрема Google, Microsoft, Amazon, та фінансові інституції інвестують у створення хмарних обчислювальних платформ і модернізацію серверних систем [100]. Це спрямовано на формування так званих «обчислювальних фабрик», здатних забезпечити роботу великих моделей ШІ, генеративних систем, інструментів аналітики та автоматизації.

Динаміка прогнозованого зростання світового ринку ШІ відображена на рис. 2.2.

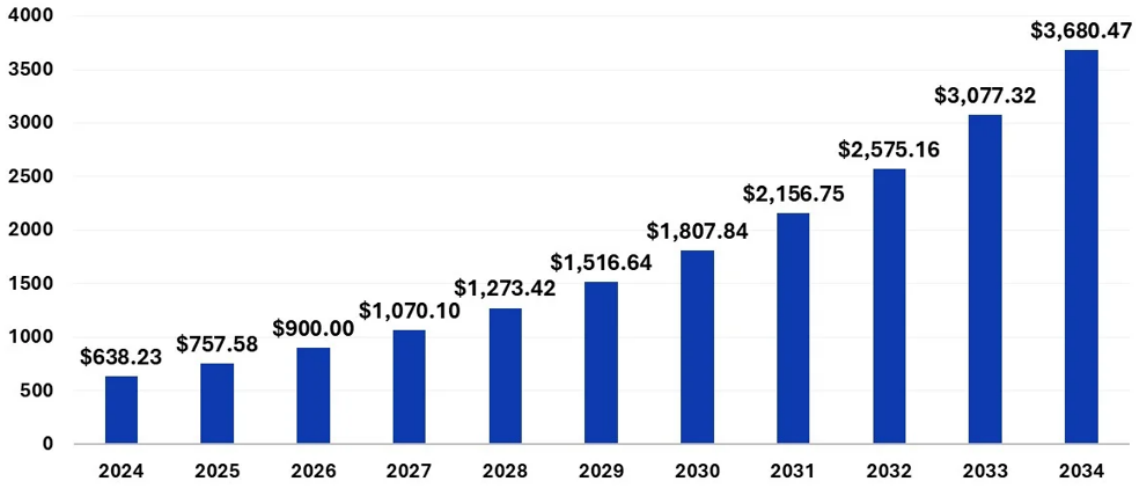


Рисунок 2.2 – Динаміка прогнозованого зростання світового ринку ШІ у 2024-2034 рр., млрд дол. США (*джерело*: [101])

Згідно з прогнозами провідних консалтингових компаній, сукупні витрати на виробництво високопродуктивних чипів, побудову центрів обробки даних та створення обчислювальних кластерів можуть досягти масштабів у 2,3 трлн долл у 2025-2028 роках, що підкреслює довгостроковість і стратегічний характер інвестиційних планів у цій сфері [100].

Інвестування у ШІ та інфраструктурні потужності для його функціонування є провідним глобальним трендом і одним з основних драйверів цифрової трансформації економік світу. Розвиток дата-центрів,

хмарних платформ та обчилювальних ресурсів формує технологічний базис, що визначатиме конкурентоспроможність підприємств і держав.

Хмарні технології та моделі «everything-as-a-service» (далі – XaaS) стали фундаментом сучасної цифрової трансформації підприємств. Вони забезпечують гнучкість, масштабованість та економічну ефективність, що робить їх ключовим напрямом глобальних інвестицій. У світі, де бізнес-моделі швидко змінюються під впливом кризових факторів, перехід до хмари та сервісної економіки стає стратегічною необхідністю. Прогноз динаміки світового ринку хмарних технологій відображено на рис. 2.3.

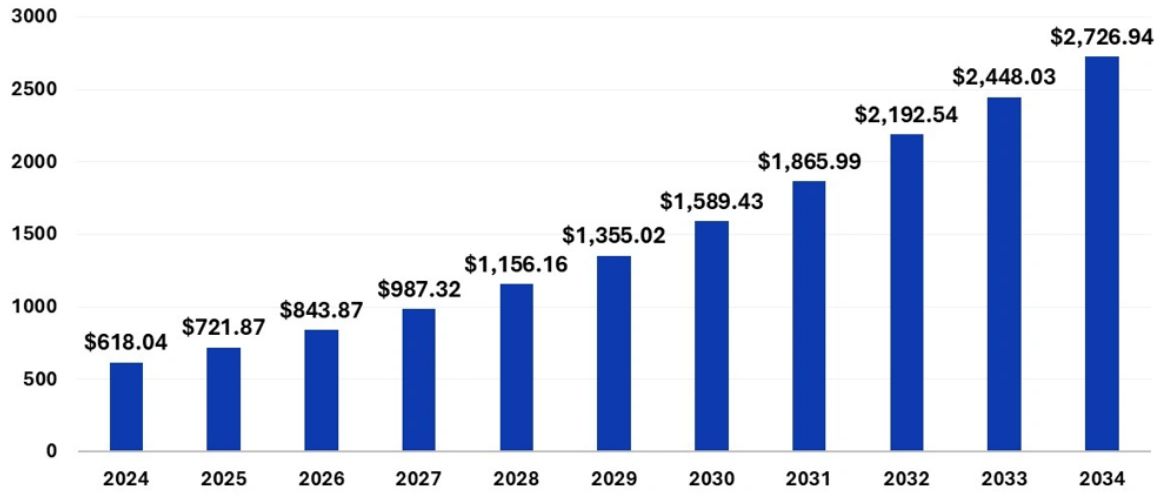


Рисунок 2.3 – Прогноз динаміки світового ринку хмарних технологій у 2024-2034 рр., млрд дол. США (*джерело*: [101])

Відповідно до результатів міжнародних аналітичних досліджень, компанії, що активно інвестують у хмарні рішення, автоматизацію ШІ та кібербезпеку, демонструють найвищі темпи зростання прибутковості та операційної ефективності [102]. Це підтверджує синергію між цифровою інфраструктурою та сучасними управлінськими моделями. Поширення моделей SaaS, PaaS, IaaS та XaaS дозволяє підприємствам мінімізувати капітальні витрати н IT-інфраструктуру, замінюючи їх операційними витратами залежно від фактичного використання ресурсів. Такий підхід

прискорює цифровізацію та дає змогу інтегрувати інноваційні сервіси без значних стартових інвестицій.

Хмарні сервіси, XaaS-платформи та цифровізація бізнес-процесів формують базовий технологічний набір взаємопов'язаних інструментів, технологій, сервісів, компонентів, що направлено на модернізацію рідприємстсва. Саме вони забезпечують гнучкість, швидкість інновацій, оптимізацію витрат та операційну стійкість, що робить їх пріоритетним напрямом цифрових інвестицій у світі.

У сучасних умовах стрімкої цифровізації підприємств *кібербезпека* стає однією з найпріоритетніших сфер інвестування. Зростання масштабів кіберзагроз, поширення хмарних платформ, розвиток дистанційних форм роботи та збільшення обсягів даних радикально підвищують вимоги до захисту інформаційних систем. Тому цифрова безпека перетворюється на стратегічний елемент забезпечення стійкості бізнесу та його репутаційної надійності.

Прогноз динаміки світового ринку кібербезпеки відображено на рис. 2.4.

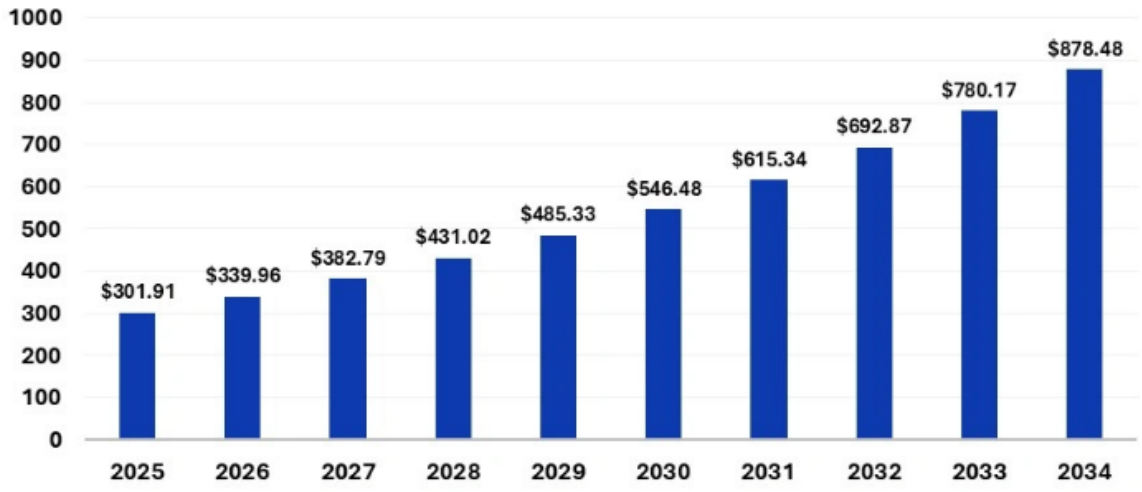


Рисунок 2.4 – Прогноз динаміки світового ринку кібербезпеки у 2024-2034 рр., млрд дол. США (*джерело*: [101])

Згідно з міжнародними опитуваннями, значна частина у різних секторах економіки визначають кібербезпеку пріоритетним напрямом інвестицій, що

випереджає традиційні IT-напрями [103, 104]. Це свідчить про системне усвідомлення загроз, пов’язаних із цифровою трансформацією. На тлі зростання обсягів даних, активного впровадження хмарних рішень, використання віддалених режимів роботи та поширення цифрових сервісів зростають кіберризики, а разом з ними – потреба у косплексних рішеннях для захисту даних, контролю доступів, криптографічних протоколів та безпечного зберігання інформації.

Тим самим кібербезпека є критично важливою складовою інвестиційного портфеля цифрових рішень, оскільки вона забезпечує стабільність роботи підприємства, захист репутації та збереження довіри клієнтів у глобальному цифровому середовищі. Саме тому інвестиції у безпеку розглядаються як стратегічно необхідні для забезпечення довгострокової стійкості бізнесу.

Автоматизація та цифровізація виробництва, промисловості й операцій (промисловий IT, IoT, Digital Twin, «розумні» рішення, Industry 4.0/5.0), що пояснюється тим, що автоматизація та цифрова модернізація виробничих і операційних процесів стають фундаментальною передумовою підвищення ефективності та стійкості підприємств у глобально турбулентному середовищі. Перехід від традиційних, ручних або частково механізованих процесів до інтегрованих цифрових систем Industry 4.0 та майбутньої Industry 5.0 зумовлює зростання попиту на інвестиції у сучасні промислові технології.

Поточні тенденції у виробничих та підприємницьких секторах характеризуються активним впровадженням автоматизованих систем управління, IoT-технологій, «цифрових двійників», інтелектуальних сенсорних платформ та «розумних» ланцюгів постачання, що забезпечують прозорість, контроль та оптимізацію операцій [105, 106]. Розвиток цифрового промислового IT та інтегрованих технологічних середовищ стимулює масштабне залучення інвестицій. Прогноз динаміки світового ринку автоматизації та цифровізації виробництва відображено на рис. 2.5.

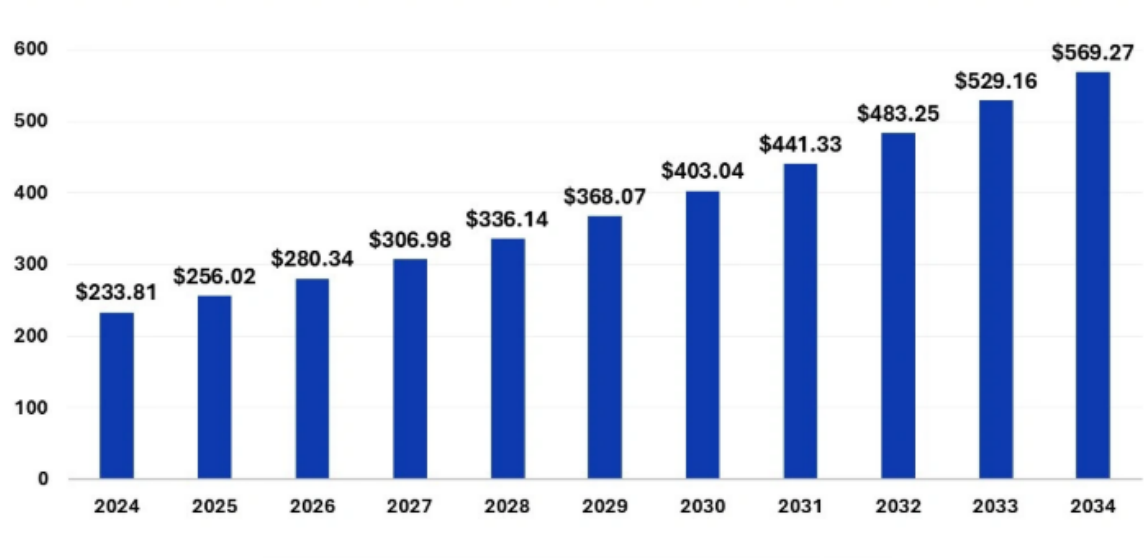


Рисунок 2.5 – Прогноз динаміки світового ринку автоматизації та цифровізації виробництва у 2024-2034 рр., млрд дол. США (*джерело*: [101])

Підприємства різних галузей дедалі частіше впроваджують цифрові виробничі екосистеми, де ключові процеси базуються на автоматизованому зборі даних, роботизованих технологіях, Smart Factory-рішеннях та прогнозній аналітиці. Така модернізація відповідає вимогам нової моделі конкурентоспроможності у світовій промисловості.

«Розумна» цифрова трансформація виробництва є пріоритетом не лише для технологічних компаній, а й для традиційних підприємств, оскільки вона забезпечує конкурентні переваги, підвищує стійкість до кризових впливів та створює умови для довгострокового інноваційного розвитку.

Інвестиції в цифрові компетенції та організаційну трансформацію, адже цифрова трансформація неможлива без відповідної еволюції організаційних структур, управлінської культури та компетенцій персоналу. Незважаючи на стрімкий розвиток технологій, саме людський капітал і організаційна готовність визначають здатність підприємства ефективно інтегрувати цифрові рішення та отримувати від них економічний і стратегічний ефект. Тому інвестиції у розвиток цифрових навичок, управління знаннями та модернізацію бізнес-процесів стають одними з ключових пріоритетів у світі.

Дослідження свідчать, що підприємства, які системно вкладають ресурси у навчання персоналу, розвиток цифрової грамотності, удосконалення бізнес-процесів та управлінської трансформації, демонструють вищу віддачу від цифрових інвестицій та швидше проходять етапи цифрової зрілості [107, 108]. Це підтверджує, що ефективність технологій безпосередньо залежить від рівня підготовленості організації до їх впровадження.

Динаміку світового ринку організаційної трансформації робочого середовища за регіонами відображено на рис. 2.6.

Рисунок 2.6 – Динаміка світового ринку організаційної трансформації робочого середовища за регіонами у 2018-2030 рр., млрд дол. США (*джерело*: [109])

У світі формується тенденція до переорієнтації інвестицій з виключно технічних напрямів на «м'які» елементи цифрової трансформації – організаційну культуру, лідерство, внутрішні комунікації, управління даними та зміну моделей прийняття рішень. Це забезпечує сталість цифрових перетворень і підвищує їхню результативність у довгостроковій перспективі.

«М’які» складові цифрової трансформації – люди, культура, процеси, навички – все частіше стають об’єктами стратегічних інвестицій. Саме вони визначають здатність підприємства ефективно впроваджувати технології, підвищувати стійкість до кризових змін і забезпечувати сталий інноваційний розвиток.

Стабільність, стійкий розвиток та «зелена»/екологічна цифровізація, адже сталий розвиток і екологічна відповідальність стають невід’ємними складовими глобальної інвестиційної політики у сфері цифрових технологій. У контексті посилення кліматичних ризиків, зростання споживання енергії цифровою інфраструктурою та підвищених вимог міжнародних стандартів підприємства дедалі частіше інтегрують принципи «зеленого» IT у свої стратегії цифрової трансформації [110, 111].

Динаміка світового ринку «зелених» дата-центрів за компонентами у 2020-2030 рр. відображена на рис. 2.7.

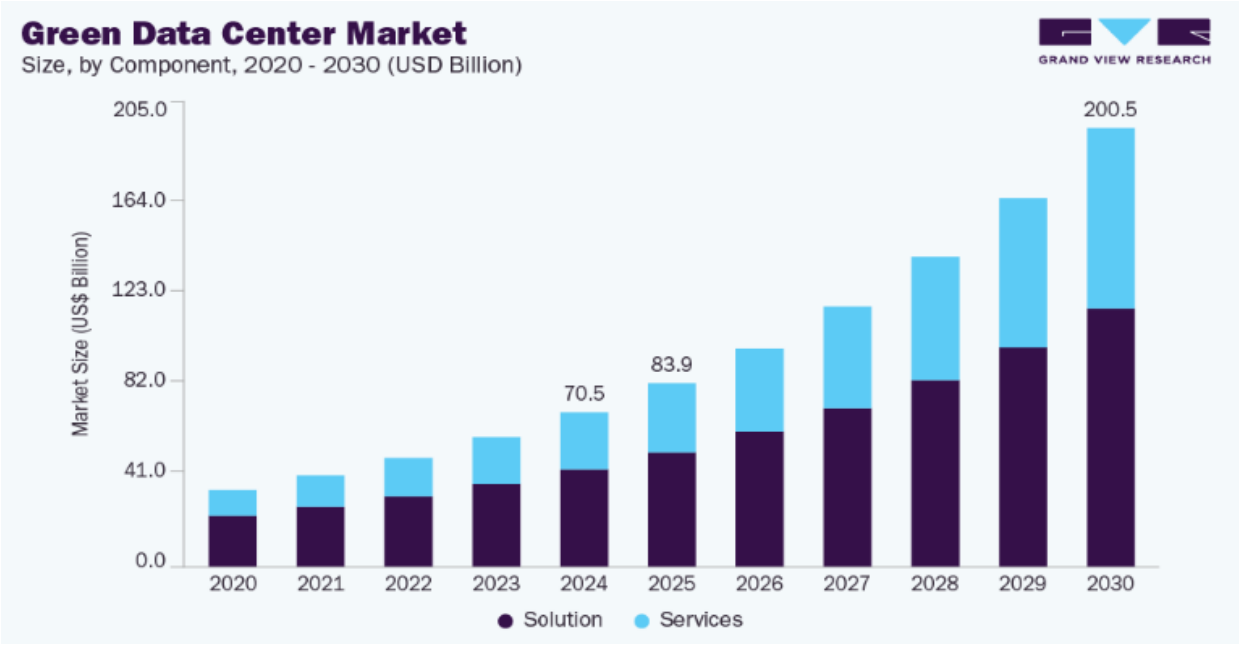


Рисунок 2.7 – Динаміка світового ринку «зелених» дата-центрів за компонентами у 2020-2030 рр., млрд дол. США (*джерело*: [109])

Як бачимо, у світі формується довгостроковий тренд, у межах якого цифрові інструменти використовуються для моніторингу екологічних

показників, оптимізації енергоспоживання, моделювання кліматичних сценаріїв та впровадження екологічно орієнтованих управлінських рішень. Це розширює функціональність цифрової інфраструктури підприємств та підвищує її стратегічну цінність як для поточної діяльності підприємств, так і перспектив їх розвитку.

Прогноз динаміки світового ринку сталих та енергоефективних цифрових технологій відображено на рис. 2.8.

Рисунок 2.8 – Прогноз динаміки світового ринку сталих та енергоефективних цифрових технологій у 2024-2034 рр., млрд дол. США (*джерело*: [101])

Парадигма «цифрове + екологічне» стає ключовим вектором глобальних інвестицій, оскільки поєднує технологічний прогрес зі стійким і відповідальним розвитком. Екологічна цифровізація формує підґрунтя для довгострокової стійкості економічних систем та забезпечує стратегічні переваги підприємствам у нових глобальних умовах.

Відповідно до проведеного аналізу основних пріоритетів інвестицій у цифрові технології у світі, відобразимо зовнішні кризові фактори, що формують загальноекономічний, політичний, техногенний, кібернетичний та соціальний тиск на діяльність підприємства (рис. 2.9).

Рисунок 2.9 – Зовнішні кризові фактори, що формують загальноекономічний, політичний, техногенний, кібернетичний та соціальний тиск на діяльність підприємства (*джерело: авторська розробка*)

Представлена систематизація демонструє, що зовнішні кризові фактори формують багатовимірний тиск на діяльність підприємства, що безпосередньо позначається на вимогах до його цифрової інфраструктури. Кожний із

пріоритетних напрямів глобальних інвестицій у цифрові технології відображає окремий аспект реагування на ці виклики: від потреби у високопродуктивних обчислювальних ресурсах і захисті даних до автоматизації виробництва, розвитку цифрових компетенцій та екологічної відповідальності.

Узагальнення пріоритетних напрямів глобальних інвестицій у цифрові технології свідчить про формування нової моделі реагування підприємств і держав на зростаючу турбулентність зовнішнього середовища. Це зумовлює необхідність вивчення практичних підходів, які продемонстрували ефективність у реальних умовах кризового впливу.

Б. Аналіз міжнародних практик реагування на зовнішні кризові впливи, зокрема досвіду Об'єднаних Арабських Еміратів щодо формування пріоритетів інвестування у цифрові технології та модернізацію цифрової інфраструктури. У глобальній економіці, що характеризується високою турбулентністю, цифровою взаємозалежністю та посиленням зовнішніх криз, ефективність антикризових механізмів дедалі більше визначається здатністю держав і підприємств швидко адаптуватися до змін зовнішнього середовища. Міжнародний досвід свідчить, що країни, які системно інвестують у цифрову інфраструктуру, розвивають інтегровані інфокомунікаційні системи та підтримують інноваційні середовища, демонструють вищу стійкість до кризових впливів та забезпечують прискорене відновлення економіки. Серед таких країн особливо виокремлюються Об'єднані Арабські Емірати (далі – ОАЕ), які протягом останніх двох десятиліть сформували стратегічну модель розвитку, орієнтовану на цифрову трансформацію та технологічне лідерство. Реагуючи на зовнішні економічні, енергетичні та геополітичні виклики, ОАЕ послідовно вибудовують багаторівневу систему інвестування у цифрові платформи, хмарні сервіси, штучний інтелект, кібербезпеку та модернізацію телекомунікаційної інфраструктури, що дозволяє їм не лише мінімізувати

наслідки криз, а й формувати стратегічні конкурентні переваги. Динаміка обсягу ринку цифрової трансформації в ОАЕ відображена на рис. 2.10.

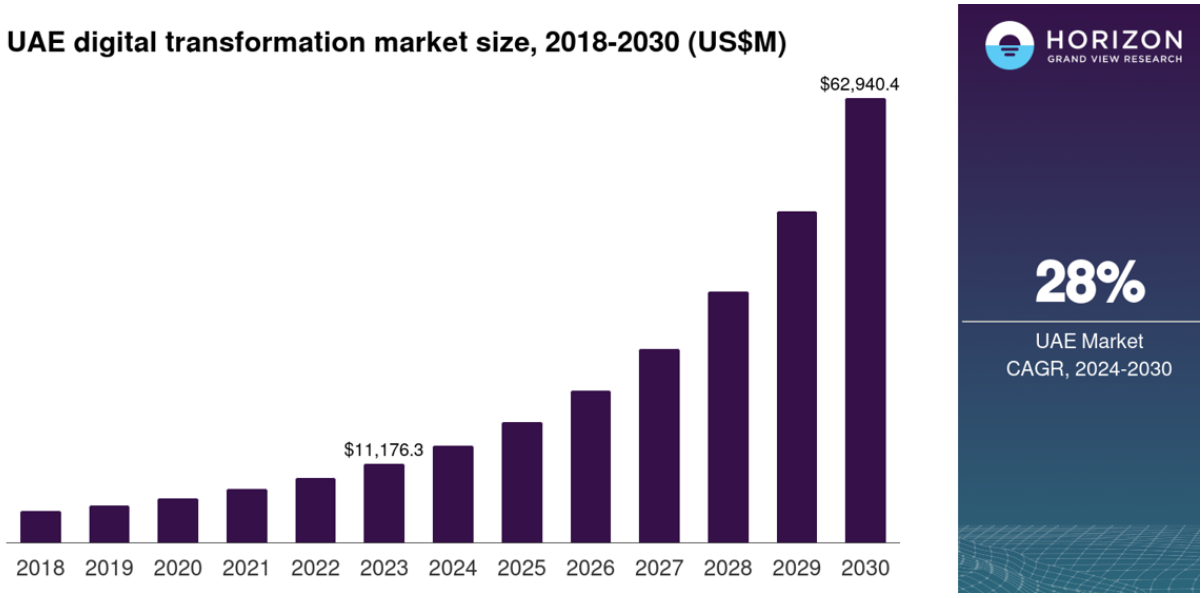


Рисунок 2.10 – Динаміка обсягу ринку цифрової трансформації в ОАЕ у 2018-2030 рр., млн дол. США (*джерело*: [115])

Відзначимо стрімке зростання ринку цифрової трансформації в ОАЕ і зазначений період. Обсяг ринку підвищується з помірних значень у 2018-2020 рр. до понад 11,1 млрд дол. США у 2023 році, а за прогнозом досягає 62,9 млрд дол. США у 2030 р. Така динаміка свідчить про аткивне інвестування у цифрові технології та інфраструктуру, що забезпечує середньорічний темп приросту ринку на рівні 28% у 2024-2030 рр.

Одним із ключових напрямів реагування ОАЕ на зовнішні кризові впливи є стратегічна концентрація інвестицій у цифрові технології та модернізацію інфокомунікаційної інфраструктури. Значну роль у цьому процесі відіграють глобальні технологічні корпорації, співпраця з якими забезпечує країні доступ до передових технологій, хмарних сервісів та рішень у сфері штучного інтелекту.

Показовим є приклад інвестиційної активності Microsoft, яка оголосила про намір інвестувати в економіку ОАЕ понад 15,2 млрд дол. у 2023–2029 рр.,

спрямовуючи ці ресурси на розбудову хмарної інфраструктури, центрів обробки даних та рішень на базі штучного інтелекту. Близько 5,5 млрд дол. у межах цього пакета передбачено для створення нових дата-центрів і розвитку хмарних платформ, тоді як решта коштів спрямовується на операційні витрати, посилення кібербезпеки та формування кадрового потенціалу цифрової економіки . Співпраця корпорації з національними IT-групами, серед яких G42, охоплює запуск суверенної хмарної платформи (sovereign cloud), що забезпечує надання хмарних і AI-послуг державному та приватному секторам ОАЕ [117-119]. Залучення такого масштабу зовнішнього капіталу формує стратегічну основу для подальшого розвитку ШІ-екосистеми, впровадження «розумних» сервісів, зміцнення кібербезпеки та прискореної цифровізації ключових сфер суспільного та економічного життя.

Важливим елементом зміцнення цифрової інфраструктури ОАЕ є стратегічне партнерство телекомунікаційного оператора du та корпорації Microsoft. У 2025 році сторони уклали угоду про будівництво гіпермасштабного дата-центру вартістю близько 2 млрд дирхамів (≈ 544,5 млн дол. США), що стало одним із найбільших проєктів цифрової інфраструктури в регіоні. Запланований центр обробки даних має виконувати роль базової інфраструктури для розвитку хмарних сервісів і рішень штучного інтелекту, забезпечуючи високий рівень безпеки, масштабованості та доступності цифрових послуг [120-121].

Реалізація цього проєкту інтегрується у національну стратегію трансформації ОАЕ, спрямовану на формування країни як глобального хаба штучного інтелекту та сучасних цифрових технологій. Масштабність інвестицій та участь провідних міжнародних корпорацій підсилюють інноваційний потенціал держави та створюють довгострокові передумови для стабільного розвитку цифрової економіки.

Важливим стратегічним проєктом у формуванні цифрової інфраструктури ОАЕ є ініціатива технологічної групи G42 щодо створення масштабного AI-кампусу Stargate UAE, загальна проєктна потужність якого

становить близько 5 ГВт. Введення в експлуатацію перших 200 МВт заплановано на 2026 рік, що свідчить про поетапний характер розвитку та високий технологічний рівень інвестицій. За даними Reuters, до реалізації проєкту залучено провідних світових виробників обладнання та технологічних партнерів, що забезпечує відповідність інфраструктури міжнародним стандартам розвитку високопродуктивних обчислень та штучного інтелекту [122].

AI-кампус Stargate розглядається не лише як центр обробки даних, а як фундаментальна інституційно-технологічна основа для розвитку майбутніх «розумних» індустрій, цифрових сервісів, дослідницьких платформ та масштабованих AI-рішень. Його функціонування сприятиме прискоренню інноваційних процесів, підвищенню цифрової спроможності економіки та зміцненню позицій ОАЕ як одного з ключових глобальних центрів розвитку штучного інтелекту.

Поряд із масштабними державними та корпоративними інвестиціями в інфраструктурні проєкти, в ОАЕ спостерігається широке поширення хмарних та AI-орієнтованих рішень серед бізнес-сектору. За результатами опитування KPMG [124], 96 % технологічних компаній країни планують нарощувати інвестиції у public та multi-cloud рішення протягом найближчих 12 місяців, що свідчить про високу готовність ринку до глибокої цифрової трансформації. Крім того, приблизно 67 % підприємств уже перенесли ключові бізнес-функції у хмарне середовище, а ще близько 22 % перебувають на завершальному етапі переходу, згідно з даними SAP News Center [124].

Основними мотивами активного переходу бізнесу до хмарних платформ є потреба у підвищенні операційної ефективності, забезпеченні гнучкості та масштабованості, оптимізації витрат, а також створенні технологічних умов для впровадження аналітичних інструментів і рішень штучного інтелекту. Це підтверджує, що сформовані інвестиційні пріоритети ОАЕ мають системний вплив на приватний сектор, стимулюючи його до швидкого впровадження сучасних цифрових технологій.

Аналіз інвестиційних кейсів у сфері цифрових технологій в ОАЕ демонструє, що поєднання інфраструктурних проєктів, значних фінансових вкладень і залучення передових технологій створює потужне підґрунтя для формування сучасної, масштабованої та надійної IT-екосистеми, здатної підтримувати розвиток хмарних сервісів, штучного інтелекту, аналітики Big Data та «розумних» рішень. Висока концентрація капіталу у цифровій інфраструктурі забезпечує швидкий стрибок у цифровій зрілості як бізнес-сектору, так і державних інституцій, дозволяючи їм впроваджувати інноваційні рішення значно оперативніше.

ОАЕ демонструють ефективну модель взаємодії держави, глобальних технологічних корпорацій і місцевого бізнесу, у межах якої формується цілісний цифровий ландшафт, що відповідає стратегічним пріоритетам національного розвитку. Системний характер таких партнерств свідчить про здатність країни створювати умови для довгострокових інноваційних процесів, технологічного суверенітету та стійкості до зовнішніх кризових впливів.

Отриманий досвід є релевантною моделлю для країн із менш розвиненою IT-сферою, зокрема України. Він дозволяє виокремити ключові чинники успішної цифрової трансформації: наявність інвестиційного ресурсу, розбудовану інфраструктуру, послідовну державну політику, розвиток стратегічних партнерств і готовність бізнесу до технологічних змін. Застосування цих принципів може суттєво прискорити формування національної цифрової екосистеми та зміцнити здатність економіки протистояти сучасним викликам.

Об’єднані Арабські Емірати сьогодні є одним із глобальних лідерів цифрової трансформації, демонструючи системний підхід до формування цифрової економіки та залучення інвестицій у високотехнологічні напрями. Урядова стратегія «UAE Digital Government Strategy 2025» та «UAE Fourth Industrial Revolution Strategy» визначають пріоритети, які спрямовують

державні та приватні інвестиції на розвиток цифрових рішень, інфраструктури та інноваційних технологічних екосистем.

Ключовою особливістю підходу ОАЕ є комплексність: інвестиції не лише підтримують розвиток технологій, а й формують нові ринки, підсилюють ефективність державного управління та підвищують конкурентоспроможність підприємств. Значну увагу приділено створенню інноваційних хабів, цифрових кластерів, стимулюванню участі міжнародних технологічних компаній, а також підтримці локальних стартапів.

Серед найбільш значущих напрямів інвестування: штучний інтелект, розумні міста, кібербезпека, фінтех, цифрове державне управління, блокчейн, автономний транспорт, хмарна інфраструктура та data-centric системи. Поєднання амбітних національних стратегій, податкових пільг та міжнародних цифрових партнерств робить ОАЕ одним із найдинамічніших цифрових центрів світу. Інвестиційні кейси ОАЕ у сфері цифрових технологій відображено у табл. 2.1.

Таблиця 2.1 – Інвестиційні кейси ОАЕ у сфері цифрових технологій *(джерело: систематизовано автором на підставі* [126-132])

Напрям цифрових інвестицій	Опис кейсу	Вплив на економіку
1	2	3
1. Штучний інтелект (AI)	Національний проєкт UAE National AI Strategy 2031, створення посади Міністра з питань ШІ – першого у світі	Розвиток ринку цифрових послуг, залучення глобальних AI-компаній, підвищення продуктивності державного сектору
2. Розумні міста (Smart City)	Платформа Smart Dubai: інтеграція IoT, Big Data, цифрових сервісів для побутових, адміністративних та транспортних систем	Значне скорочення витрат, підвищення якості державних послуг, створення нових інноваційних кластерів
3. Блокчейн	UAE Blockchain Strategy 2021: впровадження блокчейну у 50 %	Підвищення прозорості, зменшення бюрократії, розвиток фінтех-стартапів

Продовження табл. 2.1

1	2	3
	державних транзакцій; Dubai Blockchain Center.	
4. Кібербезпека	Створення UAE Cybersecurity Council; інвестиції у кіберзахист інфраструктур і бізнесу	Зміцнення цифрової стійкості підприємств та державних систем, спрощення інвестклімату
5. Автономний транспорт	Dubai Autonomous Transportation Strategy: роботизовані таксі, автономний громадський транспорт	Розвиток нової індустрії, зменшення транспортних витрат, покращення мобільності
6. Фінтех та цифрові платежі	Dubai International Financial Centre (DIFC) Innovation Hub; регуляторні пісочниці	Зростання екосистеми стартапів, залучення міжнародних фінтех-компаній, нові фінансові продукти
7. Хмарні технології та дата-центри	Інвестиції Microsoft, Amazon Web Services, Oracle у відкриття дата-центрів в ОАЕ	Формування регіонального цифрового хабу, підтримка масштабування бізнесу
8. Медичні цифрові технології	Програма цифрової медицини Dubai Health, впровадження телемедицини та AI-діагностики	Оптимізація медичних витрат, покращення доступності послуг
9. EdTech та цифрова освіта	Національна платформа Madrasa – найбільша безкоштовна цифрова освітня платформа арабською мовою	Підготовка висококваліфікованих кадрів для цифрової економіки
10. Енергетичні цифрові системи	Smart Grid Dubai, AI-оптимізація енерго-споживання	Підвищення енергоефективності, зменшення операційних витрат бізнесу

Представлені в табл. 2.1 інвестиційні кейси демонструють системність підходу ОАЕ до формування цифрової економіки та створення високотехнологічної інфраструктури на національному рівні. Урядові стратегії, партнерські програми з глобальними технологічними компаніями та розвиток локальних інноваційних центрів забезпечують швидке

масштабування цифрових рішень у ключових секторах – від транспорту й фінтеху до охорони здоров’я, кібербезпеки та освіти. Сукупність цих ініціатив формує комплексний цифровий ландшафт, що сприяє підвищенню продуктивності державного управління, зниженню транзакційних витрат бізнесу, зростанню інноваційних кластерів і залученню міжнародних інвестицій.

Досвід ОАЕ свідчить про високу результативність інвестицій у штучний інтелект, хмарні рішення, блокчейн-технології та цифрову інфраструктуру, що забезпечує швидкий перехід до моделі економіки знань. Ці інструменти не лише підвищують технологічну спроможність держави, але й прискорюють адаптацію до глобальних кризових викликів, забезпечуючи нові конкурентні переваги. Для України аналіз означених напрямів може бути корисним у формуванні власної системи пріоритетів цифрового розвитку, адаптованої до умов відновлення та модернізації економіки.

2.2 Діагностика рівня цифрової зрілості та інфокомунікаційних ресурсів підприємства

Для комплексної оцінки рівня цифрової зрілості підприємства та ефективності використання його інфокомунікаційних ресурсів діагностику доцільно структурувати у такі взаємопов’язані блоки:

а) аналіз стану цифрової зрілості підприємства за ключовими вимірами (процеси, технології, дані, персонал, управління) на макро та мікрорівнях;

б) оцінювання цифрової зрілості трьох підприємств різних секторів (IT, фінтех, виробництво);

в) порівняльний аналіз цифрової зрілості підприємств України та ОАЕ за тими ж ключовими вимірами (процеси, технології, дані, персонал, управління).

А. Аналіз стану цифрової зрілості за ключовими вимірами (процеси, технології, дані, персонал, управління). Аналіз стану цифрової зрілості підприємства за ключовими вимірами є важливим етапом діагностики його готовності до цифрової трансформації та здатності ефективно використовувати інфокомунікаційні ресурси, оскільки надає змогу системно оцінити, наскільки бізнес-процеси, технологічна база, робота з даними, компетентності персоналу та управлінські механізми відповідають сучасним вимогам цифрової економіки. Комплексне вивчення цих вимірів на макро та мікрорівнях дозволяє виявити сильні сторони, окреслити зони розвитку та сформувати обгрунтовану траєкторію цифрового оновлення підприємства.

Макрорівень. ОАЕ демонструють цілісний і чітко скоординований національний підхід до цифрової трансформації, який поєднує довгострокове стратегічне бачення держави з активною участю приватного сектору. Ключові державні програми – UAE Artificial Intelligence Strategy 2031, Digital Government Strategy, Smart Dubai Initiative, UAE Digital Economic Strategy – формують нормативно-організаційне підгрунтя для побудови цифрової економіки. Вони орієнтовані на інтеграцію штучного інтелекту в державне управління, розвиток цифрових послуг, підвищення кіберстійкості та формування інноваційного середовища. Паралельно з державними ініціативами активно розвивається інвестиційна компонента цифрової інфраструктури. Провідні корпорації та державні фонди реалізують масштабні проєкти у сферах [133]:

– хмарних обчислень і дата-центрів (Microsoft Azure, Amazon Web Services, Google Cloud, G42 Cloud);

– AI-кампусів, дослідницьких хабів та інноваційних кластерів (ADIA, Hub71, Dubai AI Campus);

– кібербезпеки та цифрової безпеки (Investments by DarkMatter, Digital14, UAE Cybersecurity Council);

– телекомунікаційної інфраструктури нового покоління (5G, FTTH, IoT-платформи Etisalat та du).

Синергія державних стратегій і приватно-державних інвестицій формує потужний інституційний простір для широкого впровадження інфокомунікаційних цифрових ресурсів у діяльність підприємств усіх секторів економіки – від промисловості та логістики до охорони здоров'я, фінансів і сфери послуг. Підприємства отримують доступ до високопродуктивних обчислювальних систем, штучного інтелекту, інаструментів аналітики великих даних, інноваційних рішень для операційної автоматизації та засобів кіберзахисту.

У таких умовах інфокомунікаційні цифрові ресурси стають не лише інструментом модернізації операційної діяльності, але й ключовим джерелом таких стратегічних переваг як: прискорення інноваційних процесів, покращення якості управлінських рішень, зниження ризиків та підвищення стійкості бізнесу до зовнішніх викликів. Тим самим цифрова політика ОАЕ створює унікальний контекст, у якому цифровізація стає системною та всебічною, забезпечуючи довгострокову конкурентоспроможність націоанльної економіки та підприємств. ОАЕ демонструють швидке та стратегічно виважене розширення хмарної інфраструктури й дата-центрів, формуючи одну з найбільш потцжних цифрових екосистем у регіоні Близького Сходу [134]. Розвиток відбувається за рахунок комбінації гіпермасштабних обчислювальних проєктів, інвестицій у штучний інтелект та створення спеціалізованих інноваційних кластерів (рис. 2.11).

По-перше, гіпермасштабні дата-центри, які реалізуються а партнерстві між du та Microsoft, забезпечують значне збільшення доступної обчислювальної потужності. Вони створюються за архітектурою hyperscale, тобто з можливістю швидкого масштабування залежно від навантаження, підтримкою хмарних сервісів Azure, високим рівнем енергоефективності та інтегрованим кіберзахистом. Такі центри розраховані на обробку великих масивів даних підприємств, підтримку корпоративних систем, IoT-платформ і цифрових сервісів державного сектору. Завдяки географічному розміщенню в

ОАЕ створюється локальна суверенна хмара, що зменшує затримки в передачі даних та підвищує безпеку.

Рисунок 2.11 – Елементи формування цифрової екосистеми ОАЕ

(джерело: авторська розробка)

По-друге, формування масштабних AI-кампусів нового покоління, зокрема ініціативи G42 – Stargate, перетворює ОАЕ на глобальний центр розвитку штучного інтелекту. Ці кампуси об’єднують надпотужні GPU-кластери, дослідницькі лабораторії, стартап-інкубатори та партнерські майданчики для співпраці з міжнародними технологічними компаніями. Їх інфраструктура оптимізована під тренування великих мовних моделей (LLM – Large Language Models), глибинні нейронні мережі, аналіз великих даних і високошвидкісні симуляції. Масштаби таких комплексів дають змогу суттєво скоротити час тренування моделей, знизити вартість обчислень та забезпечити підприємствам доступ до технологій, які раніше були доступні лише глобальним корпораціям.

По-третє, поетапне введення в експлуатацію перших черг цих об’єктів у 2025-2026 роках створює новий рівень пропозиції цифрових потужностей на ринку. Це означає, що вже найближчими роками підприємства різних секторів – фінансового, промислового, логістичного, медичного, телекомунікаційного – зможуть отримати доступ до локальних рішень із низькою затримкою, підвищеною продуктивністю та оптимізованими витратами.

Така інфраструктурна експансія формує регіональний хаб для обробки даних і розвитку штучного інтелекту, що дозволяє ОАЕ посилити позиції у глобальній цифровій економіці, забезпечуючи підприємствам умови для масштабної цифровізації, інновацій та підвищення стійкості до криз.

Розвиток AI-проєктів напряму залежить від доступності сучасних обчислювальних потужностей, зокрема GPU та AI-акселераторів. У 2023-2025 роках глобальний ринок апаратних засобів для штучного інтелекту демонструє стале зростання, що формує сприятливі умови для локального розгортання високопродуктивних систем. За даними прикладних аналітичних оглядів (Grand View Research, GM Insights, Omdia), ринок AI-акселераторів зріс до 25,6 млрд дол. у 2024 році та очікуваних 32,9 млрд дол. у 2025 році. Ринок AI-апаратного забезпечення оцінювався у 59,3 млрд дол. у 2024 році і прогнозовано зростає до 66,8 млрд дол. у 2025 році. Сегмент GPU, який є ключовим для навчання нейронних мереж, збільшився з приблизно 62,35 млрд дол. у 2024 році до орієнтовно 79,4 млрд дол. у 2025 році. Загальні глобальні поставки GPU та AI-чипів, за оцінкою Omdia, зросли зі 123 млрд дол. у 2024 році до 207 млрд дол. у 2025 році [135].

Паралельно розширюється виробництво високопродуктивних GPU. NVIDIA, яка домінує на ринку – 80–94% частки в AI-сегменті, збільшила потенціал виробництва модулів рівня H100 з орієнтовно 550 тис. одиниць у 2023 році до майже 2 млн еквівалентів у 2024–2025 роках. Це суттєво знижує ризики дефіциту обчислювальних компонентів і посилює можливість країн та компаній отримувати сучасні AI-ресурси [136].

Спрощення міжнародних процедур постачання, підтверджене технологічними оглядами Reuters і Tom’s Hardware, зменшує логістичні бар’єри та забезпечує стабільніший доступ до високопродуктивних обчислювальних модулів. Це дозволяє підприємствам формувати власні кластери HPC/HPL, скорочувати залежність від зовнішніх хмарних провайдерів, підвищувати безпеку обробки даних і прискорювати реалізацію складних AI-моделей.

У результаті створюються умови для формування локальних AI-центрів, підвищення інноваційної активності підприємств та зміцнення цифрової конкурентоспроможності економіки.

Опитування міжнародних консалтингових компаній свідчать про стрімке зростання корпоративного попиту на інфокомунікаційні ресурси та сервіси цифрової взаємодії. Згідно з аналітичними матеріалами KPMG (станом на 2024–2025 роки) [137], понад 96% керівників технологічних компаній ОАЕ декларують готовність інвестувати у хмарні рішення та моделі XaaS (Everything-as-a-Service). Значна частина підприємств або вже здійснила перенесення критичних бізнес-процесів у хмарне середовище, або планує завершити міграцію протягом 12–24 місяців. Такі тенденції свідчать про масштабний і системний перехід компаній до моделей, що базуються на даних, сервісах та швидкому доступі до цифрових ресурсів.

Масове впровадження хмарних платформ сприяє:

– скороченню операційних витрат;

– підвищенню масштабованості IT-інфраструктури;

– пришвидшенню циклу впровадження інновацій;

– розширенню можливостей для інтеграції AI-рішень та автоматизації.

Ключовим результатом є формування нової операційної логіки бізнесу, побудованої на принципах гнучкості, мобільності та цифрової стійкості. Рівень цифрової трансформації та використання інфокомунікаційних ресурсів варіює між галузями, що зумовлено специфікою технологічних потреб, регуляторних вимог і масштабами діяльності. Проте впровадження інфокомунікаційних ресурсів у різних секторах економіки має нерівномірний характер, що зумовлено специфікою бізнес-процесів, масштабом діяльності та технологічними пріоритетами підприємств. Відобразимо рівень впровадження інфокомунікаційних ресурсів у різних секторах економіки (рис. 2.12) та секторні відмінності у впровадженні інфокомунікаційних ресурсів (табл. 2.2).

Представлені дані свідчать, що рівень впровадження інфокомунікаційних ресурсів суттєво варіює між секторами економіки, що

пов’язано з різною цифровою зрілістю, ресурсними можливостями та технологічними потребами підприємств.

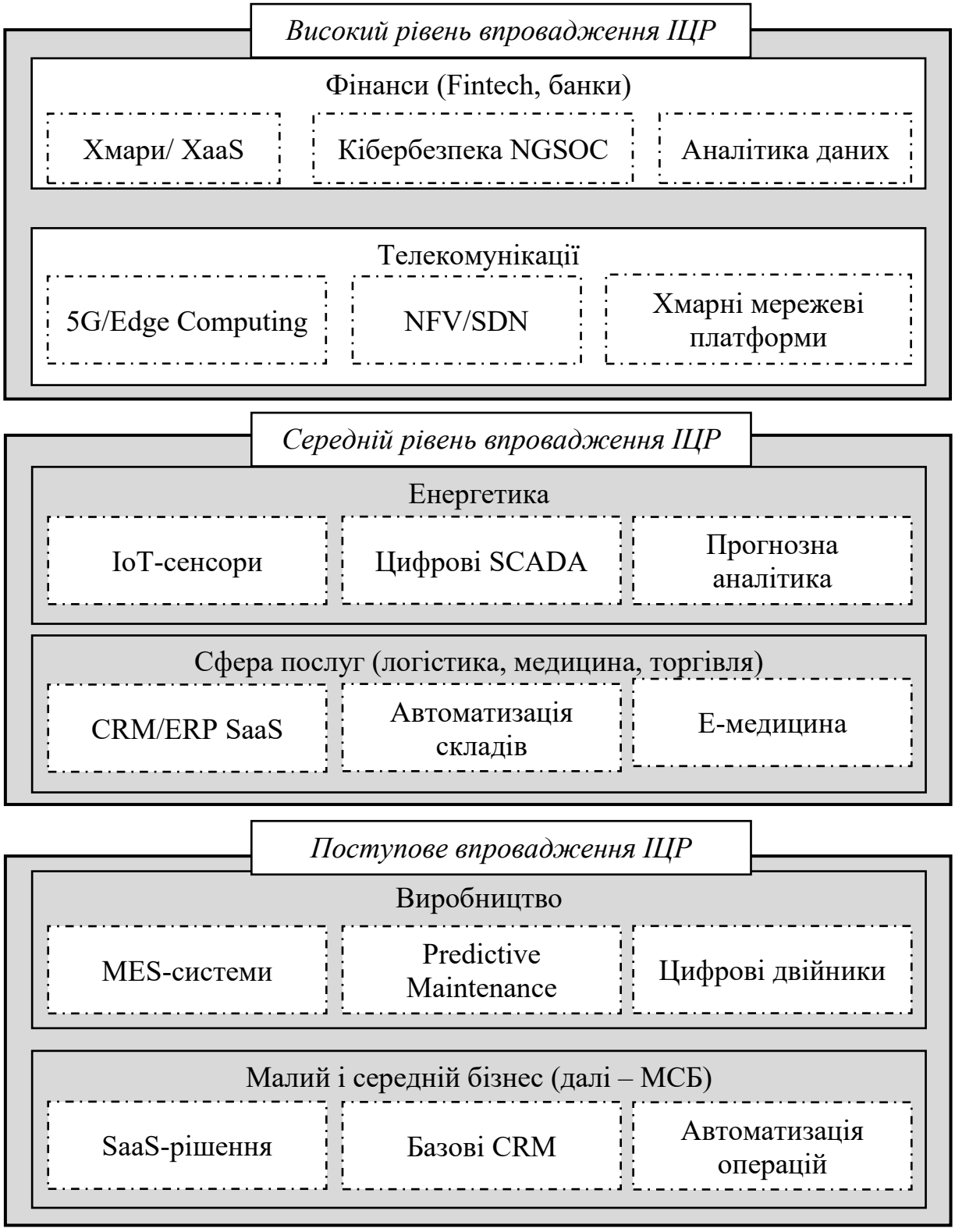


Рисунок 2.12 – Рівень впровадження інфокомунікаційних ресурсів у секторах економіки *(джерело: авторська розробка)*

Таблиця 2.2 – Секторальні відмінності у впровадженні цифрових інфокомунікаційних ресурсів *(джерело: авторська розробка)*

Сектор	Рівень впровад-ження ІЦР	Основні цифрові рішення	Ключові драйвери	Основні бар'єри
1. Фінансовий сектор (FinTech, банки)	Дуже високий	Хмари/XaaS, аналітика даних, біометрія, NGSOC	Регуляторний тиск, конкуренція, великий обсяг даних	Кіберризики, складність інтеграції
2. Телекому-нікації	Високий	5G, Edge computing, NFV/SDN, хмарні мережі	Масштабуван-ня мереж, нові стандарти зв'язку	Вартість інфраструктури, залежність від обладнання
3. Енергетика	Середній–високий	Smart Grid, IoT, SCADA, прогнозна аналітика	Оптимізація мереж та активів	Капіталомісткість модернізації
4. Сектор послуг (логістика, медицина, торгівля)	Середній	CRM/ERP SaaS, автоматизація складів, е-медицина	Орієнтація на клієнта, швидкість процесів	Нестача кадрів, фрагментованість систем
5. Виробництво	Нерівномір-ний	MES, цифрові двійники, автоматизація цехів	Підвищення продуктивності, Industry 4.0	Висока вартість обладнання, складна інтеграція
6. МСБ	Низький–середній	CRM/ERP SaaS, базова аналітика, автоматизація продажів	Доступність SaaS, конкуренція	Фінансові обмеження, дефіцит компетенцій

Галузі, для яких критичними є швидкість обробки даних і стійкість цифрових операцій (фінанси, телекомунікації), демонструють найвищу динаміку цифровізації, тоді як виробництво та МСБ впроваджують сучасні рішення поступово, орієнтуючись переважно на доступні хмарні та SaaS-сервіси. Загальна тенденція: перехід від локальних рішень → до хмарних платформ та AI-орієнтованих технологій, що забезпечує вищу

масштабованість, гнучкість, швидкість оновлення цифрових інструментів і створює основу для подальшої автоматизації та аналітичної підтримки рішень.

Мікрорівень. Стислий аналітичний огляд стану цифрової зрілості підприємств України з урахуванням умов війни, кризової нестабільності та асиметричного розвитку галузей проведено за п'ятьма ключовими вимірами – процеси, технології, дані, персонал, управління:

– процеси. Українські підприємства мають нестабільний рівень цифрової інтеграції процесів, що підтверджують офіційні ініціативи з оцінювання цифрової зрілості бізнесу. Зокрема, «Біла книга з цифрової зрілості» [138] від Дія.Бізнес включає матриці цифрової зрілості процесів (стратегія, процеси, команда, аналітика) як модель оцінювання готовності підприємств до цифровізації, що свідчить про наявність потреби стандартизованої оцінки і діагностики процесів у бізнесі [139]. Дослідження [140] показують, що підприємства не готові до руйнівної цифровізації саме через невідповідність організаційної структури і процесів вимогам цифрових змін, що вказує на низький рівень процесної зрілості. Тобто більшість українських підприємств перебуває на фрагментованому або процесному рівні цифрової зрілості: окремі бізнес-процеси цифровізовані та частково автоматизовані (облік, продажі, логістика), однак наскрізна інтеграція та оркестрація процесів залишаються обмеженими. У кризових умовах спостерігається прискорена цифровізація критичних процесів (фінанси, постачання, комунікації), але розвиток часто має реактивний, а не стратегічний характер;

– технології. За даними OECD [141], українські МСП значною мірою перебувають на ранніх етапах цифрової трансформації, показуючи обмежене використання цифрових інструментів у порівнянні з великими компаніями: близько 70 % великих підприємств мають веб-сайт, тоді як лише 47% середніх і десь 30% малих використовують його. Це означає, що технологічне впровадження цифрових платформ, хмарних рішень, API-інтеграцій та автоматизації ще не охоплює повністю малий та середній бізнес, якого в

Україні понад 99,9 % усіх підприємств [141]. Технологічна база підприємств є нерівномірною: поряд із використанням хмарних сервісів, ERP/CRM та окремих RPA-рішень значна частка підприємств зберігає застарілі IT-системи та монолітні архітектури [141-143]. Війна стимулювала перехід до хмари та віддалених інструментів, однак рівень комплексної архітектурної модернізації залишається обмеженим через фінансові та кадрові чинники;

– дані. Це один з найбільш вразливих вимірів цифрової зрілості, оскільки дані часто розпорошені між системами, відсутні єдині стандарти Data Governance, а аналітика використовується переважно для описових, а не прогнозних рішень. Data-driven підхід ще не є домінуючою управлінською практикою, за винятком окремих великих компаній та IT-орієнтованих бізнесів. Дані щодо використання ІКТ бізнесом збирає Державна служба статистики України, але статистику ще не повністю опубліковано (на 2022 р.), що відображає обмежений доступ до даних про ступінь цифрової інтеграції даних у бізнес-середовищі [144]. Низька готовність підприємств означає, що дані не завжди структуровані чи доступні для аналітики на рівні підприємства [140];

– персонал. Ключовими факторами цифрової адаптивності підприємств є наявність ICT-спеціалістів та e-commerce, які позитивно впливають на стійкість підприємств. Проте низький рівень цифрових навичок і обмежений доступ до цифрового освіти стримують розвиток цифрової компетентності персоналу [145]. Кадровий вимір характеризується дефіцитом цифрових компетентностей, високою залежністю від ключових фахівців та міграційними втратами. Водночас персонал демонструє високу адаптивність до дистанційної роботи та нових цифрових інструментів. Офіційна національна програма цифрової зрілості спрямована на підвищення цифрових компетенцій малого та середнього бізнесу з метою досягнення 80 % цифрової інтеграції до 2028 р., що свідчить про визнання кадрової проблеми на державному рівні [138];

– управління. Управлінські практики цифрової трансформації здебільшого зосереджені на операційній підтримці, а не на стратегічному розвитку. Цифровізація часто розглядається як інструмент виживання, а не довгострокового зростання. Інтеграція KPI цифрової інфраструктури, принципів екосистеми та антикризового управління перебуває на етапі становлення. Є позитивні тенденції: за даними ООН [146], Україна піднялася на 5-те місце у розвитку цифрових муніципальних і онлайн-послуг, що створює передумови для трансферу управлінських практик у бізнес.

На підставі аналізу побудовано діаграму стану цифрової зрілості підприємств України за ключовими вимірами (рис. 2.13).

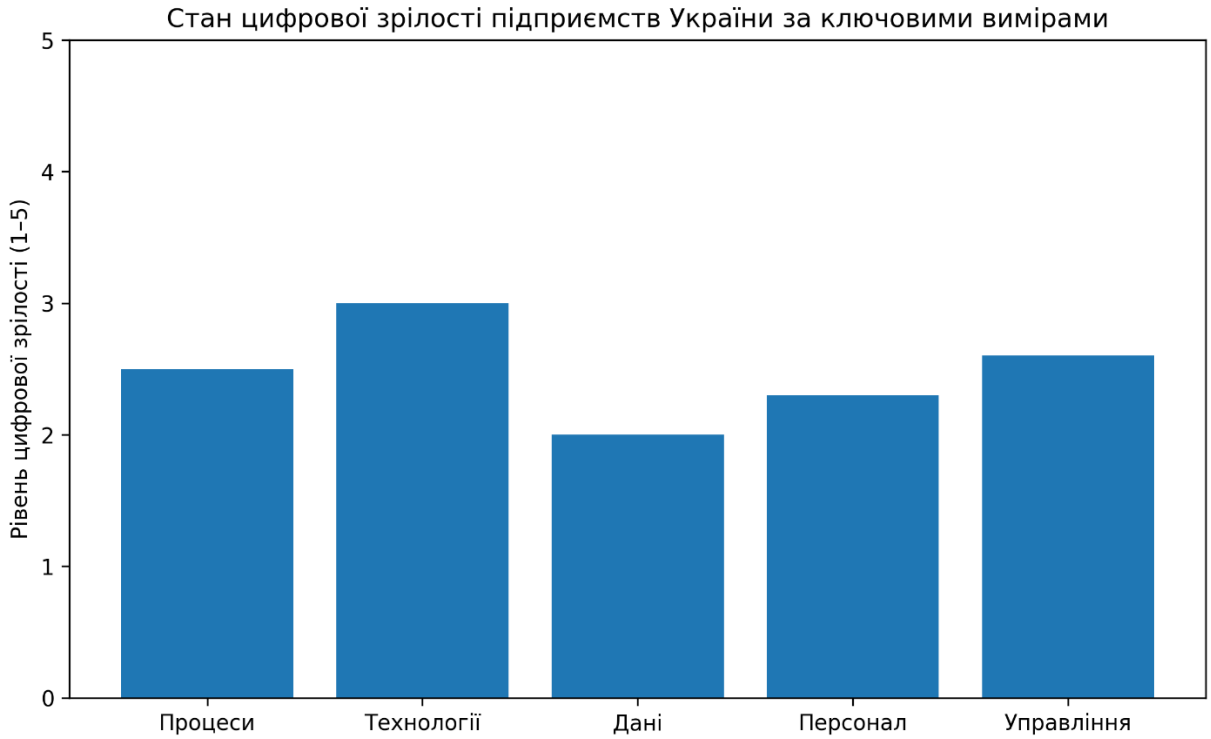


Рисунок 2.13 – Стан цифрової зрілості підприємств України за ключовими вимірами: експертна оцінка *(джерело: авторська розробка)*

Діаграма відображає узагальнену експертну експрес-оцінку рівня цифрової зрілості підприємств України за п’ятьма ключовими вимірами. Найвищі значення зафіксовано у вимірі технологій, що пов’язано з активним використанням хмарних сервісів та базових цифрових платформ, тоді як

найнижчий рівень характерний для управління даними, що свідчить про фрагментарність data-driven підходів. Процеси, персонал і управління перебувають на проміжному рівні, що підтверджує перехідний характер цифрової трансформації підприємств України в умовах кризи.

Відтак, можна узагальнити, що загалом *цифрова зрілість підприємств України перебуває між фрагментованим і процесним рівнями з окремими елементами інтегрованого розвитку,* причому війна одночасно виступає стримувальним фактором і каталізатором цифрових змін, прискорюючи трансформацію критичних інфокомунікаційних компонентів, але обмежуючи системну модернізацію всієї екосистеми.

Б. Оцінювання цифрової зрілості трьох підприємств різних секторів (IT, фінтех, виробництво). Оцінювання цифрової зрілості малих підприємств різних секторів (IT, фінтех, виробниче) проведене за наведеною методикою у п’ятьох ключових вимірах (додаток Б.1) за розробленою шкалою зрілості. На відміну від існуючих опитувальників і оцінювальників (рис. 2.14), методика сфокусована на експерес оцінюванні цифрової зрілості підприємства.

Рисунок 2.14 – Міжнародні інструменти лоцінювання цифрової трансформації малого та середнього бізнесу *(джерело: [147])*

Методика оцінювання – оцінювання здійснюється за п’ятьма вимірами цифрової зрілості: процеси, технології, дані, персонал, управління.

Шкала оцінювання: 1–5 балів, де 1 – початковий рівень, 3 – процесний / середній рівень, 5 – інтегрований / оркестрований рівень.

Таблиця 2.3 – Оцінювання цифрової зрілості підприємств* за ключовими вимірами *(джерело: авторська розробка)*

Вимір цифрової зрілості	Сфери діяльності підприємств		
	IT (П1)	Фінтех (П2)	Виробництво (П3)
1. Процеси	4,5	4,2	2,6
2. Технології	4,8	4,5	2,8
3. Дані	4,2	4,7	2,2
4. Персонал	4,6	4,0	2,4
5. Управління	4,1	4,3	2,5
6. Інтегральний рівень цифрової зрілості	4,44	4,34	2,50
Рівень зрілості	*Інтегрований / data-driven*	*Інтегрований / регуляторно-орієнтований*	*Процесний / фрагментований*
** На вимогу керівництва досліджуваних підприємств, їх назви у роботі не використані*			

Як бачимо, IT-підприємство (П1) демонструє найвищий рівень цифрової зрілості, що обумовлено глибокою інтеграцією цифрових технологій у всі бізнес-процеси, розвиненою культурою роботи з даними та високим рівнем цифрових компетенцій персоналу. Управління має чітко виражений data-driven характер, а архітектура є гнучкою та масштабованою. Фінтех-компанія (П2) характеризується високою зрілістю у вимірах даних та управління, що пояснюється жорсткими регуляторними вимогами, високим рівнем автоматизації та активним використанням аналітики і штучного інтелекту. Дещо нижчі показники персоналу пов’язані з високою спеціалізацією кадрів і дефіцитом окремих цифрових компетенцій. Виробниче підприємство (П3) перебуває на процесному рівні цифрової зрілості: основні цифрові рішення зосереджені на окремих функціях (облік, логістика, планування), при цьому інтеграція даних, автоматизація та цифрове управління залишаються

фрагментарними. Управлінські рішення здебільшого підтримуються даними постфактум, а не прогнозною аналітикою.

Порівняльне оцінювання свідчить, що рівень цифрової зрілості залежить від виду діяльностіи: *IT- та фінтех- підприємства досягають інтегрованого рівня завдяки природній цифровій орієнтації бізнес-моделей, тоді як виробничі підприємства переважно перебувають на процесному етапі,* що зумовлює необхідність цілеспрямованого розвитку управління даними, інфокомунікаційної інфраструктури, цифрових компетенцій персоналу.

В. Порівняльний аналіз цифрової зрілості підприємств України та ОАЕ за п'ятьма ключовими вимірами (процеси, технології, дані, персонал, управління). Оцінювання цифрової зрілості підприємств України та ОАЕ здійснено шляхом зіставлення ключових вимірів (процеси, технології, дані, персонал, управління) з релевантними аналітичними показниками, сформованими на основі звітів OECD, World Bank, IMD, національних програм цифрової трансформації та галузевих оглядів, що забезпечує методичну обґрунтованість і порівнянність результатів.

Порівняльний аналіз цифрової зрілості підприємств України та ОАЕ за одними ж ключовими вимірами у межах однієї методики дозволяє коректно зіставляти результати. Оцінювання здійснено за шкалою 1–5 балів, де: 1 – початковий рівень; 3 – процесний (середній); 5 – інтегрований / оркестрований рівень цифрової зрілості. Показники для України та ОАЕ є узагальненими середніми значеннями, сформованими на основі:

– національних і міжнародних аналітичних оглядів (OECD, World Bank, UAE Digital Government) [148-153];

– відкритих звітів Diia.Business, UAE Vision 2031, Smart Dubai [154-159];

– типових галузевих практик IT, фінтех та виробництва.

Порівняння цифрової зрілості підприємств України та ОАЕ представлено у табл. 2.4

Таблиця 2.4 – Порівняння цифрової зрілості підприємств України та ОАЕ *(джерело: авторська розробка за даними [148-159])*

Вимір цифрової зрілості	Підприємства України (середнє)	Підприємства ОАЕ (середнє)
1. Процеси	2,6	4,1
2. Технології	3,0	4,5
3. Дані	2,2	4,3
4. Персонал	2,4	3,9
5. Управління	2,6	4,2
6. Інтегральний рівень цифрової зрілості	2,56	4,20
Домінуючий рівень зрілості	*Фрагментовано-процесний*	*Інтегрований / data-driven*

Аналітична інтерпретація за вимірами така:

Процеси – якщо в Україні цифровізація процесів підприємств має переважно фрагментарний характер і часто зосереджена на підтримці операційної діяльності, то в ОАЕ процеси цифровізовані системно, з орієнтацією на end-to-end інтеграцію, автоматизацію та клієнтоцентричність, що забезпечує високу узгодженість бізнес-функцій.

Технології – українські підприємства активно використовують хмарні сервіси та базові платформи, однак архітектури часто залишаються гібридними й несистемними, тодіяк в ОАЕ домінують сучасні модульні архітектури, масштабовані хмарні рішення, API-екосистеми та активне впровадження ШІ.

Дані – в Україні управління даними є найслабшим виміром цифрової зрілості: дані розпорошені, аналітика здебільшого описова, а в ОАЕ data-driven підхід є основою управління, широко застосовуються predictive analytics, big data та державні й корпоративні data-платформи.

Персонал – українські підприємства стикаються з дефіцитом цифрових компетенцій, міграційними втратами та обмеженими програмами системного навчання, тоді як в ОАЕ активно інвестують у розвиток цифрових навичок, залучення міжнародних фахівців і корпоративні програми upskilling/reskilling.

Управління – в Україні цифрове управління часто має реактивний характер і спрямоване на виживання в кризових умовах, тоді як в ОАЕ цифрова трансформація інтегрована у стратегічне управління, підтримується національними програмами та чіткими KPI цифрової зрілості.

Порівняння свідчить, що підприємства ОАЕ перебувають на інтегрованому рівні цифрової зрілості з домінуванням data-driven управління та оркестрованих цифрових екосистем, тоді як підприємства України в середньому знаходяться на фрагментовано-процесному рівні, де цифровізація виконує переважно підтримувальну та антикризову функцію, що формує значний потенціал для подальшого розвитку інфокомунікаційного забезпечення.

2.3 Оцінювання результативності застосування цифрових ресурсів у забезпеченні розвитку та стійкості підприємства

Оцінювання результативності застосування цифрових ресурсів у забезпеченні розвитку та стійкості підприємтсва доцільно здійснювати за такими аналітичними напрямами:

а) аналіз структурних та динамічних змін у використанні цифрових ресурсів і їх внеску в операційну та стратегічну ефективність;

б) оцінка впливу цифрових рішень на підвищення стійкості підприємства до кризових чинників, зокрема через покращення безперервності процесів, кіберзахищеності та адаптивності;

в) визначення управлінських викликів і необхідних трансформацій у системі менеджменту для забезпечення максимального ефекту від впровадження цифрових інструментів.

А. Аналіз структурних та динамічних змін у використанні цифрових ресурсів і їх внеску в операційну та стратегічну ефективність. Трансформація цифрових ресурсів підприємства відбувається не лише за

рахунок нарощування їх кількісного обсягу, а насамперед через зміну їхньої структури, функціонального призначення та ролі у забезпеченні операційної та стратегічної ефективності. У сучасних умовах ключове значення мають цифрові рішення, здатні забезпечити інтегрованість інформаційних потоків, автоматизацію критично важливих процесів та формування єдиної інформаційної архітектури підприємства. У цьому контексті особливу увагу привертають такі програмні рішення як Система оплати документів (СОД), архітектурно-інтеграційна платформа DPS та TapXPhone (GERCPay), розроблені ТОВ «Герц», які відображають різні рівні та напрями розвитку цифрової інфраструктури підприємства. Їх упровадження дозволяє оцінити структурні зміни у використанні цифрових ресурсів (від локальних інструментів до централізованих платформ), а також динаміку їхнього впливу на швидкість обробки даних, прозорість операцій, рівень автоматизації, інтегрованість інформаційного середовища та здатність підприємства до стратегічного масштабування.

Система оплати документів (далі – СОД) є спеціалізованою інформаційною платформою, призначеною для автоматизації процесів створення замовлень, прийому та обліку платежів, а також забезпечення повного контролю їх проходження у фінансовій інфраструктурі підприємства. Її впровадження спрямоване на уніфікацію та централізацію транзакційних даних, підвищення прозорості й оперативності фінансових операцій, а також мінімізацію ризиків, пов’язаних із ручною обробкою платежів.

Функціональна структура СОД включає модулі адміністративного управління, технічного супроводу та контролю потоків транзакцій. Система забезпечує інтеграцію з зовнішніми платіжними сервісами, банківськими системами та партнерами через стандартизовані API, що дозволяє формувати єдиний інформаційний контур для обробки фінансових даних. Важливою властивістю СОД є високий рівень інформаційної безпеки: застосовуються механізми шифрування, багатофакторної аутентифікації та журналювання операцій, що підвищує стійкість інфраструктури до кіберризиків.

Архітектурно-інтеграційна платформа DPS є системним програмним рішенням стратегічного рівня, яке забезпечує формування цілісної цифрової архітектури підприємства та взаємодію між усіма його інформаційними системами. Її основне призначення полягає у створенні єдиного інтеграційного середовища, що дозволяє об'єднати різнорідні сервіси, модулі й інформаційні потоки в узгоджену інфокомунікаційну інфраструктуру. DPS виконує функції маршрутизації та синхронізації даних, керування доступами, стандартизації протоколів обміну, а також забезпечення масштабованості цифрової інфраструктури. На рівні архітектури система орієнтована на використання сервісно-орієнтованих або мікросервісних підходів, що дозволяє підвищити гнучкість і адаптивність IT-ландшафту підприємства. DPS також відіграє важливу роль у забезпеченні цифрової стійкості: завдяки централізованим механізмам логування, контролю подій і управління потоками даних знижується ризик збоїв та інформаційних розривів. У стратегічному вимірі DPS формує основу для розвитку цифрових сервісів, оскільки забезпечує спроможність швидко підключати нові програмні модулі, масштабувати бізнес-функції та інтегрувати зовнішні цифрові екосистеми.

TapXPhone є програмним продуктом у сфері фінансових технологій (FinTech), призначеним для забезпечення приймання безконтактних платежів суб'єктами господарювання із використанням стандартних мобільних пристроїв на базі операційної системи Android, оснащених NFC-модулем. Програмне рішення розроблене та функціонує в межах платіжної інфраструктури GERCPay і реалізує концепцію Software POS (SoftPOS), за якої фізичний платіжний термінал замінюється програмним застосунком. Ключові переваги TapXPhone GERCPAY для бізнесу відображено на рис. 2.15.

Функціональне призначення TapXPhone полягає у трансформації смартфона продавця на повноцінний інструмент для приймання безконтактних платежів з використанням банківських карток, мобільних гаманців та інших NFC-сумісних платіжних засобів. Таким чином, програмний продукт усуває потребу у придбанні та обслуговуванні

традиційних POS-терміналів, що є особливо актуальним для малого та середнього бізнесу, мобільної торгівлі та сервісних підприємств.

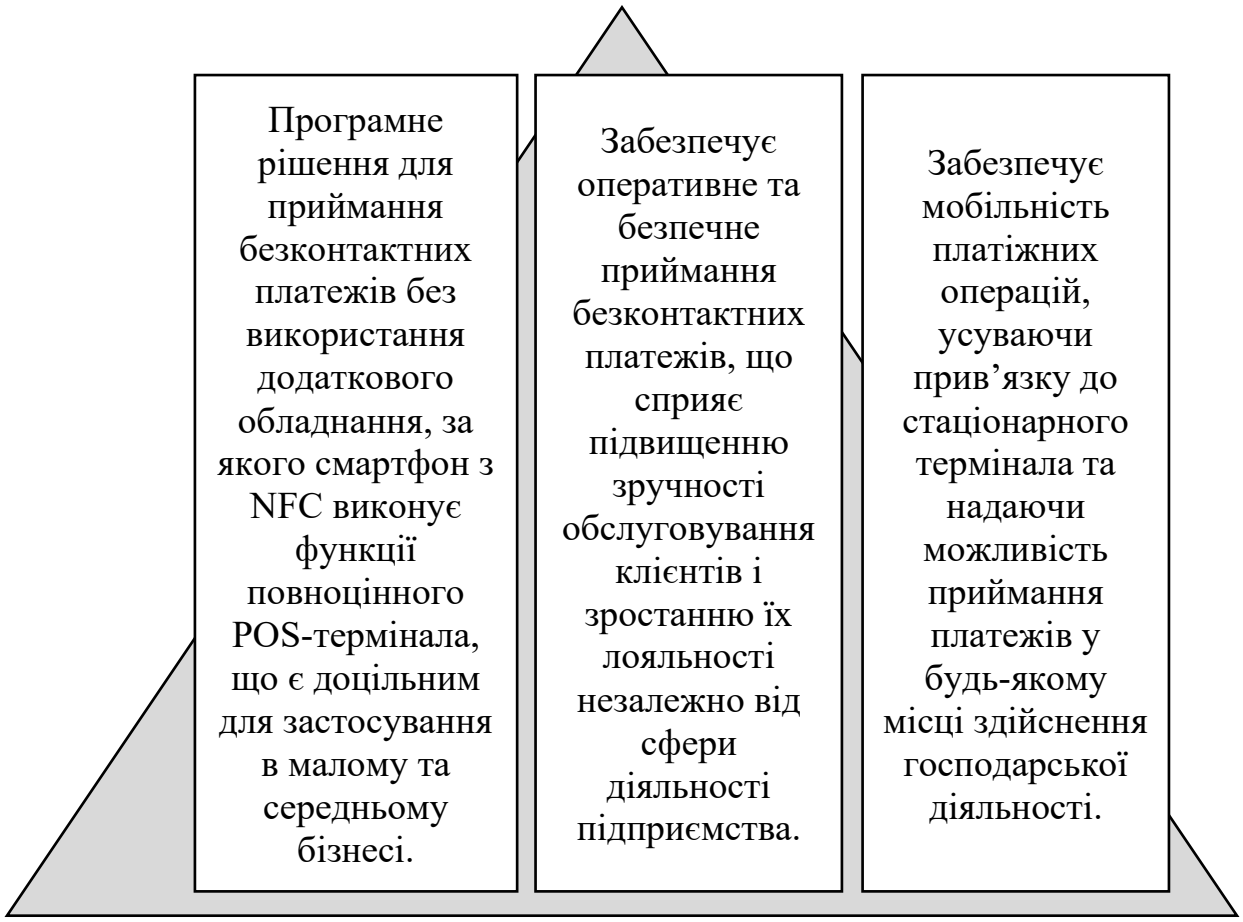


Рисунок 2.15 – Ключові переваги TapXPhone GERCPAY для бізнесу *(джерело: дані розробника)*

З позицій архітектури бізнес-процесів TapXPhone забезпечує повний цикл платіжної операції, який включає:

– авторизацію продавця в платіжній системі;

– ідентифікацію мобільного пристрою як платіжного інструменту;

– формування платіжної транзакції відповідно до заданого бізнес-флоу;

– обробку та підтвердження платежу;

– фіксацію результатів операції з можливістю формування електронного чека та перегляду історії транзакцій.

Важливою характеристикою програмного продукту є його гнучкість у налаштуванні платіжних сценаріїв. TapXPhone підтримує декілька моделей

ініціювання платежу: за каталогом товарів або послуг, за попередньо створеним замовленням у зовнішній системі партнера, а також шляхом ручного введення суми платежу. Така варіативність дозволяє інтегрувати програмне рішення у різні організаційні моделі продажів без суттєвого перегляду наявних бізнес-процесів підприємства.

Робота з TapXPhone складається з кількох ключових етапів (рис. 2.16). Інфографіка основних етапів та візуалізація процесів представлена в Додатках Б.2-Б.3.

Рисунок 2.16 – Етапи роботи з TapXPhone *(джерело: дані розробника)*

З погляду інформаційної безпеки TapXPhone реалізує багаторівневу систему захисту, що включає ідентифікацію користувача, прив’язку застосунку до конкретного пристрою, використання PIN-коду та застосування

сучасних механізмів шифрування платіжних даних. Це забезпечує відповідність базовим вимогам до безпеки фінансових транзакцій та знижує операційні ризики при використанні мобільних платіжних рішень.

У контексті цифровізації бізнес-процесів підприємства TapXPhone може розглядатися як інструмент підвищення операційної мобільності, скорочення капітальних витрат на платіжну інфраструктуру та розширення можливостей приймання платежів у нестандартних умовах (виїзна торгівля, сервісні послуги, тимчасові торгові точки). Його впровадження сприяє формуванню більш гнучкого та клієнтоорієнтованого платіжного середовища, що відповідає сучасним тенденціям розвитку цифрової економіки та безготівкових розрахунків.

Порівняльна характеристика всіх трьох програмних продуктів відображена у табл. 2.5.

Таблиця 2.5 – Порівняльна характеристика програмних рішень у платіжній екосистемі ГЕРЦ *(джерело: побудовано за даними розробника)*

Критерій	TapXPhone (GERCPAY)	Система оплати документів (СОД)	Інтерфейсна платформа СОД
1	2	3	4
1. Клас програмного продукту	Мобільний SoftPOS-застосунок	Централізована платіжно-облікова система	Веб-орієнтована платформа користувацьких інтерфейсів
2. Основне призначення	Приймання безконтактних платежів	Створення, облік і контроль платіжних замовлень	Забезпечення доступу користувачів до функцій СОД
3. Рівень у системі	Фронтальний інтсрумент приймання платежів	Ядро платіжної інфраструктури	Представницький (інтерфейсний) рівень
4. Цільова аудиторія	Бізнес-користувачі, продавці, оператори послуг	Партнери, платіжні організації, отримувачі коштів	Адміністратори, клієнти/платники, аналтіики

Продовження табл. 2.5

1	2	3	4
5. Тип використання	Мобільний, децентралізований	Централізований, системний	Веб-доступ через браузер
6. Основні функції	Ініціювання та проведення платежу; ідентиікація пристрою	Управління замовленнями; маршрутизація платежів; облік транзакцій	Адміністрування; перегляд оплат; звітність і статистика
7. Технологічна основа	Android + NFC	Серверна платформа з інтеграцією платіжних систем	REST API та інші
8. Інтеграція з іншими компонентами	Інтегрується з СОД через GERCPAY	Інтегрує всі канали приймання платежів	Працює поверх СОД через API
9. Роль у бізнес-процесах	Операційна	Процесоутворююча	Управлінсько-інформаційна
10. Вплив на ефективність	Підвищує мобільність і швидкість	Забезпечує прозорість і контроль грошових потоків	Підтримує управлснькі рішення і контроль

Відповідно до табл. 2.5, сукупне використання програмних рішень TapXPhone, СОД та інтерфейсної платформи формує багаторівневе інформаційне середовище підприємства, що забезпечує інтеграцію операційних, облікових та управлінсько-аналітичних функцій у межах єдиного цифрового контуру. TapXPhone у цій системі виконує роль мобільного фронтального інструменту збору платіжної інформації, Система оплати документів (СОД) виступає ядром обробки, маршрутизації та обліку транзакцій, тоді як інтерфейсна платформа забезпечує доступ користувачів до даних, налаштувань і результатів функціонування системи.

Б. Оцінка впливу цифрових рішень на підвищення стійкості підприємства до кризових чинників, зокрема через покращення безперервності процесів, кіберзахищеності та адаптиності.

Зазначена архітектура сприяє підвищенню цілісності інформаційних потоків, зменшенню фрагментації даних та формуванню єдиного

інформаційного простору підприємства, що є необхідною передумовою для підвищення прозорості фінансових процесів і своєчасного управлінського реагування. Наявність декількох взаємопов'язаних цифрових рівнів дозволяє забезпечити безперервність платіжних операцій навіть в умовах обмежень фізичної інфраструктури або зовнішніх збурень.

У контексті цифрової стійкості підприємства така модель підвищує здатність системи зберігати функціональність, керованість та контроль над ключовими фінансовими процесами за умов зростання невизначеності та кризових викликів. Інтеграція мобільних каналів приймання платежів, централізованої обробки даних та аналітичних інтерфейсів створює організаційно-технологічні передумови для реалізації антикризового управління, орієнтованого на оперативний моніторинг, швидке прийняття рішень і мінімізацію операційних ризиків.

З урахуванням результатів попереднього огляду архітектури платіжних рішень та особливостей їх функціонування в межах інформаційного середовища підприємства, доцільно зазначити, що для оцінювання економічної результативності впровадження і подальшого використання програмних продуктів на практиці вже застосовується формалізована методика фінансово-економічних розрахунків. Дана методика використовується підприємством-розробником платіжних рішень у процесі планування, аналізу та контролю ефективності функціонування платіжної інфраструктури.

Зазначений підхід дозволяє системно оцінювати початкові витрати партнерів на підключення до платіжного рішення, прогнозувати доходи від комісійної діяльності та визначати строки окупності з урахуванням масштабів використання і сценаріїв розвитку платіжних операцій. Використання методики в операційній діяльності підприємства забезпечує обґрунтованість управлінських рішень щодо розвитку програмних продуктів, коригування тарифної політики та масштабування платіжних сервісів.

Для формалізації розрахунків економічної ефективності платіжного рішення використовується система взаємопов'язаних показників, що дозволяє оцінити витрати, доходи та строк окупності в межах комісійної моделі:

1. Первинні витрати партнери – сукупні первинні витрати партнера визначаються як сума витрат на обладнання та фіскалізацію платіжних операцій:

$$C_{п} = C_{обл} + C_{фіск} , \quad (2.1)$$

де $C_п$ – загальні первинні витрати партнера, грн;

$C_{обл}$ – витрати на придбання мобільного пристрою з NFC, грн;

$C_{фіск}$ – витрати на фіскальний ключ для одного платіжного пункту, грн;

2. Формування доходу від комісійної діяльності – місячний дохід від функціонування платіжного пункту розраховується як добуток загального обсягу прийнятих платежів та ставки комісії:

$$D_{м} = V_{м} * r , \quad (2.2)$$

де $D_м$ – місячний дохід платформи (або партнера), грн;

$V_м$ – загальний обсяг платіжних операцій за місяць, грн;

r – ставка комісії, частка одиниці.

Річний дохід визначається за формулою:

$$D_{р} = D_{м} * 12 , \quad (2.3)$$

3. Сценарне моделювання доходів – для оцінювання чутливості фінансового результату до ключових параметрів використовується множина сценаріїв S=$\{S_1, S_2, S_3\}$, для кожного з яких:

$$D_m^{(S)} = V_m^{(S)} * r^{(S)}, \quad (2.4)$$

де S – номер сценарію (консервативний, базовйи, оптимістичний).

4. Розрахунок строку окупності – строк окупності первинних витрат партнера визначається як відношення сукупних початкових витрат до середнього місячного доходу:

$$PP = \frac{C_п}{D_m}, \quad (2.5)$$

PP – строк окупності, місяців.

5. Дохід платформи з урахуванням масштабування (опційно) – у разі аналізу ефективності платформи загальний місячний дохід визначається як:

$$D_m^{plat} = \sum_{i=1}^{N} V_{m,i} * r_i \ , \quad (2.6)$$

де N – кількість активних партнерів у мережі;

$V_{m,i}$ – місячний обсяг платежів і-ого партнера;

r_i – відповідна ставка комісії.

6. Узагальнюючий показник економічної привабливості – для узагальненої оцінки доцільності впровадження рішення використовується критерій швидкої окупності:

$$PP \leq PP_{кр}\ , \qquad (2.7)$$

де $PP_{кр}$ – гранично допустимий строк окупності, визначений інвестором або платформою.

Наведена методика, незважаючи на її практичну цінність та апробацію в діяльності підприємства-розробника, характеризується низкою суттєвих обмежень, що звужують можливості її застосування для комплексної оцінки цифрової інновації (далі – ЦІКР) у ширшому контексті розвитку та стійкості підприємства, які відображено на рис. 2.17.

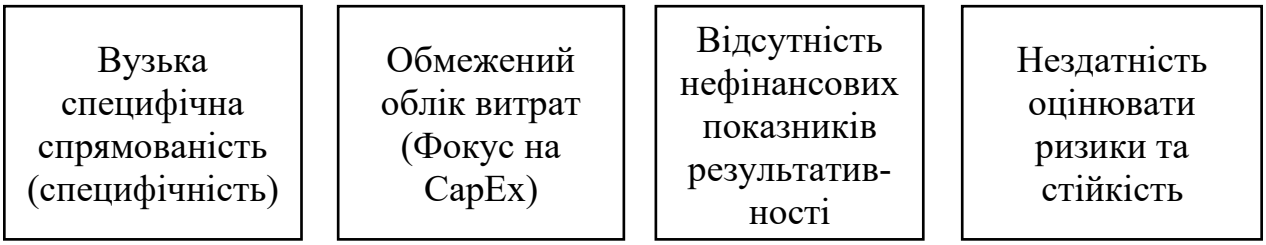


Рисунок 2.17 – Недоліки діючої методики оцінювання результативності цифрової інновації *(джерело: авторська розробка)*

Відповідно до рис. 2.17, недоліками діючої методики оцінювання результативності цифрової інновації є:

1) вузька функціональна спрямованість (специфічність), тобто методика є надто вузькоспеціалізованою, оскільки орієнтована виключно на оцінку комісійної моделі платіжного рішення (економічна ефективність для партнера та платформи). Вона не може бути застосована для оцінки інших видів цифрових ресурсів (ERP-систем, хмарних сервісів, IoT-рішень, систем кіберзахисту), які не генерують прямого доходу від комісії;

2) обмежений облік витрат (фокус на CapEx), а саме у розрахунку первинних витрат ($C_п$) враховуються лише початкові інвестиційні витрати на обладнання ($C_{обл}$) та фвскалізацію ($C_{фіск}$). Повінстю ігноруються критичні для ЦІКР операційні витрати (*OpEx*), такі як:

- абонентська плата за використання платформи (SaaS);
- витрати на супровід, оновлення, технічне обслуговування;
- персонал, необхідний для навчання та підтримки функціонування ресурсу.

3) відсутність нефінансових показників результативності, адже методика є суто фінансовою – її єдиним інтегральним критерієм є строк окупності (*PP*). Вона повністю ігнорує ключові нефінансові ефекти цифрової інновації, такі як:

- підвищення операційної ефективності та продуктивності;
- покращення якості даних та управлінських рішень;
- зростання лояльності клієнтів (Customer Experience).

4) нездатність оцінювати ризики та стійкість, адже математичний апарат не містить жодних інструментів для оцінки ризиків (кіберзагрози, збої, втрата даних) або показників цифрової стійкості (доступність, час відновлення після збоїв – RTO, RPO), які є критично важливими в умовах криз.

Для визначення можливостей практичного використання наведеної методики в ширшому аналітичному контексті доцільно оцінити її застосовність не лише з позицій фінансової результативності, а й з урахуванням впливу на розвиток та стійкість підприємства. З цією метою представлено узагальнену характеристику відповідності методики ключовим напрямам оцінювання розвитку та цифрової стійкості підприємства (табл. 2.6).

Таблиця 2.6 – Застосовність методики для оцінювання розвитку та стійкості підприємства *(джерело: авторська розробка)*

Критерій	Застосовність методики	Обґрунтування
1	2	3
1. Розвиток підприємства	Низька	Методика оцінює розвиток лише через один, дуже вузький фінансовий канал – дохід від комісійної діяльності (D_m). Вона не відображає інтегральний вплив ЦІКР на зростання бізнес-моделі, розширення ринків

Продовження табл. 2.6

1	2	3
		чи формування нових стратегічних можливостей, які є основою розвитку.
2. Стійкість підприємства (Digital Resilience)	Відсутня	Методика не містить жодного показника, який би відображав здатність підприємства протистояти кризам (кібербезпека, надійність інфраструктури, адаптивність, швидкість реагування на збої), що є центральною темою Вашої дисертації.
3. Як частковий компонент	Часткова, але необхідна	Цей математичний апарат є корисним лише як фінансовий блок у складі набагато ширшої, комплексної методики. Він може використовуватися для розрахунку економічної привабливості інвестицій (*ROI/PP*) у конкретний транзакційний ЦІКР, але повинен бути доповнений нефінансовими, ризиковими та стійкісними показниками.

Зазначена методика потребує суттєвого розширення та методологічного доопрацювання, зокрема шляхом її інтеграції як одного з розрахункових модулів у більш широку, багатовимірну систему оцінювання. Така система має поєднувати кількісні та якісні критерії аналізу й охоплювати не лише фінансово-економічні результати впровадження цифрового інноваційного комплексного рішення, але й його вплив на розвиток інформаційного середовища та управлінську стійкість підприємства.

В. Визначення управлінських викликів і необхідних трансформацій у системі менеджменту для забезпечення максимального ефекту від впровадження цифрових інструментів.

Особливу увагу в межах удосконаленої методики доцільно приділити оцінюванню складових цифрової стійкості, зокрема надійності функціонування цифрових сервісів, рівня кіберзахисту, здатності системи адаптуватися до змін зовнішнього середовища та кризових впливів. Включення зазначених параметрів дозволить забезпечити комплексне бачення

результатів цифрової трансформації та сформувати аналітичну основу для прийняття обґрунтованих управлінських рішень.

Блок І. Економічна ефективінсть (Фінансові показники). Даний блок оцінює прямі фінансові вигоди та інвестиційну привабливість ЦІКР, враховуючи повний цикл витрат (CapEx + OpEx), що відображено у табл. 2.7.

Таблиця 2.7 – Показники економічної ефективності *(джерело: систематизовано автором на підставі [60; 63; 86; 94])*

Показник	Формула	Опис
1. Сукупні річні витрати (C_{Σ}^{P})	$C_{\Sigma}^{P} = C_{п} + C_{OpEx}$	Сума первинних (капітальних) витрат $C_{п}$ (обладнання, ліцензії) та річних операційних витрат C_{OpEx} (супровід, абонплата, хмарні сервіси, зарплата техперсоналу).
2. Чистий річний дохід (D_P^{Net})	$D_P^{Net} = D_p - C_{OpEx}$	Річний дохід від ЦІКР D_p, що може включати комісії, економію від автоматизації) за вирахуванням річних операційних витрат.
3. Рентабельність інвестицій у ЦІКР ($ROI_{ц}$)	$ROI_{ц} = \frac{D_p^{Net}}{C_{п}} * 100$	Показує відсоток прибутковості капітальних інвестицій у цифрові ресурси.
4. Строк окупності *PP*	$PP = \frac{C_{п}}{D_M^{Net}}$	Строк окупності первинних витрат у місяцях, де D_M^{Net} – середній чистий місячний дохід.

Блок ІІ. Операційна результативність (нефінансові показники). Даний блок оцінює, як ЦІКР впливають на ефективність внутрішніх процесів та якість управління, що є критичним для розвитку. Основні показники відображено у табл. 2.8.

Блок ІІІ. Цифрова стійкість та ризики (fнтикризовий блок). Даний блок є ключовим для оцінки гіпотези дисертації і відображає здатність підприємства протистояти кризам (Digital Resilience), яка забезпечується функціями ЦІКР, такими як моніторинг загроз та відновлення. Основні показники відображено у табл. 2.9.

Таблиця 2.8 – Показники операційної результативності *(джерело: систематизовано автором на підставі [51; 56; 99; 107; 108])*

Показник	Формула	Опис
1. Рівень автоматизації ($I_{автом}$)	$I_{автом} = \frac{N_{авт}}{N_{заг}} * 100$	Частка автоматизованих процесів ($N_{авт}$) відносно загальної кількості ($N_{заг}$) в межах функціонального блоку (бухгалтерії, логістики, ін.).
2. Якість та доступність даних ($P_{даних}$)	$P_{даних} = 1 - \frac{N_{помилок}}{N_{всього}}$	Частка коректних даних. Оцінює, наскільки ЦІКР підвищують достовірність інформації для управлінських рішень.
3. Швидкість комунікації координації ($T_{коорд}$)	$T_{коорд}$ (мін)	Середній час на виконання міжфункціональної операції (наприклад, від запиту до виконання) завдяки використанню комунікаційних ресурсів (CR) та інтегрованих платформ.
4. Ефективність використання потужностей ($E_{потуж}$)	$E_{потуж}(\%)$	Ступінь завантаження інфраструктурних ресурсів (наприклад, використання хмарних сховищ, $v_{викор}/v_{заг}$

Таблиця 2.9 – Показники цифрової стійкості та ризиків *(джерело: систематизовано автором на підставі [160-161])*

Показник	Формула	Опис
1	2	3
1. Час відновлення після збою (RTO)	$T_{віднов}(год)$	Середній час, необхідний для повного відновлення роботи критичних ЦІКР (технологічні ресурси, інфраструктура) після збою (наприклад, кібератаки, збою сервера).
2. Індекс кібербезпеки ($I_{безпека}$)	$I_{безпека} = 1 - \frac{N_{інцид}}{T_{спост}}$	Показує частоту кіберінцидентів ($N_{інцид}$) за період $T_{спост}$. Чим ближче до 1, тим вищий рівень захищеності ЦІКР. Забезпечується ресурсами цифрової безпеки (CSR).

Продовження табл. 2.9

1	2	3
3. Індекс адаптивності архітектури ($I_{адапт}$)	Якісна оцінка (0 до 1)	Оцінює гнучкість ЦІКР до змін, наприклад, частка хмарних сервісів/віртуалізації, які дозволяють масштабувати ресурси. Оцінюється експертно або через співвідношення *Гнучкі Активи / Загальні Активи.*
4. Коефіцієнт покриття критичних процесів ($К_{крит}$)	$К_{крит} = \frac{N_{резерв}}{N_{крит}}$	Частка критичних бізнес-процесів ($N_{крит}$), які мають забезпечене резервне копіювання (BDR) та план відновлення ($N_{резерв}$).

Блок IV. Інтегральна оцінка результативності. Для узугальненої оцінки доцільно використовувати Інтегральний показник результативності ЦІКР ($I_{\Sigma}^{ЦІКР}$), який дозволяє звести фінансові, операційні та стійкісні показники до єдиної оцінки:

$$I_{\Sigma}^{ЦІКР} = \sum_{j=1}^{3} w_j * I_j, \quad (2.8)$$

де I_j – узагальнений індекс для j-го блоку (I. Фінансова ефективність, II. Операційна результативність, III. Цифрова стійкість);

w_j – ваговий коефіцієнт j-го блоку ($w_{фін}+w_{опер} + w_{стійк} = 1$). Ваги встановлюються експертно, при цьому у кризових умовах ваговий коефіцієнт $w_{стійк}$ має бути найвищим;

Успішним впровадженням ЦІКР є умова, за якої $I_{\Sigma}^{ЦІКР}$ перевищує встановлений підприємством або галузевий поріг, а ключові показники стійкості (RTO, $I_{безпека}$) відповідають вимогам антикризового плану. Застосовність показників методики для оцінювання економічної ефективності та стійкості підприємства представлена в табл. 2.10.

Таблиця 2.10 – Застосовність показників методики для оцінювання економічної ефективності та стійкості підприємства *(джерело: авторська розробка)*

Блок методики	Показник (змінна)	Одиниця виміру/ Тип даних	Джерело інформації на підприємстві
1	2	3	4
I. Економічна ефективність			
1.1 Первинні (капітальні) витрати	$C_{п}$	грн/валюта	Бухгалтерський облік, фінансові звіти, договори купівлі-продажу обладнання та ліцензій.
1.2 Річні операційні витрати	C_{OpEx}	грн/валюта	Бюджет IT-підрозділу, договори на технічне обслуговування, рахунки провайдерів хмарних послуг (SaaS, PaaS).
1.3 Річний дохід від ЦІКР / економія	$D_{р}$	грн/валюта	Фінансові звіти, аналітичні дані систем CRM/ERP, розрахунки економії від скорочення витрат на персонал (RPA) або часу обробки.
II. Операційна результативність			
2.1 Кількість автомтаизованих процесів	$N_{авт}$	од.	Регламенти бізнес-процесів, звіти BPM-систем, карти процесів.
2.2 Загальна кількість процесів	$N_{заг}$	од.	Мапа бізнес-процесів підприємства.
2.3 Кількість помилок у даних	$N_{помилок}$	од.	Звіти систем BI, аналітика якості даних (Data Quality), аудит інформаційних ресурсів (IR).
2.4 Загальна кількість даних/ транзакцій	$N_{всього}$	од.	Журнали транзакцій ERP/CRM систем, Data Lake.
2.5 Середній час на виконання операції (координації)	$T_{коорд}$	хвилини/ години	Таймінги процесів, журнали комунікаційних платформ (CR), хронометраж.
2.6 Ступінь завантаження інфраструктурних ресурсів	$E_{потуж}$	%	Системи моніторингу IT-інфраструктури, звіти хмарних провайдерів

Продовження табл. 2.10

1	2	3	4
III. Цифрова стійкість та ризики			
3.1 Час відновлення після збою (RTO)	$T_{віднов}$	години	Документація плану безперервності бізнесу (BCP/DRP).
3.2 Кількість кіберінцидентів	$N_{інцид}$	од.	Журнали SIEM-систем, звіти IT-безпеки (CSR), реєстр інцидентів.
3.3 Період спостереження	$T_{спост}$	місяці/рік	Визначається аналітиком (як правило, 1 рік).
3.4 Параметри для якісної оцінки адаптивності	$I_{адапт}$	% / якісна шкала	Дані про інфраструктуру (ISR), експертні опитування, аудит архітектури.
3.5 Кількість критичних процесів з резервуванням	$N_{резерв}$	од.	Перелік критичних процесів, звіти систем резервного копіювання (Backup & Recovery).
3.6 Загальна кількість критичних процесів	$N_{крит}$	од.	Регламент управління критичними процесами.
3.7 Вагові коефіцієнти блоків (w_j)	$w_{фін}$, $w_{опер}$, $w_{стійк}$	частка одиниці (0 до 1)	Експертна оцінка (визначається керівництвом або групою експертів відповідно до стратегічних пріоритетів підприємства в умовах кризи).

З урахуванням обмежень наведеного фінансово-економічного інструментарію та необхідності його розширення в межах комплексного підходу до оцінювання розвитку підприємства, доцільним є поглиблення аналізу інфокомунікаційних ресурсів як ключового елементу сучасного інформаційного середовища. Саме стан і характеристики інфокомунікаційної інфраструктури визначають здатність підприємства забезпечувати безперервність операційної діяльності, підтримувати стратегічні управлінські процеси та адаптуватися до умов цифрової невизначеності.

Оцінювання доступності, цілісності та результативності інфокомунікаційних ресурсів у підтримці операційної та стратегічної діяльності підприємства відзначено у табл. 2.11.

Таблиця 2.11 – Оцінювання доступності, цілісності та результативності інфокомунікаційних ресурсів у підтримці операційної та стратегічної діяльності підприємства *(джерело: авторська розробка)*

Критерій	Опис блоку оцінювання
1	2
1. Об’єкт оцінювання	Інфокомунікаційні ресурси (ЦІКР) критичних процесів підприємства. Об'єктом є системна архітектура ЦІКР (Інформаційні, Комунікаційні, Технологічні, Інфраструктурні та Кібербезпекові ресурси), що задіяні у підтримці операційної (щоденні транзакції, виробництво) та стратегічної (прийняття управлінських рішень, розвиток) діяльності. Фокус на ресурсах, які впливають на Безперервність Бізнесу (BC) та Адаптивність
2. Мета оцінювання	Визначення рівня надійності та результативності ЦІКР для забезпечення стійкого розвитку підприємства в умовах криз. Оцінка має встановити:
	а) технологічну зрілість: фактичний рівень доступності, цілісності та конфіденційності критичних даних та систем;
	б) операційну підтримку: внесок ЦІКР у підвищення продуктивності, швидкості комунікації та якості управлінських рішень;
	в) ризик-профіль: ідентифікація вразливостей (технічних, процесуальних, користувацьких) та оцінка ризиків операційних збоїв.
3. Метод оцінювання	Комбінований метод (кількісно-якісний аналіз) включає:
	1) кількісний (метричний) аналіз: розрахунок показників, що базуються на журналах систем (логістичні, фінансові, технічні);
	2) якісний (експертний) аналіз: оцінювання рівня зрілості процесів, експертне зважування (визначення вагових коефіцієнтів) та оцінка індексу адаптивності;
	3) аудит на відповідність: Перевірка дотримання внутрішніх політик та галузевих стандартів (наприклад, ISO 27001 для цілісності).

Продовження табл. 2.11

1	2
4. Методики оцінювання	1. Методика оцінки цифрової стійкості (Digital Resilience Score): Застосування показників RTO (Recovery Time Objective) та RPO (Recovery Point Objective) для оцінки доступності та цілісності (антикризовий блок) [див. Блок III удосконаленої методики].
	2. Аналіз ефективності операцій (Productivity/Efficiency Metrics): Використання метрик, таких як Рівень автоматизації () та Швидкість комунікації ($Р_{даних}$) [див. Блок II удосконаленої методики].
	3. Методика оцінки якості даних (Data Quality Assessment): Використання індексу якості даних () для оцінки цілісності та достовірності інформаційних ресурсів.
	4. Матричний аналіз ризиків (Risk Matrix Analysis): Ідентифікація та оцінка ймовірності та впливу вразливостей ЦІКР (технологічні/кібернетичні ризики) на безперервність операцій.
Інтегральний результат	Формування Інтегрального індексу результативності ЦІКР ($I_{\Sigma}^{\text{ЦІКР}}$), який є основним показником у блоці діагностики

На підставі удосконаленої багатовимірної методики, а також з метою практичної демонстрації можливостей діагностики рівня цифрового інноваційного комплексного рішення (ЦІКР) в умовах функціонування підприємств різних галузей.

Результати діагностики залежать від вагових коефіцієнтів (w_j), які відображають стратегічні пріоритети підприємства в умовах криз (наприклад, для фінансової структури безпека та цілісність даних є важливішими, ніж для виробництва).

Порівняльну таблицю діагностичих показників ЦІКР наведено у табл. 2.12. Для спрощення інтегральні показники блоків (I_j) та вагові коефіцієнти (w_j) прийняті умовно (за шкалою від 0 до 1, де 1 – найкращий результат).

Таблиця 2.12 – Результати оцінювання за удосконаленою методикою *(джерело: авторська розробка)*

Показник	Вид діяльності/підприємство*		
	IT/ П1	ФінТех/П2	Виробниче/П3
Ваговий коефіцієнт стійкості ($w_{\text{стійк}}$)	0,40	0,35	0,30
Ваговий коефіцієнт операційної результативності ($w_{\text{опер}}$)	0,40	0,30	0,40
Ваговий коефіцієнт фінансової ефективності ($w_{\text{фін}}$)	0,20	0,35	0,30
Ключові показники стійкості (Блок III):			
Час відновлення (RTO) (Ціль: хв./год.)	1.0 год. (ЦІКР в хмарі, висока адаптивність)	0.5 год. (надкритично, регулятивні вимоги)	4.0 год. (задовільно, залежність від фізичної інфраструктури)
Індекс кібербезпеки ($I_{\text{безпека}}$)	0,90	0,98 (суворі вимоги CSR)	0,75 (низька, недостатня увага)
Ключові показники результативності (Блок II):			
Рівень автоматизації ($I_{\text{автом}}$)	95% (Високий, автоматизація Dev/Ops)	70% (Середній, ручна робота в комплаєнсі)	85% (Високий, Індустрія 4.0)
Якість та доступність даних ($P_{\text{даних}}$)	0,95	0,99 (Висока цілісність)	0,80
Інтегральний показник результативності ЦІКР ($I_{\Sigma}^{\text{ЦІКР}}$)	0,882	0,847	0,745
** Назва підприємств за вимогою власників не вказується*			

Відповідно до проведених розрахунків, проведемо аналіз результатів діагностики:

1. IT-компанія (розробка ПЗ): найвищі вагові коефіцієнти надано операційній результативності (швидкість розробки, $I_{\text{опер}}$) та цифровій стійкості ($I_{\text{стійк}}$), оскільки безперервність процесів розробки та захист інтелектуальної

власності є критичними для розвитку; підприємство демонструє високі показники в обох пріоритетних блоках ($I_{опер}$=0,95, $I_{стійк}$=0,88), що забезпечує найвищий інтегральний показник. Стійкість ($I_{стійк}$) відносно висока за рахунок хмарних рішень та високої адаптивності (RTO=1,0 год).

2. Фінансова структура (ФінТех): найвищі вагові коефіцієнти надано фінансовій ефективності ($w_{фін}$) та цифровій стійкості ($w_{стійк}$), оскільки цілісність даних і кібербезпека є регуляторними вимогами та основою довіри клаєнтів. Ризик втрати даних (цілісність) тут має найбільший вплив; фінансова структура має найкращі показники цілісності даних ($P_{даних}$=0,99), кібербезпека ($I_{безпека}$=0,98) та найнижчий RTO (0,5 год), що свідчить про високу технологічну зрілість у сфері захисту ЦІКР. Однак помірна результативність ($I_{опер}$=0,70) знижує загальний інтегральний показник, вказуючи на необхідність автоматизації комплаєнсу та управлінських процесів.

3. Виробниче підприємство: найвищі вагові коефіцієнти надано операційній результативності ($w_{опер}$), оскільки ефективність ЦІКР безпосередньо впливає на виробничий цикл та мінімізацію простоїв; підприємство демонструє найнижчий інтегральний показник ($I_{\Sigma}^{ЦІКР}$=0,745) через низький рівень кібербезпеки ($I_{безпека}$=0,75) та тривалий час відновлення (RTO=4,0 год), що створює високу вразливість до зовнішніх кризвоих викликів. Діагностика чітко вказує, що для забезпечення стійкості підприємству необхідно інвестувати в елемент цифрової безпеки та стійкості ЦІКР (Блок III).

Відтак, діагностика за багатовимірною методикою дозволяє не лише кількісно оцінити результативність ЦІКР, але й стратегічно перерозподілити пріоритети інвестицій відповідно до галузевої специфіки та рівня кризових ризиків. У кризових умовах найнижчі показники RTO та високі Ібезпека (фінтех) відображають найбільшу стійкість, а найнижчий $I_{\Sigma}^{ЦІКР}$ (виробниче підприємство) вказує на найбільшу потребу у вдосконаленні ЦІКР.

Висновки до розділу 2

Проведене у розділі 2 дослідження дозволило комплексно проаналізувати стан, структуру та динаміку цифрової зрілості підприємств у контексті розвитку інфокомунікаційного цифрового забезпечення в умовах кризових трансформацій дозволило дістати *таких висновків і узагальнюючих тверджень*:

1. Аргументоване, що цифрова зрілість підприємства є багатовимірною характеристикою, яка формується під впливом сукупності процесних, технологічних, інформаційно-аналітичних, кадрових та управлінських чинників, а не зводиться виключно до рівня впровадження окремих цифрових технологій. Аналіз ключових вимірів цифрової зрілості показав, що найбільш розвиненими у сучасних підприємств є технологічний компонент, зокрема використання хмарних сервісів, цифрових платформ, інфокомунікаційних інструментів та базових елементів цифрової інфраструктури. Водночас рівень цифрової зрілості бізнес-процесів, управління даними та управлінських практик залишається істотно диференційованим залежно від галузевої належності підприємства, його розміру та інституційного середовища функціонування. Це свідчить про *фрагментарний характер цифрової трансформації*, за якого технологічні рішення нерідко впроваджуються без належної інтеграції в систему управління підприємством.

2. Порівняльний аналіз підприємств різних секторів (IT, фінтех, виробничий сектор) засвідчив, що найвищий рівень цифрової зрілості характерний для IT-підприємств, які функціонують у логіці інтегрованих та data-driven моделей управління. Фінтех-компанії також демонструють високий рівень цифрової зрілості, однак їх розвиток значною мірою детермінований регуляторними вимогами, що формує специфічну модель цифрової трансформації, орієнтовану на безпеку, комплаєнс та безперервність

діяльності. Натомість виробничі підприємства перебувають переважно на процесному рівні цифрової зрілості, що проявляється у локальній автоматизації окремих функцій без формування цілісної цифрової інфокомунікаційної екосистеми.

3. Результати оцінювання цифрової зрілості підприємств України та їх зіставлення з підприємствами економічно більш стабільних країн, зокрема ОАЕ, засвідчили *наявність структурного розриву між рівнем цифрових технологій та рівнем цифрового управління і використання даних.* В умовах криз цей розрив набуває особливої значущості, оскільки саме управлінські та аналітичні компоненти цифрової зрілості визначають здатність підприємства забезпечувати стійкість, безперервність та адаптивність діяльності. Недостатній рівень централізації даних, обмежене застосування прогнозної аналітики та слабка інтеграція цифрових KPI у систему управління знижують ефективність використання наявних інфокомунікаційних ресурсів.

4. *Запропонована методика оцінювання цифрової зрілості підприємств* дозволила не лише кількісно виміряти рівень розвитку окремих вимірів, але й виявити критичні зони цифрової вразливості. Використання системи субіндикаторів і розрахунок інтегрального індексу цифрової зрілості забезпечили можливість міжгалузевого та міжкраїнового порівняння, а також створили аналітичну основу для формування управлінських рішень щодо пріоритетів цифрового розвитку в умовах кризових обмежень.

5. *Обгрунтовано роль інфокомунікаційного цифрового забезпечення як системоутворюючого елементу цифрової зрілості*. Доведено, що ефективне інфокомунікаційне забезпечення виступає не лише технічною інфраструктурою, а й інституційним механізмом інтеграції процесів, даних, персоналу та управлінських рішень. В умовах криз саме інфокомунікаційні цифрові ресурси забезпечують оперативний обмін інформацією, підтримку управлінських рішень у реальному часі та координацію внутрішніх і зовнішніх взаємодій підприємства. Отримані аналітичні результати також підтвердили *доцільність використання інтегрального індексу цифрової зрілості як*

інструменту моніторингу динаміки розвитку підприємства. Такий індекс дозволяє відстежувати не лише загальний рівень цифрової трансформації, але й структурні зрушення між окремими вимірами, що є критично важливим для антикризового управління. Виявлено, що підприємства з високим рівнем цифрової зрілості мають істотно вищу здатність до адаптації, швидшого відновлення після кризових шоків та підтримки операційної безперервності.

6. Можна констатувати, що *цифрова зрілість підприємства формується як результат цілеспрямованого розвитку інфокомунікаційної екосистеми, узгодженої з управлінськими цілями та антикризовими пріоритетами*. Виявлені диспропорції між окремими вимірами цифрової зрілості обґрунтовують *необхідність переходу від фрагментарної цифровізації до системної моделі цифрового інфокомунікаційного забезпечення розвитку підприємства*, що й зумовлює логічний перехід до розробки концептуальних і прикладних рішень у наступному розділі роботи.

7. *Перевірка робочої гіпотези* здійснювалася шляхом формування та застосування методики оцінювання цифрової зрілості підприємств за ключовими вимірами, аналізу інфокомунікаційного забезпечення та порівняння рівнів цифрової стійкості підприємств різних галузей і інституційних середовищ. Встановлене, що підприємства з інтегрованим підходом до управління цифровими інфокомунікаційними ресурсами демонструють вищі показники адаптивності, безперервності та стійкості в кризових умовах.

Відтак, за результатами аналітичних і порівняльних досліджень розділу 2, *робоча гіпотеза підтверджується*, оскільки встановлено пряму залежність між рівнем інтеграції управління цифровими інфокомунікаційними ресурсами та зростанням цифрової стійкості підприємств у кризових умовах.

Основні результати та положення, викладені в розділі 2, висвітлено у працях автора, що наведено у Додатку А. Це публікації: [2, 7, 2].

РОЗДІЛ 3
СИСТЕМНЕ ЦИФРОВЕ ІНФОКОМУНІКАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ РОЗВИТКУ ПІДПРИЄМСТВА В УМОВАХ КРИЗ

3.1 Концептуальна модель фокусного цифрового інфокомунікаційного забезпечення розвитку підприємства

Розкриття авторського підходу та бачення фокусного цифрового інфокомунікаційного забезпечення розвитку підприємства полягає у *вирішенні таких чотирьох концетуально важливих завдань:*

а) визначити сутність та особливості фокусного цифрового інфокомунікаційного забезпечення розвитку та діяльності підприємства, обгрунтувати потребу в ньому для підприємства в умовах кризи та розробити його концептуальну структурно-логічну модель;

б) сформулювати та обгрунтувати принципи побудови інфокомунікаційної екосистеми;

в) розробити архітектуру та ключові елементи цифрового інфокомунікаційного забезпечення розвитку підприємства;

в) визначити KPI розвитку цифрової інфраструктури підприємства в блоці цифрового інфокомунікаційного забезпечення розвитку підприємства.

А. Сутність та особливості фокусного цифрового інфокомунікаційного забезпечення розвитку та діяльності підприємства, обгрунтування потреби в ньому для підприємства в умовах кризи та розробка його концептуальної структурно-логічної моделі. На нашу думку, *фокусне цифрове інфокомунікаційне забезпечення розвитку підприємства* – це цілеспрямована система цифрових ресурсів, технологій, інструментів і каналів комунікації, яка концентрується на ключових пріоритетах підприємства та забезпечує безперервність інформаційних потоків, оперативність

управлінських рішень і стійкість бізнес-процесів у нестабільних умовах. Воно охоплює інтегроване використання цифрових платформ, мережевої інфраструктури, аналітики даних, систем комунікації та кіберзахисту для підтримання стратегічного розвитку і здатності підприємства адаптуватися до кризових ситуацій.

Головним аргументом з обґрунтування потреби у фокусності цифрового інфокомунікаційного забезпечення розвитку підприємства в умовах кризи є такі міркування. У кризових умовах підприємства стикаються з різкими порушеннями комунікацій, перебоями в операційній діяльності, підвищеною невизначеністю та необхідністю приймати рішення швидше, ніж у мирний час. Фокусне цифрове інфокомунікаційне забезпечення дозволяє зменшити ці ризики за рахунок централізації критичних цифрових процесів, посилення захищеності даних, оптимізації внутрішніх і зовнішніх комунікацій та забезпечення мобільного управління бізнес-процесами. Завдяки концентрації цифрових ресурсів на ключових напрямах діяльності підприємство підвищує свою стійкість, зберігає контроль над операціями, мінімізує втрати та отримує можливість швидко відновлюватися після зовнішніх потрясінь. Це робить фокусне цифрове інфокомунікаційне забезпечення не лише технічним інструментом, а стратегічною передумовою виживання й подальшого розвитку підприємства під час криз (табл. 3.1).

Таблиця 3.1 – Переваги фокусного цифрового інфокомунікаційного забезпечення розвитку підприємства в умовах криз *(джерело: авторська розробка)*

Перевага	Зміст переваги (розгорнутий опис)
1	2
1. Забезпечення безперервності бізнес-процесів	Фокусне забезпечення концентрує ресурси на критичних функціях, що дозволяє підприємству підтримувати операційну діяльність навіть у разі перебоїв зв’язку, релокації персоналу чи зовнішніх загроз.
2. Підвищення швидкодії	Оперативний обмін даними, доступ до цифрових платформ у реальному часі та централізація

Продовження таблиці 3.1

1	2
управлінських рішень	інформаційних потоків зменшують час реагування на кризові ситуації.
3. Посилення інформаційної безпеки	Застосування багаторівневих механізмів захисту, резервування даних та шифрування мінімізує ризики витоку інформації, кібератак та несанкціонованого доступу.
4. Інтеграція цифрових платформ і оптимізація комунікацій	Об’єднання CRM, ERP, SCM, HRM та комунікаційних сервісів в єдину екосистему усуває розриви в даних і забезпечує синхронність інформаційних потоків між підрозділами.
5. Гнучкість і адаптивність цифрової інфраструктури	Можливість швидкої перебудови цифрових процесів, масштабування ресурсів і переходу на хмарні платформи забезпечує стійкість у непередбачуваних ситуаціях.
6. Підтримка віддаленої та гібридної роботи	Забезпечує повноцінний доступ до ресурсів підприємства з будь-яких локацій, що дозволяє зберегти продуктивність персоналу в умовах фізичних обмежень або небезпеки.
7. Зменшення витрат та ресурсна оптимізація	Концентрація цифрових інвестицій на критичних напрямках дозволяє скоротити непродуктивні витрати та спрямувати ресурси на найважливіші технологічні рішення.
8. Підвищення стійкості до зовнішніх загроз	Системна цифрова підтримка та захищені комунікації дають змогу протистояти впливу воєнних, економічних, кібернетичних чи логістичних криз.
9. Покращення аналітики та ситуаційної обізнаності	Використання аналітичних панелей, моніторингу ризиків та прогнозних алгоритмів формує точнішу картину ситуації та підвищує якість стратегічних рішень.
10. Швидке відновлення діяльності після кризи	Дублювання цифрових ресурсів, резервні канали зв’язку та хмарна інфраструктура забезпечують можливість швидкого перезапуску операцій після руйнувань або технічних збоїв.

Водночас, *порівняння фокусного та традиційного цифрового інфокомунікаційного забезпечення діяльності та розвитку підприємства за дванадцятю критеріями* (табл. 3.2) демонструє як переваги першого, так і

його недоліки.

Таблиця 3.2 – Порівняння фокусного та традиційного цифрового інфокомунікаційного забезпечення підприємства *(джерело: розроблене автором на підставі аналізу [160-169] та результатів власних досліджень)*

Критерій порівняння	Фокусне цифрове інфокомунікаційне забезпечення	Традиційне цифрове забезпечення
1	2	3
1. Стратегічна орієнтація	Спрямоване на критичні процеси, що визначають стійкість підприємства; має чіткі пріоритети відповідно до кризових умов.	Орієнтоване на широке охоплення функцій; пріоритети розмиті або стабільні, не враховують кризовий контекст повною мірою.
2. Реакція на кризові умови	Адаптується швидко, перебудовується, масштабується, змінює структуру інформаційних потоків.	Модифікується повільно; потребує додаткових ресурсів для адаптації; часто працює нестабільно під час криз.
3. Інформаційні потоки	Централізовані, швидкі, спрямовані на забезпечення безперервності та оперативності управління.	Фрагментовані, повільні; часто існують організаційні «розриви» між підрозділами.
4. Канали комунікації	Інтегровані корпоративні платформи, захищені канали, мультирівневе резервування.	Застарілі або роз'єднані канали зв’язку, відсутність резервних шляхів передачі даних.
5. Інформаційна безпека	Посилена, багаторівнева, включає кіберзахист, дублювання, шифрування, SOC, MFA.	Базова або середня; застосовується мінімальний набір інструментів кіберзахисту.
6. Віддалена та гібридна робота	Організована на системному рівні, безпечна, підтримується хмарою та VPN.	Часткова або епізодична, нерідко без достатнього рівня захисту даних.
7. Інтеграція цифрових платформ	Високий рівень інтеграції: CRM + ERP + SCM + HRM + комунікації в єдиній системі.	Платформи роз'єднані; обмін даними ускладнений; часто використовуються різні несумісні системи.

Продовження таблиці 3.2

1	2	3
8. Управління даними	Орієнтація на єдиний цифровий контур, аналітику в реальному часі, BI-системи.	Дані часто зберігаються сегментарно; аналітика базується на запізнілій інформації.
9. Підхід до інвестицій	Інвестиції спрямовані тільки на ключові напрямки з найбільшим антикризовим ефектом.	Інвестиції рівномірні або традиційні, без урахування зміни ризиків та пріоритетів.
10. Гнучкість цифрової інфраструктури	Висока: швидке масштабування, хмарні рішення, дублювання ресурсів.	Низька: важко масштабувати, переважно локальні серверні системи.
11. Швидкість прийняття рішень	Забезпечується завдяки оперативній аналітиці, швидким даним і централізованим потокам.	Залежить від повільного збору інформації та ручної обробки даних.
12. Стійкість до зовнішніх загроз	Висока стійкість завдяки захищеним комунікаціям, резервуванню та антикризовому плануванню.	Обмежена, оскільки системи не враховують екстремальні сценарії.

Порівняння фокусного цифрового інфокомунікаційного забезпечення та традиційних підходів до цифровізації підприємства *(див. табл. 3.1-3.2)* засвідчує *суттєві відмінності у стратегічній орієнтації, швидкодії, гнучкості та рівні стійкості до кризових впливів.* Традиційні ІКТ-системи демонструють достатню ефективність у стабільних умовах, проте їхня фрагментарність, обмежена інтегрованість і недостатня адаптивність роблять їх вразливими в умовах турбулентності. Натомість фокусне цифрове забезпечення побудоване на принципах пріоритезації критичних процесів, централізації інформаційних потоків, багаторівневого кіберзахисту та швидкої масштабованості цифрової інфраструктури, що дозволяє підприємству підтримувати керованість і безперервність діяльності за умов високих ризиків. Висока інтеграція платформ, якісний інформаційний супровід, орієнтація на аналітику в реальному часі та можливість оперативного реагування формують

значні переваги фокусного підходу, роблячи його ключовим елементом антикризового розвитку та цифрової стійкості сучасних підприємств.

Важливою складовою сучасного управління підприємством є вибудова ефективної системи цифрового інфокомунікаційного забезпечення. Разом із тим, *доцільно розрізняти фокусне цифрове інфокомунікаційне забезпечення діяльності підприємства та фокусне цифрове інфокомунікаційне забезпечення розвитку підприємства в умовах криз*, оскільки ці поняття мають різну стратегічну спрямованість, різний набір функціональних компонентів та неоднаковий вплив на організаційну стійкість.

Фокусне цифрове інфокомунікаційне забезпечення діяльності підприємства зосереджене на підтримці поточного функціонування та забезпеченні безперервності щоденних бізнес-процесів. Його головна мета полягає у створенні надійного цифрового середовища, яке дозволяє персоналу ефективно виконувати свої операційні завдання, швидко обмінюватися службовою інформацією, координувати дії та забезпечувати синхронізацію між підрозділами. Для такого типу забезпечення характерне застосування базових інформаційних систем (CRM, ERP, HRM), систем внутрішнього документообігу та стандартних засобів комунікації. Основні результати проявляються у стабільності операційної роботи, мінімізації внутрішніх збоїв та підвищенні продуктивності персоналу.

Натомість *фокусне цифрове інфокомунікаційне забезпечення розвитку підприємства в умовах криз* має зовсім іншу природу. Воно спрямоване не стільки на підтримку поточних процесів, скільки на забезпечення стратегічної стійкості та здатності підприємства адаптуватися до зовнішніх викликів. В умовах криз (воєнних, економічних, кадрових, енергетичних або кібернетичних) цифрові ресурси мають працювати у режимі підвищених вимог. Тому фокусне забезпечення розвитку базується на механізмах антикризового прогнозування, гнучкого масштабування, міграції у хмарні середовища, резервування даних і каналів зв’язку, інтеграції цифрових платформ у єдиний інформаційний контур. Особливе значення набувають

аналітичні інструменти реального часу, які дозволяють моделювати сценарії та швидко приймати рішення.

Таким чином, ключова відмінність полягає у тому, що в першому випадку цифрове забезпечення виконує операційну, підтримувальну функцію, тоді як у другому – стратегічну, трансформаційну й антикризову. У кризових умовах саме фокусне цифрове інфокомунікаційне забезпечення розвитку визначає здатність підприємства зберегти керованість, забезпечити життєві цикли критично важливих процесів, швидко реагувати на невизначеність і відновлювати діяльність після зовнішніх потрясінь. Це дає підстави розглядати його як один із ключових факторів сучасної моделі цифрової стійкості підприємства.

Концептуальна структурно-логічна модель фокусного цифрового інфокомунікаційного забезпечення розвитку та діяльності підприємства (рис.3.1) демонструє зв’язок управлінських впливів у динаміці. Крім того, фокусне цифрове забезпечення формує адаптивну цифрову інфраструктуру, здатну швидко перебудовуватись відповідно до змін середовища:

- масштабувати обчислювальні потужності;
- дублювати канали зв’язку;
- забезпечувати доступ до ресурсів із різних локацій;
- підтримувати безпечний віддалений формат роботи.

Це надає підприємству можливість продовжувати операційну діяльність навіть за умов обмеженої доступності фізичних офісів, порушення логістики чи руйнування економічної інфраструктури.

Узагальнюючи зазначене, можна стверджувати, що фокусне цифрове інфокомунікаційне забезпечення виступає фундаментом цифрової стійкості підприємства. Воно забезпечує цілеспрямоване управління цифровими активами, мінімізує ризики, пов'язані з інформаційною вразливістю, і створює умови для швидкого відновлення діяльності після кризи. Формування такої системи стає стратегічною необхідністю для сучасних підприємств, що діють у кризових ситуаціях та швидкозмінному середовищі.

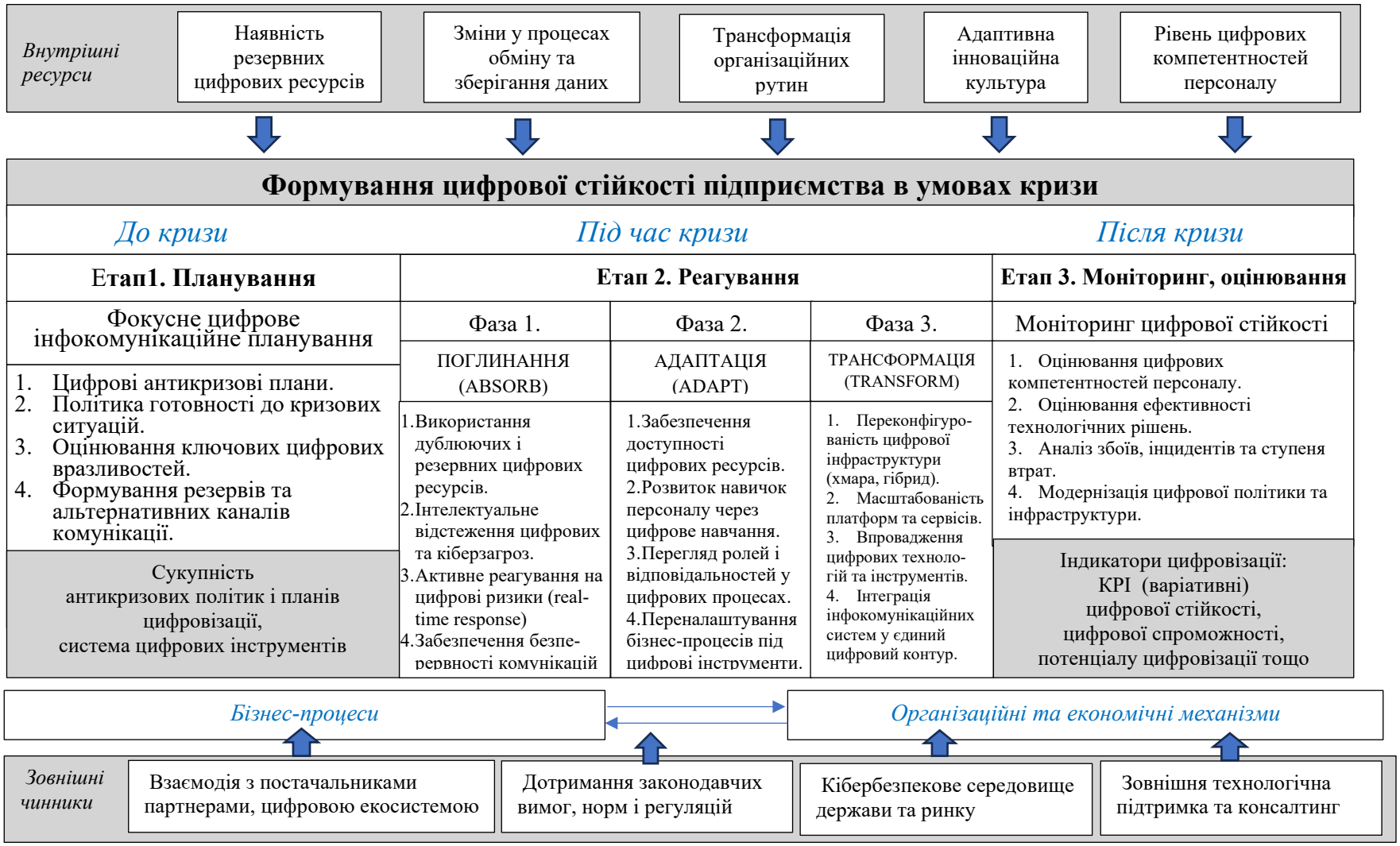


Рисунок 3.1 – Модель формування цифрової стійкості підприємства на основі фокусного цифрового інфокомунікаційного забезпечення *(джерело: авторська розробка)*

Б. Принципи побудови інфокомунікаційної екосистеми. *Основними принципами побудови інфокомунікаційної екосистеми підприємства в умовах цифровізації та кризи* є такі:

– адаптивність, що передбачає здатність цифрових систем швидко перебудовуватися до змін, оперативно інтегрувати нові інструменти;

– стійкість, яка забезпечує працездатність інформаційно-комунікаційної інфраструктури під впливом зовнішніх загроз, кібератак або технічних збоїв;

– безперервність, орієнтована на гарантовану підтримку критичних функцій і бізнес-процесів навіть за умов пікових навантажень чи порушень;

– відкритість і інтегрованість дозволяє співпрацювати з зовнішніми платформами, партнерами, державними і галузевими цифровими сервісами;

– орієнтація на дані, яка передбачає пріоритетність якісного збору, обробки й аналітики інформації для прийняття управлінських рішень;

– кібербезпека за принципом «вбудованого захисту», що гарантує включення політик, механізмів та інструментів безпеки в архітектуру екосистеми на всіх рівнях, а не лише як окремий компонент.

Доцільність застосуівання наведених принципів в умовах цифровізації та кризи доводять аргументи, наведені у табл.3.3.

Таблиця 3.3 – Принципи побудови інфокомунікаційної екосистеми: доцільність *(джерело: авторська розробка)*

Принцип	Обґрунтування доцільності
1	2
1. Адаптив-ність	Швидка перебудовова процесів, цифрових сервісів та комунікаційних каналів до нових умов, оперативне реагування на зовнішні загрози, ринкові зміни та внутрішні збої. Зниження часу переходу до альтернативних рішень і підвищує гнучкість екосистеми.
2. Стійкість	Здатність цифрової інфраструктури функціонувати при технічних збоях, кібератаках, втраті даних або ресурсних обмеженнях. Це – фундаментальний елемент антикризового управління та мінімум ризиків критичних відмов.

Продовження таблиці 3.3

1	2
3. Безперервність	Неперервність ключових бізнес-процесів та доступність цифрових сервісів навіть у період інцидентів, нестабільності або порушення ланцюгів постачання, що є вирішальним для підтримки діяльності підприємства та утримання клієнтів.
4. Відкритість та інтегрованість	Умови для взаємодії з державними, галузевими та партнерськими цифровими платформами. Масштабування екосистеми, розширення функціоналу та доступ до зовнішніх інновацій. Розбудова мережевої моделі співпраці, що підвищують стійкість підприємства в умовах кризи.
5. Орієнтація на дані (data-driven)	Зростання якості та швидкостіь прийняття управлінських рішень через використання аналітики, моделей прогнозування та штучного інтелекту. У кризових умовах дані стають визначальним ресурсом, який дозволяє прогнозувати ризики, оптимізувати процеси та зменшувати невизначеність.
6. Кібербезпека як вбудований принцип (security-by-design)	Стабільність та захищеність екосистеми, мінімізування ризиків втрати конфіденційних даних, фінансових збитків і зупинки операцій. У кризових періодах рівень кіберзагроз суттєво зростає, тому інтеграція безпеки на всіх етапах архітектурного проєктування є критично необхідною.

Наведені аргументи на користь запропонованих принципів доводять, що інфокомунікаційна екосистема підприємства має бути адаптивною, стійкою, безперервною, відкритою до інтеграцій, керованою даними та захищеною на всіх рівнях цифрової архітектури.

В. Архітектура та ключові елементи цифрового інфокомунікаційного забезпечення розвитку підприємства. Структуровану архітектуру та ключові елементи цифрового інфокомунікаційного забезпечення розвитку підприємства слід будувати відповідно до наведених вище принципів цифровізації, вимог антикризового управління та логіки інфокомунікаційних екосистем [162-167].

Пропонована архітектура цифрового інфокомунікаційного забезпечення розвитку підприємства складається з *чотирьох взаємопов'язаних рівнів*, кожен

з яких виконує окремі функції, але колективно забезпечує стійку, адаптивну, безперервну та захищену цифрову інфраструктуру (рис. 3.2).

Рисунок 3.2 – Архітектура та ключові елементи цифрового інфокомунікаційного забезпечення розвитку підприємства *(джерело: авторська розробка)*

Перший рівень – інфраструктурно-технічний рівень (Foundation Layer), що забезпечує підприємству масштабованість, надійність та безперервність роботи цифрових сервісів. Це базова технічна платформа, на якій функціонує вся екосистема. Її ключові елементи: сервери, дата-центри, хмарні середовища (IaaS); корпоративні мережі, VPN, SD-WAN; системи зберігання даних (NAS/SAN); резервні платформи та системи відновлення (DRaaS).

Другий рівень – платформенно-сервісний рівень (Platform Layer), що забезпечує функціонування бізнес-процесів, комунікацій і взаємодії користувачів. Його ключові елементи: інтегровані бізнес-платформи ERP, CRM, SCM; комунікаційні сервіси (email, корпоративні месенджери, VoIP,

відеоконференції); BPM-платформи та RPA-інструменти; інтеграційні шини (API Gateway, ESB). Цей рівень оптимізує операційні процеси, підвищує продуктивність, автоматизує рутинні функції.

Третій рівень – аналітично-інтелектуальний (Intelligence Layer), що відповідає за аналітику, прогнозування, підтримку рішень та адаптацію до змін. Його ключові елементи: системи Business Intelligence (BI); моделі прогнозної аналітики; інструменти обробки великих даних (Big Data); штучний інтелект і машинне навчання (AI/ML); моніторинг продуктивності та операційних ризиків. Цей рівень сприяє прийняттю швидких і точних управлінських рішень, виявляє ризики, створює передумови для адаптивності.

Четвертий рівень – комунікаційно-взаємодієвий рівень (Interaction Layer), що забезпечує внутрішню та зовнішню комунікацію підприємства. Його ключові елементи: корпоративні портали та внутрішні інформаційні системи; платформи для клієнтів (особисті кабінети, мобільні застосунки); омніканальні канали (чат-боти, соціальні мережі, контакт-центри); системи управління знаннями (KMS). Цей рівень покращує взаємодію із клієнтами та персоналом, забезпечує обмін знаннями та швидкість комунікацій.

Окрім інструментів наведених рівнів, потрібні *ключові системні елементи, що забезпечують розвиток екосистеми в цілому.* До них віднесено:

а) цифрову інтеграцію (API-економіка, ESB, Microservices), що забезпечує об’єднання всіх компонентів у єдину інфокомунікаційну екосистему;

б) кібербезпеку як наскрізну складову (Security-by-Design), яка охоплює шифрування, Zero Trust, моніторинг загроз, контроль доступу, SOC;

в) управління даними (Data Governance), яке включає політики якості даних, стандартизацію, каталоги даних, моделі доступу;

г) автоматизацію та роботизацію процесів (RPA, IPA), які зменшують ризики, підвищує швидкість операцій, забезпечує стійкість процесів;

д) механізми безперервності діяльності (BCM/DRP), які підтримують роботу у надзвичайних ситуаціях та підвищують операційну готовність;

е) цифрову взаємодію і співпрацю (Collaboration Tools), які забезпечують єдине середовище комунікацій для персоналу, партнерів та клієнтів.

Відтак, цифрове інфокомунікаційне забезпечення розвитку підприємства являє собою багаторівневу архітектуру, що включає технічну інфраструктуру, бізнес-платформи, аналітичні модулі та комунікаційні інструменти, інтегровані в єдине середовище. Побудова такої екосистеми забезпечує стійкість, безперервність, адаптивність та стратегічну гнучкість підприємства, що є критично важливими в умовах цифровізації та кризи.

В. KPI розвитку цифрової інфраструктури підприємства в блоці цифрового інфокомунікаційного забезпечення розвитку підприємства. Відмінність авторського підходу полягає у тому, що *пропонуються дворівневе визначення KPI* – на рівні принципів побудови інфокомунікаційної екосистеми підприємства в умовах цифровізації та кризи і на рівні цифрової інфраструктури підприємства в блоці цифрового інфокомунікаційного забезпечення розвитку підприємства. Для принципів побудови інфокомунікаційної екосистеми пропонуються такі KPI (табл. 3.4).

Таблиця 3.4 – KPI для принципів побудови інфокомунікаційної екосистеми (кількісні та якісні індикатори) *(джерело: авторська розробка)*

Принцип	Обрані KPI	
	KPI – показник	Об’єкти виміру
1	2	3
1.Адаптивність	– час переходу на резервні процеси (год.); – час впровадження нових цифрових інструментів (год.); – частка процесів, що мають альтернативні сценарії (%); – рівень гнучкості IT-інфраструктури (оцінка 0–2).	Швидкість і легкість перебудови системи, готовність інтегрувати нові рішення, стійкість до змін середовища.
2. Стійкість	– Кількість критичних інцидентів на місяць (од.); – середній час відновлення після збою (MTTR) (год.); – середній час безвідмовної роботи (Uptime %) (год.); – рівень відповідності стандартам безпеки (ISO/NIST).	Здатність системи працювати під навантаженням, опірність збоям, надійність архітектури та технологій.

Продовження таблиці 3.4

1	2	3
3.Безперерв-ність	– Доступність ключових сервісів (%); – час простою критичних процесів (год.); – частка автоматизованих процесів (%); – запас пропускної здатності при пікових навантаженнях (%).	Гарантія того, що ключові сервіси залишаються доступними, навіть під час інцидентів або криз.
4. Відкритість та інтегрованість	– Кількість підключених зовнішніх платформ (од.); – час інтеграції зовнішнього сервісу (дні/год.); – рівень сумісності API (оцінка 0–2); – частка даних, доступних через стандартизовані інтерфейси (%).	Можливість взаємодії екосистеми з партнерами, державними та/або галузевими платформами, інтеграційна готовність.
5.Орієнтація на дані (data-driven)	– Час доступу до аналітичної звітності (год.); – частка управлінських рішень, що приймаються на основі аналітики (%); – якість даних (повнота, актуальність); – кількість використаних моделей прогнозування (од.).	Здатність підприємства приймати рішення на основі даних, розвиток аналітики та інтелектуальних інструментів.
6.Кібербезпека як вбудований принцип (security-by-design)	– Кількість інцидентів кібербезпеки (од.); – час реагування на інцидент (MTTR Security) (год.); – рівень покриття систем моніторингом загроз (%); – частка систем, розроблених за принципом “security-by-design” (%).	Здатність екосистеми бути захищеною на всіх етапах роботи, відповідність вимогам кіберстійкості та безпеки.

Матриця відповідності принципів побудови екосистеми KPI оцінювання (рис.3.3) демонструє, що:

– адаптивність найбільше залежить від KPI часу реагування та аналітичної швидкості (data-driven);

– стійкість найкраще вимірюється кіберпоказниками та автоматизацією;

– безперервність базується на доступності сервісів, автоматизації та контролі інцидентів;

– відкритість і інтегрованість чітко виражаються через KPI API, сумісності та кількості інтеграцій;

– орієнтація на дані напряму корелює з KPI якості та використання даних;

– кібербезпека охоплює найбільше KPI: від інцидентів до моніторингу інфраструктури.

Принцип	KPI					
	часу реагування / переходу	автоматизації процесів	інцидентів та кіберзахисту	доступності сервісів	інтеграційної сумісності	data-driven управління
1. Адаптивність	✓ Час переходу на резервні процеси; ✓ Час впровадження нових інструментів	○ Частка альтернативних сценаріїв автоматизації	○ Кіберінциденти, що потребують перебудови системи	○ Доступність при пікових навантаженнях	○ Швидкість інтеграцій	✓ Час доступу до аналітики; ✓ Рішення на основі даних
2. Стійкість	○ Швидкість переходу під час інциденту	✓ Автоматизація стабілізує роботу	✓ Кількість інцидентів; ✓ MTTR Security; ✓ відповідність стандартам	○ Доступність сервісів у кризах	○ Інтеграції як засіб резервування	○ Прогнозні моделі для попередження збоїв
3. Безперервність	✓ Час простою; ✓ Перехід на резервні канали	✓ Частка автоматизованих процесів	✓ Порушення безпеки, що впливають на сервіс	✓ Доступність ключових сервісів	○ Інтеграції для дублювання потоків	○ Аналітика для підтримки безперервності
4. Відкритість та інтегрованість	○ Час адаптації до зовнішніх змін	○ Автоматизація на рівні API	○ Кіберризики інтеграцій	○ Доступність сервісів через зовнішні платформи	✓ Час інтеграції; ✓Число підключених платформ; ✓ Сумісність API	○ Наявність даних для міжорганізаційного обміну
5. Орієнтація на дані (data-driven)	○ Оптимізація часових рішень через аналітику	○ Автоматизація збору даних	○ Моніторинг кіберінцидентів на основі даних	○ Аналітика стабільності сервісів	○ Дані для інтеграцій	✓ Якість даних; ✓ Частка рішень на основі аналітики; ✓ Моделі прогнозування
6. Кібербезпека як вбудований принцип	○ Перехід на безпечні резервні процеси	○ RPA як мінімізація людських вразливостей	✓ Усі KPI кібербезпеки (інциденти, MTTR, покриття моніторингом)	○ Захищеність каналів доступності	○ Захищеність інтеграцій	○ Аналітика інцидентів і аномалій

Позначення:

✓– KPI напряму вимірює реалізацію принципу;

○ – KPI частково відображає реалізацію принципу (додатковий ефект)

Рисунок 3.3 – Матриця відповідності принципів побудови екосистеми KPI оцінювання *(джерело: авторська розробка)*

KPI для цифрової інфраструктури управління підприємством представлено у табл. 3.5.

Таблиця 3.5 – KPI цифрової інфраструктури управління підприємством *(джерело: розроблене автором з врахуванням підходів [166-169])*

Блок цифрової інфраструктури	Опис KPI	
	KPI	що вимірює
1	2	3
1. Інфраструктурно-технічний рівень	– Uptime (%); – MTTR (час відновлення); – пропускна здатність мережі; – затримка передачі даних (latency).	Надійність, стабільність роботи, швидкість і доступність систем.
2. Платформенно-сервісний рівень (ERP, CRM, BPM)	– Час обробки транзакцій ; – рівень автоматизації процесів (%); – кількість збоїв у сервісах; – SLA виконання.	Ефективність бізнес-платформ, швидкість процесів, стабільність виконання.
3. Аналітично-інтелектуальний рівень (BI, AI)	– Швидкість формування аналітичних звітів; – точність моделей прогнозування; – обсяг оброблених даних; – частка рішень на основі аналітики (%).	Ефективність прийняття рішень, аналітична спроможність та цифрова зрілість.
4. Комунікаційно-взаємодієвий рівень	– Час відповіді комунікаційних каналів; – доступність корпоративних сервісів (%); – рівень навантаження контактних каналів.	Якість внутрішніх та зовнішніх комунікацій, стабільність взаємодії.
5. Безпека та захищеність (Security Layer)	– кількість кіберінцидентів; – час реагування (MTTR Security); – покриття моніторингом загроз (%); – дотримання стандартів ISO / NIST	Кіберстійкість, готовність до криз і рівень безпеки даних.

Продовження таблиці 3.5

1	2	3
6. Управління даними (Data Governance)	– Якість даних (актуальність, повнота); – доступність даних (%); – швидкість доступу до даних; – частка стандартизованих наборів даних (%).	Здатність підприємства ефективно управляти даними, їх структурованість і доступність.
7. Інтеграції та API	– Кількість активних інтеграцій; – час підключення нової інтеграції; – надійність API(відмови/місяць).	Можливість швидко розширювати екосистему та забезпечувати сумісність.
8. Автоматизація та роботизація (RPA/IPA)	– Кількість роботизованих задач; – економія часу (%); – рівень зниження ручних операцій (%).	Продуктивність, стійкість процесів і зменшення операційних ризиків.

Порівнюючи зміст табл. 3.4 та табл. 3.5, можна побачити, що різниця між KPI розвитку цифрової інфраструктури підприємства (у блоці цифрового інфокомунікаційного забезпечення розвитку) та KPI, що вимірюють реалізацію принципів побудови інфокомунікаційної екосистеми, є суттєвим.

KPI розвитку цифрової інфраструктури підприємства відображають технічний, платформний та операційний стан цифрових ресурсів, тобто наскільки ефективно й результативно функціонують елементи архітектури цифрового інфокомунікаційного забезпечення. Вони вимірюють:

- продуктивність цифрових сервісів;
- швидкість роботи інфраструктури;
- надійність та доступність систем;
- рівень автоматизації;
- кіберзахист і стабільність;
- ефективність використання даних.

Тобто фокус KPI інфраструктури – це фактична робота платформи, її технічні характеристики та операційні результати.

KPI принципів побудови інфокомунікаційної екосистеми оцінюють ступінь реалізації управлінських, стратегічних та концептуальних правил, що лежать в основі створення сучасної цифрової екосистеми. Вони вимірюють:

- наскільки система є адаптивною;
- наскільки вона стійка до загроз;
- чи забезпечує безперервність бізнес-процесів;
- чи є відкритою та інтегрованою;
- чи керується підприємство даними;
- чи вбудована кібербезпека в архітектуру.

Отже KPI принципів мають стратегічний вимір і оцінюють відповідність системи базовим концептуальним засадам, а не її технічні параметри.

Відтак, ключова різниця полягає у тому, що KPI цифрової інфраструктури вимірюють технічну та операційну ефективність цифрових ресурсів підприємства, тоді як KPI принципів оцінюють стратегічну відповідність системи ключовим вимогам адаптивності, стійкості, безперервності, відкритості, орієнтації на дані та кібербезпеки.

Цифрова зрілість підприємства проходить розвиток від початкового стану несистемного використання інструментів до рівня інтегрованої та інтелектуально оркестрованої цифрової екосистеми, у якій дані, автоматизація та штучний інтелект забезпечують стійкість, адаптивність, безперервність і стратегічну здатність підприємства до трансформації.

Рівні цифрової зрілості підприємства описано з характеристиками інфраструктури та управлінських можливостей (рис. 3.4). Виділено *п'ять рівнів цифрової зрілості підприємства* для їх ідентифікації*:*

1. Початковий рівень (Initial / Ad-hoc). Базові цифрові інструменти підприємство використовує точково, без системності та без єдиної інфокомунікаційної інфраструктури. Дані зберігаються фрагментарно, інтеграції відсутні, кібербезпека має мінімальний рівень. Управлінські рішення приймаються інтуїтивно, без аналітичної підтримки. Цифрова трансформація не визначена як стратегічний напрям.

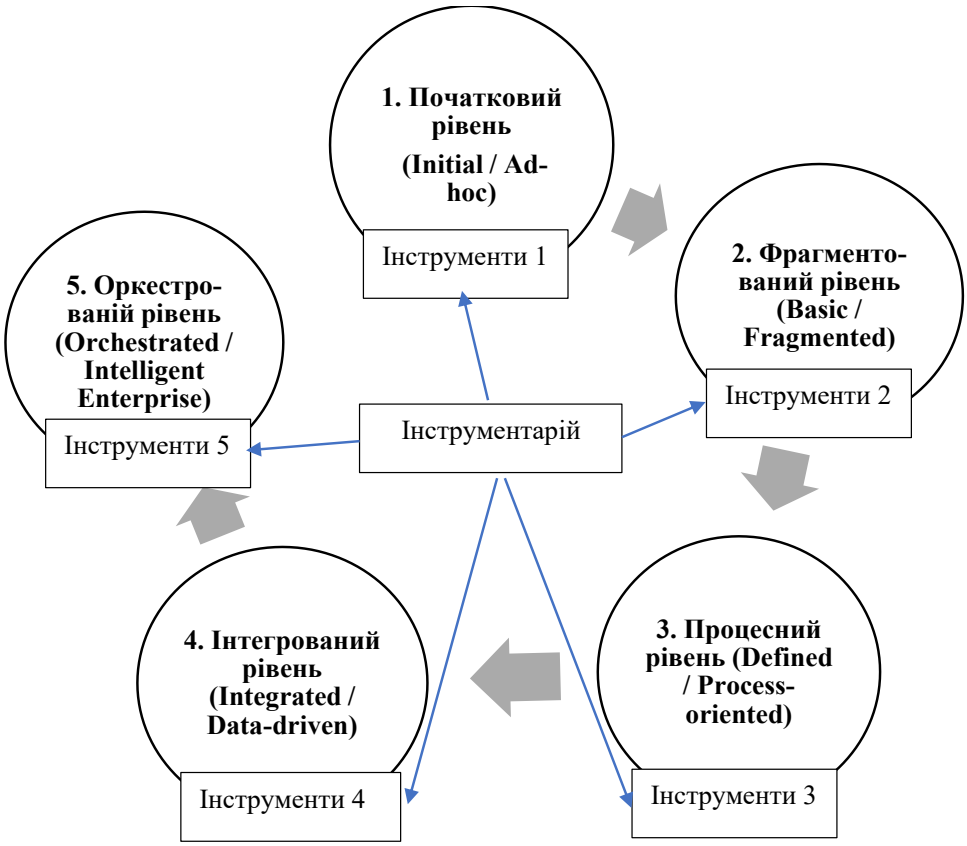


Рисунок 3.4 – Рівні цифрової зрілості підприємства (Digital Maturity Levels) *(джерело: розроблене автором з врахуванням підходів [161-165])*

2. Фрагментований рівень (Basic / Fragmented). Впроваджено окремі цифрові платформи (CRM, бухгалтерські системи, окремі хмарні сервіси), але вони не інтегровані між собою. Автоматизація часткова та стосується окремих завдань. Дані починають відігравати роль, але їх якість і доступність обмежені. Інфокомунікаційні процеси підтримують операційну діяльність, однак не впливають на стратегічні рішення.

3. Процесний рівень (Defined / Process-oriented). Цифрові інструменти інтегруються в ключові бізнес-процеси; з’являється стандартизована інфокомунікаційна інфраструктура. Дані уніфікуються та централізуються, використовуються аналітичні панелі та дашборди. Автоматизація процесів системна, RPA застосовується для повторюваних задач. Формується політика кіберзахисту та управління даними. Цифрова трансформація підтримує стратегічне планування.

4. Інтегрований рівень (Integrated / Data-driven). Цифрові платформи об’єднані в єдину екосистему, забезпечено API-взаємодію та наскрізні дані. Прийняття управлінських рішень базується на аналітичних моделях, прогнозній аналітиці та алгоритмах штучного інтелекту. Інфокомунікаційна система є стійкою, масштабованою та здатною підтримувати безперервність роботи навіть у кризах. Розвинена цифрова культура та управління змінами.

5. Оркестрованій рівень (Orchestrated / Intelligent Enterprise). Підприємство повністю управляється даними та алгоритмами, бізнес-процеси адаптивні, самооптимізовані та гнучкі. ШІ інтегровано в усі функціональні підсистеми (управління, планування, виробництво, логістика, комунікації). Цифрова інфраструктура є модульною, хмарною, високозахищеною і керованою у режимі реального часу. Забезпечується стратегічна стійкість, антикризова готовність та здатність до швидкої трансформації бізнес-моделі.

Узагальнюючи наведене, можна стверджувати, що удосконалення системи управління підприємства у сфері інфокомунікаційного цифрового забезпечення забезпечується інтеграцією комплексного підходу, який включає стратегічні, технологічні, архітектурні та оціночні інструменти. Саме така інтеграція дозволяє підприємству ефективно вирішити *чотири концептуально важливі завдання:*

а) визначення сутності, особливостей та потреби у фокусному цифровому інфокомунікаційному забезпеченні, а також побудова структурно-логічної моделі дозволяє чітко визначити, навіщо потрібне цифрове інфокомунікаційне забезпечення в кризових умовах, які саме його компоненти є критичними та як вони взаємодіють;

б) формулювання та обґрунтування принципів побудови інфокомунікаційної екосистеми підприємства дозволяють підприємству обґрунтувати правила, за якими має функціонувати сучасна інфокомунікаційна система як єдина екосистема;

в) завдяки розробленню архітектури та ключових елементів цифрового інфокомунікаційного забезпечення розвитку підприємства підприємство отримує чітку архітектурну модель цифрового розвитку;

г) визначення KPI розвитку цифрової інфраструктури підприємства дозволяє об'єктивно виміряти ефективність інфокомунікаційного розвитку та оцінити його прогрес.

Таким чином, розроблений комплекс стратегічних, архітектурних, методичних та оціночних інструментів забезпечує цілісне бачення цифрового інфокомунікаційного розвитку, створення екосистеми, побудову архітектури та визначення KPI, удосконалення систему управління підприємством.

3.2 Науково-методичні засади формування інфокомунікаційної цифрової стратегії підприємства з урахуванням кризових умов

Науково-методичні засади формування інфокомунікаційної цифрової стратегії підприємства з урахуванням кризових умов складають:

- стратегічні вектори цифрової трансформації;
- механізми антикризового управління на основі цифрових даних;
- пріоритети інвестування в інфокомунікаційні цифрові технології;
- проєктування інфокомунікаційної цифрової системи підприємства:

  а) фокусний вибір цифрових платформ і інструментів;

  б) побудова внутрішніх комунікацій та захисту даних;

  в) впровадження штучного інтелекту, аналітики та хмарних сервісів.

А. Стратегічні вектори цифрової трансформації. *Стратегічні вектори цифрової трансформації підприємства* формують комплексну рамку напрямів, у межах яких відбувається модернізація бізнес-моделі, операційної системи та інфокомунікаційної інфраструктури (рис. 3.5). Їхня системна реалізація забезпечує перехід підприємств до цифрової форми

функціонування, підвищення стійкості та здатності діяти в умовах високої турбулентності.

Рисунок 3.5 – Класифікація стратегічних векторів цифрової трансформації підприємства (*джерело: авторська розробка*)

Класифікація стратегічних векторів цифрової трансформації підприємства *(див. рис.3.5)* складається з *трьох великих блоків:*

а) *технологічні вектори,* сфокусовані на інфраструктурі, автоматизації, ШІ, хмарі, кіберзахисті та технологічній гнучкості;

б) *організаційно-управлінські вектори,* сфокусовані на інтеграції процесів, компетентностях персоналу та управлінні ризиками;

в) *комунікаційно-кооперацийні вектори,* сфокусовані на аналітиці даних, клієнтській взаємодії й партнерських цифрових мережах.

Технологічні вектори визначають базис цифрової трансформації, оскільки саме вони формують технічну готовність підприємства до змін. Хмаризація, гібридні інфраструктури, автоматизація, RPA, інтелектуальні системи штучного інтелекту та модульні архітектури дозволяють забезпечити масштабованість, гнучкість і стійкість у кризових умовах. Такі вектори

зменшують залежність від фізичної інфраструктури, що є критично важливим у періоди воєнних, енергетичних чи логістичних криз. Впровадження цифрових інновацій і нових бізнес-моделей посилює конкурентоспроможність підприємства та відкриває можливості для трансформаційного зростання.

Організаційно-управлінські вектори підкреслюють, що цифрова трансформація – це зміна управлінської логіки і внутрішньої побудови підприємства. Інтеграція бізнес-процесів у єдиний цифровий контур усуває інформаційні розриви й формує основу для «data-driven» управління. Розвиток цифрових компетентностей персоналу є передумовою успішності цифрових стратегій, адже навіть найсучасніші технології не дають ефекту без відповідних навичок і цифрової культури. Особливе значення мають інструменти цифрового управління ризиками та безперервністю діяльності, які дозволяють підприємствам функціонувати у непередбачуваних кризових ситуаціях, забезпечуючи стійкість та операційну безпеку.

Комунікаційно-кооперaційні вектори спрямовані на розширення інформаційної взаємодії підприємства із зовнішнім середовищем та формування єдиного цифрового простору. Аналітика даних і прогнозування дають змогу оцінювати ризики, моделювати сценарії розвитку та ухвалювати обґрунтовані стратегічні рішення. Розвиток цифрових каналів взаємодії з клієнтами та партнерами формує мережеві переваги, підвищує швидкість і якість сервісу, створює синергію в партнерських екосистемах та підсилює гнучкість бізнесу.

Наведені у табл.3.6 *десять стратегічних векторів цифрової трансформації* відображають цілісну логіку переходу підприємства до цифрової моделі діяльності: від модернізації технологічної інфраструктури та розвитку цифрових компетентностей до формування управлінської стійкості та інтеграції у цифрові ринки.

Рейтингування наведених у табл. 3.6 стратегічних векторів цифрової трансформації підприємств в умовах криз, виконане із залученням експертів

(додаток Б.4*)* дозволяє побудувати *матрицю пріоритетності стратегічних векторів цифрової трансформації підприємств* (рис.3.6).

Таблиця 3.6 – Розширений перелік стратегічних векторів цифрової трансформації підприємств в умовах криз (*джерело: авторська розробка*)

Стратегічний вектор	Опис стратегічного вектора	
	що передбачає	чим спричинено
1	2	3
1. Цифрова інтеграція бізнес-процесів	– побудову єдиного цифрового контуру; – синхронізацію даних і процесів; – наскрізну цифровізацію; – усунення інформаційних розривів;	– ускладненням операцій; – потребою швидких даних; – ризиками фрагментації IT-систем;
2. Хмаризація та гібридні інфраструктури	– перенесення даних у хмару; – змішану архітектуру (on-premise + cloud); – автоматичне резервування; – масштабування потужностей;	– зростанням вимог до стійкості; – дистанційною роботою; – збільшенням цифрових операцій;
3. Кіберстійкість та інформаційна безпека	– багаторівневий кіберзахист; – SOC, MFA, VPN; – реагування на інциденти; – резервування каналів зв’язку;	– збільшенням кібератак; – залежністю від цифрових технологій; – високою вартістю втрати даних;
4. Автоматизація та інтелектуалізація процесів	– роботизацію операцій (RPA); – ШІ, машинне навчання; – скорочення ручної праці; – прискорення виконання процесів;	– дефіцитом кадрів; – потребою у швидких рішеннях; – необхідністю зниження витрат;
5. Аналітика даних і прогнозування	– використання BI, дашбордів; – моделювання ризиків; – аналіз великих даних; – прогнозування сценаріїв;	– невизначеністю ринку; – зростанням ролі даних; – потребою адаптації до криз;
6. Цифрова взаємодія з	– омніканальні комунікації; – цифрові сервіси підтримки;	– зміною поведінки клієнтів;

Продовження таблиці 3.6

1	2	3
клієнтами та партнерами	автоматизацію зворотного зв’язку; – інтеграцію з партнерами;	поширенням онлайн-сервісів; – необхідністю швидкої реакції;
7. Розвиток цифрових компетентностей персоналу	– навчання ІТ-інструментам; – формування культури цифрової адаптивності; – підтримку команд цифрової стійкості; – підготовку до кризових режимів	– динамікою технологій; – нестачею цифрових фахівців; – людським фактором цифрових трансформацій;
8. Побудова стійких і модульних цифрових екосистем	– гнучкі ІТ-архітектури; – модульність систем; – інтеграцію з цифровими ринками; – підключення зовнішніх сервісів	– швидкими змінами середовища; – загрозами та збоями; – необхідністю швидкого відновлення
9. Цифрове управління ризиками та безперервністю діяльності	– цифрові карти ризиків; – автоматизоване оцінювання загроз; – цифрові системи резервування; – управління безперервністю (BCM)	– зростанням кризових явищ (війна, кібератаки, енергетичні збої); – потребою швидко відновлювати операції
10. Впровадження цифрових інновацій і нових бізнес-моделей	– використання платформних рішень; – впровадження цифрових продуктів; – перехід до data-driven бізнес-моделей; – експерименти з новими інструментами	– цифровою конкуренцією; – зміною ринкових правил; – появою нових технологій (AI, IoT, blockchain)

Як бачимо. експерти чітко виокремили перші три вектори як критично значущі для стійкості підприємства під час кризових ситуацій: кіберстійкість, управління ризиками та хмаризація. Ці напрями формують основу цифрового виживання й адаптації бізнесу. Натомість найнижчі пріоритети отримали вектори, пов’язані з інноваціями, крос-організаційною взаємодією та

компетентностями, що є типовим для кризових періодів, коли підприємства зосереджуються на оперативній стійкості, а не на стратегічному розвитку.

C **Стратегічні, але пізні** 7. Інновації	**B** **Висока цінність** 4. Екосистеми. 5. Автоматизація	**A** **Критичні вектори** 1. Кіберстійкість. 2. BCM. 3. Хмаризація.
F **Середньострокові**	**E** **Організаційний розвиток.** 8. Компетентності.	**D** **Оперативна підтримка.** 6. Цифрова взаємодія 7. Інтеграція.
I **Довгострокова цінність.** 7. Аналітика. 8. Взаємодія.	**H** **Другорядні процеси.**	**G** **Тактична підтримка**

Рисунок 3.6 – Матриця пріоритетності стратегічних векторів цифрової трансформації підприємств *(джерело: авторська розробка)*

На основі узагальнених експертних оцінок пропонується застосовувати *контурну карту пріоритетів відображає розподіл значущості стратегічних векторів цифрової трансформації підприємства в умовах криз (див.додаток Б.4)*. На ній чітко простежується *градієнт зміни пріоритетів:* від низьких значень у зоні інновацій, взаємодії та розвитку компетентностей до високих пріоритетів, що концентруються у напрямках кіберстійкості, управління ризиками та безперервністю діяльності, а також інтеграції ключових цифрових процесів. Лінії рівнів, розташовані діагонально, демонструють логіку зростання важливості – від довгострокових, менш критичних напрямів до векторів, що забезпечують оперативну стійкість і безпеку підприємства під час кризових подій. *Побудовна контурна карта* дозволяє легко інтерпретувати відносну вагу кожного вектора та *підтверджує концентрованість експертного фокусу на базових елементах цифрової стійкості підприємства.*

Таким чином, експертне оцінювання формує чітку структуру пріоритетів цифрової трансформації, що дає можливість об’єктивно обґрунтувати напрями розвитку підприємства в умовах нестабільності та високої турбулентності.

Б. Механізми антикризового управління на основі цифрових даних. Ці механізми охоплюють *комплекс інструментів, що забезпечують своєчасне виявлення загроз, оперативне прийняття рішень та підтримання стійкості підприємства в умовах кризових ситуацій*. До них належать:

- системи моніторингу в реальному часі, які дозволяють відслідковувати ключові показники діяльності та зовнішні ризики;
- аналітичні платформи та алгоритми прогнозування, що формують сценарії розвитку подій та оцінюють потенційні наслідки;
- модулі цифрового управління ризиками (ERM/BCM), які забезпечують стійкість основних процесів, автоматизують процедури реагування;
- інструменти штучного інтелекту та машинного навчання, здатні виявляти приховані закономірності, аномалії та ранні сигнали криз;
- системи підтримки управлінських рішень (DSS), що інтегрують багатовимірні дані у зручні дашборди;
- цифрові канали координації та комунікації для швидкої взаємодії між підрозділами;
- хмарні середовища, які забезпечують доступність даних і функціонування бізнес-процесів за будь-яких умов;
- інструменти кіберзахисту, що запобігають порушенню цілісності цифрових ресурсів; а також модулі автоматизованого документообігу, які зменшують залежність від фізичних ресурсів.

Кожний механізм антикризового управління на основі цифрових даних оцінено *за трьома критеріями:* мета застосування, обмеження, здатність врахувати технологічні (Т), організаційно-управлінські (ОУ), комунікативно-кооперaційні (КК) вектори трансформації (табл.3.7).

Таблиця 3.7 – Механізми антикризового управління на основі цифрових даних (*джерело: авторська розробка з врахуванням [164-167])*

Механізм	Характеристика механізму				
	Мета застосування	Обмеження	Врахування векторів трансформації		
			Т	ОУ	КК
1	2	3	4	5	6
1. Системи моніторингу в реальному часі (Real-time Monitoring)	Виявлення відхилень і критичних змін у бізнес-процесах під час кризи	Висока залежність від якості даних і стабільності IT-інфраструктури	В	С	Н
2. Аналітичні платформи та прогнозування (Predictive Analytics)	Формування сценаріїв розвитку ризиків, оцінка наслідків і ймовірностей	Потреба у великих масивах історичних даних, значні ресурси обчислення	В	В	С
3. Цифрове управління ризиками (ERM/BCM)	Автоматизація процедур реагування, забезпечення безперервності діяльності	Складність інтеграції в існуючі процеси, потреба у налаштуванні	В	ДВ	С
4. Алгоритми ШІ та машинного навчання	Виявлення аномалій, ранніх сигналів криз, оптимізація рішень	Чутливість до зміни середовища, необхідність кваліфікованих фахівців	ДВ	С	Н
5. Системи підтримки управлінських рішень (DSS)	Інтеграція даних у зрозумілі дашборди для управлінців	Необхідність коректного налаштування KPI та джерел даних	В	В	С
6. Цифрові канали координації та комунікації	Швидка взаємодія підрозділів у кризових умовах	Перевантаження інформацією, кіберризики	С	С	ДВ
7. Хмарні середовища та віддалений доступ (Cloud)	Забезпечення доступності даних і сервісів у будь-яких умовах	Залежність від постачальника, інтернет-каналу та кіберзагроз	ДВ	С	С

Продовження таблиці 3.7

1	2	3	4	5	6
1. Інструменти кіберзахисту (Cybersecurity Stack)	Захист даних і процесів від атак, забезпечення цифрової цілісності	Висока вартість, потреба у постійному оновленні	ДВ	С	Н
2. Автоматизо-ваний документообіг	Зменшення залежності від фізичної інфраструктури, прискорення обігу інформації	Складність переходу із паперових процедур, супротив персоналу	С	В	С
3. Інтеграційні платформи (ESB/API)	Забезпечення узгодженості потоків даних між системами	Висока складність розгортання та підтримки	В	В	С
**Опис відповідності: ДВ – дуже висока, В – висока, С – середня, Н – низька.*					

Запропоновані механізми антикризового управління на основі цифрових даних *(див. табл.3.7)* грають різну роль у забезпеченні готовності, реагування та відновлення в умовах кризових ситуацій. Кожен механізм виконує окрему функцію з підтримки життєздатності підприємства, проте їхня ефективність суттєво залежить від характеру кризи, ступеня цифрової зрілості його організації та інтегрованості механізмів між собою:

– системи моніторингу та прогнозної аналітики утворюють фундамент раннього виявлення загроз і прийняття рішень, оскільки дозволяють підприємству оперативно виявляти аномалії, аналізувати динаміку ризиків і формувати сценарії реагування. Вони мають високу відповідність технологічним вимогам, проте їхня ефективність обмежується якістю даних та стабільністю інфраструктури, що робить їх критично важливими на етапі підготовки до кризи;

– механізми управління ризиками та безперервністю діяльності (ERM/BCM) є ядром організаційно-управлінського реагування у кризовий період. Вони забезпечують структурованість дій, автоматизацію процедур перемикання на резервні процеси та збереження керованості системи навіть за

умов руйнування частини операційної інфраструктури. Їхня адаптивність і інтеграційний характер дозволяють поєднати технологічні ресурси з управлінськими компетенціями та координаційними процесами;

– інструменти ШІ та машинного навчання підсилюють аналітичну складову антикризового управління, забезпечуючи виявлення прихованих патернів та ранніх ознак ескалації загроз. Водночас вони мають обмеження, пов’язані з чутливістю до змін у зовнішньому середовищі, та потребують значної кваліфікації персоналу. Це робить їх перспективними, але не універсальними механізмами швидкого реагування;

– системи підтримки управлінських рішень (DSS) та цифрові канали комунікації відіграють ключову роль у забезпеченні оперативності управління. DSS дозволяють консолідувати багатовимірні дані в одне інформаційне поле, забезпечуючи прозорість ситуації для менеджерів. Цифрові канали комунікації забезпечують взаємодію між підрозділами, що важливо для коопераційної координації під час кризових сценаріїв. Обмеження пов’язані головним чином з інформаційним перевантаженням і необхідністю уніфікації комунікаційних протоколів;

– хмарні сервіси та інструменти кіберзахисту створюють інфраструктурну основу цифрової стійкості. Хмарні платформи забезпечують відмовостійкість і доступність ресурсів за будь-яких умов, а кіберзахист гарантує безпеку цифрових активів, мінімізуючи ризик порушення даних. Однак їхня ефективність залежить від зрілості корпоративних політик безпеки та якості інтеграції з іншими IT-компонентами;

– автоматизований документообіг і інтеграційні платформи сприяють операційній оптимізації та забезпечують цілісність потоків даних у межах підприємства. Вони мають високу організаційно-управлінську цінність, але потребують чіткої формалізації процесів і гнучкості персоналу до змін.

Комплекс цифрових механізмів антикризового управління забезпечує високу ефективність у кризових умовах, проте одночасно генерує

багатовимірний ризиковий профіль, який необхідно враховувати при формуванні цифрової стратегії (рис.3.7).

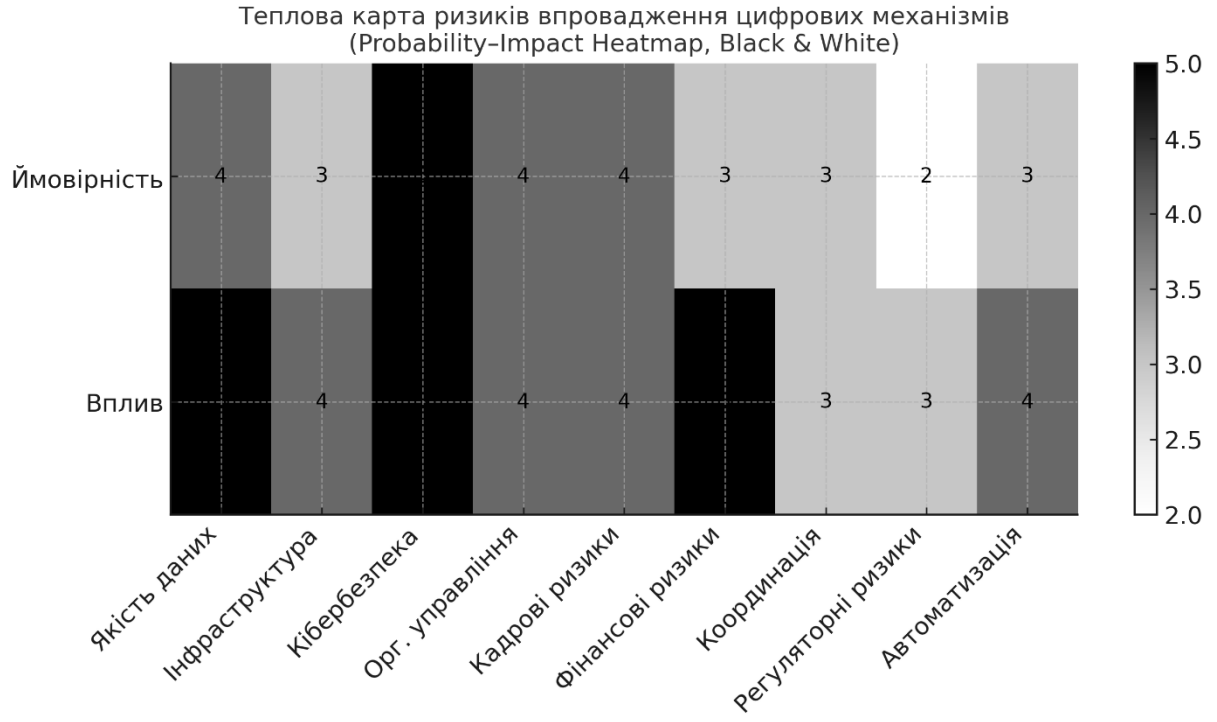


Рисунок 3.7 – Ризиковий профіль цифрових механізмів антикризового управління: теплова карта *(джерело: авторська розробка)*

Основними зонами ризику, як видно з рис. 3.7, є: дані, інфраструктура, кібербезпека, кадрові компетентності, координація та регуляторні обмеження. Їх ігнорування може істотно знизити результативність цифрової трансформації та збільшити операційні втрати підприємства під час кризи. Тому впровадження цифрових механізмів має супроводжуватися системним аудитом ризиків та створенням інтегрованих моделей цифрової стійкості.

Враховуючи наведені міркування, розроблено *рекомендації щодо застосування запропонованих механізмів* (табл.3.8).

Як бачимо, у *різних фазах кризи домінують різні механізми*:

– до кризи – заходи з підготовки. Це: побудова моделей, налаштування інфраструктури, тестування резервних сценаріїв та формування цифрових стандартів;

– під час кризи – акцент зміщується на забезпечення оперативності, безперервності діяльності та швидкого реагування. Найбільш критичними є BCM, кіберзахист, DSS та моніторинг;

– після кризи – механізми переходять у фазу аналітики та оптимізації, що дозволяє врахувати досвід пережитих інцидентів і підсилити цифрову готовність до майбутніх загроз.

Таблиця 3.8 – Рекомендації щодо застосування механізмів антикризового управління на основі цифрових даних у різні фази кризи *(джерело: авторська розробка)*

Механізм антикризового управління	Фази кризи		
	До кризи (pre-crisis)	Під час кризи (crisis response)	Після кризи (post-crisis)
1	2	3	4
1. Системи моніторингу в реальному часі	Налаштувати ключові показники (KRI), створити дашборди та канали сповіщень	Використовувати для фіксації аномалій, швидкого інцидент-менеджменту	Аналізувати збої, оновлювати алгоритми та сценарії сповіщень
2. Аналітика та прогнозування ризиків	Побудувати моделі прогнозування сценаріїв; зібрати історичні дані	Використовувати моделі для передбачення ескалацій, управління ресурсами	Перекалібрувати моделі на основі фактичних подій, інтегрувати нові дані
3. ERM/BCM – управління ризиками та безперервністю діяльності	Розробити плани безперервності, протестувати резервні сценарії	Активувати процедури BCM, виконувати перемикання на резервні процеси	Переглянути політику BCM, оновити ризик-реєстри, посилити протоколи
4. Штучний інтелект та ML	Створити моделі виявлення аномалій, підготувати навчальні вибірки	Застосовувати для розпізнавання кризових патернів у потоках даних	Донавчити моделі на реальних кейсах кризи та оптимізувати

Продовження таблиці 3.8

1	2	3	4
5. Системи підтримки управлінських рішень (DSS)	Налаштувати KPI, інтегрувати внутрішні джерела даних	Використовувати DSS для швидкого ухвалення рішень під тиском часу	Розширити систему новими показниками, інтегрувати досвід кризи
6. Цифрові канали координації та комунікації	Стандартизувати канали, провести навчання персоналу	Забезпечити швидку взаємодію підрозділів, розсилки рішень і наказів	Аналізувати ефективність, оптимізувати канали та комунікаційні протоколи
7. Хмарні сервіси та віддалений доступ	Впровадити гібридну інфраструктуру, налаштувати резервування	Забезпечити доступність даних та сервісів незалежно від локації	Перевірити відмовостійкість, розширити хмарні компоненти
8. Інструменти кіберзахисту	Провести аудит безпеки, налаштувати багаторівневий захист	Відстежувати атаки, виконувати ізоляцію інцидентів, застосовувати SOC	Провести розслідування інцидентів, посилити політику кібербезпеки
9. Автоматизований документообіг	Оцифрувати документообіг, забезпечити доступність	Застосовувати для прискорення інформаційних потоків у кризу	Аналізувати затримки, оптимізувати маршрути та інтеграції
10. Інтеграційні платформи (API/ESB)	Побудувати цифрові зв’язки між ключовими системами	Забезпечити синхронізацію потоків даних під час турбулентності	Оптимізувати маршрути, впровадити нові інтеграційні сценарії

Відтак, запропоновані механізми формують багаторівневу систему цифрової готовності підприємства до кризових станів, яка забезпечує одночасне покриття технологічних, організаційно-управлінських і комунікативно-кооперaційних векторів трансформації, що робить модель антикризового управління цілісною та адаптивною до різних типів загроз.

В. Пріоритети інвестування в інфокомунікаційні цифрові технології. При виборі пріоритетів інвестування в інфокомунікаційні цифрові технології підприємству *потрібно врахувати такі чинники:*

- рівень доступного капіталу та очікуваний ROI: дешевші й швидкоокупні рішення доцільні для малого бізнесу; дорогі трансформаційні технології – для великих корпорацій;
- поточний рівень цифрової зрілості: інвестиції мають нарощувати ефект поетапно: дані → хмарні сервіси → автоматизація → AI;
- стратегічні цілі розвитку: чи орієнтоване підприємство на зниження витрат, масштабування, створення нових бізнес-моделей;
- ризики кібербезпеки: рівень інвестицій у захист має відповідати масштабам цифровізації;
- кваліфікацію персоналу: навіть найкращі технології не дають ефекту без підготовлених кадрів;
- інфраструктурну готовність: наявність даних, мереж, інтегрованих систем, сумісності з майбутніми рішеннями.

Узагальнювальна матриця пріоритетів інвестування в інфокомунікаційні цифрові технології пропонуються у такому вигляді (табл.3.9):

Таблиця 3.9 – Узагальнювальна матриця пріоритетів інвестування в інфокомунікаційні цифрові технології *(джерело: авторська розробка)*

Рівень капіталу	Основна мета	Пріоритетні технології	Орієнтовний ROI	Горизонт окупності
1. Низький	Швидка окупність	SaaS, RPA, BI, e-commerce	20–60%	1–2 роки
2. Середній	Підвищення ефективності	ERP, IoT, хмара, кібербезпека	30–80%	2–4 роки
3. Високий	Стратегічна трансформація	AI, Digital Twin, Industry 4.0	50–120%	3–7 років

Як бачимо, саме залежність від вказаних вище чинників створює обмеження інвестування та вимоги до цифрових характеристик підприємства.

Типологія пріоритетів інвестування в цифрові технології за рівнем капіталу та окупністю розроблена на підставі узагальнення даних джерел [165-168] представлена у табл.3.10-3.12.

Таблиця 3.10 – Пріоритети інвестування в цифрові технології при низькому рівні доступного капіталу *(джерело: авторська розробка)*

Капітал / ROI /окупність	Стратегічний пріоритет	Ключові напрями інвестування	Тип підприємств
до $0,5 млн на цифрові-зацію / ROI 20–60% за 1–2 роки	швидкоокупні цифрові рішення з мінімальними капітальними витратами (CAPEX) та швидким ефектом.	– хмарні сервіси (SaaS): економія операційних витрат (OPEX) 15–35%; – цифрові канали продажів і маркетингу: приріст виручки 10–25%; – RPA (роботизація бізнес-процесів): скорочення витрат 20–50%; – аналітика даних (BI): зростання продуктивності управлінських рішень 10–30%.	МСП, торговельні компанії, логістичні оператори, сервісні компанії.

Таблиця 3.11 – Пріоритети інвестування в цифрові технології при середньому рівні доступного капіталу *(джерело: авторська розробка)*

Капітал / ROI /окупність	Стратегічний пріоритет	Ключові напрями інвестування	Тип підприємств
$0,5–5 млн / ROI 30–80% за 2–4 роки	підвищення операційної ефективності та масштабу-вання бізнес-процесів	– ERP/CRM інтегровані системи управління: зростання узгодженості процесів 25–40%; – IoT та сенсорика виробництва / логістики: зниження простоїв 15–30%. – кібербезпека середнього рівня (Zero Trust, SOC-lite): зменшення збитків від інцидентів 40–70%; – хмарні інфраструктури (IaaS / PaaS): економія капітальних витрат до 50%.	Промисловість, дистрибуція, логістика, енергетика, агробізнес.

Таблиця 3.12 – Пріоритети інвестування в цифрові технології при високому рівні доступного капіталу *(джерело: авторська розробка)*

Капітал / ROI /окупність	Стратегічний пріоритет	Ключові напрями інвестування	Тип підприємств
5–50+ млн / ROI 50–120% за 3–7 років	інноваційні та трансформаційні рішення, що формують довгострокову конкурентоспро- можність	– штучний інтелект (Advanced ML, Generative AI): вплив на прибутковість: скорочення витрат / збільшення доходів 20–45%; – цифрові двійники виробництв і складних об'єктів: зменшення аварійності 40–60%; – повна автоматизація та роботизація (Industry 4.0): підвищення продуктивності 30–70%; – кібербезпека високого рівня (SOC 24/7, SIEM/XDR): зменшення стратегічних ризиків 70–90%; – Big Data платформи та власні дата-центри: прискорення прийняття рішень у 5–10 разів.	Інфраструк-турні компанії, порти, банки, великі корпорації, мегапроєкти.

Розмір підприємства є також важливим чинником вибору пріоритетів інвестування в інфокомунікаційні цифрові технології (табл.3.13), оскільки впливає на інфраструктурну готовність, стартегічні цілі, цифрову зрілість підприємства, а головне – на доступний підприємству капітал.

Аналіз пріоритетів інвестування в інфокомунікаційні цифрові технології *(див. табл.3.10-3.13)* показує, що ефективність цифровізації підприємств безпосередньо залежить від обсягу доступного капіталу, рівня технологічної зрілості та стратегічних цілей бізнесу. Малий бізнес забезпечує найшвидшу окупність інвестицій за рахунок впровадження маловитратних, але високопродуктивних рішень (SaaS, RPA, BI). Середні підприємства досягають максимального ефекту через інтеграцію ERP/CRM, IoT та хмарної

інфраструктури, що скорочує операційні втрати, підвищує узгодженість процесів. Великі корпорації демонструють найбільший стратегічний результат, коли інвестиції спрямовані у трансформаційні технології (цифрові двійники, AI, повну автоматизацію, кіберзахист високого рівня).

Таблиця 3.13 – Узагальнювальна матриця пріоритетів інвестування в інфокомунікаційні цифрові технології за ознакою розміру підприємства *(джерело: авторська розробка)*

Розмір підприємства	Обсяг доступного капіталу	Типові напрями інвестування	Очікуваний економічний ефект / ROI	Приклади ІКТ-рішень
1	2	3	4	5
1. Малі (МСП)	До 0,5 млн дол.	- Хмарні сервіси (SaaS); - RPA у бек-офісних процесах; - цифрові канали продажів; - BI-аналітика;	ROI 20–60% за 1–2 роки. Економія OPEX 15–35%. Зростання виручки 10–25%	CRM SaaS, e-commerce, чат-боти, Power BI, RPA UiPath.
2. Середні	0,5–5 млн дол.	- ERP/CRM-системи; - IoTмоніторинг; - Кібербезпека середнього рівня Zero Trust; - Хмарні інфраструктури (IaaS/PaaS);	ROI 30–80% за 2–4 роки . Зниження простоїв 15–30% . Економія CAPEX до 50%.	SAP/Oracle ERP, IoT-сенсори, SOC-lite, Azure/AWS PaaS.
3. Великі та корпорації	5–50+ млн дол.	- штучний інтелект (Advanced/ Generative AI); - цифрові двійники виробничих систем; - повна автоматизація (Industry 4.0);	ROI 50–120% за 3–7 років. Зростання продуктивності 30–70%. Зменшення аварійності 40–60%. Прискорення прийняття	Generative AI, AI-навантаження у DC, цифрові двійники, роботизовані лінії, SIEM/XDR.

Продовження таблиці 3.13

1	2	3	4	5
		- кібербезпека високого рівня (SOC 24/7); - Big Data, власні дата-центри.	рішень у 5–10 разів.	

Враховуючи наведене, *основні рекомандації з вибору пріоритетів інвестування в інфокомунікаційні цифрові технології для підприємств* такі:

– встановити відповідність між масштабом бізнесу та допустимим рівнем цифрових інвестицій, концентруючись на технологіях з найвищим ROI у відповідній групі;

– розвивати цифрову інфраструктуру поетапно, починаючи з базових рішень (дані, аналітика, хмара), а потім переходити до складних технологій (AI, цифрові двійники);

– оптимізувати витрати через хмарні моделі (SaaS/IaaS), що дозволяє різко скоротити CAPEX та підвищити гнучкість ресурсів;

– інвестувати у кібербезпеку пропорційно до масштабу цифрового середовища, оскільки ризики зростають разом з рівнем цифровізації;

– забезпечити підготовку кадрів та розвиток цифрових компетенцій, оскільки людський фактор є ключовим для отримання економічного ефекту від технологій;

– використовувати аналітику даних для обґрунтування рішень щодо інвестування, переводячи цифрову трансформацію зі сфери витрат у сферу стратегічних інвестицій.

Водночас, не завжди доцільно інвестувати у власні розробки, у певних випадках слід готові рішення. Зокрема *власні розробки доцільні*, коли:

а) потрібна унікальна конкурентна перевага, яку неможливо купити;

б) існують високі вимоги до безпеки та локалізації даних;

в) підприємство має значний капітал, R&D-команду й довгостроковий горизонт окупності;

г) необхідна глибока інтеграція з внутрішніми процесами, яких не покривають ринкові продукти.

Готові (ринкові) рішення доцільно залучати, коли:

а) важлива швидкість впровадження та швидка окупність;

б) існують перевірені технології (SaaS, ERP, CRM, IoT), які вже показали ефективність;

в) підприємство має обмежений бюджет;

г) немає потреби у кастомізації понад 30%;

д) важливо зменшити ризики та витрати на підтримку.

Відтак, підприємство має обирати пріоритети інвестування в інфокомунікаційні цифрові технології, виходячи з їх стратегічної значущості, економічної доцільності, швидкості отримання ефекту: власні розробки варто створювати для довгострокових конкурентних переваг і унікальності, а готові рішення доцільно залучати для швидкої цифровізації та оптимізації витрат.

Г. Проєктування інфокомунікаційної цифрової системи підприємства. Інфокомунікаційна система повинна не лише підтримувати основні інформаційні потоки, а й забезпечувати їхню безпеку, відмовостійкість та включати інтелектуальні компоненти, здатні виявляти та попереджати ризики в реальному часі. З огляду на це, проєктування такої системи доцільно здійснювати *на основі цілісного алгоритму, який охоплює послідовність технічних, організаційних та комунікаційних рішень (рис.3.8)*. Як бачимо, проєктування інфокомунікаційної системи підприємства передбачає багатоступеневий процес, у якому поєднуються технологічні, організаційні та ризик-орієнтовані підходи. Алгоритм охоплює повний життєвий цикл створення системи за кількома етапами.

Першим етапом формування інфокомунікаційної системи є ґрунтовна діагностика потреб підприємства, яка передбачає оцінювання стратегічних цілей, ступеня цифрової зрілості та ключових характеристик бізнес-процесів. На етапі здійснюється аудит існуючих інформаційних потоків, визначаються їхні слабкі місця, рівень автоматизації, критичні вузли та залежності від

зовнішніх систем. Особливу увагу приділяється якості наявних даних, структурам їх зберігання та доступності для подальшої аналітики. Результат фази – формування вимог до інфокомунікаційної системи, включаючи функціональні характеристики, вимоги до безпеки, інтеграційні можливості та критерії масштабованості.

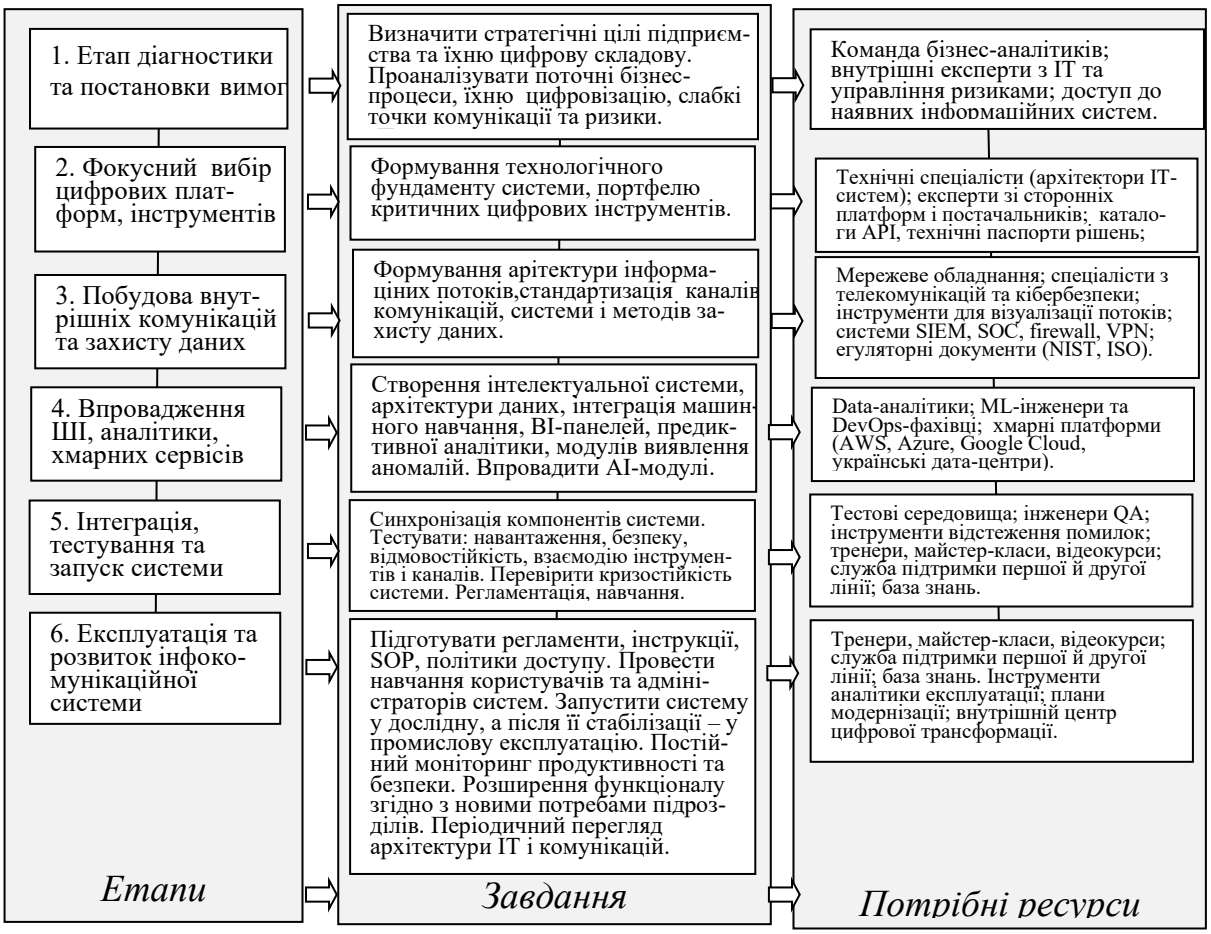


Рисунок 3.8 – Алгоритм проєктування інфокомунікаційної системи підприємства *(джерело: авторська розробка)*

Другий етап – формування технологічного фундаменту системи – починається з вибору цифрових платформ, які забезпечуватимуть управління процесами, комунікаціями та інформаційними ресурсами. Фокус етапу – визначення рішень, найбільш релевантних бізнес-моделі підприємства, його операційній структурі та рівню цифрової готовності. До базових елементів платформенного вибору належать ERP-системи для управління ресурсами,

CRM-продукти для підтримки маркетингової та клієнтської діяльності, BPM-платформи для моделювання і оптимізації процесів, DMS/ECM-рішення для організації документообігу, а також спеціалізовані модулі DSS для підтримки управлінських рішень. Важливо, щоб обрані інструменти мали відкриту архітектуру, підтримували API-взаємодію та забезпечували високу модульність і масштабованість. Формується *портфель критичних цифрових інструментів*: систем моніторингу, корпоративних месенджерів, платформ відеозв'язку, модулів кіберзахисту для побудови безпечної та гнучкої інфокомунікаційної інфраструктури підприємства.

Третій етап – проєктування внутрішньої комунікаційної системи, яка визначає архітектуру інформаційних потоків між підрозділами підприємства. Створюються регламенти взаємодії, встановлюються маршрути передачі даних, визначаються відповідальні ролі та рівні доступу. Важливо забезпечити узгодженість каналів комунікації від корпоративних месенджерів і електронної пошти до внутрішніх порталів та систем сповіщень. Паралельно формується система захисту даних, що включає аудит інформаційних активів, класифікацію даних за рівнями критичності, визначення політик доступу та впровадження технологічних рішень (шифрування, багатофакторної автентифікації, засобів DLP, систем SIEM/SOC, інструментів захисту хмарних сервісів). Цей етап є ключовим у формуванні інфокомунікаційної стійкості підприємства, оскільки саме безпека та надійність комунікацій визначають готовність організації протистояти кібератакам, збереженню критичних активів та підтримці безперервності діяльності. Для цього потрібно мережеве обладнання; спеціалісти з телекомунікацій та кібербезпеки; інструменти для візуалізації потоків (BPMN, ArchiMate); системи SIEM, SOC, firewall, VPN; регуляторні документи (NIST, ISO 27001, GDPR-подібні норми).

Четвертий етап – впровадження штучного інтелекту, аналітики та хмарних сервісів. Система отримує інтелектуальні можливості та здатність прогнозувати ризики й оптимізувати рішення. Впровадження ШІ та аналітики передбачає інтеграцію алгоритмів машинного навчання, BI-панелей,

предиктивної аналітики та модулів виявлення аномалій. Створюється сучасна архітектура даних (Data Lake або Data Warehouse), яка дозволяє підприємству опрацьовувати великі масиви структурованої та неструктурованої інформації. Хмарні сервіси забезпечують відмовостійкість, мобільність, масштабованість інфокомунікаційної системи. Використання гібридних або повністю хмарних моделей дозволяє підприємству підтримувати діяльність у кризових умовах, забезпечуючи доступ до ресурсів незалежно від фізичної локації.

П'ятий етап – інтеграція, тестування та запуск системи. Після побудови всіх функціональних модулів відбувається інтеграція платформи в єдиний цифровий контур підприємства. Проводиться тестування на сумісність, навантаження, відмовостійкість, кіберзахист та відповідність регламентам. Особливе значення має моделювання кризових ситуацій, що дає змогу оцінити готовність системи до аномальних сценаріїв. Запуск системи супроводжується навчанням персоналу, створенням інструкцій, SOP, бази знань, а також формуванням служби підтримки. Це забезпечує плавне впровадження і зменшує операційні ризики.

Шостий етап – експлуатація та розвиток інфокомунікаційної системи. Етап передбачає регулярний моніторинг продуктивності, оновлення модулів безпеки, адаптацію аналітичних моделей та інноваційне розширення функцій системи. Підприємство формує внутрішній центр цифрової трансформації, який відповідає за підтримку актуальності інфокомунікаційної архітектури та її стійкість у довгостроковому періоді.

Відтак, запропонований алгоритм забезпечує поетапну побудову інфокомунікаційної системи, у якій фокусний вибір цифрових платформ, побудова безпечних каналів комунікації та впровадження інтелектуальних технологій створюють системне інтегроване інформаційне середовище, здатне підтримувати розвиток підприємства навіть у високотурбулентних умовах:

- платформи і сервіси (етап а) формують технологічний фундамент;
- комунікації та безпека (етап б) гарантують безперервність взаємодії й захищеність даних;

– AI, аналітика та хмари (етап в) створюють інтелектуальну надбудову та забезпечують стійкість у кризах.

Такий підхід забезпечує підприємству здатність адаптуватися до змін зовнішнього середовища, знижувати ризики та підтримувати стратегічну керованість завдяки цифровим ресурсам. Розроблений алгоритм втілює системний підхід до проєктування інфокомунікаційної системи підприємства, враховуючи і технічні, і управлінські вимоги, забезпечує її стійкість до криз.

3.3 Інструменти та рекомендації щодо оцінювання інфокомунікаційних цифрових рішень підприємства

Розробка інструментів та рекомендацій щодо оцінювання інфокомунікаційних цифрових рішень підприємства включає:

а) опис та аргументація складу обраних інструментів;

б) добір інструментів, застосовних для формування організаційних ефектів (скорочення часу, автоматизація, безпека) та антикризових ефектів (стійкість, безперервність, адаптивність);

в) розробка рекомендацій щодо оцінювання цифрових ресурсів підприємства: політика оцінювання цифрових ресурсів; механізми моніторингу й методика оцінювання інфокомунікаційних цифрових рішень; підвищення відповідних компетентностей персоналу.

А. Опис та аргументація складу обраних інструментів. *Інструменти оцінювання інфокомунікаційних цифрових рішень підприємства у загальному сенсі* – це методи, показники та аналітичні підходи, що дозволяють виміряти економічну, організаційну та стратегічну ефективність цифрових технологій, які впроваджує підприємство. По суті вони складають комплекс фінансових, організаційних, стратегічних, технологічних і клієнтських методів, які

дозволяють визначити ефективність, доцільність та вплив цифровізації на розвиток підприємства відповідними методиками та показниками.

Вичерпний перелік основних інструментів оцінювання інфокомунікаційних цифрових рішень підприємства, структурований за групами, наделено у табл.3.14.

Таблиця 3.14 – Інструменти оцінювання інфокомунікаційних цифрових рішень підприємства *(джерело: розроблене автором на підставі [160-163])*

Група інструментів	Зміст та характеристики інструменту	Ціль оцінювання / Результат для підприємства
1	2	3
1. Економічні інструменти	ROI – визначає окупність інвестицій; NPV – відображає теперішню вартість майбутніх потоків; IRR – оцінює рентабельність; Cost–Benefit – співставляє витрати і вигоди; TCO – повна вартість володіння; Payback Period – строк окупності.	Дозволяють оцінити економічну доцільність цифрових рішень, розрахувати фінансовий ефект, визначити пріоритетність інвестицій.
2. Організаційні інструменти	KPI бізнес-процесів; рівень автоматизації; показники продуктивності персоналу; SLA/OLA; оцінка безпеки та рівня цифрової зрілості процесів; якість та доступність даних.	Оцінюють вплив цифровізації на ефективність операцій, продуктивність працівників, швидкість і безпечність виконання процесів.
3. Антикризові та стратегічні інструменти	Business Continuity Metrics; Resilience Index; оцінка адаптивності бізнес-моделі; аудит кіберстійкості (ISO 27001, NIST); рівень вразливості цифрової інфраструктури.	Дозволяють визначити стійкість підприємства до криз, готовність працювати в умовах невизначеності, здатність швидко відновлюватися та адаптуватися.
4. Технологічні інструменти оцінювання	Моделі цифрової зрілості (Gartner, Deloitte, McKinsey); ITIL 4 Metrics; оцінка масштабованості і сумісності	Дають змогу оцінити технологічну готовність, якість IT-інфраструктури, її продуктивність та

Продовження таблиці 3.14

1	2	3
	ІКТ-рішень; технічний аудит (performance audit).	потенціал масштабування.
5. Інструменти оцінювання клієнтського впливу	NPS, CES, CSAT; аналіз конверсій у цифрових каналах; показники задоволеності та взаємодії клієнтів із цифровими сервісами.	Вимірюють вплив цифрових рішень на клієнтський досвід, попит, лояльність, ефективність цифрових сервісів і збутових каналів.

Якщо стисло узагальнити призначення наведений комплекс інструментів, то можна зробити узагальнення, що:

а) економічні інструменти оцінювання спрямовані на визначення фінансової доцільності цифрових інвестицій;

б) організаційні інструменти оцінювання показують зміну продуктивності, ефективності та якості операцій внаслідок організаційних дій;

в) антикризові та стратегічні інструменти оцінюють готовність підприємства працювати в умовах змін і криз;

г) технологічні інструменти оцінювання показують зрілість і готовність цифрової інфраструктури;

д) інструменти оцінювання впливу на клієнтів і ринок важливі для підприємств, що цифровізують сервіси або продажі.

Аргументація вибору інструментів оцінювання інфокомунікаційних цифрових рішень підприємства полягає у такому. Ефективне оцінювання інфокомунікаційних цифрових рішень підприємства потребує застосування комплексного інструментарію, який дозволяє визначити рівень технологічної готовності, економічну доцільність та управлінську результативність впроваджених рішень. До таких інструментів належать ROI та інші показники економічної ефективності, моделі цифрової зрілості, аудит інформаційної інфраструктури, аналіз ризиків та кіберстійкості, методи оцінювання якості даних та інформаційних потоків. Застосування кожного з них зумовлене вимогами цифрової трансформації, потребою у забезпечення сталих

комунікаційних процесів у діяльності підприємства, підвищенні рівня його конкурентоспроможності. Підтримка вибору вказаних інструментів ґрунтується на *таких ключових аргументах*:

а) комплексність охоплення: інструменти дозволяють оцінити цифрові рішення з економічної, технологічної та управлінської точки зору, забезпечуючи багатовимірний аналіз;

б) об'єктивність та вимірюваність результатів: використання стандартизованих метрик (ROI, TCO, моделі цифрової зрілості) гарантує порівнянність і достовірність оцінювання;

в) підтримка стратегічного управління: результати оцінювання формують інформаційну основу для прийняття рішень щодо інвестицій, модернізації ІКТ-інфраструктури та пріоритезації цифрових проєктів;

г) підвищення кіберстійкості підприємства: включення інструментів аналізу ризиків та інформаційної безпеки дає змогу ідентифікувати вразливості та запобігати критичним інцидентам;

д) оцінювання впливу на ефективність бізнес-процесів – інструменти дають можливість визначити, наскільки цифрові рішення оптимізують комунікаційні, виробничі та управлінські процеси підприємства.

Таким чином, обраний інструментарій забезпечує всебічне, науково обґрунтоване оцінювання інфокомунікаційних цифрових рішень підприємства, що є необхідною умовою для їх ефективного впровадження, розвитку та стратегічного управління цифровою трансформацією.

Б. Добір інструментів, застосовних для формування організаційних (критерії: скорочення часу, автоматизація, безпека) та антикризових (критерії: стійкість, безперервність, адаптивність) ефектів. Оцінювання організаційних ефектів цифровізації (скорочення часу процесів, автоматизація операцій, підвищення інформаційної та операційної безпеки) потребує застосування інструментів, які дозволяють вимірювати не лише фінансові, але й процесні, продуктивні та ризик-орієнтовані характеристики. *До таких інструментів належать:* Time-Saving Analysis, Process Automation Index,

Security Maturity Assessment, Productivity Metrics, Operational Risk Assessment. Їх відбір є обґрунтованим з огляду на такі аргументи *(табл.3.15)*.

Таблиця 3.15 – Інструменти для оцінювання організаційних ефектів інфокомунікаційних цифрових рішень підприємства: критерії – час, автоматизація, безпека *(джерело: розроблене автором з врахуванням [160-170])*

Інструмент оцінювання	Що вимірює	Критерій	Причини відбору (обґрунтування)
1	2	3	4
1. Time-Saving Analysis	Скорочення тривалості виконання бізнес-процесів, часу циклу, затримок	Час	Безпосередньо вимірює ключовий організаційний ефект – швидкість операцій; надає кількісні показники для порівняння «до/після»; дозволяє оптимізувати процеси.
2. Process Automation Index	Рівень автоматизації операцій та частку цифрових рішень у процесах	Автома-тизація	Дає змогу об’єктивно оцінити глибину цифровізації; дозволяє визначити зони надлишкової чи недостатньої автоматизації; підтримує створення оптимальної цифрової архітектури.
3. Security Maturity Assessment (ISO/NIST)	Рівень інформаційної та операційної безпеки, вразливості, рівень відповідності стандартам	Безпека	Ґрунтується на міжнародних стандартах; забезпечує кількісну та якісну оцінку; зменшує операцій-ні ризики та забезпечує стійкість бізнес-процесів.
4. Productivity Metrics (OEE, Lead Time, Throughput)	Зміни продуктивності праці, ефективності виконання завдань, пропускної здатності процесів	Час, автома-тизація	Дає комплексну оцінку ефектів цифровізації на результативність; інтегрується у фінансові моделі ефективності; підтримує управління ресурсами.

Продовження табл. 3.15

1	2	3	4
5. Operational Risk Assessment	Рівень операційних ризиків, уразливості процесів, вплив людського фактору	Безпека, автома-тизація	Дає змогу виміряти ризики, що зменшуються завдяки цифровим рішенням; дозволяє оцінити надійність та безперервність операцій.

Відібрані інструменти *(див. табл.3.15)* є кількісними, універсальними, стандартизованими та адаптованими до процесної логіки сучасних підприємств. Вони є оптимальними, оскільки прямо вимірюють ключові організаційні ефекти цифровізації – скорочення часу, автоматизацію, безпеку.

Відбір інструментіів для оцінювання оцінювання цифрових рішень у контексті антикризових критеріїв (стійкість, безперервність, адаптивність) аргументовано у табл.3.16.

Таблиця 3.16 – Інструменти для оцінювання оцінювання цифрових рішень у контексті антикризових критеріїв: стійкість / безперервність / адаптивність *(джерело: розроблене автором з врахуванням [160-169, 171])*

Інструмент	Що вимірює	Критерій	Причини відбору
1	2	3	4
1. Time-Saving Analysis	Тривалість та швидкість виконання бізнес-процесів, економія часу	Безперерв-ність	Скорочення часу операцій уможливлює виконання критич-них процесів за умов дефіциту ресурсів чи підвищеного навантаження. Підтримує ста-більність потоків робіт, зменшує ризик затримок у кризах.
2. Process Automation Index	Рівень автоматизації процесів, зниження залежності від ручної праці	Стійкість / безпе-рервність	Автоматизація мінімізує людські помилки та забезпечує стабільну роботу систем у нестабільних умовах. Підвищує стійкість процесів та гарантує їх безпе-рервне виконання при кадрових ризиках, кібератаках або ресурс-них обмеженнях.

Продовження табл. 3.16

1	2	3	4
3. Security Maturity Assess-ment	Рівень кіберза-хисту, здатність виявляти загрози, реагу-вати та відно-влюватися.	Стійкість / адаптив-ність / безперер-вність	Ключовий інструмент у період криз, коли зростає кількість кібератак. Забезпечує захище-ність, стійкість до порушень, здатність швидко адаптуватися до нових загроз та підтримує безперервність роботи при кібер-інцидентах.
4. Produc-tivity Metrics	Продуктивність персоналу та систем, операційна ефективність.	Безперер-вність / частково стійкість	Допомагає оцінити стабільність операцій при пікових навантаженнях. Частково відображає стійкість, показуючи, наскільки цифрові рішення знижують ризики перевантаження й збоїв.
5. Opera-tional Risk Assess-ment	Рівень операційних ризиків, слабкі місця процесів, ймовірність і наслідки збоїв.	Стійкість / безпе-рервність / частково адаптивні сть	Забезпечує виявлення процесів, що можуть зруйнувати безперервність роботи. Підсилює стійкість завдяки ранній ідентифікації вразливостей та дозволяє формувати адаптивні сценарії реагування на кризи.

Фокусування критеріїв на стійкість, безперервність та адаптивність дозволяє оцінювати цифрові інструменти не лише за ефективністю, а й за їх здатністю підтримувати підприємство під час кризових впливів. Аналіз показує, що *найбільш комплексно всі три критерії охоплює Security Maturity Assessment*, тоді як Process Automation Index і Operational Risk Assessment забезпечують значний внесок у стійкість і безперервність. Інструменти Time-Saving Analysis та Productivity Metrics підсилюють переважно безперервність, забезпечуючи стабільне виконання операцій, але не охоплюють адаптивні та системностійкі компоненти в повній мірі.

Узагальнуючи наведене, можна дістати висновку, що *жоден з відібраних інструментів не охоплює всі визначені критерії – ані організаційні, ані антикризові ефекти* (табл.3.17).

Time-Saving Analysis орієнтований на вимірювання економії часу виконання операцій, що безпосередньо підтримує безперервність діяльності та

частково підсилює стійкість і адаптивність. Опосередковано стимулює автоматизацію та покращення процедур безпеки, але не охоплює їх як окремі об’єкти аналізу.

Process Automation Index характеризує рівень автоматизації бізнес-процесів, зменшує ймовірність помилок, підвищує стійкість і безперервність роботи. Скорочення часу досягається як наслідок автоматизації, а безпека враховується лише частково – через зниження впливу людського фактора, але без повного охоплення кіберризиків.

Таблиця 3.17 – Врахування антикризових ефектів та ключових критеріїв цифровими інструментами оцінювання *(джерело: авторська розробка)*

Інструмент оцінювання	Критерії – види ефектів					
	1	2	3	4	5	6
1. Time-Saving Analysis	частково	так	частково	так	частково	
2. Process Automation Index	так		частково		так	частково
3. Security Maturity Assessment	так			частково		так
4. Productivity Metrics	частково	так	частково			
5. Operational Risk Assessment	так		частково			

Security Maturity Assessment оцінює зрілість системи кіберзахисту, здатність до виявлення, реагування та відновлення після інцидентів, повністю охоплюючи аспект безпеки. Сприяє стійкості, безперервності та адаптивності завдяки гнучким політикам захисту; скорочення часу та автоматизація проявляються через використання автоматизованих засобів моніторингу й реагування.

Productivity Metrics фокусуються на вимірюванні результативності праці та завантаження ресурсів, що підтримує безперервність операцій і частково сприяє стійкості та адаптивності. Скорочення часу та автоматизація

враховуються непрямо – через підвищення ефективності процесів; питання безпеки відображається лише в тій мірі, в якій воно впливає на продуктивність.

Operational Risk аналізує операційні ризики, вразливості процесів та ймовірні точки відмови, що забезпечує підвищення стійкості й безперервності. Адаптивність розглядається через сценарний підхід до реагування. Скорочення часу, автоматизація та безпека враховуються частково – як компоненти заходів з мінімізації ризиків, але не як самостійні цілі оцінювання.

Наведене означає, що *наведені інструменти потрібно застосовувати системно – як єдиний комплекс.*

В. Рекомендації щодо оцінювання цифрових ресурсів підприємства. Розробка таких рекомендацій охоплює:

- політику оцінювання цифрових ресурсів;
- механізми моніторингу та оцінювання інфокомунікаційних цифрових рішень (методичні підходи, методика та інструментарій);
- підвищення відповідних компетентностей персоналу.

В.1 Політику оцінювання цифрових ресурсів підприємства розроблено на основі характеристик запропонованих вище інструментів, Time-Saving Analysis, Process Automation Index, Security Maturity Assessment, Productivity Metrics, Operational Risk Assessment (додаток Б.5).

Політика оцінювання цифрових ресурсів встановлює принципи, критерії та процедури аналізу ефективності, стійкості та готовності цифрової інфраструктури підприємства до дії зовнішніх та внутрішніх кризових факторів. Мета політики – забезпечення системного підходу до вимірювання результативності цифрових рішень, підвищення рівня операційної надійності, кіберстійкості та адаптивності підприємства. Політика поширюється на всі цифрові платформи, інформаційні системи, канали комунікацій, аналітичні сервіси, автоматизовані бізнес-процеси, кіберзахисні механізми та технологічні рішення, що використовуються у діяльності підприємства.

В.2 Опис механізмів моніторингу та оцінювання інфокомунікаційних цифрових рішень сформовано на основі політики й

характеристик інструментів, напведених вище. Моніторинг та оцінювання інфокомунікаційних цифрових рішень підприємства здійснюються на основі системного поєднання методичних підходів, структурованої методики та стандартизованого інструментарію. *Основна мета цих механізмів* полягає у забезпеченні стійкості, безперервності та адаптивності цифрової інфраструктури, що є критичними чинниками в умовах кризових впливів.

Пропонуємий механізм моніторингу ґрунтуються *на таких методичних підходах* як:

– критеріально-орієнтований підхід – оцінювання цифрових рішень на основі ключових критеріїв антикризової спроможності: стійкість, безперервність, адаптивність.

– процесний підхід – аналіз стану й ефективності цифрових процесів, інформаційних потоків і каналів комунікацій.

– ризик-орієнтований підхід – визначення вразливостей та операційних ризиків, які можуть порушити функціонування цифрових систем.

– інтегрально-аналітичний підхід – поєднання кількісних і якісних показників для формування узагальненого цифрового профілю підприємства.

– динамічний підхід – регулярне оновлення даних і відстеження змін у цифровій інфраструктурі з урахуванням кризових тригерів.

Кожний з підходів спирається на інструментарій оцінювання, мета та процедури застосування якого відрізняються (табл. 3.18).

З табл. 3.18 випливає, що *основу інструментарію моніторингу складають п'ять стандартизованих методів,* кожен з яких забезпечує оцінювання окремих інфокомунікаційних цифрових рішень в котексті антикризової цифрової спроможності:

– Time-Saving Analysis, який оцінює безперервність операцій через вимірювання швидкості цифрових процесів;

– Process Automation Index, що визначає рівень автоматизації як джерело стійкості та мінімізації операційних збоїв;

Таблиця 3.18 – Порівняльна характеристика методичних підходів до моніторингу та інструментів оцінювання інфокомунікаційних цифрових рішень *(джерело: авторська розробка)*

Методичні підходи	Мета застосування інструменту оцінювання				
	Time-Saving Analysis	Process Automation Index	Security Maturity Assessment	Productivity Metrics	Operational Risk Assessment
1	2	3	4	5	6
1. Критеріально-орієнтований	Вимірює швидкість процесів для визначення рівня безперервності	Визначає частку автоматизованих операцій для оцінки стійкості	Дає оцінку кіберзрілості і стійкості	Вимірює продуктивність для оцінки беззбійності роботи системи	Виявляє ризики порушення стійкості та безперервності
2. Процесний	Аналізує часові характеристики процесів	Оцінює ступінь автоматизації процесних ланцюгів	Аналізує потоки даних і їх захище-ність	Дає уявлення про ефективність процесів	Ідентифікує вразливі елементи процесу
3.Ризико-орієнтований	Виявляє часові вузькі місця як фактор ризику	Визначає ризики, пов’язані з ручними операціями	Оцінює загрози, вразливості, інциденти	Може вказувати на непрямі ризики продуктивності	Прямо вимірює операційні ризики
4. Інтегрально-аналітичний	Формує частину інтегрального індексу безперервності	Формує індекс технологічної стійкості	Формує індекс кіберзахищеності	Додає показники стабільності роботи	Формує підсумковий індекс ризику
5. Динамічний	Моніторинг змін у часі	Динаміка автоматизації	Тренди кіберінцидент-тів	Тренди продуктивності	Динаміка ризиків

– Security Maturity Assessment, який аналізує стійкість, безперервність і адаптивність цифрових систем через вимірювання кіберзрілості;

– Productivity Metrics, що характеризує стабільність та ефективність роботи персоналу і цифрової інфраструктури;

– Operational Risk Assessment, що виявляє ризики, що можуть підірвати цифрову стійкість і безперервність, та формує сценарії адаптації.

Пропонується *методичний підхід та методика паспортизації інструментів* для наведених вище методів оцінювання інфокомунікаційних цифрових рішень (табл.3.19).

Таблиця 3.19 – Паспорти інструментів інфокомунікаційних цифрових рішень: інтегрована схема *(джерело: авторська розробка)*

TIME-SAVING ANALYSIS		**PROCESS AUTOMATION INDEX**	
1		**2**	
Призначення	Оцінювання економії часу та швидкості виконання цифрових процесів.	Призначення	Оцінювання рівня автоматизації бізнес-процесів.
Що вимірює	– тривалість операцій; – швидкість обробки даних; – динаміку скорочення часу.	Що вимірює	– частку автоматизованих операцій; – зниження ручної праці; – стабільність процесів.
Антикризовий критерій	Безперервність, адаптивність.	Антикризовий критерій	Стійкість, безперервність, адаптивність.
Метод вимірювання	Порівняння «до/після», аналіз логів, вимірювання циклу процесу.	Метод вимірювання	Аналіз BPMN-моделей, аудит операцій, інвентаризація процесів.
Типові показники	– час обробки заявки; – відгук системи; – затримки (%).	Типові показники	– індекс автоматизації; – RPA-операції; – частка автоматизованих задач.
Ризики використання	Спотворення даних через нерівні умови або неправильний збір логів.	Ризики використання	Завищення рівня автоматизації, ігнорування винятків.
SECURITY MATURITY ASSESSMENT		**PRODUCTIVITY METRICS**	
Призначення	Оцінка кіберзрілості та здатності систем протистояти загрозам.	Призначення	Призначення: Оцінка продуктивності роботи персоналу та цифрових систем.
Що вимірює	– стан кіберзахисту; – готовність реагувати на атаки; – відповідність стандартам.	Що вимірює	– результативність; – стабільність виконання операцій; – пропускну здатність.
Антикризовий критерій	Стійкість, безперервність	Антикризовий критерій	Безперервність, адаптивність
Метод вимірювання	NIST, COBIT, ISO 27001; аудит політик безпеки; аналіз інцидентів.	Метод вимірювання	KPI (output/hour), workflow-аналітика, порівняння з нормами.
Типові показники	– кількість інцидентів; – час реагування; – впроваджені політики.	Типові показники	– продуктивність; – завантаження систем; – виконання задач.

Продовження табл. 3.19

1	2	3	4
Ризики використання	Залежність від компетентності аудиторів, приховані інциденти.	Ризики використання	Вплив людського фактора, коливання навантажень.
OPERATIONAL RISK ASSESSMENT			
Призначення	Визначення операційних ризиків цифрової інфраструктури.	Метод вимірювання	Карта ризиків, FMEA, аудит процесів.
Що вимірює	– слабкі місця процесів; – ймовірність збоїв; – наслідки порушення безперервності.	Типові показники	– рівень ризику (L×I×C); – частота інцидентів; – пріоритет ризику (RPN).
Антикризовий критерій	Стійкість, безперервність, частково адаптивність	Ризики використання	Суб'єктивність експертів; неповна ідентифікація слабких місць.

Паспортизація інструментів інфокомунікаційних цифрових рішень – це формалізований процес документування характеристик, функціональних можливостей, технічних параметрів, витрат, ризиків, очікуваних ефектів і умов застосування кожного цифрового рішення. Її застосування забезпечує підприємству такі *ключові управлінські переваги як:* системність, прозорість, керованість і економічна раціональність цифрового розвитку підприємства, створюючи фундамент для ефективної цифрової трансформації, підвищення кіберстійкості та оптимального інвестування.

Розроблена методика моніторингу та оцінювання інфокомунікаційних цифрових рішень включає наступні етапи:

Етап 1. Ідентифікація цифрових рішень та інформаційних компонентів, що підлягають оцінюванню (платформи, сервіси, комунікаційні системи, AI/аналітика, кіберзахист).

Етап 2. Вибір релевантних інструментів оцінювання відповідно до критеріїв стійкості, безперервності та адаптивності.

Етап 3. Збір та верифікація показників (час виконання процесів, рівень автоматизації, інциденти безпеки, обсяги навантаження, продуктивність).

Етап 4. Аналітична інтерпретація показників:

– формування матриць відповідності;

– ранжування критеріїв;

– визначення інтегрального індексу стійкості цифрової інфраструктури.

Етап 5. Побудова теплових карт та профілів цифрової спроможності – візуалізація ступеня відповідності цифрових рішень антикризовим критеріям.

Етап 6. Формування рекомендацій та плану підвищення цифрової готовності – визначення необхідних змін, модернізації платформ, корекції політик безпеки, оптимізації процесів.

Відтак, механізми моніторингу та оцінювання ґрунтуються на інтеграції критеріїв стійкості, безперервності та адаптивності з аналітичними інструментами, що охоплюють часову ефективність, автоматизацію, кіберзахист, операційну стабільність та ризики.

На їх основі формується *багатовимірний профіль цифрової інфраструктури підприємства,* який дозволяє своєчасно виявляти слабкі місця, посилювати антикризову готовність і оптимізувати управління цифровими ресурсами.

Для успішного запровадження удосконаленої багатовимірної методики оцінювання цифрових інфокомунікаційних ресурсів/рішень *(додаток Б.6)*, що охоплює фінансові показники, операційну результативність та цифрову стійкість *(див. п. 2.3),* підприємству необхідна комплексна підготовка за такими ключовими напрямами (рис. 3.9).

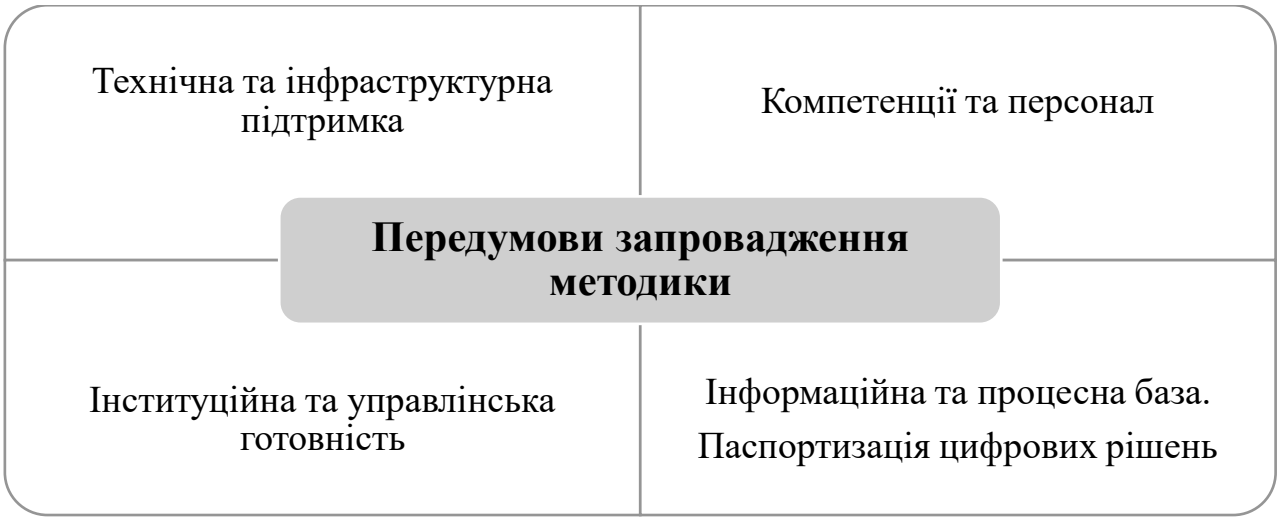


Рисунок 3.9 – Передумови для запровадження багатовимірної методики оцінювання цифрових інфокомунікаційних ресурсів/рішень *(джерело: авторська розробка)*

Інституційна та управлінська готовність – це основа, яка визначає, як підприємство буде використовувати отримані результати. Вона передбачає:

– стратегічне узгодження та визначення пріоритетів. Керівництво має офіційно визнати цифрову стійкість (Digital Resilience) як стратегічний пріоритет (особливо в умовах криз) та затвердити вагові коефіцієнти (w_j) для блоків методики;

– створення міжфункціональної робочої групи. Необхідно залучити фахівців з IT-підрозділу, фінансового відділу, фахівця або відділу кібербезпеки, відділу управління бізнес-процесами (якщо такий є) для забезпечення коректного збору даних з усіх трьох блоків;

– формалізація критичних процесів. Чітке визначення та документування критичних бізнес-процесів ($N_{крит}$) та цифрових інфокомунікаційних ресурсів, які їх підтримують. Це є передумовою для розрахунку показників RTO, $K_{крит}$ та $I_{автом}$;

– запровадження політик DRP/BCP. Наявність затверджених та протестованих планів аварійного відновлення (DRP) і забезпечення безперервності бізнесу (BCP), які є вихідними даними для показників часу відновлення (RTO).

Інформаційна та процесна база – це забезпечення підприємства якісними та доступними даними для розрахунків. Вона має забезпечувати:

– централізований збір фінансових даних. Необхідно забезпечити точний облік усіх видів витрат, пов'язаних з цифровими інфокомунікаційними ресурсами: як капітальних (C_n), так і операційних (C_{OpEx}), включаючи хмарні послуги та технічний супровід);

– впровадження систем логування та моніторингу. Для оцінки блоків II та III потрібні автоматизовані дані: а) інциденти безпеки: журнали SIEM-систем для фіксації $N_{інцид}$; б) час роботи/простою: журнали моніторингу інфраструктури (для RTO); в) якість даних: системи контролю якості даних для розрахунку $P_{даних}$;

– регламентацію процесів автоматизації. Наявність актуальної мапи бізнес-процесів, що дозволяє коректно визначити загальну кількість процесів ($N_{заг}$) та обсяг уже автоматизованих ($N_{авт}$);

– паспортизація цифрових решень. Вона є обов'язковим формалізованим процесом документування характеристик, функціональних можливостей, технічних параметрів, витрат, ризиків, очікуваних ефектів і умов застосування кожного цифрового рішення.

Технічна та інфраструктурна підтримка – це технологічний фундамент, необхідний для генерації метрик стійкості. Вона має створювати:

– рішення для резервного копіювання та відновлення (BDR). Впровадження надійних систем, які забезпечують регулярне резервне копіювання критичних даних, дозволяють протестувати час відновлення RTO;

– системи кіберзахисту та моніторингу. Наявність активних засобів кіберзахисту (брандмауери, антивіруси) та систем моніторингу загроз, які фіксують інциденти та є джерелом для $I_{безпека}$;

– інтеграційні платформи. Наявність інтегрованих ERP/CRM/MES-систем, які забезпечують єдиний інформаційний простір та дозволяють оцінити швидкість комунікації ($T_{коорд}$).

Компетенції та персонал, які створюють людський капітал, є критичним для застосування якісних критеріїв. Персонал представляють:

– експерти з антикризового управління. Наявність персоналу, здатного експертно оцінити Індекс адаптивності архітектури ($I_{адапт}$) та визначити вагові коефіцієнти (w_j);

– фахівці з Data Governance. Співробітники, відповідальні за якість, цілісність та доступність даних, що є критичним для забезпечення достовірності всіх розрахунків;

– персонал, навчений DRP-процедурам. Команди повинні регулярно проходити навчання та тренування з відновлення систем після збоїв, щоб фактичні показники RTO відповідали плановим.

Паспортизацію цифрових решень пропонується здійснювати за

наведений форматом та послідовністю (табл. 3.20). Типова структура паспорта цифрового рішення (продукту) є стандартизованою формою документування, що забезпечує комплексний опис характеристик, ризиків та економічних ефектів інфокомунікаційних цифрових рішень. Його ключові розділи містять:

1. Загальні відомості про інструмент:

- назва продукту: повна та коротка назва цифрового рішення;
- призначення: основна мета використання та ключові функції продукту;
- розробник / провайдер: назва компанії-розробника або постачальника рішення;
- тип інструменту: класифікація рішення (ERP, CRM, SoftPOS, BI-система, хмарний сервіс та ін.);
- об'єкт/сфера застосування: вказати бізнес-процеси, підрозділи або галузі, де використовується рішення.

Таблиця 3.20 – Паспортизація інструментів інфокомунікаційних цифрових рішень: типовий формат паспорту *(джерело: авторська розробка)*

Назва розділу паспорта	Зміст та ключові елементи
1	2
1. Загальні відомості про інструмент	Повна назва продукту, основне призначення та функціональна мета, назва розробника/провайдера, тип інструменту (ERP, CRM, PaaS, SoftPOS, BI) та сфера/об’єкт його застосування.
2. Функціональні можливості та призначення	Детальний опис ключових функцій рішення, його переваг, що вирішуються бізнес-завдання, а також можливості для інтеграції з іншими інформаційними системами підприємства (API, протоколи).
3. Технічні та архітектурні параметри	Опис технологічної основи (AI, NFC, IoT, Cloud), вимоги до апаратного та програмного забезпечення, архітектура рішення (локальна, хмарна, гібридна) та рівень безпеки/захисту даних.
4. Витрати та умови застосування	Капітальні витрати (CapEx) на придбання та впровадження, операційні витрати (OpEx) на комісії, супровід та абонентську плату, умови ліцензування та орієнтовний термін впровадження.

Продовження табл. 3.20

1	2
5. Ризики та обмеження застосування	Систематизація потенційних загроз: технологічні збої, кібербезпекові вразливості, операційні ризики (пов'язані з персоналом / процесами) та обмеження щодо масштабованості або інтеграції.
6. Очікувані результати та ефекти	Ключові показники ефективності (KPI), за якими буде оцінюватися успіх, очікуваний економічний ефект (ROI, PP), а також стратегічний внесок у підвищення цифрової стійкості та конкурентоспроможності підприємства.

2. Функціональні можливості та призначення інструменту:

– ключові функції: детальний опис того, які завдання вирішує продукт (автоматизація виробництва, обробка транзакцій, забезпечення комунікації);

– переваги: основні вигоди, які отримує користувач або підприємство від впровадження;

– інтеграційні можливості: опис здатності взаємодіяти з іншими інформаційними системами (через API, сумісність з ERP/CRM).

3. Технічні та архітектурні параметри інструменту:

– технологічна основа: використовувані технології (NFC, AI/ML, IoT, хмарні сервіси);

– вимоги до інфраструктури: необхідне обладнання, операційна система, мінімальні вимоги до мережі та пам'яті;

– архітектура рішення: опис структури (локальна, хмарна, гібридна);

– параметри безпеки: вбудовані механізми захисту, відповідність стандартам (GDPR, ISO).

4. Витрати та умови застосування інструменту:

– первинні (капітальні) витрати (CapEx): витрати на придбання обладнання, ліцензій, впровадження;

– операційні витрати (OpEx): комісії, абонентська плата, витрати на супровід та оновлення;

– умови ліцензування: тип ліцензії (одноразова, SaaS-підписка, річна);

– термін впровадження: орієнтовний час, необхідний для запуску рішення.

5. Ризики та обмеження застосування:

– технологічні ризики: можливі збої, залежність від зовнішніх провайдерів;

– операційні ризики: ризик низької адаптивності, необхідність перенавчання персоналу;

– кібербезпекові ризики: потенційні вразливості, загрози цілісності та конфіденційності даних;

– обмеження масштабованості: максимальна кількість користувачів або обсяг оброблюваних транзакцій.

6. Очікувані результати та ефекти:

– ключові показники ефективності (KPI): показники, за якими буде оцінюватися успіх (зростання доходу, скорочення витрат, підвищення продуктивності);

– ефект для стійкості: внесок у підвищення цифрової стійкості (наприклад, скорочення RTO, підвищення $I_{безпека}$);

– стратегічний ефект: довгостроковий вплив на конкурентоспроможність та розвиток бізнес-моделі.

Паспортизацію інфокомунікаційних цифрових рішень продемонстровано на двох кейсах, для яких розроблено формалізований опис характеристик, функціональних можливостей, технічних параметрів, витрат, ризиків, очікуваних ефектів і умов застосування кожного інструменту:

Кейс 1. Паспорт цифрового рішення: Багатовимірна методика оцінювання результативності та цифрової стійкості інфокомунікаційних ресурсів (БМ ОР-ЦІКР).

Кейс 2. Паспорт цифрового рішення: TAPXPHONE GercPay (технологічне рішення для прийому платежів).

Паспорти розроблених інструментів як цифрових рішень містить додаток Б7.

Відтак, інструменти та рекомендації щодо оцінювання інфокомунікаційних цифрових рішень підприємства повинні доповнювати

один одного. Це забезпечує трансформацію інфокомунікаційних цифрових рішень з технічного активу на стратегічний чинник безперервності діяльності та підвищення адаптивності підприємства до зовнішніх кризових викликів.

Саме тому запровадження багатовимірної методики оцінювання інфокомунікаційних цифрових рішень спільно з паспортизацією цифрових рішень дозволить підприємству перейти від реактивного управління IT-інфраструктурою до проактивного, даних-орієнтованого стратегічного менеджменту розвитку підприємства.

Висновки до розділу 3

У розділі 3 розроблено та обгрунтовано авторське бачення системного цифрового інфокомунікаційного забезпечення розвитку підприємства в умовах криз, яке ґрунтується на концепції інтегрованої та фокусної системи, яка ставить цифрову стійкість у центр стратегічного управління. Це забезпечення є не статичним набором технологій, а цілеспрямованою системою цифрових ресурсів та технологій, необхідних для діяльності підприємства в умовах кризи. Отримано такі результати:

1. *Розроблено концептуальну модель фокусного цифрового інфокомунікаційного забезпечення*, яка визначає його як цілеспрямовану систему цифрових ресурсів та технологій, необхідних для розвитку та діяльності підприємства в умовах кризи. Сутність цього забезпечення полягає у вирішенні чотирьох ключових завдань: визначення особливостей забезпечення в умовах кризи, формулювання принципів побудови інфокомунікаційної екосистеми, розробка архітектури та визначення ключових показників ефективності (KPI). Ключові особливості цього забезпечення в умовах криз полягають у: а) фокусному виборі ресурсів, коли замість загальної цифровізації стратегія вимагає пріоритетного інвестування у цифрові інфокомунікаційні рішення, критично важливі для безперервності

бізнесу та здатності до швидкого відновлення; б) системному підході та інтеграції, коли забезпечення реалізується поетапно у трьох ключових напрямах: технологічний фундамент через фокусним вибір цифрових платформ і сервісів, гарантію безперервності через побудову безпечних внутрішніх комунікацій та захисту даних, інтелектуальну надбудову через впровадження AI, аналітики та хмарних сервісів для підвищення адаптивності та стратегічної керованості; в) антикризовій орієнтації, де забезпечення є комплексною рамкою, що інтегрує стратегічні вектори цифрової трансформації та механізми антикризового управління на основі даних, що є вирішальним фактором у високотурбулентних умовах.

2. Обґрунтовано, що *фокусне цифрове забезпечення є критично необхідним в умовах кризи*, оскільки воно дозволяє підприємству цілеспрямовано концентрувати обмежені ресурси на тих інфокомунікаційних цифрових рішень (інструментів), що мають найвищий пріоритет для забезпечення безперервності бізнесу та адаптивності. Модель передбачає перехід від загальної цифровізації до пріоритетного інвестування у ресурси, що безпосередньо впливають на стійкість та здатність до швидкого відновлення.

3. *Сформульовано основні принципи побудови інфокомунікаційної екосистеми*, які є основою для розробки архітектури фокусного забезпечення. Ці принципи мають бути орієнтовані на адаптивність, кібербезпеку, інтеграцію даних та стійкість і слугують критеріями для вибору технологічних рішень та формування KPI розвитку цифрової інфраструктури. Обґрунтовано *необхідність формування інфокомунікаційної цифрової стратегії,* яка є комплексною рамкою, що інтегрує стратегічні вектори цифрової трансформації, механізми антикризового управління на основі даних та пріоритети інвестування в цифрові інфокомунікаційні рішення. Доведено, що ця стратегія має забезпечувати не просто модернізацію, а перехід підприємства до цифрової форми функціонування та підвищення його стійкості в умовах високої турбулентності зовнішнього середовища.

4. *Розроблено науково-методичний підхід до проєктування інфокомунікаційної цифрової системи*, який передбачає три ключові інтегровані напрями: а) фокусний вибір цифрових платформ і сервісів (технологічний фундамент); б) побудова внутрішніх комунікацій та захисту даних (гарантія безперервності взаємодії й захищеності); в) впровадження штучного інтелекту, аналітики та хмарних сервісів (інтелектуальна надбудова для стійкості). Це забезпечує системне інтегроване інформаційне середовище. *Запропоновано поетапний алгоритм побудови інфокомунікаційної системи*, який включає шість етапів, від стратегічного планування та проєктування до експлуатації та розвитку. Це створює системне інтегроване інформаційне середовище, яке підтримує розвиток підприємства, забезпечує його здатність адаптуватися до змін та знижувати ризики завдяки цифровим ресурсам.

5. *Розроблено та обґрунтовано методичний підхід та багатовимірну методику оцінювання результативності та цифрової стійкості інфокомунікаційних цифрових рішень,* яка є основним інструментом та доповнює традиційну фінансову оцінку (PP, ROI) показниками операційної результативності та цифрової стійкості (*RTO, $I_{безпека}$)*, забезпечуючи комплексне та об'єктивне вимірювання внеску ЦІКР у розвиток підприємства.

6. *Обґрунтовано необхідність та розроблено рекомендації щодо паспортизації інфокомунікаційних цифрових рішень*. Доведено, що паспортизація є формалізованим процесом документування характеристик, витрат, ризиків, очікуваних ефектів і умов застосування кожного цифрового рішення. Вона забезпечує прозорість, мінімізацію ризиків та стратегічну проактивність управління. Паспорти, розроблені для реальних цифрових рішень, слугують аналітичною базою для системного оцінювання та управління ризиками, пов'язаними з цифровими інфокомунікаціями. Поєднання багатовимірної методики оцінювання результативності та цифрової стійкості інфокомунікаційних цифрових рішень з їх паспортизацією забезпечує трансформацію цифрових інфокомунікапційних рішень з технічного активу на стратегічний чинник. Це дозволяє підприємству

здійснювати поетапне оцінювання (ідентифікація рішень, збирання показників, оцінка за критеріями стійкості) та формувати аналітичну базу для стратегічного управління розвитком з метою мінімізації ризиків та підвищення адаптивності до кризових викликів.

7. *Робоча гіпотеза отримала практичне підтвердження через розроблення та обґрунтування інтегрованої системи управління цифровими інфокомунікаційними ресурсами підприємства,* яка поєднує проактивні механізми управління ризиками, адаптивну цифрову архітектуру та узгоджену взаємодію технологічних, комунікаційних і кібербезпекових компонентів. *Запропоновані інструменти, архітектурні рішення та управлінські процедури продемонстрували здатність забезпечувати підвищення цифрової стійкості, безперервності та адаптивності діяльності підприємства в умовах кризових викликів, що підтверджує реалізацію гіпотези на рівні прикладних управлінських рішень і створює підґрунтя для їх практичного впровадження.*

Відтак, апробація розробленого інструментарію аргументує результативність запропонованих науково-методичних підходів, доцільність системного цифрового інфокомунікаційного забезпечення розвитку підприємства в умовах криз, а *завершене дослідження підтверджує робочу гіпотезу.*

Основні результати та положення розділу 3 висвітлено у працях автора, що наведені у Додатку А. Це публікації: [3, 4, 9, 10, 11].

ВИСНОВКИ

В дисертації наведено теоретичне узагальнення і нове вирішення *наукового завдання*, яке полягає в удосконаленні управління підприємствами шляхом системного управління цифровими інфокомунікаційними ресурсами в умовах криз. Його вирішено за рахунок розроблення та обґрунтування теоретичних і науково-методичних підходів до використання цифрових інфокомунікаційних ресурсів забезпечення розвитку підприємства в умовах криз на засадах системного підходу, що забезпечує підвищення цифрової стійкості та ефективності розвитку підприємства.

Всі поставлені задачі розв’язано. У підсумку сформульовано ряд таких висновків і рекомендацій:

1. *Визначено сутність, класифікацію, еволюцію, обґрунтовано теоретичні підходи та моделі впливу цифрових інфокомунікаційних ресурсів на розвиток і стійкість підприємства в умовах кризових викликів.* Запропоноване *визначення поняття цифрових інфокомунікаційних ресурсів підприємства* розглядає їх як інтегровану соціотехнічну систему, що функціонально поєднує п'ять ключових елементів (інформаційні, комунікаційні, технологічні, інфраструктурні та кібербезпекові ресурси). *Структурно-функціональна модель інфокомунікаційних цифрових ресурсів підприємства* обґрунтовує їхню роль як стратегічного активу та критичного фактора не лише інноваційного розвитку, а й забезпечення цифрової стійкості підприємства в умовах криз. Розроблені класифікації інфокомунікаційних цифрових ресурсів: вузька (інформаційні, комунікаційні, технологічні, інфраструктурні та безпекові ресурси) та широка (ознаки: функціональне призначення, рівень формування цифрового середовища, джерело походження, ступінь інгерованості, тип оброблення інформації, ступінь – критичності для підприємства, розміщення, стандартизації) дають змогу системно впорядкувати інфокомунікаційні цифрові ресурси, окреслити їх змістове, функціональне й технологічне наповнення. Еволюція

інфокомунікаційних цифрових ресурсів демонструє динаміку змін їх структури та функціоналу: вони змінюються разом із трансформацією бізнес-моделей і розвитком цифрових технологій. Цифрові ресурси стають міждисциплінарним феноменом, який одночасно охоплює технологічні, організаційні, управлінські та соціальні виміри функціонування підприємства. Виокремлено три ключових блоки, які формують основу цифрової трансформації та забезпечують здатність підприємства ефективно функціонувати в умовах криз. Це: діджиталізаційні та смарт-моделі управління, концепції цифрової стійкості, інфокомунікаційні платформи. *Структурно-логічна схема діджиталізаційних та смарт-моделей управління* демонструє синергію ефективної цифрової інфраструктури, здатності оперативно реагувати на цифрові збої, використання даних та аналітики для підтримки управлінських рішень, стратегічного управління цифровими змінами, та змінюють принципи організації управлінської діяльності. Розроблена модель та характеристика структурних елементів цифрової стійкості підприємства відображає системний характер її формування.

2. *Досліджено зовнішні кризові фактори та обгрунтовано їхній вплив на функціонування цифрової інфраструктури підприємств.* У підсумку виокремлено *зовнішні кризові фактори, що формують загальноекономічний, політичний, техногенний, кібернетичний та соціальний тиск на діяльність підприємства.* Аналіз досвіду та кейсів ОАЕ свідчить про високу результативність інвестицій у штучний інтелект, хмарні рішення, блокчейн-технології та цифрову інфраструктуру, що забезпечує швидкий перехід до моделі економіки знань. Ці інструменти не лише підвищують технологічну спроможність держави, але й прискорюють адаптацію до глобальних кризових викликів, забезпечуючи нові конкурентні переваги. Для України цей аналіз може бути корисним у формуванні власної системи пріоритетів цифрового розвитку, адаптованої до умов відновлення та модернізації економіки.

3. *Здійснено діагностику рівня цифрової зрілості та інфокомунікаційних ресурсів підприємства і оцінено результативність їх*

застосування для забезпечення розвитку та стійкості в аналітичному розрізі. Аналіз стану цифрової зрілості за ключовими вимірами (процеси, технології, дані, персонал, управління) на макро- і мікрорівнях виявив секторальні відмінності у впровадженні цифрових інфокомунікаційних ресурсів: IT- та фінтех-компанії демонструють більш інтегровані моделі цифрового управління, тоді як виробничі підприємства переважно перебувають на процесному рівні цифрової зрілості, що свідчить про фрагментарний характер цифрової трансформації без формування цілісної інфокомунікаційної екосистеми. Зіставлення результатів оцінювання цифрової зрілості підприємств України з підприємствами ОАЕ виявило структурний розрив між рівнем цифрових технологій та рівнем цифрового управління і використання даних, який в умовах криз суттєво обмежує здатність підприємств забезпечувати стійкість, безперервність та адаптивність діяльності. *Запропонована методика оцінювання цифрової зрілості* дозволила ідентифікувати критичні зони цифрової вразливості та обґрунтувати роль інфокомунікаційного цифрового забезпечення як системоутворюючого елементу інтеграції процесів, даних, персоналу й управлінських рішень. Отримані результати підтвердили доцільність використання *інтегрального індексу цифрової зрілості як інструменту аналітичного моніторингу та антикризового управління*, необхідність переходу від фрагментарної цифровізації до системної моделі цифрового інфокомунікаційного забезпечення розвитку підприємства.

4. *Розроблено концептуальну модель фокусного цифрового інфокомунікаційного забезпечення розвитку підприємства*, яка ґрунтується на системному підході до управління цифровими інфокомунікаційними ресурсами в умовах кризових викликів. Модель інтегрує технологічні, комунікаційні, аналітичні та кібербезпекові компоненти в єдину керовану архітектуру, орієнтовану на досягнення стратегічних цілей розвитку підприємства. *Фокусне цифрове інфокомунікаційне забезпечення розвитку підприємства* як цілеспрямована система цифрових ресурсів, технологій,

інструментів і каналів комунікації концентрується на ключових пріоритетах підприємства та забезпечує безперервність інформаційних потоків, оперативність управлінських рішень і стійкість бізнес-процесів у нестабільних умовах. Воно охоплює інтегроване використання цифрових платформ, мережевої інфраструктури, аналітики даних, систем комунікації та кіберзахисту для підтримання стратегічного розвитку і здатності підприємства адаптуватися до кризових ситуацій. Тому *фокусність моделі формування цифрової стійкості підприємства на основі фокусного цифрового інфокомунікаційного забезпечення* полягає у цільовій концентрації цифрових інфокомунікаційних рішень навколо ключових управлінських завдань забезпечення цифрової стійкості, безперервності та адаптивності діяльності. Реалізація моделі через архітектуру та ключові елементи цифрового інфокомунікаційного забезпечення розвитку підприємства, а також KPI цифрової інфраструктури управління підприємством дозволяє перейти від фрагментарного використання цифрових інструментів до інтегрованого управління цифровими інфокомунікаційними ресурсами, створюючи передумови для стійкого розвитку підприємства в умовах криз.

5. *Сформовано науково-методичні засади побудови цифрової інфокомунікаційної стратегії підприємства з урахуванням кризових умов*, що передбачають визначення стратегічних векторів цифрової трансформації як комплексну рамку напрямів, у межах яких відбувається модернізація бізнес-моделі, операційної системи та інфокомунікаційної інфраструктури підприємства. Їх класифікація та контурне картографування пріоритетів дозволили виокремити комунікаційно-кооперaційний блок як самостійний стратегічний вимір поряд із технологічним та організаційно-управлінським, фокус на інфокомунікаційних цифрових ресурсах як інтегрувальному чиннику розвитку підприємства в умовах криз. На відміну від поширених підходів, де цифрова трансформація здебільшого зводиться до технологічних або процесних змін, запропоновані підходи акцентують на взаємозв’язку цифрових технологій з управлінськими рішеннями, антикризовим ризик-

менеджментом та цифровими мережами взаємодії з клієнтами й партнерами, що дозволяє розглядати цифрову трансформацію як системний інструмент забезпечення цифрової стійкості та розвитку підприємства. Кожний механізм антикризового управління на основі цифрових даних оцінено *за трьома критеріями:* мета застосування, обмеження, здатність врахувати вектори трансформації. Побудований ризик-профіль цифрових механізмів антикризового управління визначив, що їх основними зонами ризику є: дані, інфраструктура, кібербезпека, кадрові компетентності, координація та регуляторні обмеження. Обгрунтовано пріоритети інвестування в інфокомунікаційні цифрові технології для різних рівнів доступності капіталу, розміру підприємств. Розроблено рекомендації та алгоритм проєктування інфокомунікаційної цифрової системи підприємства.

6. *Обґрунтовано методичний підхід, розроблено багатовимірну методику та рекомендації щодо оцінювання результативності та цифрової стійкості інфокомунікаційних цифрових рішень*. *Методичний підхід є* критеріально-орієнтованим та містить, по-перше, структурований перелік основних інструментів оцінювання інфокомунікаційних цифрових рішень підприємства (економічні, організаційні, антикризові та стратегічні, техологічні, оцінювання клієнтського впливу), склад яких забезпечує всебічне, науково обґрунтоване оцінювання. По-друге, критеріальний добір інструментів, застосовних для формування організаційних (критерії: скорочення часу, автоматизація, безпека) та антикризових (критерії: стійкість, безперервність, адаптивність) ефектів доводить, що *їх потрібно застосовувати як єдиний комплекс,* оскільки жоден з них не охоплює ані організаційні, ані антикризові ефекти. *Розроблені рекомендації щодо оцінювання цифрових ресурсів підприємства* містять: політику оцінювання цифрових ресурсів; механізми моніторингу й оцінювання інфокомунікаційних цифрових рішень; відповідні компетентності персоналу. Механізми моніторингу та оцінювання для забезпечення стійкості, безперервності та адаптивності цифрової інфраструктури застосовують критеріально-

орієнтований, процесний, ризик-орієнтований, інтегрально-аналітичний та динамічний підходи та п'ять інструментів оцінювання (Time-Saving Analysis, Process Automation Index, Security Maturity Assessment, Productivity Metrics, Operational Risk Assessment). Ці механізми ґрунтуються на інтеграції критеріїв стійкості, безперервності та адаптивності з аналітичними інструментами, що охоплюють часову ефективність, автоматизацію, кіберзахист, операційну стабільність та ризики. На їх основі формується *багатовимірний профіль цифрової інфраструктури підприємства,* який дозволяє своєчасно виявляти слабкі місця, посилювати антикризову готовність і оптимізувати управління цифровими ресурсами. *Запропоновані методичний підхід, типова структура паспорту цифрового рішення та методика паспортизації інструментів для методів оцінювання інфокомунікаційних цифрових рішень, паспортизації цифрових решень* забезпечують підприємству системність, прозорість, керованість і економічну раціональність цифрового розвитку.

Апробація на реальних підприємствах розроблених автором методик та рекомендацій (додаток В) довела їх практичний характер, а завершене дисертаційне дослідження підтвердило висунуту у розділі 1 та аргументовану у розділі 2 робочу гіпотезу дисертації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кузьмінова О. В., Ільїн Д. М. Інформаційні ресурси як об’єкт управління підприємством. Інтелект XXI. 2023. №1. С. 60–64. DOI: https://doi.org/10.32782/2415-8801/2023-1.11

2. Мороз В. М. Інформаційний ресурс як об’єкт державного управління: зміст, принципи та характеристика системи. Державне управління: удосконалення та розвиток. 2020. №1. С. 1–9. DOI: 10.32702/2307-2156-2020.1.1

3. Шукліна В. В., Набока Р. М, Критерії якості ітерації в циклі формування інформаційно-комунікаційного потенціалу підприємства. Innovative technologies and scientific solutions for industries. 2020. №2(12). С. 90–99.

4. Mutaz M. Al-Debei, Enas M. Al-Lozi Implementations of ICT Innovations: A Comparative Analysis in terms of Challenges between Developed and Developing Countries. International Journal of Information, Business and Management. 2012. Vol. 4, №1. P. 224–252. DOI: https://doi.org/10.48550/arXiv.1208.0887

5. Jinsong Wu, Song Guo, Huawei Huang, William Liu, Yong Xiang Information and Communications Technologies for Sustainable Development Goals: State-of-the-Art, Needs and Perspectives. 2018. DOI: https://doi.org/10.48550/arXiv.1802.09345

6. Anandhi S. Bharadwaj A resource-based perspective on information technology capability and firm performance: an empirical investigation. MIS Quarterly. 2000. Vol. 24, №1. P. 169–196. DOI: https://doi.org/10.2307/3250983

7. Porter, M. E., Heppelmann, J. E. How Smart, Connected Products Are Transforming Competition. Harvard Business Review, 2014, No. 92(11), pp. 64–88.

8. Weill P., Ross J. W. IT Governance: how top performers manage it decision rights for superior results : Harvard Business School Press. 2004. 274 p.

9. Zott, C., Amit, R. Business Model Design: An Activity System Perspective. Long Range Planning, 2010, Vol. 43, No. 2–3, pp. 216–226.

10. Teece D. J. Explicating dynamic capabilities: The nature and microfoundations of sustainable enterprise performance. Strategic Management Journal. 2007. №28(13), P. 1319–1350. DOI: https://doi.org/10.1002/smj.640

11. Bharadwaj A., El Sawy O. A., Pavlou P. A., Venkatraman N. Digital Business Strategy: Toward a Next Generation of Insights. MIS Quarterly. 2013. №37(2). P. 471–482.

12. Liu H., Ke W., Wei K. K., Hua Z. The impact of IT capabilities on firm performance: The mediating role of absorptive capacity and supply chain agility. Decision Support Systems. 2013. №54(3). P. 1452–1462. DOI: https://doi.org/10.1016/j.dss.2012.12.016

13. Tallon P. P., Pinsonneault A. Competing perspectives on the link between strategic information technology alignment and organizational agility. MIS Quarterly. 2011. №35(2). P. 463–486.

14. Sambamurthy, V., Bharadwaj, A., Grover, V. Shaping agility through digital options: Reconceptualizing the role of information technology in contemporary firms. MIS Quarterly. 2003. №27(2). P. 237–263. DOI: 10.2307/30036530

15. Henderson, J. C., Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. IBM Systems Journal, 32(1), 4–16.

16. Ross J. W., Weill P., Robertson D. Enterprise Architecture as Strategy: Creating a Foundation for Business Execution. Harvard Business Press. 2006. 233 p.

17. Luftman, J. Assessing Business-IT Alignment Maturity. Communications of the AIS. 2000. №4(14). P. 1–50. DOI: https://doi.org/10.17705/1CAIS.00414

18. Jonkers, H., Lankhorst, M., Van Buuren, R., Hoppenbrouwers, S., Bonsangue, M., Van der Torre, L. Enterprise architecture: Management tool and

blueprint for the organisation. Information Systems Frontiers. 2006. №8(2). P. 63–66. DOI: 10.1007/s10796-006-7970-2

19. Bernard, S. A. (2012). An Introduction to Enterprise Architecture. AuthorHouse, 3rd edition. 2012. 340 p.

20. Adner R. Ecosystem as Structure: An Actionable Construct for Strategy. Journal of Management. 2016. №43(1). P. 39–58. DOI: https://doi.org/10.1177/0149206316678451

21. Jacobides M., Cennamo C., Gawer A. Towards a Theory of Ecosystems. Strategic Management Journal. 2018. №39(8). P. 2255–2276. DOI: 10.1002/smj.2904

22. Tiwana A. Platform Ecosystems: Aligning Architecture, Governance, and Strategy. MIT Press. 2014. Morgan Kaufmann Publishers Inc.340 Pine Street, Sixth FloorSan FranciscoCAUnited States. 300 p.

23. Autio E., Nambisan S., Thomas L. D. W., Wright M. Digital Affordances, Spatial Affordances, and the Genesis of Entrepreneurial Ecosystems. Strategic Entrepreneurship Journal. 2018. №12. P. 72–95. DOI: https://doi.org/10.1002/sej.1266

24. Lusch R.F., Nambisan S. Service Innovation: A Service-Dominant Logic Perspective. MIS Quarterly. 2015. №39. P. 155–175. DOI: https://doi.org/10.25300/MISQ/2015/39.1.07

25. Iyamu, T. A framework for developing and implementing the enterprise technical architecture. International Journal of Information Management, 2012. №9(1). P. 189–206. DOI: 10.2298/CSIS101103040I

26. Widjajarto, A., Suroso, A., et al. Architecture model of information technology infrastructure services. Procedia Computer Science. 2019. №161. P. 841–850. DOI: 0.1016/j.procs.2019.11.191

27. Majstorovic Milosav N., Terzic Rajko M. Enterprise architecture as an approach to the development of Information systems. Vojnoteh. glas. 2018. №2. DOI: http://dx.doi.org/10.5937/vojtehg66-15850

28. Van de Wetering R. Dynamic enterprise architecture capabilities and organizational benefits: an empirical study. arXiv preprint, 2021. DOI: https://doi.org/10.48550/arXiv.2105.10036

29. Srisawat S., Wannapiroon P., Nilsook P. Distributed digital enterprise architecture for transformation of educational organizations. TEM Journal. 2024. Vol. 13. №2. DOI: 10.18421/TEM132-77

30. El-Hajj M., Itapelo T., Gebremariam T. «Systematic Literature Review: Digital Twins' Role in Enhancing Security for Industry 4.0 Applications». Authorea. March 26, 2024. DOI: 10.22541/au.171142917.74831577/v1

31. Empl P., Pernul G. Digital-Twin-Based Security Analytics for the Internet of Things. Information. 2023. №14(2). DOI: https://doi.org/10.3390/info14020095

32. El-Hajj M. Leveraging Digital Twins and Intrusion Detection Systems for Enhanced Security in IoT-Based Smart City Infrastructures. Electronics. 2024. №13. P. 1–24. DOI: 10.3390/electronics13193941

33. Varghese S. A., Dehlaghi Ghadim A., Balador A., Alimadadi Z., Papadimitratos P. Digital Twin-based Intrusion Detection for Industrial Control Systems. IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events. 2022. P. 611–617. DOI: https://doi.org/10.48550/arXiv.2207.09999

34. Qureshi A. R. et al. A survey on security enhancing Digital Twins: Models, Techniques and Tools. Computer Communications. 2025. Vol. 238. DOI: https://doi.org/10.1016/j.comcom.2025.108158

35. Sola S. R. Security and Innovation in ERP Systems Best Practices for AI, OIC, and Automation Integration. International Journal Research of Leading Publication (IJLRP). 2023. Vol. 4 Issue 8. P.1–14. DOI:10.5281/zenodo.15259092

36. Hou E., Zhang T., Yin X., Chen J., Ding Yu. The evolution of digitalization capabilities during strategic renewal: A case study based on the ecological restoration enterprise practice. Journal of Cleaner Production 459(4):142570. DOI:10.1016/j.jclepro.2024.142570

37. Chen J., Shen L. A Synthetic Review on Enterprise Digital Transformation: A Bibliometric Analysis. Sustainability. 2024. №16(5). DOI: https://doi.org/10.3390/su16051836

38. Makovoz O., Lysenko S. Evolution of digital transformations in IT companies. Proceedings of London International Conferences. 2024. №9. P. 1–7. DOI: https://doi.org/10.31039/plic.2024.9.199

39. Sahid A. I. M., Suhardi, Munawar W. Information System Evolution. In: Strategic Information System Agility: From Theory to Practices. Emerald Publishing Limited. 2020. pp. 29–66. DOI:10.1108/978-1-80043-810-120211004

40. Krogstie J. Information systems evolution over the last 15 years. 2010. DOI: 10.1007/978-3-642-13094-6_24

41. Rashid M. A., Hossain L., Patrick J. D. The Evolution of ERP Systems: A historical perspective. Enterprise Resource Planning: Solutions and Management. 2002. 287 p.

42. Evolution of IT Infrastructure. URL: https://www.ibexpakistan.co/blogs/evolution-of-it-infrastructure

43. Hsu C.-C., Tsaih R.-H., Yen D. C. The Evolving Role of IT Departments in Digital Transformation. Sustainability. 2018. №10(10). 3706; DOI: https://doi.org/10.3390/su10103706

44. Krogstie J., Ahlers D., Helvik B. Open, Autonomous Digital Ecosystems – How to Create and Evolve Trustworthy Systems of Systems? AI for Science. 2015. URL: https://ercim-news.ercim.eu/en102/special/open-autonomous-digital-ecosystems-how-to-create-and-evolve-trustworthy-systems-of-systems

45. Guanqun J., Xiya Z. Evolutionary Mechanisms for Digital Innovation Ecosystem and Value Co-Creation and Co-Sharing -Based the Perspective of Dynamic Capabilities and Resource Orchestration. Information Systems and Economics. 2025. Vol. 6. P. 86-95. DOI: http://dx.doi.org/10.23977/infse.2025.060112.

46. Kulzhambekova, B., Tashenova, L., & Mamrayeva, D. (2023). Theoretical and practical approach to the essential characteristics and structure of

digital ecosystems of industrial enterprises. Economic Annals-XXI. 2023.№205(9-10). P. 14-33. DOI: https://doi.org/10.21003/ea.V205-02

47. Яценко М. Інфокомунікації як чинник соціально-економічного та науково-технічного розвитку Україні та її регіонів у контексті розбудови інформаційного суспільства. Економіка: реалії часу. Науковий журнал. 2012. №1 (2). С. 143-146. URL: http://economics.opu.ua/files/archive/2012/n1.html

48. Parida V., Sjödin D., Reim W. Reviewing literature on digitalization, business model innovation, and sustainable industry: Past achievements and future promises. Sustainability. 2019. Vol. 11, No. 2. DOI: https://doi.org/10.3390/su11020391

49. Rachinger M., Rauter R., Müller C., Vorraber W., Schirgi E. Digitalization and its influence on business model innovation. Journal of Manufacturing Technology Management. 2019. Vol. 30, No. 8. P. 1143–1160. DOI: https://doi.org/10.1108/JMTM-01-2018-0020

50. Tim Y., Leidner D. Digital resilience: A conceptual framework for information systems research. Journal of the Association for Information Systems. 2023. Vol. 24, No. 5. DOI: 10.17705/1jais.00842

51. Mehedintu A., Soava G. A structural framework for assessing the digital resilience of enterprises in the context of the technological revolution 4.0. Electronics. 2022. Vol. 11, No. 15. Art. 2439. DOI: https://doi.org/10.3390/electronics11152439

52. Winarsih Indriastuti M., Fuad K. Impact of Covid-19 on Digital Transformation and Sustainability in Small and Medium Enterprises (SMEs): A Conceptual Framework. In: Barolli, L., Poniszewska-Maranda, A. and Enokido, T., Eds., Complex, Intelligent and Software Intensive Systems. CISIS 2020. Advances in Intelligent Systems and Computing. 2021. Vol. 1194, Springer, Cham, P. 471-476. DOI: https://doi.org/10.1007/978-3-030-50454-0_48

53. Gun L, Xu L. The effects of digital transformation on firm performance. Evidence from China`s manufactoring sector. Sustainability. 2021. Vol. 13, №22. Art. 12844. DOI: https://doi.org/10.3390/su132212844

54. Zheng, P., wang, H., Sang, Z. et al. Smart manufacturing systems for Industry 4.0: Conceptual framework, scenarios, and future perspectives. Front. Mech. Eng. 2018. №13. P. 137–150. DOI: https://doi.org/10.1007/s11465-018-0499-5

55. Parhi S., Joshi K., Akarte M. Smart manufacturing: a framework for managing performance. International Journal of Computer Integrated Manufacturing. 2021. №34(3). P. 227-256. DOI: https://doi.org/10.1080/0951192X.2020.1858506

56. Badamasi A., Xie X., Kassem M. Enterprise digital twins for strategic data utilisation from construction sites. Proceedings of the 2024 European Conference on Computing in Construction. July 14-17, 2024. Chania, Crete, Greece. URL: https://ec-3.org/publications/conferences/EC32024/papers/EC32024_326.pdf

57. Rohan Kapoor. The Digital Twin of the Enterprise: Revolutionizing Organizational Intelligence. Journal of Computer Science and Technology Studies. 2025. №7(8). P. 762-770. DOI: https://doi.org/10.32996/jcsts.2025.7.8.89

58. Нікітін Ю.О., Кульчицький О.І. Цифрова парадигма як основа визначень: цифровий бізнес, цифрове підприємство, цифрова трансформація. Маркетинг і цифрові технології. 2019. Том 3. № 4. С. 77–87. DOI: 10.15276/mdt.3.4.2019.7. URL: https://mdt-opu.com.ua/index.php/mdt/article/view/86/83

59. Zhang J., Long J., von Schaewen A.M.E. How Does Digital Transformation Improve Organizational Resilience? – Findings from PLS-SEM and fsQCA. Sustainability 2021, 13(20), 11487. DOI: https://doi.org/10.3390/su132011487

60. Őri D, Szabó I, Kő A, Kovács T. Digitalizing in crisis: the role of organizational resilience in SMEs' digitalization. Journal of Enterprise Information Management. 2024. Vol. 37 No. 4 pp. 1185–1205, DOI: https://doi.org/10.1108/JEIM-03-2023-0141

61. Burlacu S., Mocanu V., Platagea Gomboș S., Dobre F. Organizational resiliency through digitalization. Proceedings of the International Management

Conference “Management and resilience strategies for a post-pandemic future”. Bucharest: Faculty of Management, The Bucharest University of Economic Studies, 2022. Vol. 16, No. 1. P. 643–650. DOI: 10.24818/IMC/2022/04.06

62. Tang Chaoli, Dong Shuyun, Zhou Rui. "The impact of digitalization on corporate resilience," International Review of Economics & Finance, Elsevier. 2025. Vol. 97(C). DOI: 10.1016/j.iref.2024.103834

63. Dupin J.-J., Pascal A., Godé C. Unfolding digital resilience in organizations: a systematic review and research agenda on digital resilience in organizations. Proceedings of the 56th Hawaii International Conference on System Sciences (HICSS-56). 2023. P. 1–6.

64. Chon Abraham, France Bélanger, Sally Daultrey Promoting research on cyber threat intelligence sharing in ecosystems. Journal of Cybersecurity. 2025. Volume 11, Issue 1. DOI: https://doi.org/10.1093/cybsec/tyaf016

65. Buckley R., Pasquale L., Nuseibeh B.,Helfert M. A Review of Cyber Information Sharing in Information Sharing Analysis Centres (Isacs). DOI: http://dx.doi.org/10.2139/ssrn.4770617

66. Ali Pala, Jun Zhuang Information Sharing in Cybersecurity: A Review. Decision Analysis. 2019. №16(3). P. 172-196. DOI: https://doi.org/10.1287/deca.2018.0387

67. Chang K.,Huang H. Exploring the management of multi-sectoral cybersecurity information-sharing networks. Government Information Quarterly. 2023. Vol. 40 Issue 4. DOI: https://doi.org/10.1016/j.giq.2023.101870

68. Josiah Dykstra, Lawrence A Gordon, Martin P Loeb, Lei Zhou Maximizing the benefits from sharing cyber threat intelligence by government agencies and departments. Journal of Cybersecurity. 2023. Volume 9, Issue 1. DOI: https://doi.org/10.1093/cybsec/tyad003

69. The Cyber Threat Alliance – Official Website. URL: https://www.cyberthreatalliance.org

70. Financial Services Information Sharing and Analysis Center – Official Website. URL: https://www.fsisac.com

71. National Cyber-Forensics and Training Alliance – Official Website. URL: https://www.ncfta.net

72. Ntoko A. Global Cybersecurity Agenda (GCA) A framework for international cooperation. Open-ended Intergovernmental Expert Group on Cybercrime Vienna, 17-21 January 2011. URL: https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/ITU_Cybercrime_EGMJan2011.pdf

73. Perry, D., Taylor, M., & Doerfel, M. Internet-based communication in crisis management. Management Communication Quarterly, 2003, Vol. 17(2), pp. 206–232. DOI: https://doi.org/10.1177/0893318903256227

74. Poblet M., Fitzpatrick M., Chhetri P. Microtasking: Redefining crowdsourcing practices in emergency management. The Australian Journal of Emergency Management. 2017. №32(2). P. 47–53.

75. Fischer-Preßler D., Bonaretti D., Bunker D. Digital transformation in disaster management: A literature review. Journal of Strategic Information Systems. 2024, Vol. 33. DOI: https://doi.org/10.1016/j.jsis.2024.101865

76. Mahesh Reddy Pathoori Digital transformation of crisis management: Building resilient recovery platforms. World Journal of Advanced Engineering Technology and Sciences. 2025. №15(03). P. 1453-1466. DOI: https://doi.org/10.30574/wjaets.2025.15.3.1054

77. Upadhyay N., Upadhyay S., Mehra P., Gour A. Managing Crises in the Digital Age: Navigating the Complexities of Technology and Management. Engineering Management Journal. 2025. №37(5). P. 499–504. DOI: https://doi.org/10.1080/10429247.2025.2557152

78. Зайченко К.С, Реклізон Ю.І. Удосконалення організаційної структури управління на різних етапах життєвого циклу підприємницьких структур. Економіка та суспільство. 2024. No 60. DOI: 10.32782/2524-0072/2024-60-52

79. Saka T.N., Hormiga E., Valls-Pasola J. Crisis response strategies: a digital reluctance perspective. Rev Manag Sci. 2025. №19. P. 2569–2607. DOI: https://doi.org/10.1007/s11846-024-00822-5

80. Філиппова С.В., Кульчицький О.І. Удосконалення моделі розробки інноваційних послуг із застосуванням цифрових технологій. Економіка: реалії часу. 2024. №3(73). С. 130-140. DOI: 10.15276/ETR.03.2024.13

81. Mohammed A. N. N. A. M., Hu W. Using Management Information Systems (MIS) to Boost Corporate Performance. The international journal of management science and business administration. 2015. Vol. 1, No. 11. P. 55–61. DOI: 10.18775/ijmsba.1849-5664-5419.2014.111.1006

82. Lusianah, Meiryani. The Role of Management Information Systems in Achieving Excellent Operational Performance. International Journal of Scientific & Technology Research. 2019. Vol. 8, No. 4. P. 304–306.

83. Huber G. Organizational Information Systems: Determinants of Their Performance and Behavior. Management Science. 1982. №28(2). P. 138–155.

84. Tarigan Z. J. H., Siagian H., Jie F. Impact of Enhanced Enterprise Resource Planning (ERP) on Firm Performance through Green Supply Chain Management. Sustainability. 2021. №13(8). DOI: https://doi.org/10.3390/su13084358

85. Voulgaris F., Lemonakis C., Papoutsakis M. The Impact of ERP Systems on Firm Performance: The Case of Greek Enterprises. Global Business and Economics Review. 2015. Vol. 17, No. 1. P. 112–129. DOI: 10.1504/GBER.2015.066536

86. Chen X., Dai Q., Na C. The Value of Enterprise Information Systems Under Different Corporate Governance Aspects. Information Technology and Management. 2019. №20. P. 223-247. DOI: https://doi.org/10.1007/s10799-019-00310-3

87. Berente N., Lyytinen K., Yoo Y., King J. L. Routines as Shock Absorbers During Organizational Transformation: Integration, Control, and NASA's

Enterprise Information System," Organization Science, INFORMS. 2016. Vol. 27(3). P. 551-572. DOI: 10.1287/orsc.2016.1046

88. Mentzas G. Towards Intelligent Organisational Information Systems. International Transactions in Operational Research. 1994. Vol. 1, No. 2. P. 169–187. DOI: https://doi.org/10.1016/0969-6016(94)90018-3

89. Saarinen T. Evolution of information systems in organizations. Behaviour & Information Technology. 1989. №8(5). P. 387–398. DOI: https://doi.org/10.1080/01449298908914568

90. Kanellou A., Spathis C. Accounting Benefits and Satisfaction in an ERP Environment. International Journal of Accounting Information Systems. 2013. Vol. 14, No. 3. P. 209–234. DOI: https://doi.org/10.1016/j.accinf.2012.12.002

91. McCallister E., Grance T., Scarfone K. Guide to protecting the confidentiality of personally identifiable information. Recommendations of the National Institute of Standards and Technology. 2009. 58 p.

92. Shameli-Sendi A., Aghababaei-Barzegar R., Cheriet M. Taxonomy of information security risk assessment (ISRA). Computers & Security. Vol. 57. P. 14–30. DOI: https://doi.org/10.1016/j.cose.2015.11.001

93. Fenz, S., Ekelhart, A. Formalizing information security knowledge. In Proceedings of the 2009 ACM symposium on Information, computer and communications security. 2009. P. 183–194.

94. Башинська І.О. Удосконалення системи управління ризиками на підприємстві. Причорноморські економічні студії. 2017. № 17. С. 91–94.

95. Shedden, P., Ahmad, A., Smith, W. Information security risk assessment: Towards a business practice perspective. Proceedings of the 8th Australian Information Security Management Conference. 2010. P. 119–130.

96. Ahmad, A., Maynard, S. B., Shanks, G. A case analysis of information systems security incident responses. International Journal of Information Management. 2015. Vol. 35, No. 6. P. 717–723.

97. Böhme, R., Kataria, G. Models and Measures for Correlation in Cyber-Insurance. Workshop on the Economics of Information Security. 2006. URL:

https://www.semanticscholar.org/paper/Models-and-Measures-for-Correlation-in-Böhme-Kataria/24af7e7832277628c9fa108e31c31d75d3c494bc

98. Tankard, C. Advanced Persistent Threats and How to Monitor and Deter Them. Network Security. 2011. Vol. 2011 №8. P. 16–19.

99. Башинська І. О., Валянська А. О., Гомонюк Г. І. Управління ризиками як напрям забезпечення конкурентоспроможності підприємств. Молодий вчений. 2019. № 1(2). С. 413-416.

100. Інвестиції техногігантів у ШІ перевершать оборонні витрати ЄС. 2025. URL: https://minfin.com.ua/ua/2025/08/01/155801478/

101. Precedence Research. Artificial Intelligence Market – Global Industry Analysis, Size, Share, Growth, Trends, and Forecast 2024–2034. Precedence Research, 2024. URL: https://www.precedenceresearch.com/artificial-intelligence-market

102. Інвестиції у технології допомогли 87% компаній у світі збільшити прибутки. 2025. URL: https://forbes.ua/news/87-kompaniy-zafiksuvali-zrostannya-pributkiv-zavdyaki-investitsiyam-u-tekhnologii-kpmg-10022025-27014

103. Розбудова кібербезпеки завдяки співпраці топ-менеджменту. Результати «Міжнародного аналітичного дослідження довіри до цифрових технологій, 2025» від PwC для регіону ЦСЄ. 2025. URL: https://www.pwc.com/ua/uk/survey/2025/cee-findings-from-the-2025-global-digital-trust-insights-survey.html

104. Міхєєва А. В. Переваги та недоліки цифровізації в банківській справі. Управління розвитком соціально-економічних систем: Матеріали IX Міжнародної науковопрактичної конференції (присвячена пам’яті професора Григорія Євтійовича Мазнєва). (м. Харків, 06-07 березня 2025 року). Харків : ДБТУ. Ч. 2. 2025. С. 73-75.

105. Лисенко С. М. Цифрова трансформація та стандарти якості: модернізація управління бізнес-процесами для сталого розвитку. Управління розвитком соціально-економічних систем: Матеріали IX Міжнародної

науковопрактичної конференції (присвячена пам'яті професора Григорія Євтійовича Мазнєва). (м. Харків, 06-07 березня 2025 року). Харків : ДБТУ. Ч. 2. 2025. С. 145-149.

106. Експерти визначили топ-10 трендів у технології IoT та їхній вплив на світ. 2023. URL: https://proit.ua/kliuchovi-rozrobki-ta-tiendientsiyi-v-intiernieti-riechiei-iot-d/

107. Семчук Ж., Іваш А., Хоростіль О., Вовк Ю., Хміль Ю., Підгірняк О., Зубрицький В. Роль цифрових технологій у трансформації бізнес-моделей сучасних підприємств. Академічні візії, 2024. №28. DOI: https://doi.org/10.5281/zenodo.11356659

108. Антохов А., Руденко В., Яременко Л. Вплив цифрової трансформації на продуктивність праці в IT секторі. Актуальні питання економічних наук. 2025. №12. DOI: https://doi.org/10.5281/zenodo.15586217

109. Grand View Research. Workplace Transformation Market Size, Share & Trends Analysis Report, 2018–2030. San Francisco: Grand View Research, 2023. URL: https://www.grandviewresearch.com/industry-analysis/workplace-transformation-market

110. The roadmap to sustainable IT. 2025. URL: https://www.techradar.com/pro/the-roadmap-to-sustainable-it

111. Organisation for Economic Co-operation and Development. OECD Digital Economy Outlook 2024. Paris: OECD Publishing, 2024. 320 p.

112. World Economic Forum. Global Technology Governance Report 2023: The Future of Digital Infrastructure. Geneva: WEF, 2023. 142 p.

113. PricewaterhouseCoopers. Global Digital Trust Insights 2024: The Leadership Agenda to Build Digital Trust. PwC, 2024. 56 p.

114. McKinsey Global Institute. The Economic Potential of Generative AI: The Next Productivity Frontier. New York: McKinsey & Company, 2023. 76 p.

115. United Nations Conference on Trade and Development (UNCTAD). Digital Economy Report 2024: The Shift Toward Data-Driven Growth. New York – Geneva: United Nations, 2024. 210 p.

116. Horizon Market Research. UAE Digital Transformation Market Size, 2018–2030. Grand View Research, 2024.

117. Microsort інвестує понад 15 млрд дол в ОАЕ. URL: https://minfin.com.ua/ua/2025/11/03/161693858

118. Microsoft to invest $8 billion in UAE by 2029 in cloud technologies and chips development. URL: https://unn.ua/en/news/microsoft-to-invest-dollar8-billion-in-uae-by-2029-in-cloud-technologies-and-chips-development

119. Microsoft showcases remarkable innovations accelerating AI transformation and growth across the UAE. URL: https://news.microsoft.com/en-xm/2025/02/06/microsoft-showcases-remarkable-innovations-accelerating-ai-transformation-and-growth-across-the-uae/

120. Zhavoronok A., Filyppova S., Tochylina Yu., Ozarko K., Neykov S., Krylov D. The impact of artificial intelligence on the development of the digital business ecosystem Journal of Theoretical and Applied Information Technology Vol. 103. №. 9. 2025. URL: https://www.jatit.org/volumes/Vol103No9/29Vol103No9.pdf

121. UAE Accelerates AI Ambitions with Strategic Data Centre Investments. URL: https://www.1arabia.com/2025/04/uae-accelerates-ai-ambitions-with_25.html

122. First 200 MW from UAE's Stargate AI campus to come online next year. URL: https://www.reuters.com/business/media-telecom/first-200-mw-uaes-stargate-ai-campus-come-online-next-year-2025-10-14/

123. UAE tech leaders anticipate stronger demand for AI and cloud capabilities over next 12 months: KPMG tech report. URL: https://kpmg.com/ae/en/media/press-releases/2024/12/uae-tech-leaders-anticipate-stronger-demand-for-ai-and-cloud-capabilities.html

124. UAE Companies Rapidly Adopting Cloud and Increasing AI Investment to Boost Business Performance, New SAP Survey Shows. URL: https://news.sap.com/mena/2024/12/uae-companies-rapidly-increase-ai-investment

125. United Arab Emirates. UAE National Artificial Intelligence Strategy 2031. Abu Dhabi, 2019.

126. Smart Dubai Government Establishment. Smart Dubai Strategy 2021. Dubai, 2020.

127. United Arab Emirates Government. UAE Blockchain Strategy 2021. Abu Dhabi, 2018.

128. UAE Cybersecurity Council. National Cybersecurity Strategy of the UAE. Abu Dhabi, 2020.

129. Dubai Autonomous Transportation Strategy. Dubai Roads and Transport Authority (RTA). Dubai, 2019.

130. Dubai International Financial Centre. DIFC Innovation Hub Annual Report 2023. Dubai, 2023.

131. Microsoft Corporation. Digital Transformation in the UAE: Cloud and Data Center Expansion Report. Redmond, 2024.

132. Dubai Health Authority. Dubai Health Digital Transformation Program: Annual Review 2022. Dubai, 2023.

133. UAE National Strategy for Artificial Intelligence 2031. URL: https://staticcdn.mbzuai.ac.ae/mbzuaiwpprd01/2022/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf

134. Dubai's du announces 2 billion dirhams hyperscale data center deal with Microsoft. 2025. URL: https://www.reuters.com/business/media-telecom/dubais-du-announces-2-billion-dirhams-hyperscale-data-center-deal-with-microsoft-2025-04-22

135. 'Stargate UAE' AI datacenter to begin operation in 2026. 2025. URL: https://www.reuters.com/business/media-telecom/stargate-uae-ai-datacenter-begin-operation-2026-2025-05-22/

136. U.S. delays Nvidia, AMD AI GPU export licenses to Middle East. URL: https://www.tomshardware.com/pc-components/gpus/us-delays-nvidia-amd-ai-gpu-exports-licenses-to-middle-east

137. UAE tech report 2024. URL: https://kpmg.com/ae/en/insights/ai-and-technology/uae-tech-report-2024.html

138. Програма цифрової зрілості малого та середнього бізнесу в Україні. URL: https://business.diia.gov.ua/initiative/national-program-for-digital-maturity

139. Оцініть цифрову зрілість бізнесу та економте час і ресурси з новими інструментами від Дія.Бізнес. URL: https://thedigital.gov.ua/news/business/otsinit-tsyfrovu-zrilist-biznesu-ta-ekonomte-chas-i-resursy-z-novymy-instrumentamy-vid-diiabiznes

140. Pasko M., Lisna I., Morozova N., Denchyk I. Readiness of Ukrainian business for digital transformation: drivers and barriers. Financial and Credit Systems: Prospects for Development. 2025. № 1(16). С. 125–137. DOI: https://doi.org/10.26565/2786-4995-2025-1-10

141. Enhancing resilience by boosting digital business transformation in Ukraine. URL: https://www.oecd.org/en/publications/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_4b13b0bb-en.html

142. United Nations, Department of Economic and Social Affairs. United Nations E-Government Survey 2024. URL: https://desapublications.un.org/sites/default/files/publications/2024-09/%28Web%20version%29%20E-Government%20Survey%202024%201392024.pdf

143. OECD. SME and Entrepreneurship Policy Review: Ukraine. Paris: OECD Publishing, 2023. URL: https://www.oecd.org/industry/smes/ukraine-sme-policy-review.htm

144. Use of information and communication technologies at enterprises / State Statistics Service of Ukraine. URL: https://stat.gov.ua/en/datasets/use-information-and-communication-technologies-enterprises

145. Sorokina A., Lebedeva L. The impact of digital transformation on enterprises' resilience: evidence from Ukraine. Agora International Journal of

Economical Sciences. 2025. Vol. 19, No. 1. DOI: https://doi.org/10.15837/aijes.v19i1.7161

146. Ukraine's Digital Transformation: Innovation for Resilience. URL: https://www.hks.harvard.edu/centers/cid/voices/ukraines-digital-transformation-innovation-resilience

147. Біла книга з цифрової зрілості традиційних МСБ. URL: https://drive.google.com/file/d/1SBp3iXEtBrfP3fhyJB9uzX7DSvq_-Ezj/view

148. OECD. OECD Digital Economy Outlook 2024. Volume 2: Strengthening connectivity, innovation and trust. Paris : OECD Publishing, 2024. URL: https://www.oecd.org/en/publications/2024/11/oecd-digital-economy-outlook-2024-volume-2_9b2801fc.html

149. Зайченко К.С. Діджиталізація економік та суспільства: світові тенденції. Актуальні проблеми економіки. №9 (267). 2023. DOI: 10.32752/1993-6788-2023-1-267-21-30

150. Diia.Business; Міністерство цифрової трансформації України. Інструменти оцінювання цифрової зрілості бізнесу. Київ, 2023. URL: https://business.diia.gov.ua

151. Selivanova N.M., Kvasha K.S., Sibikovska A.O. Prospects for Introducing Digitalization Tools for Accounting Processes at Ukrainian Enterprises. Економіка: реалії часу. Науковий журнал. 2023. № 4 (68). С. 69-75. DOI: 10.15276/ETR.04.2023.7.

152. World Bank Group. Digital Transformation in Ukraine: Opportunities and Challenges. Washington, 2023. URL: https://www.worldbank.org/en/country/ukraine

153. Harvard Kennedy School; Center for International Development. Ukraine's Digital Transformation: Innovation and Resilience. 2023. URL: https://www.hks.harvard.edu/centers/cid

154. UAE Government. UAE Digital Government Strategy 2025. URL: https://u.ae/en/about-the-uae/digital-uae

155. Smart Dubai Office. Dubai Digital Strategy & Smart Dubai Reports. URL: https://www.digitaldubai.ae

156. World Bank Group. GovTech Maturity Index: United Arab Emirates. Washington, 2022–2023. URL: https://www.worldbank.org/en/topic/governance/brief/govtech-putting-people-first

157. OECD. Digital Government Review of the United Arab Emirates. 2020. URL: https://www.oecd.org/gov/digital-government-review-of-the-united-arab-emirates-9789264312169-en.htm

158. IMD World Competitiveness Center. World Digital Competitiveness Ranking 2023. Lausanne : IMD, 2023. URL: https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/

159. PwC Middle East. Digital Transformation in the UAE: Industry Insights. 2022–2023. URL: https://www.pwc.com/m1/en/publications.html

160. Лисенко С. М. Оцінка ефективності цифрової трансформації в управлінні бізнес-процесами агропромислових підприємств. Бізнес-Навігатор. 2025. № 6. DOI: https://doi.org/10.32782/business-navigator.83-60

161. Хіміч С. В. Методичні підходи до оцінювання рівня цифрової трансформації промислових підприємств. Економічний вісник КПІ. 2023. № 27. DOI: https://doi.org/10.20535/2307-5651.27.2023.297217

162. Alshammari K. H. Managing digital transformation in a global environment. Dialnet. 2023. URL: https://dialnet.unirioja.es/descarga/articulo/9385607.pdf

163. Alzarooni A. I. Navigating digital transformation in the UAE: Benefits and challenges. Computers. 2024. Vol. 13, No. 11. Art. 281. DOI: https://doi.org/10.3390/computers13110281

164. Digital Dubai. Dubai State of AI Report. Dubai: Digital Dubai, 2023. URL: https://www.digitaldubai.ae/docs/default-source/publications/dubai-state-of-ai-report.pdf

165. Telecommunications and Digital Government Regulatory Authority. UAE Digital Government Maturity Model. Abu Dhabi: UAE Digital Government, 2022.

166. Wernicke B. Introduction of a digital maturity assessment framework for construction site operations : master's thesis. Luleå : Luleå University of Technology, 2023.

167. Zhang P., Wang Y. Digital transformation: A systematic review and bibliometric analysis from the corporate finance perspective. SSRN, 2024. DOI: https://doi.org/10.2139/ssrn.5053864

168. O'Higgins D. Impacts of business architecture in the context of digital transformation: An empirical study using PLS-SEM approach. Journal of Business and Management Studies. 2023. Vol. 5, No. 4. DOI: https://doi.org/10.32996/jbms.2023.5.4.7

169. Nosratabadi S., Atobishi T., HegedHus Sz. Social sustainability of digital transformation: Empirical evidence from EU-27 countries. Administrative Sciences. 2023. Vol. 13, No. 5. Art. 126. DOI: https://doi.org/10.3390/admsci13050126

170. Чукурна, О., Базика, С., Федчик, О. Вплив цифрової трансформації бізнесу на консалтингові послуги в сфері інформаційно-комуникативних технологій. Економіка та суспільство .2024. №66. DOI: https://doi.org/10.32782/2524-0072/2024-66-112

171. Гончар О.І., Чорна Л.О., Коваленко О.О. Інтеграція інформаційних та управлінських процесів в системі менеджменту сучасного підприємства. Вісник Хмельницького національного університету. Економічні науки. 2021. № 5 (298). Т. 2 С. 209–213. https://doi.org/10.31891/2307-5740-2021-298-5(2)-34

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Статті у фахових виданнях України

1. Алі Рашид Халіфа Бумекайр Альмансурі. Формування інфокомунікаційної інфраструктури підприємства в умовах криз. *Економічний журнал Одеського політехнічного університету*. 2025. №1(31). С. 136-145. URL: https://economics.net.ua/ejopu/2025/No1/136.pdf (Дата звернення 05.10.2025). DOI: 10.15276/EJ.01.2025.14, DOI: 10.5281/zenodo.18025510 *(Кат. Б., Index Copernicus, Google Scholar) (1,15 д.а.).*

2. Ткач К.І., Алі Рашид Халіфа Бумекайр Альмансурі. Оцінювання стану та ефективності використання інфокомунікаційних цифрових ресурсів на підприємствах. *Економіка: реалії часу. Науковий журнал.* 2025. № 1 (77). С. 129-139. URL: https://economics.net.ua/files/archive/2025/No1/129.pdf (Дата звернення 05.10.2025). DOI: 10.15276/ETR.01.2025.15 DOI: 10.5281/ zenodo.18036081 *(Кат. Б., Index Copernicus, Ulrich's Periodicals Directory, EBSCO Publishing, Google Scholar) (1,1 д.а., особистий внесок: розроблено рекомендації, методику оцінювання цифрових ресурсів підприємства, систему для формування організаційних і антикризових ефектів – 0,6 д.а.).*

3. Алі Рашид Халіфа Бумекайр Альмансурі. Діагностика цифрової зрілості у котнексті інфокомунікаційніих ресурсів підприємства. *Економічний журнал Одеського політехнічного університету.* 2025. № 2 (32). С. 141-151. URL: https://economics.net.ua/ejopu/2025/No2/141.pdf (Дата звернення 05.09.2025). DOI: 10.15276/EJ.02.2025.16, DOI: 10.5281/zenodo.18025967 *(Кат. Б., Index Copernicus, Google Scholar) (1,05 д.а.).*

4. Ткач К.І., Алі Рашид Халіфа Бумекайр Альмансурі. Системне цифрове інфокомунікаційне забезпечення розвитку підприємства: фокусування в умовах криз. *Економіка: реалії часу. Науковий журнал.* 2025. № 2 (78). С. 150-161. URL: https://economics.net.ua/files/archive/2025/No2/150.pdf.

(Дата звернення 05.10.2025). DOI: 10.15276/ETR.02.2025.16, DOI: 10.5281/zenodo.18039087 *(Index Copernicus, Google Scholar). (1,2 д.а., особистий внесок: обґрунтувано концептуальні засади системного цифрового інфокомунікаційного забезпечення розвитку підприємства, напрями його фокусування в умовах криз: структурно-логічну модель, принципи побудови інфокомунікаційної екосистеми, архітектуру, ключові елементи і KPI) (0,7 д.а.).*

Опубліковані праці апробаційного характеру

5. Алі Рашид Халіфа Бумекайр Альмансурі. Принципи побудови інфокомунікаційної екосистеми в умовах криз. *Актуальні проблеми теорії та практики менеджменту*: Матеріали XII міжнар. наук.-практ. конф. 26 травня 2023, Україна, м. Одеса. С. 201-203. URL: https://economics.net.ua/files/science/men/2023/s7.pdf. (Дата звернення 20.10.2022) (*0,15 д.а.*).

6. Алі Рашид Халіфа Бумекайр Альмансурі. Структура інфокомунікаційних цифрових ресурсів підприємства. *Економічна кібернетика: теорія, практика та напрямки розвитку* : Матеріали міжнар. наук.-практ. конф. 29-30 листопада 2022, Україна, м. Одеса, С.148-150. URL: https://economics.net.ua/files/science/ek_kiber/2022/tezy.pdf. (Дата звернення 20.01.2023) *(0,1 д.а.)*.

7. Ткач К.І., Алі Рашид Халіфа Бумекайр Альмансурі. Концептуальна структурно-логічна модель фокусного цифрового інфокомунікаційного забезпечення розвитку та діяльності підприємства. *Сучасні управлінські та соціально-економічні аспекти розвитку держави, регіонів та суб'єктів господарювання в умовах трансформації публічного управління*. Матеріали міжнар. наук. конф. 14 листопада 2024, Україна, м. Одеса. С.110-112. URL: https://economics.net.ua/files/science/admin_men/2024/tezy24.pdf. (Дата звернення 15.12.2024) *(0,15 д.а., особистий внесок: опис переваг фокусного цифрового інфокомунікаційного забезпечення розвитку підприємства в*

умовах криз – 0,1 д.а.).

8. Алі Рашид Халіфа Бумекайр Альмансурі. Зовнішні кризові фактори та їх вплив на цифрову інфраструктуру підприємств. *Обліково-аналітичне забезпечення інноваційної трансформації економіки України (в умовах воєнного стану та поствоєнний період)* : Матеріали всеукраїнської наук.-практ. конф. 24 листопада 2024, Україна, м. Одеса, С.170-172. URL: https://economics.net.ua/files/science/oblik/2024/Tezy.pdf. (Дата звернення: 15.01.2025) (*0,15 д.а.*).

9. Алі Рашид Халіфа Бумекайр Альмансурі. Архітектура та ключові елементи цифрового інфокомунікаційного забезпечення розвитку підприємства. *Сучасні управлінські та соціально-економічні аспекти розвитку держави, регіонів та суб´єктів господарювання в умовах трансформації публічного управління.* Матеріали міжнар. наук. конф. 14 листопада 2025, Україна, м. Одеса. С.55-57. URL: https://economics.net.ua/publ. (Дата звернення 17.11.2025) (*0,15 д.а.*).

10. Ткач К.І., Алі Рашид Халіфа Бумекайр Альмансурі. Міжнародна практика реагування на зовнішні кризові впливи щодо формування пріоритетів інвестування у цифрові технології та модернізацію цифрової інфраструктури: кейси ОАЕ. *Обліково-аналітичне забезпечення інноваційної трансформації економіки України (в умовах воєнного стану та поствоєнний період)* : Матеріали всеукраїнської наук.-практ. конф. 24 листопада 2025, Україна, м. Одеса, С.72-74. URL: https://economics.net.ua/oaz. (Дата звернення: 15.01.2025) *(0,15 д.а., особистий внесок: систематизація інвестиційних кейсів ОАЕ у сфері цифрових технологій (0,1 д.а.).*

11. Алі Рашид Халіфа Бумекайр Альмансурі. Управлінські виклики і трансформацій у системі менеджменту для ефективного впровадження цифрових інструментів. *Економічна кібернетика: теорія, практика та напрямки розвитку* : Матеріали міжнар. наук.-практ. конф. 27-28 листопада 2025, Україна, м. Одеса. С.280-286. URL: https://economics.net.ua/files/science/ek_kiber/2025/tezy25.pdf (Дата звернення 01.12.2025) *(0,1 д.а.).*

Додаток Б. Результати досліджень та апробація авторських методик

Б.1. Методика оцінювання цифрової зрілості підприємств

Мета методики – комплексне оцінювання рівня цифрової зрілості підприємства з урахуванням інфокомунікаційних, технологічних, організаційних та управлінських аспектів розвитку, а також забезпечення порівнянності результатів між підприємствами різних галузей.

Об'єкт і предмет оцінювання. Об'єктом оцінювання є підприємство як соціально-економічна система. Предметом оцінювання є рівень цифрової зрілості підприємства, сформований під впливом цифрових інфокомунікаційних рішень, управління даними, персоналом і процесами.

Ключові виміри цифрової зрілості. Оцінювання здійснюється за п'ятьма базовими вимірами, які відображають системну логіку цифрової трансформації підприємства: процеси; технології; дані; персонал; управління.

Кожен вимір розглядається як самостійна аналітична складова, що формується на основі набору субіндикаторів.

Система субіндикаторів. Для кожного виміру використовується 4–5 субіндикаторів, адаптованих до галузевої специфіки підприємства:

- процеси: рівень автоматизації, інтеграція процесів, гнучкість, використання BPM/RPA;
- технології: хмарні рішення, сучасність IT-архітектури, масштабованість, API-інтеграція;
- дані: централізація даних, бізнес-аналітика, прогнозування, data-driven управління;
- персонал: цифрові компетенції, готовність до змін, дистанційна взаємодія, навчання;
- управління: цифрова стратегія, KPI цифрової інфраструктури, антикризова готовність.

Субіндикатори формують аналітичну основу для кількісного оцінювання кожного виміру цифрової зрілості за п'ятибальною шкалою та дозволяють здійснювати як галузеві, так і міжкраїнові порівняння (табл.Б.1.1).

Шкала оцінювання. Кожен субіндикатор оцінюється за п'ятибальною шкалою:

1 – початковий (фрагментарний) рівень;
2 – обмежений рівень цифровізації;
3 – процесний (систематизований) рівень;
4 – інтегрований рівень;

5 – інтелектуальний (data-driven, оркестрований) рівень.

Продовження додатку Б

Таблиця Б.1.1 – Система субіндикаторів оцінювання цифрової зрілості підприємства

Вимір цифрової зрілості	Субіндикатор	Зміст субіндикатора (що оцінюється)
Процеси	Рівень автоматизації бізнес-процесів	Частка процесів, що виконуються з використан-ням цифрових систем та автоматизованих рішень
	Інтегрованість процесів	Наявність наскрізних (end-to-end) цифрових процесів між підрозділами
	Гнучкість процесів	Здатність процесів швидко адаптуватися до змін умов діяльності
	Використання BPM / RPA	Застосування систем управління процесами та роботизації
Технології	Сучасність IT-архітектури	Відповідність IT-інфраструктури сучасним архітектурним підходам
	Використання хмарних рішень	Рівень застосування SaaS, PaaS, IaaS
	Масштабованість інфраструктури	Здатність системи витримувати зростання навантажень
	API-інтеграції	Наявність та якість інтеграцій між цифровими платформами
Дані	Централізація та якість даних	Ступінь консолідації, повноти та актуальності даних
	Аналітичні інструменти	Використання інструментів бізнес-аналітики (BI)
	Прогнозна аналітика	Застосування моделей прогнозування та сценарного аналізу
	Data-driven управління	Використання даних як основи управлінських рішень
Персонал	Цифрові компетенції	Рівень володіння персоналом цифровими навичками
	Готовність до цифрових змін	Сприйняття персоналом цифрових трансформацій
	Дистанційна та цифрова взаємодія	Використання цифрових каналів комунікації та спільної роботи
	Навчання та розвиток	Наявність системи підвищення цифрових компетенцій
Управління	Цифрова стратегія розвитку	Наявність та реалізація стратегії цифрової трансформації
	KPI цифрової інфраструктури	Використання показників ефективності цифрових ресурсів
	Антикризова цифрова готовність	Здатність системи підтримувати управління в кризових умовах
	Інституційна підтримка цифровізації	Наявність організаційних структур та відповідальності

Продовження додатку Б

Розрахунок значень за окремими вимірами. Значення кожного виміру цифрової зрілості визначається як середнє арифметичне оцінок відповідних субіндикаторів:

$$D_i = \frac{1}{n}\sum_{j=1}^{n} d_{ij}$$

де

D_i– значення і-го виміру цифрової зрілості;

d_{ij}– оцінка j-го субіндикатора;

n– кількість субіндикаторів у межах виміру.

Розрахунок інтегрального рівня цифрової зрілості. Інтегральний показник цифрової зрілості підприємства визначається як середнє арифметичне значень усіх п’яти вимірів:

$$IDM = \frac{P + T + D + S + G}{5}$$

де

P– процеси;

T– технології;

D– дані;

S– персонал;

G– управління.

Інтерпретація результатів. На основі інтегрального показника визначається рівень цифрової зрілості підприємства:

4,1–5,0 – інтегрований / data-driven рівень;
3,0–4,0 – процесно-інтегрований рівень;
2,0–2,9 – процесний рівень;
1,0–1,9 – початковий рівень.

Продовження додатку Б

Б.2 Контурний опис цифрових рішень: процеси та інструменти

Б.2.1 Інфографіка основних етапів TAPXPHONE

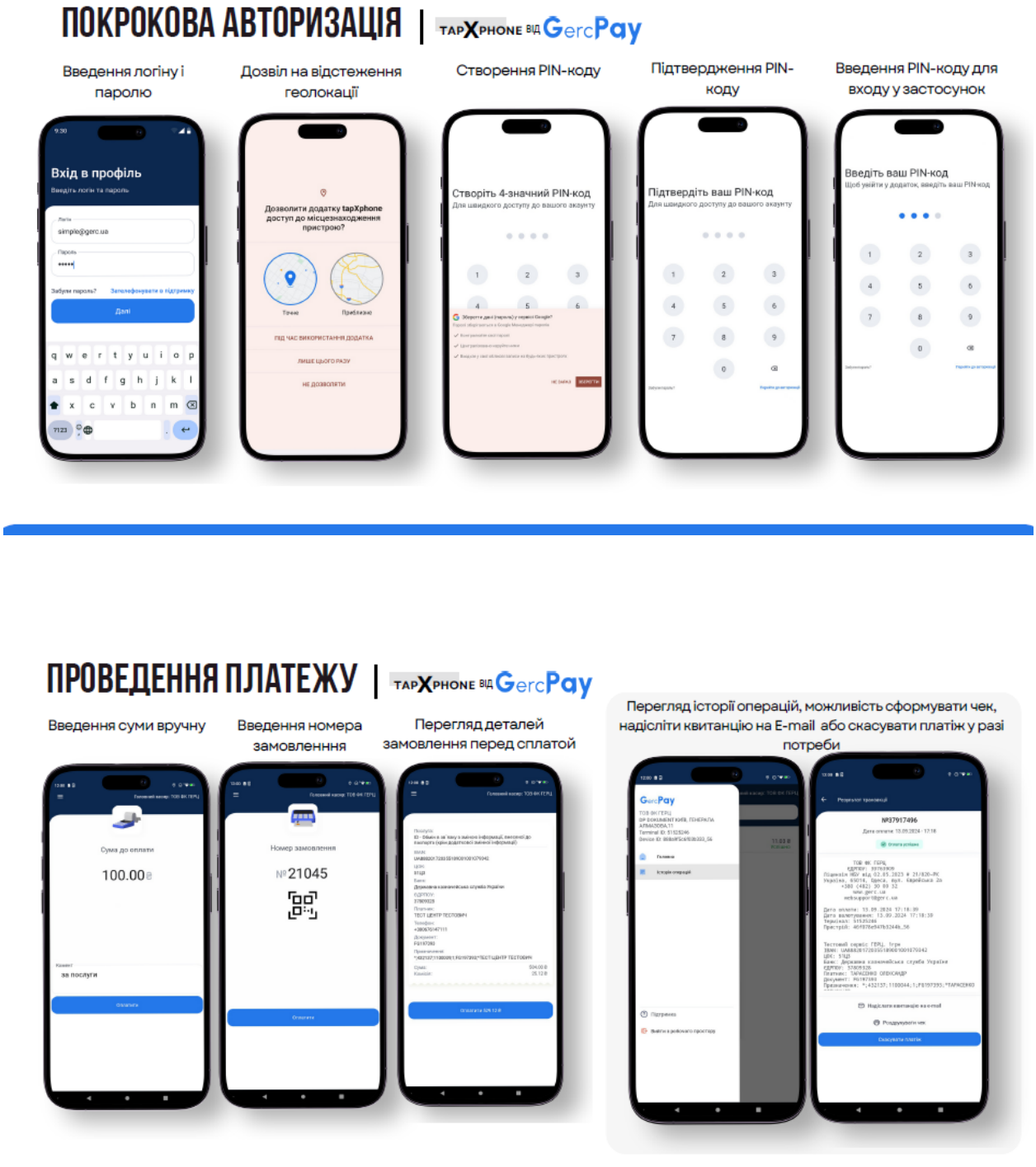
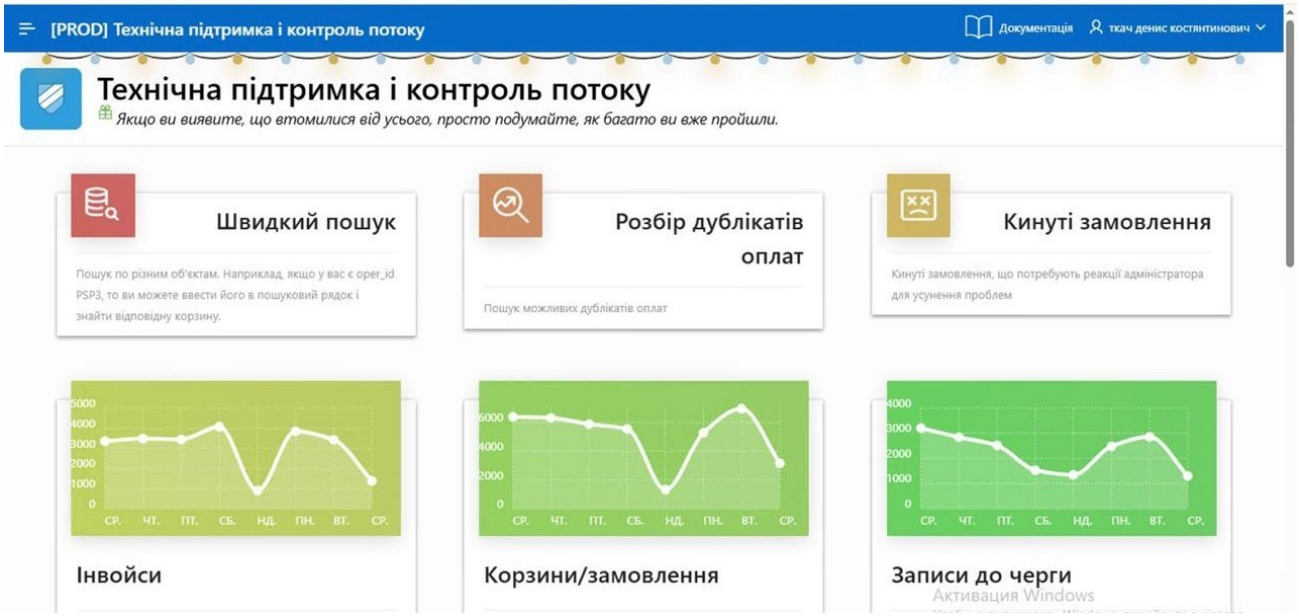


Рисунок Б.2.1.1 – Інфографіка основних етапів tapxphone

Продовження додатку Б

Б.2.2 Візуалізація процесів у цифровій інфраструктурі підприємства



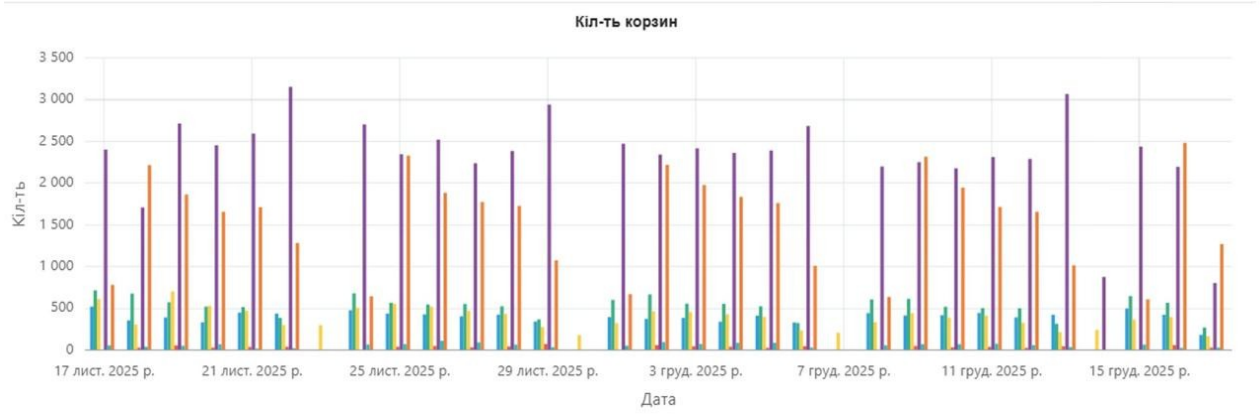


Рисунок Б.2.2.1 – Візуалізація процесів в цифровій інфраструктурі підприємства

Продовження додатку Б

Б.3 Обгрунтування комплексу стратегічних, архітектурних, методичних та оціночних інструментів для вирішення чотирьох ключових завдань цифрового інфокомунікаційного розвитку

Мета – удосконалити систему управління для вирішення чотирьох ключових завдань цифрового інфокомунікаційного розвитку:

1. Визначення сутності, особливостей та потреби у фокусному цифровому інфокомунікаційному забезпеченні, а також побудова структурно-логічної моделі.
2. Формулювання та обґрунтування принципів побудови інфокомунікаційної екосистеми підприємства.
3. Розроблення архітектури та ключових елементів цифрового інфокомунікаційного забезпечення розвитку підприємства.
4. Визначення KPI розвитку цифрової інфраструктури підприємства.

Припущення – *удосконалення системи управління підприємства у сфері інфокомунікаційного цифрового забезпечення забезпечується інтеграцією комплексного підходу*, який включає стратегічні, технологічні, архітектурні та оціночні інструменти.

Саме така інтеграція дозволяє підприємству ефективно вирішити чотири концептуально важливі завдання:

1. Визначення сутності, особливостей та потреби у фокусному цифровому інфокомунікаційному забезпеченні, а також побудова структурно-логічної моделі можливе завдяки:

- стратегічному аналізу цифрової зрілості підприємства (Digital Maturity Assessment)4
- аудиту IT-інфраструктури та інфокомунікаційних потоків;
- виділенню фокусних цифрових напрямів, що генерують найбільшу цінність (наприклад, автоматизація, кіберзахист, аналітика даних, CRM);
- методам системного моделювання (DFD, BPMN, IDEF0) для побудови структурно-логічної моделі цифрової підтримки бізнес-процесів.

Це дозволяє підприємству чітко визначити, *навіщо потрібне цифрове інфокомунікаційне забезпечення в кризових умовах*, які саме його компоненти є критичними та як вони взаємодіють.

2. Формулювання та обґрунтування принципів побудови інфокомунікаційної екосистеми підприємства. Підприємство може це зробити завдяки впровадженню таких управлінських інструментів:

- принципи системного підходу, які забезпечують цілісність цифрової екосистеми;
- принципи інтегрованості та інтероперабельності технологічних рішень;

– принципи кібергігієни та захищеності даних;
– Lean-підхід до оптимізації інформаційних потоків;
– побудова корпоративної IT-архітектури на основі стандартів TOGAF, COBIT або ITIL.

Ці інструменти дозволяють підприємству обґрунтувати правила, за якими має функціонувати сучасна інфокомунікаційна система як єдина екосистема.

3. Розроблення архітектури та ключових елементів цифрового інфокомунікаційного забезпечення розвитку підприємства. Удосконалити систему управління в цьому напрямі дозволяють:

– методологія архітектурного дизайну (TOGAF, Zachman Framework);
– принципи мікросервісної архітектури, які забезпечують гнучкість;
– картування інформаційних потоків та побудова "as-is" → "to-be" моделей;
– виділення ключових блоків архітектури:
    а) цифрова інфраструктура (обладнання, мережі, дата-центри);
    б) інформаційні системи (ERP, CRM, SCM);
    в) інфокомунікаційні сервіси (хмари, API, інтеграційні платформи);
    г) кіберзахист (IAM, SOC, DDoS-захист);
    д) аналітика та управління даними (DWH, BI);

Завдяки цьому підприємство отримує чітку архітектурну модель цифрового розвитку.

4. *Визначення KPI розвитку цифрової інфраструктури підприємства*. Цьому сприяє впровадження стандартних оціночних практик:

– KPI інфокомунікаційної ефективності:
    а) час обробки інформації;
    б) частка автоматизованих процесів;
    в) рівень доступності цифрових сервісів (uptime %);
    г) швидкість передачі та якості даних;
    д) індикатори кіберстійкості.
– фінансові показники ефективності цифрових рішень (ROI, NPV, TCO, Payback Period);
– побудова карти показників цифрової трансформації (Digital KPI Map).

Ці інструменти дозволяють об’єктивно виміряти ефективність інфокомунікаційного розвитку та оцінити прогрес.

Підсумкове узагальнення: удосконалити систему управління для розв’язання чотирьох ключових завдань підприємству дозволяє *комплекс стратегічних, архітектурних, методичних та оціночних інструментів*, які забезпечують цілісне бачення цифрового інфокомунікаційного розвитку, створення екосистеми, побудову архітектури та визначення KPI.

Продовження додатку Б

Б.4 Рейтингування стратегічних векторів цифрової трансформації

А. Опис 10 експертів, залучених до рейтингування стратегічних векторів цифрової трансформації та якості їх експертних оцінок.

1. Експерт з кібербезпеки та цифрової стійкості (15 років досвіду).

Профіль: керівник відділу кіберзахисту великої компанії, спеціалізація – кіберінциденти, криптозахист, SOC, управління цифровими ризиками.

Якість оцінки: висока – оцінки послідовні, аргументовані, ґрунтуються на практичних кейсах з воєнного часу.

2. Експерт з IT-архітектури та хмарних інфраструктур (12 років досвіду).

Профіль: архітектор хмарних рішень, сертифікований AWS/Azure, досвід впровадження гібридних систем у промисловому секторі.

Якість оцінки: висока – демонструє глибоке розуміння технічної стійкості, масштабованості та резервування.

3. Експерт зі штучного інтелекту та автоматизації (10 років досвіду).

Профіль: керівник лабораторії з машинного навчання, займається впровадженням RPA, NLP, ML у бізнес-процеси.

Якість оцінки: вище середньої – сильні технічні аргументи, але можливе переоцінювання ролі ШІ у кризових умовах.

4. Експерт з цифрової аналітики та BI-систем (11 років досвіду).

Профіль: спеціаліст із побудови систем предиктивної аналітики, ризик-моделювання та управлінських дашбордів.

Якість оцінки: висока – оцінки раціональні, базуються на реальних сценаріях прогнозування.

5. Експерт з управління ризиками та безперервністю діяльності (BCM) (14 років досвіду).

Профіль: консультант у сфері business continuity, crisis management, operational resilience.

Якість оцінки: дуже висока – один із найнадійніших експертів, продемонстрував глибоку системність.

6. Експерт з цифрової трансформації підприємств (18 років досвіду).

Профіль: управлінець, який відповідає за комплексні програми цифровізації, реінжиніринг процесів та диджитал-стратегії.

Якість оцінки: висока – досяг балансу між технічними та управлінськими аргументами.

7. Експерт з організаційного розвитку та управління персоналом (HR Tech) (13 років досвіду).

Профіль: спеціаліст у сфері цифрових HR-платформ, культури змін і компетентнісного розвитку персоналу.

Якість оцінки: середня – надає якісні аргументи, але іноді недооцінює технологічні аспекти.

8. Експерт зі стратегічного менеджменту та інновацій (20 років досвіду).

Профіль: консультант з інноваційних стратегій, впровадження нових бізнес-моделей, digital value creation.

Якість оцінки: вище середньої – сильна стратегічна логіка, але слабша технічна деталізація.

9. Експерт з клієнтського досвіду та цифрових комунікацій (8 років досвіду).

Профіль: фахівець з омніканальності, CRM, сервісних платформ, автоматизації

взаємодії з клієнтами.

Якість оцінки: середня – обґрунтовані, але з акцентом на клієнтських процесах, що знижує універсальність оцінок у системних кризах.

10. Експерт з IT-аудиту та відповідності стандартам (16 років досвіду).

Профіль: аудитор ISO 27001, 22301, консультант у сфері цифрових регуляцій та відповідності.

Якість оцінки: висока – чіткі, нормативно обґрунтовані, базуються на міжнародних практиках.

Таблиця Б. 4.1 – Узагальнена оцінка якості експертних оцінок

Показник	Висновок
1. Консистентність оцінок	Висока: більшість експертів погоджувалися щодо критичності кіберстійкості, BCM та хмарних систем.
2. Валідність	Висока: експерти мають багаторічний практичний досвід у відповідних цифрових сферах.
3. Різноманітність позицій	Забезпечена: експерти охоплюють технічні, управлінські та стратегічні аспекти.
4. Надійність середнього ранжування	Висока: відхилення між оцінками незначні, більшість ранжувань збігається.
5. Можливі обмеження	Певне переоцінювання ролі ШІ та клієнтських інновацій окремими фахівцями.

Б. Методика експертного оцінювання (комбінований підхід).

1. Вибір методів. Використовується поєднання трьох підходів, що підвищує валідність і надійність оцінок:

– метод Delphi (модифікована версія) використовувався для:
  а) збору індивідуальних оцінок експертів у першому раунді;
  б) узгодження позицій у другому раунді;
  в) виключення крайніх або упереджених думок.

  Перевага методу – анонімність експертів знижує груповий тиск і ефект авторитів.

– рангове оцінювання. Експерти здійснювали ранжування 10 стратегічних векторів за критерієм «значущості в умовах криз». Формат: 1 = найважливіший, … 10 = найменш важливий.

– метод Борда (Borda Count) застосовано для *визначення колективного рангу,* оскільки він дає:
  а) узагальнене зважене ранжування;
  б) стійкі результати при різниці в індивідуальних оцінках;
  в) можливість врахувати «середню думку».

  Сума балів = (10 – ранг експерта). Чим вища сума балів, тим вищий пріоритет вектора.

2. *Формування рангової матриці* – рангові оцінки експертів зводяться у таблицю:

Таблиця Б. 4.2 – Рангові оцінки експертів

Вектор	E1	E2	…	E10	Сума рангів
Вектор 1	1	2	…	1	...
Вектор 2	3	1	…	4	...
…	…	…	…	…	…

3. *Аналіз узгодженості.* Для оцінки того, наскільки узгоджено експерти оцінили 10 векторів, розраховується *коефіцієнт конкордації Кендалла (W)*:

$$W = \frac{12S}{m^2(n^3-n)},$$

де:

m – кількість експертів (10 осіб);

n – кількість об'єктів рейтингування (10);

$S = \sum(R_j - \bar{R})^2$;

R_j – сума рангів j-го вектора;

$\bar{R}$ – середнє значення сум рангів.

Критерій узгодженості:

$W = 0{,}7–1{,}0$ – висока узгодженість, експертні оцінки надійні;

$W = 0{,}5–0{,}7$ – середня узгодженість, допускається у соціально-економічних дослідженнях;

$W < 0{,}5$ – низька узгодженість, потрібний додатковий раунд Delphi.

4. Перевірка статистичної значущості проводиться через χ^2-критерій:

$$\chi^2 = m(n-1)W$$

Отримане значення порівнюється з табличним χ^2 при ступенях свободи = $n - 1 = 9$, рівень значущості $\alpha = 0.05$. Якщо $\chi^2_{emp} > \chi^2_{crit}$, то узгодженість статистично значуща.

6. *Розрахунок параметрів опитування. Рангова матриця* для 10 експертів, яка узгоджується з нашим підсумковим рейтингом векторів (1 – найважливіший, 10 – найменш важливий у кризу).

Таблиця Б.4.3 – Рангові оцінки стратегічних векторів цифрової трансформації підприємства 10 експертами

№	Стратегічний вектор	Експерти									
		1	2	3	4	5	6	7	8	9	10
		Рейтингування									
1	Кіберстійкість та інформаційна безпека	1	1	1	1	1	1	1	1	1	1
2	Цифрове управління ризиками та безперервністю діяльності (BCM)	2	2	2	2	2	2	2	3	2	2
3	Хмаризація та гібридні інфраструктури	3	3	3	3	3	3	4	2	3	3
4	Модульні цифрові екосистеми	4	4	4	4	4	4	3	4	4	4
5	Автоматизація та інтелектуалізація (RPA, AI)	5	5	6	5	5	5	5	5	5	5
6	Аналітика даних і прогнозування	6	6	5	7	6	6	6	6	6	6
7	Цифрова інтеграція бізнес-процесів	7	7	7	6	7	7	7	7	7	7
8	Розвиток цифрових компетентностей персоналу	8	8	8	8	9	8	8	8	8	8
9	Цифрова взаємодія з клієнтами та партнерами	9	9	9	9	8	9	9	9	9	10
10	Цифрові інновації та нові бізнес-моделі	10	10	10	10	10	10	10	10	10	9
(1 – найвищий пріоритет, 10 – найнижчий)											

Висновок: матриця відображує високу узгодженість експертів: перші три вектори мають ранги 1–3, а інновації та клієнтська взаємодія – найвищі (гірші) ранги.

Підсумкова таблиця сум рангів і середніх оцінок. На основі сформованої рангової матриці обчислено суму балів за кожним вектором.

Продовження додатку Б

Таблиця Б.4.4 – Підсумкові результати експертного рейтингування стратегічних векторів

Стратегічний вектор	Сума рангів (Rj)	Середній ранг	Підсумковий пріоритет
1. Кіберстійкість та інформаційна безпека	10	1,00	1
2. Управління ризиками та безперервністю (BCM)	21	2,10	2
3. Хмаризація та гібридні інфраструктури	30	3,00	3
4. Модульні цифрові екосистеми	39	3,90	4
5. Автоматизація та AI/RPA	51	5,10	5
6. Аналітика даних і прогнозування	61	6,10	6
7. Інтеграція бізнес-процесів	69	6,90	7
8. Цифрові компетентності персоналу	82	8,20	8
9. Цифрова взаємодія з клієнтами та партнерами	90	9,00	9
10. Цифрові інновації та нові бізнес-моделі	99	9,90	10

Проміжні підсумки:

– експерти демонструють високу узгодженість у перших трьох позиціях;
– останні три позиції також стабільні в оцінках.

Розрахунок коефіцієнта конкордації Кендалла W.

Крок 1. Розрахунок S:

Середня сума рангів:

$$\bar{R} = \frac{\sum R_j}{n} = \frac{10 + 21 + 30 + 39 + 51 + 61 + 69 + 82 + 90 + 99}{10} = 55{,}2$$

Обчислюємо:

$$S = \sum (R_j - \bar{R})^2$$

Обчислимо для кожного:

Rj	Rj – 55.2	(Rj – 55.2)²
10	–45,2	2040,04
21	–34,2	1169,64
30	–25,2	635,04
39	–16,2	262,44
51	–4,2	17,64
61	5,8	33,64
69	13,8	190,44
82	26,8	718,24
90	34,8	1211,04
99	43,8	1918,44

$$S = 2040{,}04 + 1169{,}64 + 635{,}04 + 262{,}44 + 17{,}64 + 33{,}64 + 190{,}44 + 718{,}24 + 1211{,}04 + 1918{,}44 = 8196{,}6$$

Крок 2. Підставлення у формулу *W*:

$$W = \frac{12S}{m^2(n^3 - n)}$$

де

m = 10 експертів;

n = 10 об’єктів.

$$W = \frac{12 \cdot 8196{,}6}{10^2(10^3 - 10)}$$
$$W = \frac{98359{,}2}{100 \cdot 990}$$
$$W = \frac{98359{,}2}{99000} = 0{,}994$$

Висновок щодо узгодженості думок експертів: узгодженість дуже висока (W = 0,994).

Крок 3. Перевірка значущості (χ^2)

$$\chi^2 = m(n-1)W = 10 \cdot 9 \cdot 0{,}994 = 89{,}46$$

Критичне χ^2 (*df*=9, α=0,05):

$$\chi^2_{crit} = 16{,}92$$

Висновок щодо значущості експертності: оскільки: $89{,}46 > 16{,}92$, узгодженість статистично значуща.

Зведена аналітична інтерпретація отриманих результатів. Результати експертного оцінювання стратегічних векторів цифрової трансформації в умовах криз продемонстрували практично абсолютну узгодженість думок фахівців. Значення коефіцієнта конкордації Кендалла *W* = 0,994, що відповідає дуже високому рівню узгодженості та свідчить про системність, продуманість і чіткість оцінок експертів. Перевірка за критерієм χ^2 підтвердила статистичну значущість узгодженості (χ^2 = 89,46 > χ^2crit), що дозволяє вважати отримані результати надійними та валідними для подальшого використання в моделі цифрової трансформації підприємства.

Важливі висновки:

а) експерти чітко виокремили перші три вектори як критично значущі для стійкості підприємства під час кризових ситуацій: кіберстійкість, управління ризиками та хмаризація. Ці напрями формують основу цифрового виживання й адаптації бізнесу;

б) найнижчі пріоритети отримали вектори, пов'язані з інноваціями, крос-організаційною взаємодією та компетентностями, що є типовим для кризових періодів, коли підприємства зосереджуються на оперативній стійкості, а не на стратегічному розвитку.

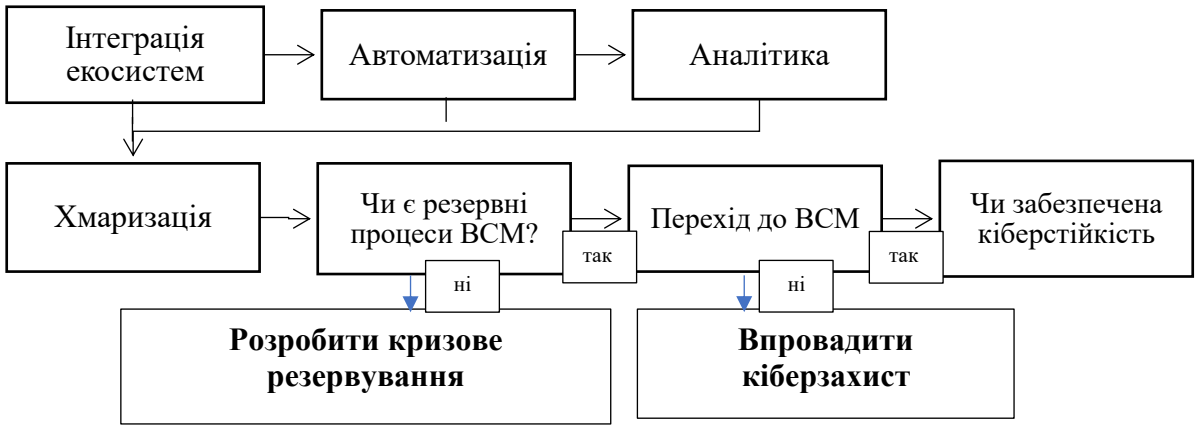


Рисунок Б.4.1 – Дерево рішень цифрової трансформації

Продовження додатку Б

Контурна карта приіоритетів стратегічних векторів цифрової трансформації

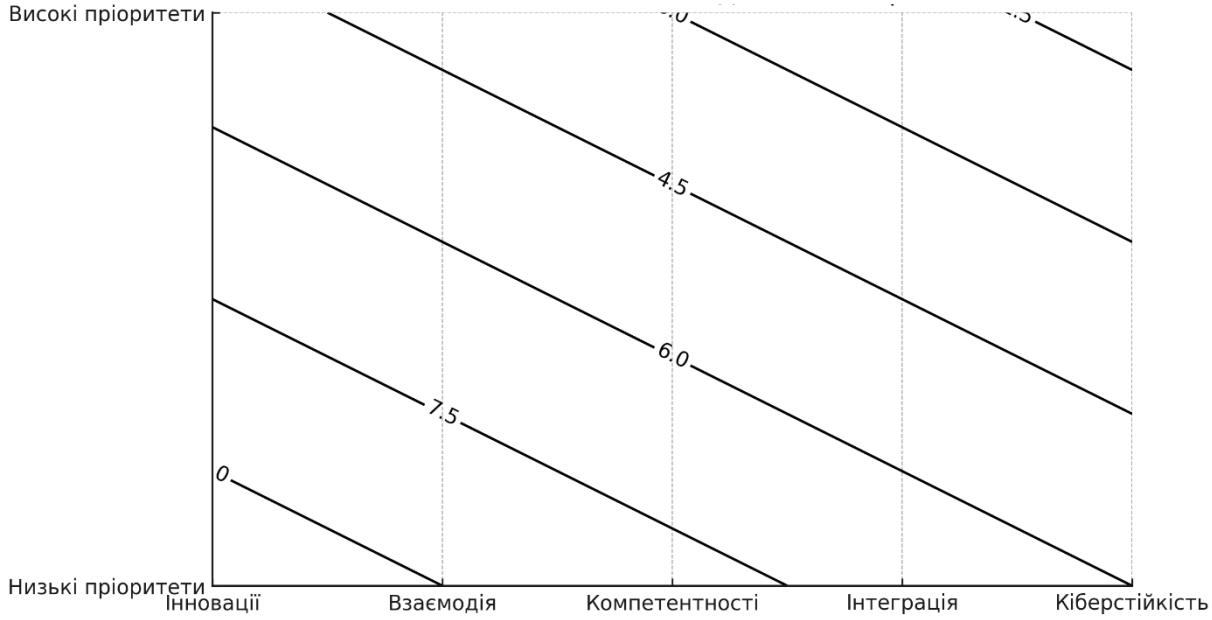


Рисунок Б.4.2 – Контурування приіоритетів стратегічних векторів цифрової трансформації

Зведена аналітична інтерпретація контурування приіоритетів стратегічних векторів цифрової трансформації. Отримана контурна карта пріоритетів демонструє просторовий розподіл важливості стратегічних векторів цифрової трансформації, побудований на основі згрупованих експертних рангів:

- у нижній частині карти розміщені контурні лінії з найвищими числовими значеннями (6–10), що відповідають векторами з низьким пріоритетом у кризових умовах: цифрові інновації, взаємодія з клієнтами та партнерами, розвиток цифрових компетентностей персоналу та інтеграція окремих бізнес-процесів. Вони визначаються як стратегічно важливі, але такі, що не забезпечують негайної стійкості підприємства в умовах турбулентності;
- у верхній частині контурної карти спостерігається різке зниження показників (1–3), що відображає зону високих пріоритетів. Саме тут концентруються ключові напрями — кіберстійкість, управління ризиками та безперервністю діяльності, а також хмаризація. Їх низькі рангові значення формують щільні контурні лінії, які вказують на одностайність експертів щодо критичної ваги цих векторів у забезпеченні стабільності підприємства під час кризи.

Висновки аналітична інтерпретація контурування приіоритетів стратегічних векторів цифрової трансформації:

по-перше, загальна форма ліній рівня свідчить про поступовий перехід від стратегічних, довгострокових напрямів до тактичних і операційних, які є необхідними для виживання бізнесу в умовах невизначеност;

по-друге, контурна карта демонструє логічну, структуровану ієрархію, де найвищі пріоритети зміщені до технологічних компонентів безпеки та стійкості, що узгоджується з результатами експертного рейтингування та підтверджує їхню високу конкордацію.

Продовження додатку Б

Б.5 Політика оцінювання цифрових ресурсів підприємства

1. Загальні положення

Політика оцінювання цифрових ресурсів встановлює принципи, критерії та процедури аналізу ефективності, стійкості та готовності цифрової інфраструктури підприємства до дії зовнішніх та внутрішніх кризових факторів. Метою політики є забезпечення системного підходу до вимірювання результативності цифрових рішень, підвищення рівня операційної надійності, кіберстійкості та адаптивності підприємства. Політика поширюється на всі цифрові платформи, інформаційні системи, канали комунікацій, аналітичні сервіси, автоматизовані бізнес-процеси, кіберзахисні механізми та технологічні рішення, що використовуються у діяльності підприємства.

2. Принципи оцінювання

Оцінювання цифрових ресурсів здійснюється відповідно до принципів:

Комплексності – охоплення технологічних, організаційних та комунікаційних компонентів цифрової системи.

Антикризової орієнтації – обов’язкове врахування впливу цифрових рішень на стійкість, безперервність та адаптивність підприємства.

Прозорості та відтворюваності – застосування стандартизованих інструментів оцінювання.

Операційної релевантності – прив’язка результатів оцінювання до реальних бізнес-процесів.

Постійного оновлення – регулярна ревізія показників у зв’язку зі зміною технологій та умов середовища.

3. Критерії оцінювання цифрових рішень

Оцінювання здійснюється за трьома базовими критеріями антикризової спроможності:

Стійкість (Resilience)

- здатність цифрових систем працювати у режимах підвищених навантажень;
- опірність технічним збоям, кібератакам та зовнішнім загрозам;
- стабільність архітектури та наявність захисних механізмів.

Безперервність (Continuity)

- забезпечення підтримки критично важливих процесів під час криз;
- мінімізація затримок, збоїв, операційних провалів;
- гарантування доступності цифрових ресурсів для користувачів.

Адаптивність (Adaptability)

- здатність систем швидко перебудовуватися відповідно до умов кризи;
- масштабованість, гнучкість бізнес-процесів та цифрових платформ;
- можливість швидкого впровадження нових інструментів.

4. Інструменти оцінювання

Підприємство використовує такі стандартизовані інструменти:

- Time-Saving Analysis – оцінювання швидкості виконання процесів та здатності системи забезпечувати безперервність операцій.
- Process Automation Index – визначення рівня автоматизації процесів як джерела стійкості та зменшення ризику людських помилок.
- Security Maturity Assessment – комплексний аналіз кіберстійкості, готовності до атак, швидкості реагування та відновлення.
- Productivity Metrics – оцінювання ефективності та стабільності операцій, продуктивності ресурсів.
- Operational Risk Assessment – аналіз вразливостей, що можуть порушити безперервність або стійкість діяльності.

Кожен інструмент прив'язується до відповідного критерію (стійкість, безперервність, адаптивність), що забезпечує системну оцінку цифрових рішень.

5. Процедура оцінювання

Оцінювання цифрових ресурсів здійснюється поетапно:

1. Ідентифікація цифрових рішень, що підлягають аналізу (платформи, сервіси, канали комунікації).
2. Визначення релевантних інструментів оцінювання для кожного цифрового компонента.
3. Збирання кількісних та якісних показників (час виконання, рівень автоматизації, інциденти безпеки тощо).
4. Оцінювання за критеріями стійкості, безперервності та адаптивності.
5. Побудова теплової карти або матриці відповідності (за необхідності).
6. Формування інтегрального цифрового профілю підприємства.
7. Підготовка рекомендацій з вдосконалення цифрової інфраструктури.

6. Очікувані результати впровадження політики

Реалізація політики забезпечить:

- підвищення рівня цифрової стійкості;
- мінімізацію ризиків операційних збоїв;
- прискорення реагування на кризові сценарії;
- надійність цифрової інфраструктури;
- зростання адаптивності організації;
- оптимальне використання цифрових інвестицій;
- формування аналітичної бази для стратегічного управління цифровими ресурсами.

7. Перегляд та оновлення політики

Політика переглядається щороку або у випадку:

- впровадження нових цифрових технологій;
- змін у регуляторному середовищі;
- появи нових загроз безпеці;
- значних кризових подій або збоїв у системах.

Б.6 Методика оцінювання ефективності інфокомунікаційних цифрових рішень малого підприємства (з апробацією)

Для обґрунтування доцільності інвестування малого ІТ-підприємства (П1) у цифрові рішення застосовуються такі ключові економічні показники: ROI, NPV, IRR, Cost–Benefit Analysis, TCO та Payback Period.

Кейс 1, побудований на даних підприємства П1.

1. ROI (Return on Investment)

1.1. Формула розрахунку:

$$ROI = \frac{\text{Вигоди} - \text{Інвестиції}}{\text{Інвестиції}} \times 100\%$$

1.2. Вихідні дані малого підприємства П1:

- інвестиції у CRM: 200 000 грн.;
- очікуване збільшення продажів та економія часу (грошовий ефект): 320 000 грн/рік.

1.3. Розрахунок

$$ROI = \frac{320\,000 - 200\,000}{200\,000} \times 100\% = 60\%$$

1.4. Інтерпретація отриманого результату: проєкт повертає вкладені кошти та генерує 60 % додаткової вигоди за рік – високий рівень ефективності.

2. NPV (Net Present Value)

2.1. Формула розрахунку:

$$NPV = \sum_{t=1}^{n} \frac{CF_t}{(1+r)^t} - I_0$$

2.2. Вхідні дані малого підприємства П1:

- інвестиції: 200 000 грн;
- річний грошовий потік: 250 000 грн.;
- горизонт оцінки: 3 роки;
- ставка дисконту: 12 %.

2.3. Розрахунок:

$$NPV = \frac{250\,000}{1.12} + \frac{250\,000}{1.12^2} + \frac{250\,000}{1.12^3} - 200\,000$$

$$NPV = 223\,214 + 199\,300 + 177\,946 - 200\,000 = 400\,460 \text{ грн}$$

2.4. Інтерпретація отриманого результату: NPV > 0 (значно), отже проєкт створює додану вартість та є фінансово доцільним.

3. IRR (Internal Rate of Return). IRR – це ставка *r*, за якої NPV=0:

Продовження додатку Б

3.1. Формула розрахунку:

$$0 = \sum_{t=1}^{n} \frac{CF_t}{(1+r)^t} - I_0$$

3.2. Вхідні дані малого підприємства П1:
- інвестиції: 200 000 грн;
- річний грошовий потік: 250 000 грн;
- період: 3 роки.

3.3. Розрахунок (наближено) – розв'язання методом підбору:
при r = 40% → NPV = +84 тис. при r = 55% → NPV ≈ -5 тис.
Висновок: IRR ≈ **53 %**

3.4. Інтерпретація отриманого результату: оскільки IRR (53%) >> вартості капіталу (12%), проєкт є надзвичайно вигідним.

4. Cost–Benefit Analysis (CBA)

4.1. Формула розрахунку:

$$CBA = \frac{\sum \text{Вигоди}}{\sum \text{Витрати}}$$

4.2. Вхідні дані малого підприємства П1:
- загальні витрати: 200 000 грн;
- вигоди за рік: 320 000 грн.

4.3. Розрахунок:

$$CBA = \frac{320\,000}{200\,000} = 1{,}6$$

4.4. Інтерпретація отриманого результату:
Як бачимо, на кожну 1 грн витрат підприємство отримує 1,6 грн вигоди – проєкт однозначно економічно доцільний.

5. TCO (Total Cost of Ownership) – повна вартість володіння

5.1. Формула розрахунку:

$$TCO = \text{Прямі витрати} + \text{Непрямі витрати}$$

5.2. Структура витрат малого підприємства П1

Стаття	Сума, грн
1. Закупівля CRM	120 000
2. Встановлення і інтеграція	30 000
3. Ліцензії (річні)	25 000
4. Навчання персоналу	10 000
5. Підтримка	15 000
Разом TCO	200 000

5.3. Інтерпретація отриманого результату: ТСО дозволяє об’єктивно оцінити реальну ціну цифрового рішення та уникнути занижених прогнозів.

6. Payback Period – строк окупності
6.1. Формула розрахунку:

$$Payback = \frac{\text{Інвестиції}}{\text{Середній річний грошовий потік}}$$

6.2. Розрахунок:

$$Payback = \frac{200\,000}{250\,000} = 0.8 \text{ року}$$

6.3. *Анаалітитчна інтерпретація отриманих результатів:* цифровий проєкт окупиться менш ніж за 10 місяців, що є прийнятним та низькоризиковим для малого бізнесу.

Висновок: розраховані показники демонструють, що *цифровізація малого підприємства за умовними даними є економічно обґрунтованою*, оскільки характеризується високою прибутковістю (ROI 60 %, IRR ≈ 53 %, NPV > 400 тис. грн) та швидким поверненням інвестицій (менше 1 року), а застосовані методи дозволили системно оцінити фінансову ефективність цифрових рішень і знизити ризики прийняття інвестиційних рішень.

Продовження додатку Б

Б.7 Паспорти інструментів як цифрових рішень

7.1 Паспорт цифрового рішення: кейс 1.

1. Загальні відомості про інструмент

Назва продукту: Багатовимірна методика оцінювання результативності та цифрової стійкості інфокомунікаційних ресурсів (БМ ОР-ЦІКР).

Призначення: формалізований інструмент діагностики рівня цифрової зрілості та оцінки внеску цифрових інфокомунікаційних ресурсів (ЦІКР) у забезпечення операційної результативності, фінансової ефективності та підвищення цифрової стійкості (Digital Resilience) підприємства в умовах криз.

Розробник – Алі Рашид Халіфа Бумекайр Альмансурі (науковий керівник: д.е.н., доцент Ткач Костянтин Іванович).

Тип інструменту – методика оцінювання (аналітична модель).

Об'єкт застосування – інфокомунікаційні ресурси (ЦІКР) критичних бізнес-процесів (технологічні, інформаційні, комунікаційні, інфраструктурні, кібербезпекові).

Сфера застосування – стратегічний та антикризовий менеджмент, IT-управління, фінансове планування інвестицій у цифровізацію.

2. Функціональні можливості та призначення

Критерій	Функціональна можливість (що дозволяє оцінити)
Фінансова ефективність (Блок I)	Оцінка інвестиційної привабливості ЦІКР, включаючи розрахунок ROI та Строку окупності (PP) з урахуванням повного циклу витрат (CapEx + OpEx), що є удосконаленням базових фінансових моделей.
Операційна результативність (Блок II)	Вимірювання внеску ЦІКР у розвиток підприємства через нефінансові показники: рівень автоматизації *($I_{автом}$),* Якість даних *($P_{даних}$)* та Швидкість координації *($T_{коорд}$).*
Цифрова стійкість (Блок III)	Діагностика антикризової спроможності підприємства. Оцінка здатності ЦІКР забезпечувати безперервність діяльності та протидіяти загрозам через метрики часу відновлення (RTO) та індексу кібербезпеки *($I_{безпека}$).*
Інтегральна оцінка	Формування інтегрального показника результативності ЦІКР $(I_{\Sigma}^{ЦІКР})$ що враховує стратегічні пріоритети (вагові коефіцієнти wj) для прийняття зважених рішень.

3. Методологічні та технічні параметри

Параметр	Опис
1	2
1. Базові метрики	$C_П$, C_{OpEx}, D_P, $I_{автом}$, $P_{даних}$

Продовження додатку Б

Продовження табл.

1	2
2. Ключові метрики стійкості	RTO (Recovery Time Objective – час відновлення), $I_{безпека}$ (індекс кібербезпеки), $K_{крит}$ (коефіцієнт покриття критичних процесів).
3. Інтегральний розрахунок	$I_{\Sigma}^{\text{ЦІКР}} = \sum_{j=1}^{3} w_j \cdot I_j$
4. Шкала оцінювання	Від 0 до 1 (для індексів); грн./валюта (для фінансових показників); години/хвилини (для часових метрик стійкості).
5. Алгоритмічна основа	Зважене усереднення індексів, розрахунок *ROI* та *PP* із повним урахуванням OpEx.

4. Вимоги та умови застосування

Вимоги	Зміст
1. Інституційна готовність	Офіційне визнання керівництвом цифрової стійкості як стратегічного пріоритету та затвердження вагових коефіцієнтів (w*j*).
2. Інформаційна база	Наявність систем централізованого обліку витрат ($C_{П}$, C_{OpEx}) та впровадження систем логування та моніторингу для збору метрик *RTO*, $I_{безпека}$ та $T_{коорд}$.
3. Процесна готовність	Формалізація та документування критичних бізнес-процесів ($N_{крит}$) та наявність актуальної мапи автоматизації.
4. Технічна підтримка	Впровадження рішень BDR (Backup & Disaster Recovery) та систем SIEM/SOC для моніторингу загроз і фіксації інцидентів ($N_{інцид}$).
5. Кадрові компетенції	Залучення експертів з IT-архітектури, кібербезпеки та фінаналізу для якісної оцінки індексу адаптивності ($I_{адапт}$), верифікації даних.

5. Ризики та обмеження застосування

Ризик	Зміст
1. Суб'єктивність оцінки	Неправильне (упереджене) визначення вагових коефіцієнтів (w_j) та якісна оцінка $I_{адапт}$, що може спотворити інтегральний результат.
2. Ненадійність вихідних даних	Відсутність автоматизованого збору метрик (наприклад, ручний збір RTO) призводить до неточності показників стійкості та ризиків.
3. Опір змінам	Недостатня готовність персоналу IT-підрозділу до формалізації процесів та регулярної звітності за новими метриками.
4. Часткова релевантність	Методика не оцінює зовнішні (несистемні) фактори, такі як політичні чи ринкові ризики, що безпосередньо не пов'язані з ЦІКР.

6. Очікувані результати та ефекти

Результат	Ефект для підприємства
1. Підвищення цифрової стійкості	Мінімізація операційних та кібернетичних ризиків, скорочення часу простою (RTO) та забезпечення безперервності критичних процесів в умовах кризи.
2. Оптимізація інвестицій	Перехід від інвестицій з фокусом лише на дохід (D_P) до з фокусом на стійкість і розвиток $(I_{\Sigma}^{\text{ЦІКР}})$, що підвищує захищеність активів.
3. Об'єктивна діагностика	Формування аналітичної бази прийняття проактивних управлінських рішень з модернізації ЦІКР, усунення ключових вразливостей.
4. Підвищення управлінської прозорості	Можливість порівняльної оцінки ефективності ЦІКР у різних функціональних підрозділах або порівняння з галузевими бенчмарками.

Продовження додатку Б

7.2 Паспорт цифрового рішення: кейс 2.

Назва продукту: TAPXPHONE GercPay (технологічне рішення для прийому платежів).

Призначення: забезпечення можливості для бізнесу приймати безконтактну оплату за товари та послуги за допомогою звичайного смартфона, оснащеного технологією NFC.

1. Загальні відомості про інструмент

Параметр	Характеристика
Розробник/ Провайдер	ТОВ ФК ГЕРЦ (GercPay)
Тип інструменту	Інфокомунікаційний цифровий ресурс (Платіжна система / SoftPOS-рішення)
Об'єкт застосування	Суб'єкти підприємницької діяльності (бізнес) у сфері торгівлі та послуг, які потребують мобільної та гнучкої точки прийому платежів.
Сфера застосування	Електронна комерція, мобільна торгівля, сфера послуг, кур'єрська доставка, малий та середній бізнес, що працює в умовах високої мобільності.

2. Функціональні можливості та призначення

Критерій	Функціональна можливість
Прийом платежів	Прийом оплати за допомогою безконтактних банківських карт, смартфонів, розумних годинників та інших NFC-пристроїв.
Операційна гнучкість	Перетворення стандартного смартфона на повноцінний платіжний інструмент.
Зручність комунікації	Швидка, зручна та безпечна транзакція.
Інтеграція	Сумісність з платіжними системами VISA та електронними гаманцями (GPay).

3. Технічні параметри

Параметр	Опис
Ключова технологія	NFC (Near Field Communication).
Мінімальні вимоги до обладнання	Смартфон з підтримкою технології NFC.
Архітектура	Програмне забезпечення (мобільний застосунок), яке функціонує як віртуальний POS-термінал.
Безпека	Забезпечення захисту на рівні безконтактних банківських операцій (підкреслюється, що рішення безпечне).

Продовження додатку Б

4. Витрати та умови застосування

Вимоги/Умови	Зміст
Умови застосування	Необхідність приймати безконтактні платежі.
Первинні (капітальні) витрати *(C_n)*	Мінімальні: Обладнання не потрібне (використовується наявний NFC-смартфон).
Операційні витрати (C_{OpEx})	Комісійна плата за транзакцію (відсоток від платежу) згідно з тарифами GercPay.
Економія	Значне скорочення витрат на придбання та обслуговування класичних POS-терміналів.

5. Ризики та обмеження застосування

Ризик	Зміст
Технологічні ризики	Залежність від наявності NFC-модуля та технічної справності смартфона. Ризик розрядки акумулятора.
Комунікаційні ризики	Потреба у стабільному підключенні до Інтернету (мобільного зв'язку) для обробки транзакцій.
Кібербезпекові ризики	Залежність від операційної безпеки смартфона-носія та оновлень програмного забезпечення.
Обмеження обробки	Обмеження роботи платіжної системи GercPay та її партнерів.

6. Очікувані результати та ефекти

Результат	Ефект для підприємства
Підвищення мобільності	Максимум мобільності, можливість приймати платежі будь-де.
Оптимізація витрат	Мінімум обладнання, економія на касовому/банківському обладнанні.
Зростання прибутку (Фінансовий)	Збільшення швидкості обслуговування та розширення каналів збуту (збільшення обсягу прийнятих платежів).
Покращення досвіду клієнта	Швидке та зручне обслуговування, що підвищує лояльність клієнтів.

Додаток В

Україна
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»

КОД ЄДРПОУ 43861328

пр.Шевченка, 1, м.Одеса, 65044
Україна
тел. +38 048 7223474
факс. +38 048 7221992
E-mail: mail@op.edu.ua

05.12.2025 № 1950/64-07
на №

ЗАТВЕРДЖУЮ
Проректор,
д.т. техн., наук, проф.
Дмитро ДМИТРИШИН
«__» _____ 2025 р.

АКТ

використання результатів дисертаційної роботи
Алі Рашид Халіфа Бумекайр Альмансурі на тему «Інфокомунікаційні цифрові ресурси забезпечення розвитку підприємства в умовах криз»
у науково-дослідницькій діяльності Національного університету «Одеська політехніка»

Цей акт виданий Алі Рашид Халіфа Бумекайр Альмансурі в тому, що його дисертацію на тему «Інфокомунікаційні цифрові ресурси забезпечення розвитку підприємства в умовах криз» виконано згідно тематичних планів НДР Національного університету «Одеська політехніка» у 2021-2024 рр., а саме: № 155-71 «Менеджмент як фактор сталого розвитку в координатах парадигми економічних систем» (*номер державної реєстрації 0118U006802, 2018-2022 рр.*), де автором досліджено теоретичні підходи та моделі впливу цифрових ресурсів на розвиток і стійкість підприємства; НДР № 233-71 «Стратегічні імперативи менеджменту організацій в умовах глобалізаційних ризиків та кризових явищ» (*номер державної реєстрації 0123U101755*), 2023-2026 рр., де автором розроблено концептуальну модель фокусного інфокомунікаційного цифрового забезпечення розвитку підприємства; розроблено рекомендації щодо оцінювання інфокомунікаційних цифрових рішень підприємства, обґрунтовано науково-методичні засади формування інфокомунікаційної цифрової стратегії підприємства з урахуванням кризових умов; госпдоговірній НДР № 1847-81 «Діджитал-трансформація системи управління виробничого бізнесу: проблеми, перспективи, фактори адаптивності» *(27.10.2021-27.10.2022 р.)*, де автором проаналізовано зовнішні кризові фактори та їх вплив на цифрову інфраструктуру підприємства.

Дисертант приймав участь у виконанні вказаних тем як співвиконавець.

Керівник НДР №0118U006802, № 0123U101755
д.е.н., професор — Оксана ПРОДІУС

Керівник НДР № 1847-81
д.е.н., професор — Ксенія КОВТУНЕНКО

Продовження додатку В

Україна
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»

КОД ЄДРПОУ 43861328

пр.Шевченка, 1, м.Одеса, 65044
Україна
тел. +38 048 7223474
факс. +38 048 7221992
E-mail: mail@op.edu.ua

05.12.2015 № 1951/67-07
на №

ЗАТВЕРДЖУЮ
Перший проректор,
проректор з науково-педагогічної
та виховної роботи
д.т.н., професор Сергій НЕСТЕРЕНКО

АКТ

використання результатів дисертаційної роботи

Алі Рашид Халіфа Бумекайр Альмансурі

«Інфокомунікаційні цифрові ресурси забезпечення розвитку підприємства в умовах криз»

у навчальному процесі Національного університету «Одеська політехніка»

Цим актом підтверджується, що у програмі навчальної дисципліни, навчально-методичних матеріалах та курсі лекцій з дисциплін, використовуються окремі науково-прикладні результати, отримані у дисертації Алі Рашид Халіфа Бумекайр Альмансурі на тему «Інфокомунікаційні цифрові ресурси забезпечення розвитку підприємства в умовах криз», а саме:

«Інфокомунікації в освіті, науці і бізнесу» (сторінка освітньої компоненти на сайті Одеської політехніки: https://op.edu.ua/education/programs/components/6562), що вивчається здобувачами за шістьма освітньо-професійними програмами (другий освітньо-науковий рівень) – діджиталізаційні та смарт-моделі управління, концепції цифрової стійкості, інфокомунікаційні платформи, структура інфокомунікаційних систем (лекція №5. Інформаційно-комунікаційні технології в бізнесі: види та можливості застосування).

«Наукові дослідження в сфері менеджменту» (сторінка освітньої компоненти на сайті Одеської політехніки: https://op.edu.ua/education/programs/components/8920), що вивчається здобувачами спеціальності 073 «Менеджмент» за освітньо-науковою програмою «Менеджмент» (третій освітньо-науковий рівень) – концептуальна модель, інструменти та методичні підходи до фокусного цифрового інфокомунікаційного забезпечення розвитку підприємства (лекція 8. Інфокомунікаційні цифрові ресурси управління розвитком підприємства).

Голова методичної ради ІЕМ, д.е.н., проф. Олександр БАЛАН

Завідувачка кафедри міжнародного менеджменту та інновацій, д.е.н., проф. Ксенія КОВТУНЕНКО

Завідувачка кафедри обліку, аналізу і аудиту, д.е.н., проф. Лідія ВОЛОЩУК

Продовження додатку В

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
ФІНАНСОВА КОМПАНІЯ ГЕРЦ

Україна, м. Одеса, 65014
Вул. Єврейська, буд. 2А
+38 0482 30 00 32
gerc@gerc.ua

Україна, м. Київ, 01001
Вул. Хрещатик, 18/2
+38 044 300 04 30
gerc@gerc.ua

Ліцензія НБУ від 2 травня 2023 року № 21/820 - РК

www.gerc.ua www.gerc.ua www.gerc.ua www.gerc.ua

Довідка № 25/12-23/02 від 23.12.2025 р.

Про впровадження результатів дисертаційного дослідження

Алі Рашид Халіфа Бумекайр Альмансурі

на тему: «Цифрові інфокомунікаційні ресурси забезпечення розвитку підприємства в умовах криз»

Довідка видана Алі Рашид Халіфа Бумекайр Альмансурі в тому, що запропоновані ним авторські розробки – рекомендації щодо проєктування інфокомунікаційної цифрової системи підприємства, а також методику паспортизації цифрових рішень та інструментів для методів оцінювання інфокомунікаційних цифрових рішень – прийнято до впровадження в діяльність ТОВ «ФК «ГЕРЦ»».

Представлені Алі Рашид Халіфа Бумекайр Альмансурі рекомендації та методика є застосовними у практиці управління проєктами підприємства, що підтверджується керівництвом та персоналом ТОВ «ФК «ГЕРЦ»».

Директор _____ Ганна СУШКІНА

Продовження додатку В

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
ГЕРЦ

Україна, м.Одеса, 65014
Вул. Єврейська, буд 2А
+38 0482 30 00 32
gerc@gerc.ua

Україна, м.Київ, 01001
Вул. Хрещатик, 18/2
+38 044 300 04 30
gerc@gerc.ua

www.gerc.ua www.gerc.ua www.gerc.ua www.gerc.ua

Довідка №25/12-23/01 від 23.12.2025 р.

Про впровадження результатів дисертаційного дослідження

Алі Рашид Халіфа Бумекайр Альмансурі

на тему: «Цифрові інфокомунікаційні ресурси забезпечення розвитку підприємства в умовах криз»

Довідка видана в тому, що результати дисертаційної роботи, запропоновані Алі Рашид Халіфа Бумекайр Альмансурі, розглянуто керівництвом та прийнято до впровадження в діяльність ТОВ «ГЕРЦ», а саме:

- критеріально-орієнтований добір інструментів, застосовних для формування організаційних (скорочення часу, автоматизація, безпека) та антикризових (стійкість, безперервність, адаптивність) ефектів;
- багатовимірна методика з рекомендаціями щодо оцінювання результативності та цифрової стійкості інфокомунікаційних цифрових рішень.

Розроблені Алі Рашид Халіфа Бумекайр Альмансурі науково-методичні рекомендації щодо оцінювання результативності та цифрової стійкості інфокомунікаційних цифрових рішень є актуальними та корисними для підприємства, що підтверджується керівництвом ТОВ «ГЕРЦ».

В.о. Генерального директора **Олена ПИСАНА**