

DOI: 10.15276/ETR.02.2025.16
DOI: 10.5281/zenodo.18039087
UDC: 004.77:658.012.4
JEL: M15, O33, L86, M15, G01

СИСТЕМНЕ ЦИФРОВЕ ІНФОКОМУНІКАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ РОЗВИТКУ ПІДПРИЄМСТВА: ФОКУСУВАННЯ В УМОВАХ КРИЗ

SYSTEMATIC DIGITAL INFORMATION AND COMMUNICATION SUPPORT FOR ENTERPRISE DEVELOPMENT: FOCUSING IN TIMES OF CRISIS

Kostyantyn I. Tkach, Doctor of Economic Sciences, Professor
Odesa Polytechnic National University, Odesa, Ukraine
Email: tkach.k.i@op.edu.ua

Ali Rashed Khalifa Bumeqairaa Almansoori
Odesa Polytechnic National University, Odesa, Ukraine
ORCID: 0009-0005-1875-4884

Received 29.03.2025

Сучасні кризові явища, зумовлені поєднанням економічної нестабільності, геополітичних викликів, прискорення технологічних змін та зростання невизначеності зовнішнього середовища, суттєво трансформують умови функціонування підприємств. За таких обставин цифрові інфокомунікаційні ресурси перестають виконувати виключно допоміжну роль і набувають системного значення як ключовий чинник забезпечення безперервності діяльності, адаптивності управління та стійкості розвитку підприємства. Саме якість, узгодженість і цілеспрямованість цифрового інфокомунікаційного забезпечення визначають здатність підприємства своєчасно реагувати на кризові збурення та формувати передумови для подальшого відновлення і зростання.

Разом із тим у практиці управління домінують фрагментарні підходи до впровадження цифрових рішень, орієнтовані переважно на автоматизацію окремих бізнес-процесів або впровадження ізольованих інформаційних систем. Відсутність системного бачення цифрового інфокомунікаційного забезпечення, неузгодженість стратегічних цілей розвитку підприємства з цифровими ініціативами, а також недостатня увага до інтеграції інформаційних потоків і управлінських контурів знижують ефективність використання цифрових ресурсів, особливо в умовах кризових обмежень ресурсів і підвищених ризиків. У наукових дослідженнях цифрову трансформацію здебільшого розглядають крізь призму технологічного оновлення або підвищення операційної ефективності, тоді як питання системного цифрового інфокомунікаційного забезпечення розвитку підприємства та механізмів його цілеспрямованого фокусування в умовах криз залишаються недостатньо розкритими. Це обумовлює потребу в поглибленні теоретичних підходів до трактування інфокомунікаційних цифрових ресурсів як цілісної

Ткач К.І., Алі Рашид Халіфа Бумекайр Альмансурі.
Системне цифрове інфокомунікаційне забезпечення розвитку підприємства: фокусування в умовах криз. Науково-методична стаття.

Стаття присвячена обґрунтуванню концептуальних засад системного цифрового інфокомунікаційного забезпечення розвитку підприємства та визначення напрямів його фокусування в умовах кризових викликів. Визначено сутність та особливості фокусного цифрового інфокомунікаційного забезпечення розвитку та діяльності підприємства, обґрунтовано потребу в ньому для підприємства в умовах кризи та розроблено його концептуальну структурно-логічну модель. Сформульовано та обґрунтовано принципи побудови інфокомунікаційної екосистеми. Розроблено архітектуру та ключові елементи цифрового інфокомунікаційного забезпечення розвитку підприємства. Визначено КРІ розвитку цифрової інфраструктури підприємства в блоці цифрового інфокомунікаційного забезпечення розвитку підприємства.

Ключові слова: інфокомунікації, цифрове інфокомунікаційне забезпечення, розвиток, фокусування, підприємство, цифровізація, криза

Tkach K.I., Ali Rashed Khalifa Bumeqairaa Almansoori.
Systematic Digital Information and Communication Support for Enterprise Development: Focusing in Times of Crisis. Scientific and methodical article.

The article is devoted to substantiating the conceptual foundations of systematic digital information and communication support for enterprise development and determining the areas of its focus in conditions of crisis challenges. The essence and features of focused digital information and communication support for enterprise development and activities are defined, the need for it for enterprises in crisis conditions is substantiated, and its conceptual structural and logical model is developed. The principles of building an information and communication ecosystem are formulated and substantiated. The architecture and key elements of digital information and communication support for enterprise development are developed. KPIs for the development of the enterprise's digital infrastructure in the block of digital information and communication support for enterprise development are determined.

Keywords: infocommunications, digital infocommunications support, development, focus, enterprise, digitalisation, crisis

управлінської системи, здатної забезпечувати координацію рішень, прозорість інформаційних потоків і підтримку стратегічних пріоритетів розвитку.

Метою статті є обґрунтування концептуальних засад системного цифрового інфокомунікаційного забезпечення розвитку підприємства та визначення напрямів його фокусування в умовах кризових викликів. Для її виконання необхідно виконати такі завдання:

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

б) сформулювати та обґрунтувати принципи побудови інфокомунікаційної екосистеми;

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

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

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.

Аналіз останніх досліджень та публікацій

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 напрямках 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. 1).

Таблиця 1. Переваги фокусного цифрового інфокомунікаційного забезпечення розвитку підприємства в умовах криз

Перевага	Зміст переваги (розгорнутий опис)
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 управлінських рішень	Оперативний обмін даними, доступ до цифрових платформ у реальному часі та централізація 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 прогностичних 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.

Джерело: власна розробка авторів

Водночас, порівняння фокусного та традиційного цифрового інфокомунікаційного забезпечення діяльності та розвитку підприємства за

дванадцятьма критеріями (табл. 2) демонструє як переваги першого, так і його недоліки.

Таблиця 2. Порівняння фокусного та традиційного цифрового інфокомунікаційного забезпечення підприємства

Критерій порівняння	Фокусне цифрове інфокомунікаційне забезпечення	Традиційне цифрове забезпечення
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.
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.

Джерело: складено авторами за матеріалами [1-10]

Виклад основного матеріалу дослідження

Порівняння фокусного цифрового інфокомунікаційного забезпечення та традиційних підходів до цифровізації підприємства (див. табл. 1-2) 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 пріоритизації критичних процесів, централізації інформаційних потоків, багаторівневого кіберзахисту та швидкої масштабованості цифрової інфраструктури, що дозволяє підприємству підтримувати керування 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. 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.

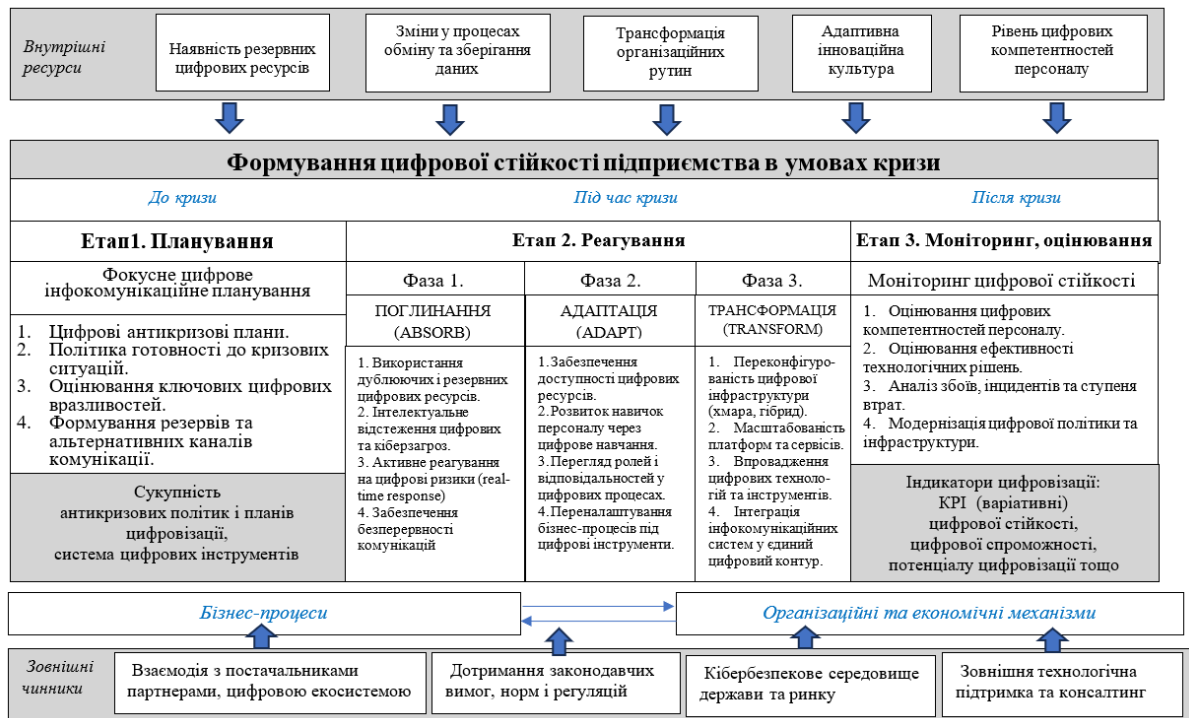


Рисунок 1. Модель формування цифрової стійкості підприємства на основі фокусного цифрового інфокомунікаційного забезпечення

Джерело: власна розробка авторів

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 застосування наведених принципів в умовах цифровізації та кризи доводять аргументи, наведені у табл. 3.

Таблиця 3. Принципи побудови інфокомунікаційної екосистеми: доцільність

Принцип	Обґрунтування доцільності
1. Адаптивність	Швидка перебудова 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.
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 швидкості 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 проектування є критично необхідною.

Джерело: власна розробка авторів

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.

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 [3-7].

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. 2).

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 прогнозування 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.

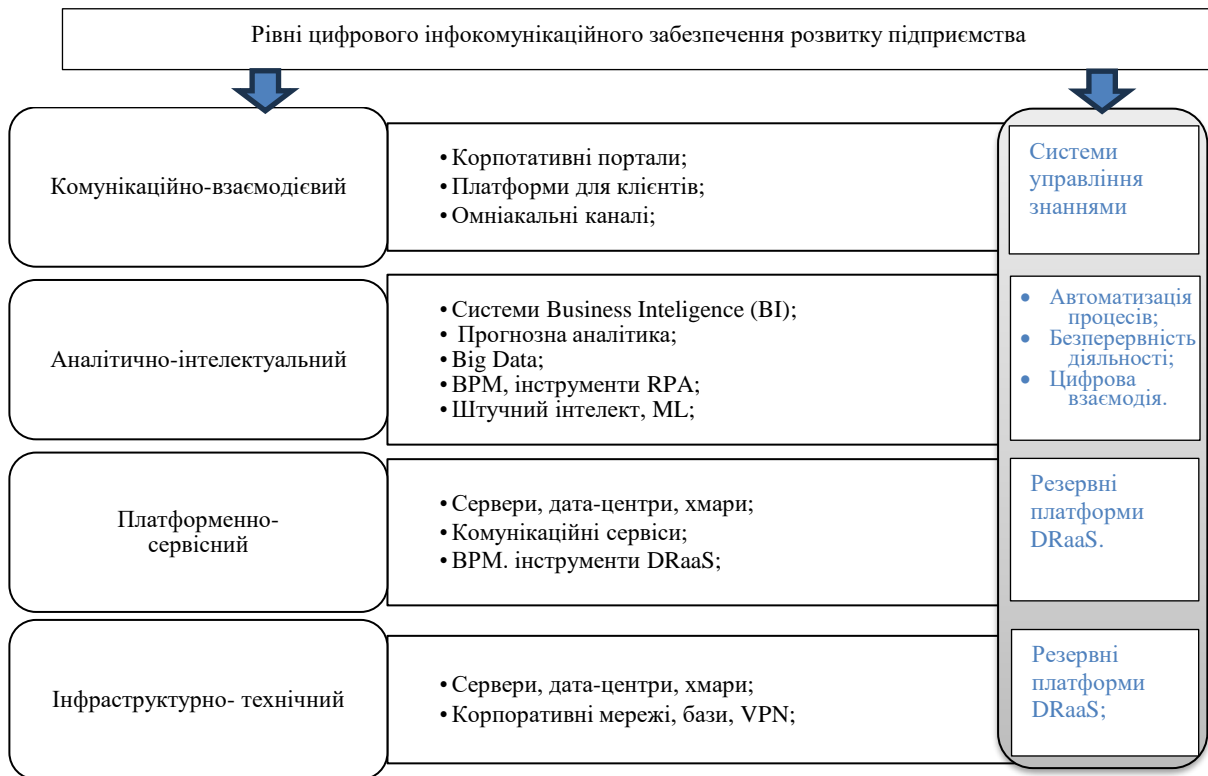


Рисунок 2. Архітектура та ключові елементи цифрового інфокомунікаційного забезпечення розвитку підприємства
Джерело: власна розробка авторів

Четвертий рівень – комунікаційно-взаємодійний 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, підвищують 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.

Відмінність авторського підходу полягає у тому, що пропонуються дворівневі 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. 4).

Таблиця 4. КРІ для принципів побудови інфокомунікаційної екосистеми (кількісні та якісні індикатори)

Принцип	Обрані КРІ	
	КРІ – показник	Об'єкти виміру
1. Адаптивність	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – 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.
3. Безперервність	<ul style="list-style-type: none"> – доступність ключових сервісів (%); – час простою критичних процесів (год.); – частка автоматизованих процесів (%); – запас пропускну здатності при пікових навантаженнях (%). 	Гарантія того, що ключові сервіси залишаються доступними, навіть під час інцидентів або криз.
4. Відкритість та інтегрованість	<ul style="list-style-type: none"> – 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)	<ul style="list-style-type: none"> – 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)	<ul style="list-style-type: none"> – 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.

Джерело: власна розробка авторів

Принцип	КРІ					
	часу реагування / переходу	автоматизації процесів	інцидентів та кіберзахисту	доступності сервісів	інтегр-аційної сумісності	data-driven управління
1. Адаптивність	<ul style="list-style-type: none"> ✓ Час переходу на резервні процеси; ✓ Час впровадження нових інструментів 	<ul style="list-style-type: none"> ○ Частка альтернативних сценаріїв автоматизації 	<ul style="list-style-type: none"> ○ Кібер-інциденти, що потребують перебудови системи 	<ul style="list-style-type: none"> ○ Доступність при пікових навантаженнях 	<ul style="list-style-type: none"> ○ Швидкість інтеграцій 	<ul style="list-style-type: none"> ✓ Час доступу до аналітики; ✓ Рішення на основі даних
2. Стійкість	<ul style="list-style-type: none"> ○ Швидкість переходу під час інциденту 	<ul style="list-style-type: none"> ✓ Автоматизація стабілізує роботу 	<ul style="list-style-type: none"> ✓ Кількість інцидентів; ✓ MTTR Security; ✓ відповідність стандартам 	<ul style="list-style-type: none"> ○ Доступність сервісів у кризах 	<ul style="list-style-type: none"> ○ Інтеграції як засіб резервування 	<ul style="list-style-type: none"> ○ Прогнозні моделі для попередження збоїв
3. Безперервність	<ul style="list-style-type: none"> ✓ Час простою; ✓ Перехід на резервні канали 	<ul style="list-style-type: none"> ✓ Частка автоматизованих процесів 	<ul style="list-style-type: none"> ✓ Порушення безпеки, що впливають на сервіс 	<ul style="list-style-type: none"> ✓ Доступність ключових сервісів 	<ul style="list-style-type: none"> ○ Інтеграції для дублювання потоків 	<ul style="list-style-type: none"> ○ Аналітика для підтримки безперервності
4. Відкритість та інтегрованість	<ul style="list-style-type: none"> ○ Час адаптації до зовнішніх змін 	<ul style="list-style-type: none"> ○ Автоматизація на рівні API 	<ul style="list-style-type: none"> ○ Кібер-ризик інтеграцій 	<ul style="list-style-type: none"> ○ Доступність сервісів через зовнішні платформи 	<ul style="list-style-type: none"> ✓ Час інтеграції; ✓ Число підключених платформ; ✓ Сумісність API 	<ul style="list-style-type: none"> ○ Наявність даних для міжорганізаційного обміну
5. Орієнтація на дані (data-driven)	<ul style="list-style-type: none"> ○ Оптимізація часових рішень через аналітику 	<ul style="list-style-type: none"> ○ Автоматизація збору даних 	<ul style="list-style-type: none"> ○ Моніторинг кіберінцидентів на основі даних 	<ul style="list-style-type: none"> ○ Аналітика стабільності сервісів 	<ul style="list-style-type: none"> ○ Дані для інтеграцій 	<ul style="list-style-type: none"> ✓ Якість даних; ✓ Частка рішень на основі аналітики; ✓ Моделі прогнозування
6. Кібербезпека як вбудований принцип	<ul style="list-style-type: none"> ○ Перехід на безпечні резервні процеси 	<ul style="list-style-type: none"> ○ RPA як мінімізація людських вразливостей 	<ul style="list-style-type: none"> ✓ Усі КРІ кібербезпеки (інциденти, MTTR, по-криття моніторингом) 	<ul style="list-style-type: none"> ○ Захищеність каналів доступності 	<ul style="list-style-type: none"> ○ Захищеність інтеграцій 	<ul style="list-style-type: none"> ○ Аналітика інцидентів і аномалій

Позначення: ✓ – КРІ напряму вимірює реалізацію принципу; ○ – КРІ частково відображає реалізацію принципу (додатковий ефект)

Рисунок 3. Матриця відповідності принципів побудови екосистеми КРІ оцінювання

Джерело: власна розробка авторів

Матриця відповідності принципів побудови екосистеми KPI оцінювання (рис. 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.

KPI для цифрової інфраструктури управління підприємством представлено у табл. 5.

Таблиця 5. KPI цифрової інфраструктури управління підприємством

Блок цифрової інфраструктури	Опис KPI	
	KPI	що вимірює
1. Інфраструктурно-технічний рівень	<ul style="list-style-type: none"> – 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)	<ul style="list-style-type: none"> – 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)	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – час відповіді комунікаційних каналів; – доступність корпоративних сервісів (%); – рівень навантаження контактних каналів. 	Якість внутрішніх та зовнішніх комунікацій, стабільність взаємодії.
5. Безпека та захищеність (Security Layer)	<ul style="list-style-type: none"> – кількість кіберінцидентів; – час реагування (MTTR Security); – покриття моніторингом загроз (%); – дотримання стандартів ISO / NIST 	Кіберстійкість, готовність до криз і рівень безпеки даних.
6. Управління даними (Data Governance)	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – кількість активних інтеграцій; – час підключення нової інтеграції; – надійність API(відмови/місяць). 	Можливість швидко розширювати екосистему та забезпечувати сумісність.
8. Автоматизація та роботизація (RPA/IPA)	<ul style="list-style-type: none"> – кількість роботизованих задач; – економія часу (%); – рівень зниження ручних операцій (%). 	Продуктивність, стійкість процесів і зменшення операційних ризиків.

Джерело: складено авторами за матеріалами [7-10]

Порівнюючи зміст табл. 4 та табл. 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 КРІ цифрової інфраструктури вимірюють технічну та операційну ефективність цифрових ресурсів підприємства, тоді як КРІ 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. 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.

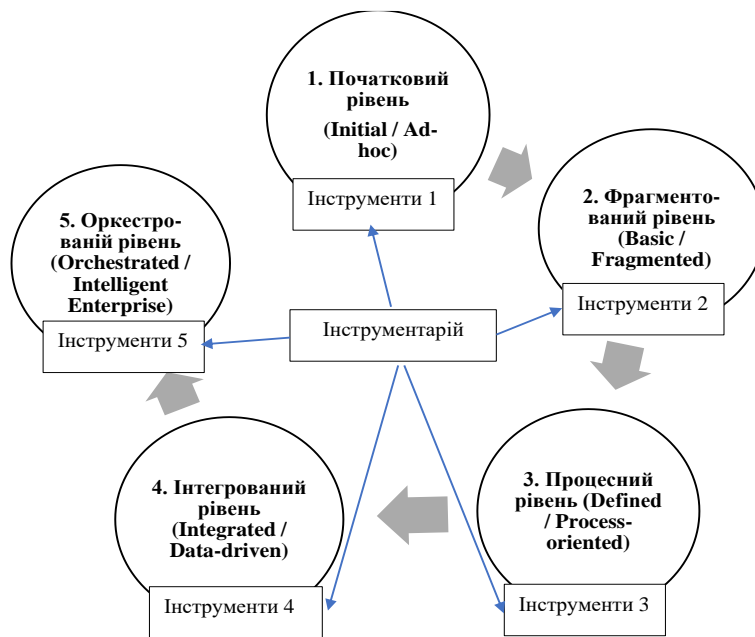


Рисунок 4. Рівні цифрової зрілості підприємства (Digital Maturity Levels)

Джерело: складено авторами за матеріалами [2-6]

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. Оркестрований 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 інстру-

менти. 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 інфокомуніка-

ційного забезпечення розвитку підприємства підприємство отримує чітку архітектурну модель цифрового розвитку;

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

Висновки

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

Abstract

The lack of a systematic vision for digital information and communication support, the inconsistency of strategic development goals with digital initiatives, and insufficient attention to the integration of information flows and management circuits reduce the effectiveness of digital resource use, especially in conditions of crisis-induced resource constraints and increased risks. In scientific research, digital transformation is mostly viewed through the prism of technological renewal or increased operational efficiency, while the issues of systematic digital information and communication support for enterprise development and mechanisms for its targeted focus in crisis conditions remain insufficiently explored. This necessitates a deepening of theoretical approaches to the interpretation of digital information and communication resources as an integrated management system capable of ensuring the coordination of decisions, transparency of information flows, and support for strategic development priorities.

The purpose of the article is to substantiate the conceptual foundations of systematic digital information and communication support for enterprise development and to determine the directions of its focus in crisis conditions. Focused digital information and communication support for enterprise development is a targeted system of digital resources, technologies, tools, and communication channels that focuses on the key priorities of the enterprise and ensures the continuity of information flows, the efficiency of management decisions, and the stability of business processes in unstable conditions. Traditional ICT systems demonstrate sufficient efficiency in stable conditions, but their fragmentation, limited integration and insufficient adaptability make them vulnerable in turbulent conditions. In contrast, focused digital support is based on the principles of prioritising critical processes, centralising information flows, multi-level cyber protection and rapid scalability of digital infrastructure, which allows the enterprise to maintain controllability and continuity of operations in high-risk conditions. The enterprise's information and communication ecosystem must be adaptive, resilient, continuous, open to integration, data-driven, and secure at all levels of the digital architecture. Digital information and communication support for enterprise development is a multi-level architecture that includes technical infrastructure, business platforms, analytical modules, and communication tools integrated into a single environment. Building such an ecosystem ensures the stability, continuity, adaptability, and strategic flexibility of the enterprise, which are critical in the context of digitalisation and crisis.

The key difference is that digital infrastructure KPIs measure the technical and operational efficiency of an enterprise's digital resources, while principle KPIs assess the strategic compliance of the system with key requirements for adaptability, sustainability, continuity, openness, data orientation, and cybersecurity. The digital maturity of an enterprise evolves from the initial state of unsystematic use of tools to the level of an integrated and intelligently orchestrated digital ecosystem in which data, automation and artificial intelligence ensure the resilience, adaptability, continuity and strategic ability of the enterprise to transform. The improvement of the enterprise management system in the field of information and communication digital support is ensured by the integration of a comprehensive approach that includes strategic, technological, architectural and assessment tools.

Список літератури:

1. Лисенко С.М. Оцінка ефективності цифрової трансформації в управлінні бізнес-процесами агропромислових підприємств. *Бізнес-Навігатор*. 2025. № 6. DOI: 10.32782/business-navigator.83-60.
2. Хімич С.В. Методичні підходи до оцінювання рівня цифрової трансформації промислових підприємств. *Економічний вісник КІП*. 2023. № 27. DOI: 10.20535/2307-5651.27.2023.297217.

3. Alshammari K.H. Managing digital transformation in a global environment. Dialnet. 2023. URL: <https://dialnet.unirioja.es/descarga/articulo/9385607.pdf>.
4. Alzarooni A. I. Navigating digital transformation in the UAE: Benefits and challenges. Computers. 2024. Vol. 13, No. 11. Art. 281. DOI: 10.3390/computers13110281.
5. 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>.
6. Telecommunications and Digital Government Regulatory Authority. UAE Digital Government Maturity Model. Abu Dhabi: UAE Digital Government, 2022. URL: <https://dgov.tdra.gov.ae/publications/uae-digital-government-maturity-model>.
7. Wernicke B. Introduction of a digital maturity assessment framework for construction site operations : master's thesis. Luleå: Luleå University of Technology, 2023. URL: <https://www.diva-portal.org/smash/get/diva2:1477311/FULLTEXT01.pdf>.
8. Zhang P., Wang Y. Digital transformation: A systematic review and bibliometric analysis from the corporate finance perspective. SSRN, 2024. DOI: 10.2139/ssrn.5053864.
9. 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: 10.32996/jbms.2023.5.4.7.
10. 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: 10.3390/admsci13050126.

References:

1. Lysenko, S.M. (2025). Assessment of the effectiveness of digital transformation in business process management of agro-industrial enterprises. Business Navigator, 6. DOI: 10.32782/business-navigator.83-60 [in Ukrainian].
2. Khimich, S.V. (2023). Methodological approaches to assessing the level of digital transformation of industrial enterprises. Economic Bulletin of KPI, 27. DOI: 10.20535/2307-5651.27.2023.297217 [in Ukrainian]
3. Alshammari, K.H. (2023). Managing digital transformation in a global environment. Dialnet. Retrieved from: <https://dialnet.unirioja.es/descarga/articulo/9385607.pdf> [in English].
4. Alzarooni, A. I. (2024). Navigating digital transformation in the UAE: Benefits and challenges. Computers, 13(11), Article 281. DOI: 10.3390/computers13110281 [in English].
5. Digital Dubai. (2023). Dubai State of AI Report. Dubai: Digital Dubai. Retrieved from: <https://www.digitaldubai.ae/docs/default-source/publications/dubai-state-of-ai-report.pdf> [in English].
6. Telecommunications and Digital Government Regulatory Authority. (2022). UAE Digital Government Maturity Model. Abu Dhabi: UAE Digital Government. Retrieved from: <https://dgov.tdra.gov.ae/publications/uae-digital-government-maturity-model> [in English].
7. Wernicke, B. (2023). Introduction of a digital maturity assessment framework for construction site operations (Master's thesis). Luleå: Luleå University of Technology. Retrieved from: <https://www.diva-portal.org/smash/get/diva2:1477311/FULLTEXT01.pdf> [in English].
8. Zhang, P., & Wang, Y. (2024). Digital transformation: A systematic review and bibliometric analysis from the corporate finance perspective. SSRN. DOI: 10.2139/ssrn.5053864 [in English].
9. O'Higgins, D. (2023). Impacts of business architecture in the context of digital transformation: An empirical study using PLS-SEM approach. Journal of Business and Management Studies, 5(4). DOI: 10.32996/jbms.2023.5.4.7 [in English].
10. Nosratabadi, S., Atobishi, T., & HegedHus, Sz. (2023). Social sustainability of digital transformation: Empirical evidence from EU-27 countries. Administrative Sciences, 13(5), Article 126. DOI: 10.3390/admsci13050126 [in English].

Посилання на статтю:

Ткач К.І. Системне цифрове інфокомунікаційне забезпечення розвитку підприємства: фокусування в умовах криз / К.І. Ткач, Алі Рашид Халіфа Бумекайр Альмансури // Економіка: реалії часу. Науковий журнал. – 2025. – № 2 (78). – С. 150-160. – Режим доступу: <https://economics.net.ua/files/archive/2025/No2/150.pdf>. DOI: 10.15276/ETR.02.2025.16. DOI: 10.5281/zenodo.18039087.

Reference a Journal Article:

Tkach K.I. Systematic Digital Information and Communication Support for Enterprise Development: Focusing in Times of Crisis / K.I. Tkach, Ali Rashed Khalifa Bumeqairaa Almansoori // Economics: time realities. Scientific journal. – 2025. – № 2 (78). – P. 150-160. – Retrieved from: <https://economics.net.ua/files/archive/2025/No2/150.pdf>. DOI: 10.15276/ETR.02.2025.16. DOI: 10.5281/zenodo.18039087.



This is an open access journal and all published articles are licensed under a Creative Commons "Attribution" 4.0.