

УДК 005.21:[338.24:004]:658.1

DOI: 10.31673/2415-8089.2026.213481

Гусєва Ольга Юрійвна,
доктор економічних наук, професор,
Державний університет
інформаційно-комунікаційних технологій
Бойко Арсеній Олегович
аспірант
Державний Університет
інформаційно-комунікаційних технологій

УПРАВЛІННЯ ДОСТУПОМ У ЦИФРОВИХ ЕКОСИСТЕМАХ ЯК ЕЛЕМЕНТ АНТИКРИЗОВОЇ СТРАТЕГІЇ ПІДПРИЄМСТВ

У статті обґрунтовано теоретико-методологічні та прикладні засади формування антикризової стратегії підприємств, які функціонують у межах цифрових екосистем. Визначено провідні тенденції розвитку екосистемного підприємства в умовах цифровізації, серед яких виділено платформізацію бізнесу, коопетицію та технологічну гіперінтеграцію, що зумовлюють втрату ефективності класичного мережевого периметра та виникнення прониких міжорганізаційних меж.

Досліджено сутність трансформації антикризового менеджменту, яка полягає у переході від ізольованого захисту окремого підприємства до забезпечення колективної стійкості (resilience) всієї партнерської мережі. Розроблено авторську архітектуру антикризової стратегії, яка інтегрує послідовні функціональні етапи реагування (контури економічної безпеки, технологічного стеку платформи, мережевої взаємодії та соціо-етичного контуру) із радіальним замиканням усіх процесів на єдиному координаційному центрі — ядрі динамічного управління доступом.

Доведено доцільність розгортання цього ядра на основі концепції нульової довіри (із застосуванням механізмів безперервної адаптивної оцінки прав користувачів на основі подієвих сигналів безпеки та контекстуального керування сесіями в реальному часі).

Визначено стратегічну роль управління доступом як базового координаційного важеля, що забезпечує глибоку мікросегментацію ресурсів, легітимність міжорганізаційних трансакцій та загальну економічну безпеку підприємств в процесі реалізації антикризової стратегії.

Ключові слова: управління доступом, цифрова екосистема, екосистемне підприємство, антикризова стратегія, нульова довіра (Zero Trust), економічна безпека, платформізація, коопетиція, стійкість (resilience).

Постановка проблеми. Сучасний етап розвитку економіки характеризується активним формуванням цифрових екосистем, у межах яких підприємства інтегрують власні інформаційні ресурси, хмарні сервіси, цифрові платформи, системи електронної взаємодії та мережі партнерських зв'язків. Такі трансформації створюють нові можливості для підвищення ефективності бізнес-процесів, водночас суттєво посилюючи ризики несанкціонованого доступу до даних, витоку конфіденційної інформації, порушення безперервності діяльності та виникнення кіберінцидентів. У цих умовах управління доступом поступово перетворюється із суто технічного інструменту інформаційної безпеки на важливий елемент антикризового стратегічного управління та забезпечення економічної стійкості підприємств.

Аналіз останніх досліджень і публікацій. Проблематика управління доступом у цифровому середовищі активно досліджується вітчизняними та зарубіжними науковцями. Так, Т. Коробейнікова та О. Кравченко, Б. Маньковський, О. Городицький та І. Опірський обґрунтовують доцільність використання концепції Zero Trust як основи сучасної системи кібербезпеки корпоративних мереж та цифрових екосистем. Т. Капелюшна, Д. Примаченко, П. Складанний, а також С. Kyriakidou, A. Parathanasiou, V. Siris та інші дослідники акцентують увагу на розвитку механізмів управління цифровими ідентичностями, контролю доступу до

інформаційних ресурсів та безперервної оцінки рівня довіри користувачів. Водночас A. Singh, I. Kuzminykh та B. Ghita досліджують сучасні виклики впровадження систем Identity and Access Management у корпоративному середовищі.

Значний внесок у розвиток теоретичних засад функціонування цифрових екосистем зробили М. Сагайдак, С. Горбань та В. Горбаньова, які розглядають цифрові екосистеми як нову форму організації бізнесу, що забезпечує інтеграцію учасників ринку на основі цифрових платформ і даних. Питання забезпечення економічної безпеки та антикризового управління підприємствами в умовах цифрових трансформацій досліджуються у працях О. Одношевної, А. Міньковської, Т. Саванчук, Л. Рибалко-Рак, Т. Гусаковської, В. Опришка, М. Лаптева, С. Лаптева, О. Захарова та К. Пріб, які наголошують на необхідності формування адаптивних механізмів управління, спрямованих на підвищення стійкості підприємств до зовнішніх та внутрішніх кризових впливів.

Разом із тим аналіз наукових публікацій свідчить, що більшість сучасних досліджень присвячена переважно технічним аспектам управління доступом, кібербезпеки та архітектури Zero Trust або окремим питанням антикризового управління підприємствами. Недостатньо дослідженими залишаються економічні та управлінські аспекти інтеграції механізмів управління доступом до системи антикризового менеджменту підприємства, оцінювання їх впливу на безперервність бізнес-процесів, економічну безпеку, цифрову стійкість та здатність підприємств адаптуватися до кризових умов. Практично відсутні комплексні наукові підходи, які б розглядали управління доступом у цифрових екосистемах як самостійний елемент антикризової стратегії підприємства.

З огляду на зазначене, дослідження теоретичних і прикладних аспектів управління доступом у цифрових екосистемах як елемента антикризової стратегії підприємств є своєчасним та актуальним, оскільки спрямоване на формування нових підходів до забезпечення цифрової стійкості, економічної безпеки та ефективного функціонування підприємств в умовах зростання кіберризиків, цифровізації бізнесу та нестабільності зовнішнього середовища.

Мета статті полягає в обґрунтуванні теоретичних положень та розробці практичних рекомендацій щодо інтеграції процесів управління доступом у стратегію антикризового управління підприємствами, які функціонують у межах цифрових екосистем, задля забезпечення їхньої економічної безпеки та цифрової стійкості в умовах турбулентного бізнес-середовища.

Методи дослідження. Методологічну основу дослідження становить поєднання загальнонаукових і спеціальних економічних підходів, що забезпечують комплексне осмислення впливу управління доступом на антикризову стійкість та економічну безпеку підприємств у межах цифрових екосистем. Вибір методів зумовлений необхідністю одночасного аналізу процесів на загальносистемному (мережевому) та мікроекономічному рівнях і виявлення їх взаємозв'язку.

Теоретичне узагальнення базується на використанні абстрактно-логічного методу, який дозволив уточнити економічну та управлінську сутність управління доступом у системі антикризового менеджменту та розкрити трансформацію моделей функціонування підприємств під впливом цифровізації. Застосування системного підходу дало змогу розглядати управління доступом як елемент ширшої економічної структури, де інституційне середовище, цифрова інфраструктура платформ та стратегічна поведінка підприємств формують єдиний механізм розвитку.

Оцінювання мікроекономічних та організаційних ефектів ґрунтувалося на методах структурно-функціонального аналізу та логічного моделювання. Це забезпечило можливість дослідити зміни у транзакційній взаємодії та безпекових контурах підприємств, визначити вплив цифрових платформ на загальну стійкість партнерської мережі та розкрити механізми формування економічної результативності в умовах кризового середовища.

Узагальнення отриманих результатів здійснено на основі методу наукової абстракції та графічного моделювання, що дозволило сформулювати концептуальну схему взаємодії

координаційного ядра та периферійних функціональних блоків стратегії. Такий підхід забезпечив цілісність дослідження та обґрунтованість висновків щодо напрямів підвищення ефективності використання інструментів управління доступом в антикризовій діяльності екосистемних підприємств.

Виклад основного матеріалу. Сучасне бізнес-середовище характеризується високим рівнем ентропії та нелінійності процесів, що робить класичні ієрархічні моделі управління неефективними через їхню інертність. У цьому контексті цифрова трансформація виступає не як «модернізація ІТ», а як інструмент організаційної адаптивності, що здатний забезпечити трансформацію структурної вразливості у динамічну стійкість.

Підтвердженням незворотності цього процесу є економічні показники. За прогнозами International Data Corporation, світові витрати на цифрову трансформацію сягнуть 4 трлн доларів США у 2027 році, що становитиме дві третини всіх інвестицій в ІКТ. Цю тенденцію підтверджують і дані OECD: сектор ІКТ зростає втричі швидше за світовий ВВП, що свідчить про фундаментальне зміщення центру створення доданої вартості у цифрову площину. Український бізнес слідує глобальному тренду: згідно з дослідженням KPMG Ukraine (2024), 94% підприємств планують впровадження штучного інтелекту, а 71% вже використовують хмарні рішення для забезпечення стійкості.

В науковій літературі часто ототожнюють поняття оцифрування, цифровізації та цифрової трансформації, що призводить до підміни понять та помилкових управлінських рішень. Хоча ці процеси є взаємопов'язаними етапами еволюції, вони мають фундаментально різну природу, об'єкти впливу та економічні наслідки.

Для розуміння механізму впливу технологій на ефективність доцільно розмежувати ці рівні:

1. Оцифрування (Digitization): Базовий рівень, що передбачає зміну формату інформації з аналогового на цифровий. Його мета — доступність даних та зниження витрат на їх зберігання.

2. Цифровізація (Digitalization): Використання оцифрованих даних для автоматизації та оптимізації існуючих процесів. Це підвищує операційну швидкість, але не змінює сутність бізнесу.

3. Цифрова трансформація (Digital Transformation): Глибинна зміна логіки створення вартості та бізнес-моделі. Це створення нових джерел доходу через використання проривних технологій (AI, IoT).

Як видно з Таблиці 1, ключова відмінність полягає у векторі змін. Якщо перші два рівні спрямовані на оптимізацію внутрішнього контуру (Operational Efficiency), то цифрова трансформація орієнтована на зовнішній контур (Value Proposition Innovation).

Як зазначають Leendertse et al. (2022), екосистемне підприємство – це сукупність взаємозалежних учасників та факторів, які управляються таким чином, що вони забезпечують (уможливлюють) продуктивне підприємництво в межах певної території [15].

Цей підхід акцентує не на окремому підприємстві, а на якості зв'язків підприємцями, інституціями, інфраструктурою, знаннями та правилами, що формують умови для нової цінності.

У сучасній цифровій економіці розвиток екосистемного підприємства дедалі більше пов'язаний із мережевими моделями координації, цифровими платформами, міжорганізаційною взаємодією та інтеграцією даних. Саме тому такі підприємства розвиваються під впливом кількох ключових тенденцій.

Таблиця 1.

Порівняльна характеристика рівнів цифрових змін у бізнес-середовищі

Критерій порівняння	Оцифрування (Digitization)	Цифровізація (Digitalization)	Цифрова трансформація (Digital Transformation)
Ключовий фокус	Дані та інформація	Процеси та операції	Бізнес-модель та екосистема

Об'єкт змін	Аналогові носії (папір, плівка, звук)	Рутинні операції, документообіг, комунікація	Логіка створення вартості, ціннісна пропозиція
Технологічний стек	Бази даних, сканери, сенсори	ERP, CRM, Cloud (SaaS), BPM-системи	AI, IoT, Big Data, Blockchain, Platforms
Вплив на персонал	Зміна інструментарію роботи	Зміна алгоритмів та швидкості роботи	Зміна мислення (Digital Mindset) та культури
Результат (KPI)	Доступність та збереження даних	Операційна ефективність, зниження витрат	Нові джерела доходу, капіталізація, клієнтський досвід

Джерело: узагальнено авторами основі джерел [18; 19]

Першою провідною тенденцією, яка визначає сучасні контури розвитку екосистемних підприємств, є платформізація їхньої діяльності, тобто перехід від лінійних моделей створення вартості до платформних архітектур, у яких ключову роль відіграють координація взаємодії учасників, динамічний доступ до ресурсів, обмін даними та мережеві ефекти [17]. У цьому контексті управління сучасним екосистемним підприємством розглядається як організація безпечної взаємодії багатьох суб'єктів навколо спільної цінності, де цифрова платформа стає ядром зв'язку між виробниками, партнерами та споживачами. Для вітчизняних господарюючих суб'єктів це означає поступове зміщення акценту з автономного функціонування фірми на її активну інтеграцію в цифрові екосистеми, де загальна конкурентоспроможність дедалі більше визначається здатністю підприємства ефективно взаємодіяти у спільному платформному середовищі [18].

Водночас вагомим значенням для стабілізації екосистемних підприємств набуває коопетиція — стратегічне поєднання конкуренції та співпраці в межах єдиного цифрового простору, коли спільне використання інфраструктури, знань, сервісів і каналів доступу до клієнта стає передумовою їхнього виживання. Дослідження практики функціонування українських підприємств показує, що їхні внутрішні екосистеми часто перебувають на етапі трансформації, а їхній розвиток потребує міжсекторальної координації, підтримки стартап-інфраструктури та впровадження надійних інструментів захисту інформаційного обміну. За таких умов коопетиція виступає не тимчасовим компромісом, а проактивною моделлю поведінки, яка дозволяє підприємствам спільно створювати цінність, знижувати транзакційні витрати та мінімізувати операційні ризики в нестабільному середовищі [19].

Третьою тенденцією є гіперінтеграція та проникність меж між підприємствами, хмарними системами й ринками, що безпосередньо впливає на архітектуру корпоративної безпеки та актуалізує впровадження гнучких моделей управління доступом до даних [11]. У сучасних умовах цифрова трансформація змінює не лише технологічний стек підприємств, а й самі механізми їхнього корпоративного управління, роблячи їх більш відкритими до зовнішніх партнерств, але водночас і більш вразливими до внутрішніх та зовнішніх кіберзагроз [21]. Цифровізація антикризового менеджменту доводить, що стійкість екосистемного підприємства дедалі більше залежить від швидкості інтеграції інформації, узгодженості дій учасників мережі та здатності надійно розмежовувати права користувачів, поєднуючи внутрішні й зовнішні цифрові контури управління [12].

Сучасні умови функціонування вітчизняної економіки характеризуються комплексом глибоких системних викликів, серед яких домінують соціально-економічні трансформації, політична нестабільність, наслідки воєнних дій та глобальна фінансова турбулентність. За умов такої невизначеності та жорстких ресурсних обмежень традиційні ізольовані моделі менеджменту втрачають свою стабільність [8]. Це зумовлює об'єктивну необхідність переосмислення класичних підходів до організації діяльності підприємств та переходу до концепції адаптивних і динамічних екосистемних структур, спроможних забезпечити синергію спільного розвитку бізнесу, науки та держави [9].

Трансформація стратегій антикризового управління в межах екосистемного підходу відображає еволюцію від локального захисту окремого підприємства до забезпечення колективної життєздатності всієї мережі взаємопов'язаних учасників. Сутність цього процесу визначається декількома фундаментальними змінами:

- Трансформація бізнес-моделей. Традиційні підходи адаптуються до нової парадигми цифрової трансформації, де успішність функціонування цифрової екосистеми безпосередньо корелює з успішністю кожного її учасника [11].
- Відмова від ізоляції. Замість жорсткої ізольованої конкуренції впроваджуються стратегії спільної генерації цінностей (co-opetition) та клієнтоорієнтованого управління, що підвищує загальну конкурентоспроможність середовища [12].
- Зміна парадигми безпеки. Замість реактивного виживання та простого скорочення витрат окремої фірми, фокус зміщується на формування довгострокової проактивної стійкості всієї партнерської мережі [13].

Отже, можна вважати, що поєднання передових технологій і гнучкими стратегічними змінами стає ключовим фактором для сталого розвитку та адаптації бізнесів до глобальних криз.

На основі аналізу сучасних наукових досліджень та прикладного досвіду функціонування мережових бізнес-моделей виділено чотири ключові напрями, за якими здійснюється системна трансформація антикризових стратегій екосистемних підприємств.

Першим фундаментальним напрямом виступає розбудова інтелектуальних цифрових платформ та комплексна автоматизація процесів прогнозування ризиків. Впровадження інструментів штучного інтелекту та технологій Big Data забезпечує точне моделювання потенційних загроз, автоматизує процеси прийняття рішень і дозволяє оптимізувати операційні витрати компанії в умовах високої невизначеності зовнішнього середовища. Водночас створення спеціалізованих цифрових платформ для дистанційної взаємодії уможливорює ефективне забезпечення бізнес-безперервності, підтримуючи стабільну продуктивність та комунікацію між персоналом, партнерами та клієнтами навіть під час критичних зовнішніх шоків. [12] Важливою характеристикою таких платформ є повноцінна реалізація мережевого ефекту, що дозволяє лідерам екосистеми не лише охоплювати ширші ринкові сегменти, а й здійснювати оперативний самостійний або координований запуск нових продуктів і послуг для безперервної підтримки життєздатності всієї системи. У такому контексті платформна архітектура стає головним технологічним ядром антикризового регулювання.[11]

Другим стратегічним напрямом є послідовний перехід екосистемних підприємств до гнучких та адаптивних моделей менеджменту. Сучасна типологія антикризового управління в цифровому середовищі передбачає динамічну диференціацію та комбінування адаптивних векторів залежно від глибини кризи, зокрема стратегій виживання, реструктуризації, проривних інновацій та кооперативного партнерства, що детально розглядається у працях К. Пріба (2024) [14]. Практична інтеграція методологій Agile, Lean та Resilience Management створює передумови для миттєвої мобілізації розподілених ресурсів екосистеми, мінімізації фінансових втрат та оперативного реагування на ринкові зміни[12]. Така трансформація охоплює також процеси планування та бюджетування, які перетворюються на цілісну систему безперервного діагностичного моніторингу, сценарного аналізу та гнучкого перерозподілу фінансів (зокрема, із залученням концепції Zero-based budgeting), що забезпечує високу швидкість загальноорганізаційної реакції.[13]

Третім вектором трансформації виступає глибока модернізація класичних систем економічної безпеки підприємств. Антикризовий механізм у сучасних умовах вимагає переходу до поетапної оптимізації та санації, яка базується на обов'язковій оцінці фактичного стану суб'єктів, своєчасному виявленні чинників розвитку кризових явищ (таких як слабкий менеджмент чи логістичні недоліки) та розробці чітких санаційних заходів, що є предметом дослідження О. Одношевної, А. Міньковської та Т. Саванчук (2023) [10]. Це передбачає комплексний технологічний upgrade виробничої бази, реструктуризацію відділів маркетингу

й логістики, а також активний пошук нових каналів збуту продукції відповідно до мінливих вимог ринку. Ключовим елементом тут виступає оновлення стратегічного бачення ведення бізнесу з боку вищого керівництва, що дозволяє інтегрувати внутрішні та зовнішні цифрові контури управління, підсилюючи загальну безпеку екосистеми [13].

Нарешті, четвертим важливим напрямом є формування розвиненої соціо-етичної інфраструктури та безперервне підвищення цифрових компетенцій персоналу. Для забезпечення сталого розвитку екосистеми критично необхідним стає поєднання процесів тотальної цифровізації із розбудовою прозорої корпоративної культури, впровадженням політики комплаєнсу та чітких етичних протоколів взаємодії. Постійне навчання та «апгрейд» цифрових компетенцій працівників і менеджерів (Digital Mindset) перетворюються на стратегічну необхідність для ефективного та безпечного використання новітніх ІТ-технологій у мінливому бізнес-середовищі, що безпосередньо впливає на загальну життєздатність та конкурентоспроможність середовища згідно з концептуальними засадами розвитку людського капіталу в екосистемах Д. Одретча (2022) [16].

Узагальнюючи виділені напрями трансформаційних зрушень, можна констатувати, що системне поєднання технологічної гнучкості, адаптивного менеджменту та безпекових оновлень вимагає конструювання чіткої архітектури стратегічного реагування. Спираючись на ці вектори, нами було сформовано комплексну авторську схему елементів антикризової стратегії екосистемного підприємства, у якій стрижневу координаційну роль відіграє управління доступом.

Для наочного відображення сутності трансформаційних зрушень сформовано узагальнену таблицю порівняння традиційного та екосистемного підходів до антикризового управління (табл.2).

Зазначені в таблиці фундаментальні розбіжності доводять, що антикризова стійкість сучасного екосистемного підприємства є інтегральною функцією гнучкості, швидкості реакції та безпеки взаємодії. Це, у свою чергу, вимагає переходу від опису загальних напрямів до конструювання чіткої внутрішньої архітектури стратегічного реагування, де всі процеси підпорядковані єдиній системній логіці.

Формування сучасної антикризової стратегії підприємств, що функціонують у межах бізнес-екосистем, вимагає відмови від фрагментарних інструментів фінансової стабілізації на користь комплексних рішень. В сучасних умовах високої турбулентності зовнішнього середовища антикризове управління трансформується у цілісний, наскрізний елемент загальної системи забезпечення економічної безпеки [10]. Будь-яка операційна, логістична чи фінансова вразливість екосистемного підприємства в період кризи критично посилюється деструктивним зовнішнім тиском, що об'єктивно актуалізує розробку адаптивних моделей менеджменту, здатних інтегрувати стратегічне прогнозування, гнучке бюджетування та глибоку цифрову трансформацію [13]. Оскільки сучасний бізнес дедалі сильніше інтегрується в цифрові екосистеми та платформні структури [9, 11], ефективна антикризова стратегія покликана забезпечувати не просто реактивне виживання, а проактивну стійкість та безперервність операційної діяльності за допомогою передових інформаційних технологій [12].

Таблиця 2.

Порівняльна характеристика трансформаційних змін в антикризових стратегіях підприємств

Критерій порівняння	Традиційна антикризова стратегія	Трансформована екосистемна стратегія
Об'єкт та мета управління	Автономне виживання та підвищення рівня економічної безпеки окремого суб'єкта.	Забезпечення колективної стійкості (resilience) та спільного розвитку відкритої структури.
Базовий інструментарій	Оцінка внутрішніх слабких місць, реактивні санаційні заходи,	Проактивне використання III, Big Data, хмарних технологій, Agile, Lean та Resilience інструментів.

	локальний Upgrade внутрішньої політики.	
Характер взаємодії	Жорстка конкуренція, закриті канали збуту, що забезпечують лише локальні потреби.	Кооперація між учасниками ринку, бізнесом, наукою і владою задля створення синергії.
Управління ресурсами	Стандартні підходи до менеджменту й маркетингу, орієнтовані на традиційну стратегію ведення бізнесу.	Сценарне моделювання, гнучке бюджетування (Zero-based budgeting), крос-функціональні команди та інвестиції в цифровізацію.
Соціально-етичний вектор	Фокус на фінансово-господарській стійкості підприємства для виходу з кризового стану.	Поєднання цифровізації з розвитком корпоративної культури, комплаєнсу та етичних протоколів.

Джерело: розроблено авторами на основі [9, 10, 11, 12, 13]

Запропонована авторська архітектура елементів антикризової стратегії екосистемного підприємства (рис. 1) поєднує часову послідовність функціональних етапів антикризового реагування із радіальним замиканням усіх процесів на єдиному координаційному центрі — ядрі динамічного управління доступом.

Початковим операційним рівнем представленої архітектури є аналітично-діагностичний процес, який безпосередньо розгортається у межах контуру економічної безпеки. Його функціональне призначення полягає у випереджальному моніторингу та експрес-оцінці поточних загроз фінансово-економічного стану підприємства, що дозволяє виявляти деструктивні чинники та слабкі сигнали наближення кризи на ранніх стадіях [10]. В умовах цифровізації цей процес зазнає якісних змін завдяки впровадженню інструментів штучного інтелекту та аналітики великих даних, уможливорюючи точне предиктивне прогнозування ризиків та оптимізацію аналітичних витрат у режимі реального часу [12]. Результатом функціонування цього контуру є сценарне моделювання та детермінація конкретного вектора реагування, який залежно від глибини виявлених деструкцій варіюється від локальної реструктуризації до масштабних проривних інновацій [13, 14].

На основі отриманих діагностичних даних активується ресурсно-платформний рівень стратегії, що охоплює функціональні блоки технологічного стеку платформи та мережевої Взаємодії. У період кризових шоків класичні жорсткі підходи до фінансового планування втрачають свою спроможність, зумовлюючи необхідність переходу до гнучкого екосистемного бюджетування та оперативної оптимізації витрат [13]. Стабілізація взаємодії з клієнтами та стейкхолдерами забезпечується через використання клієнтоорієнтованих цифрових платформ, які дозволяють утримувати мережеві ефекти та генерувати додаткову транзакційну цінність під впливом зовнішніх збурень [9, 11].

Особливе місце на цьому рівні посідає впровадження динамічних моделей управління доступом до даних у межах платформи, оскільки безпечний та санкціонований обмін комерційною інформацією із зовнішніми учасниками мережі є критичним фактором для спільного створення цінності (co-opetition) та збереження системної довіри [8].

Наступним елементом архітектури виступає модернізаційно-інфраструктурна трансформація, яка формує соціо-етичний контур екосистеми та забезпечує безпосередні операційні зміни. Подолання кризи вимагає реконфігурації бізнесу, що включає оновлення виробничо-технологічної бази, реструктуризацію відділів маркетингу, диверсифікацію логістичних ланцюгів та адаптацію товарної політики під мінливі вимоги ринку [10]. Для того щоб інфраструктурні зрушення мали сталий характер, цифровізація технічних процесів обов'язково підкріплюється інституційними змінами — трансформацією організаційної культури, підвищенням цифрових компетенцій персоналу, а також суворих етичних протоколів міжорганізаційної взаємодії [12, 13].

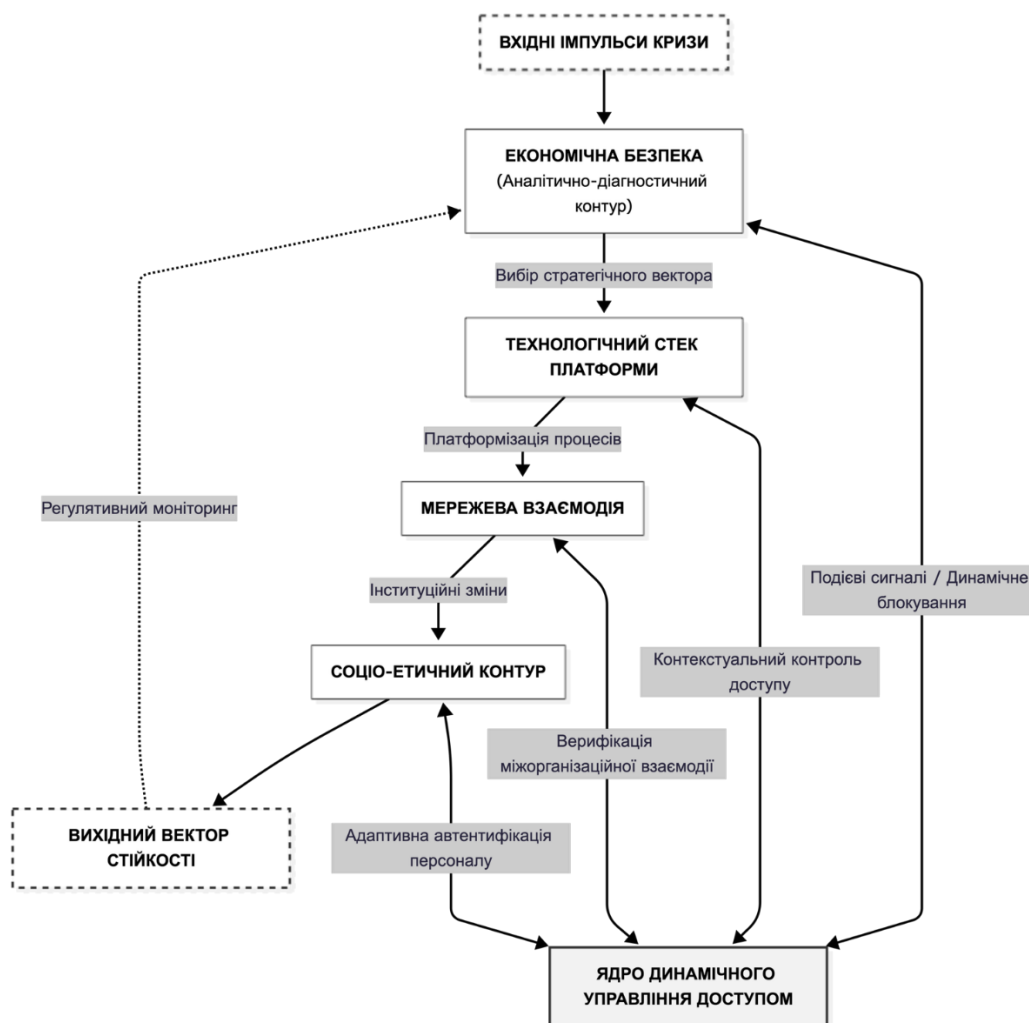


Рис. 1 Архітектура елементів антикризової стратегії екосистемного підприємства
 Джерело: розроблено авторами

Центральною віссю, яка пов'язує та забезпечує всі вищезазначені периферійні рівні авторської схеми, виступає ядровий блок динамічного управління доступом. Необхідність його виділення як автономного, наскрізного компонента антикризової стратегії зумовлена тим, що під час кризи підприємства масово переходять на гібридні або дистанційні моделі роботи, залучають хмарні обчислення та оперативно змінюють склад партнерів, що створює колосальні ризики для безпеки інформаційних ресурсів [2, 4]. У таких умовах традиційний периметральний захист мереж виявляється повністю безпорадним [4, 6], а індустрія стикається з критичними викликами у сфері управління ідентифікацією [7].

Стратегічне розгортання цього блоку в антикризовому контурі базується на прогресивній концепції нульової довіри (Zero Trust Architecture), яка вимагає відмови від апріорної довіри до будь-якого суб'єкта та передбачає обов'язкову безперервну автентифікацію [1, 3]. Замість статичної перевірки прав користувача, реалізується механізм безперервної оцінки доступу на основі подієвих сигналів безпеки та динамічного керування сесіями [5]. У разі фіксації аномальної активності чи зміни контексту взаємодії (наприклад, спроби несанкційованого вивантаження комерційних баз даних під час реструктуризації підрозділу), доступ обмежується або блокується в автоматичному режимі за допомогою інтегрованих систем SIEM та SOAR [4]. Це дозволяє здійснювати глибоку мікросегментацію ресурсів підприємства, надійно захищаючи інтелектуальний капітал та управлінську інформацію від внутрішніх і зовнішніх кіберзагроз [1, 2].

У такий спосіб сформована авторська архітектура утворює стійку синергетичну систему, де блок динамічного управління доступом виступає головним гарантом життєздатності всього підприємства. Діагностичні дані аналітичного блоку захищаються від деструктивного

спотворення, ресурсні потоки платформного контуру забезпечуються від несанкційованого перехоплення, а інфраструктурна модернізація відбувається в чітко контрольованому та легітимному цифровому середовищі. Поєднання адаптивного антикризового менеджменту із динамічним контролем інформаційних контурів на основі Zero Trust формує надійний фундамент для подолання наслідків турбулентності та подальшого конкурентоспроможного зростання екосистемного підприємства [12, 13].

Обґрунтування особливостей управління доступом у цифрових екосистемах як елемента антикризової стратегії підприємств зумовлене об'єктивними змінами в архітектурі сучасного бізнесу, що функціонує в умовах високої турбулентності та масштабної цифровізації. За умов сучасних системних криз традиційні підходи до забезпечення життєздатності господарюючих суб'єктів зазнають докорінної трансформації, оскільки антикризове управління дедалі частіше розглядається як невід'ємний складник удосконалення загальної системи економічної безпеки підприємства [10]. Інтеграція бізнесу в платформні структури та цифрові екосистеми вимагає переосмислення класичних клієнтоорієнтованих і управлінських стратегій [9, 11], оскільки в диджиталізованому просторі успішність і стійкість окремого підприємства безпосередньо залежать від стабільності та захищеності всієї партнерської мережі. Використання технологій штучного інтелекту, великих даних та автоматизації кардинально змінює інструментарій антикризового менеджменту, перетворюючи цифровізацію з фактора оптимізації на ключовий засіб виживання та підтримання конкурентоспроможності екосистеми в періоди нестабільності [12]. За таких обставин виникає гостра потреба у формуванні гнучких моделей управління ресурсами та впровадженні інноваційних стратегій стабілізації, які здатні оперативно нейтралізувати деструктивні чинники внутрішнього та зовнішнього походження [13, 14].

Центральне місце в архітектурі екосистемної антикризової стратегії посідає управління доступом. Функціонування сучасних платформних бізнес-екосистем повністю базується на безперервному обміні даними та відкритій взаємодії між багатьма автономними учасниками, що актуалізує розробку специфічних моделей управління доступом до спільної інформаційної бази [8]. Під час гострої фази кризи підприємства часто змушені швидко реструктуризувати операційні процеси, масштабувати хмарні технології, впроваджувати гібридні моделі віддаленої роботи або взаємодіяти в межах складного обчислювального континууму (computing continuum). Це призводить до стирання класичного мережевого периметра та виникнення нових критичних вразливостей [4, 6]. У таких динамічних умовах традиційні периметрові системи безпеки втрачають свою ефективність [1], а бізнес стикається з серйозними технологічними та організаційними викликами під час практичної реалізації та експлуатації сучасних рішень для управління ідентифікацією та доступом (IAM) [7]. Усе це зумовлює необхідність інтеграції в антикризові механізми концепції нульової довіри (Zero Trust Architecture), яка вимагає повної відмови від апріорної довіри до будь-яких користувачів або пристроїв як усередині корпоративної мережі, так і за її межами [1, 3]. Крім того, надійний захист інформаційних ресурсів за допомогою розроблених механізмів диференціації прав стає головною передумовою для упередження внутрішніх та зовнішніх ризиків підприємства [2].

Особливістю управління доступом як елемента антикризової стійкості є його проактивний та адаптивний характер. Впровадження моделей нульової довіри в екосистемах Інтернету речей (IoT) та корпоративних мережах дозволяє реалізувати глибоку мікросегментацію активів і багаторівневу автентифікацію, що унеможливорює поширення кіберзагроз і локалізує наслідки можливих інцидентів без зупинки загальних операційних процесів [3, 4]. Більше того, за умов динамічної зміни ризиків під час кризи критично важливим стає перехід від одноразової перевірки прав під час входу до систем безперервної оцінки доступу на основі подієвих сигналів безпеки та контекстуального керування сесіями користувачів у реальному часі [5]. Завдяки такій динамічній адаптації автоматизовані системи безпеки (зокрема SIEM та SOAR) здатні миттєво обмежувати або припиняти доступ у разі виявлення аномальної поведінки, що мінімізує вплив людського фактора та надійно захищає комерційну таємницю та інтелектуальну власність підприємства [4, 5]. Отже, управління доступом у цифрових

екосистемах виступає не просто технічним інструментом IT-підрозділів, а фундаментальним стратегічним елементом антикризового управління, що гарантує безперервність бізнес-транзакцій, легітимність партнерських взаємодій та загальну економічну безпеку підприємств у мінливому цифровому середовищі [10, 12, 13].

Висновки та перспективи подальших досліджень. У статті здійснено комплексне осмислення впливу управління доступом у цифрових екосистемах на антикризову стратегію екосистемних підприємств. Доведено, що цифровізація бізнес-моделей формує нову логіку економічної взаємодії, у межах якої регулювання інформаційних контурів, архітектура цифрових інтерфейсів та інструменти диференціації прав стають ключовими важелями забезпечення життєздатності суб'єктів господарювання в умовах турбулентності зовнішнього середовища. Управління доступом розглядається не як допоміжний інженерно-технічний механізм IT-підрозділів, а як наскрізний структурний елемент сучасної системи забезпечення економічної безпеки підприємства.

Встановлено, що на мікроекономічному рівні впровадження динамічних моделей управління доступом мінімізує вплив людського фактора, надійно захищає комерційну таємницю та підвищує операційну швидкість реагування на ринкові шоки. Зростає роль цифрових компетенцій персоналу (Digital Mindset), гнучкого сценарного бюджетування та впровадження предиктивних систем автоматизації ризиків. Водночас на загальноекосистемному рівні розвиток інтелектуальних платформ сприяє активізації міжорганізаційної коопетиції, розширенню мережових ефектів та глибшій інтеграції автономних учасників у розподілені ланцюги спільного створення цінності.

Обґрунтовано, що результативність цих процесів визначається якістю платформної інфраструктури, рівнем впровадження архітектурних принципів нульової довіри (Zero Trust Architecture) та узгодженістю стратегічного бачення вищого керівництва з правилами міжорганізаційної взаємодії в мережі. Взаємодія ядрових (координаційних) та периферійних (функціональних) ефектів має взаємопосилювальний характер і формує системний результат, який проявляється у переході від консервативної економії від масштабу до економії від швидкості й мережевого охоплення всієї структури.

Перспективи подальших досліджень доцільно пов'язувати з поглибленим кількісним оцінюванням впливу систем управління ідентифікацією та доступом (IAM) на показники фінансово-господарської стійкості фірм, аналізом галузевих особливостей розгортання хмарних технологій, а також із практичною апробацією запропонованої радіально-координаційної архітектури на прикладі вітчизняних підприємств. Особливої уваги потребує вивчення ризиків стирання мережевого периметра у межах складного обчислювального континууму, трансформації корпоративного управління в умовах гібридних моделей роботи та впливу автоматизованих систем безпеки (зокрема SIEM та SOAR) на структуру міжорганізаційної конкуренції. Подальший розвиток цієї проблематики сприятиме формуванню більш обґрунтованих управлінських рішень у сфері антикризового менеджменту підприємств в умовах цифрової економіки.

Список використаних джерел

1. Коробейнікова Т. І., Кравченко О. В. Концепція нульової довіри: сучасні методи забезпечення кібербезпеки корпоративних мереж. Вісник Львівського державного університету безпеки життєдіяльності. 2024. № 30. С. 156–165. URL: <https://journal.ldubgd.edu.ua/index.php/Visnuk/article/view/2769>
2. Капелюшна Т., Примаченко Д. Mechanism for Managing Access to Information Resources at an Enterprise. Кібербезпека: освіта, наука, техніка. 2025. № 3 (27). С. 171–183. URL: <https://www.csecurity.kubg.edu.ua/index.php/journal/article/download/743/609>
3. Маньковський Б. Дослідження можливості реалізації концепції Zero Trust в екосистемах Інтернету речей. Кібербезпека: освіта, наука, техніка. 2025. № 2. С. 89–101. URL: <https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/864>
4. Городицький О., Опірський І. Покроковий підхід до імплементації Zero Trust у гібридних

- архітектурах корпоративної безпеки. Кібербезпека: освіта, наука, техніка. 2025. № 3 (31). С. 38–54. URL: <https://csecurity.kubg.edu.ua/index.php/journal/article/download/1029/865>
5. Складаний П. М. Безперервна оцінка доступу в Zero Trust Access Management на основі подієвих сигналів безпеки та динамічного керування сесіями. Математичні машини і системи. 2026. № 1. С. 5–18.
URL: https://www.immsp.kiev.ua/publications/articles/2026/2026_1/01_26_Skladannyi.pdf
6. Kyriakidou C. D. N., Papathanasiou A. M., Siris V. A., Fotiou N. et al. Identity and Access Management for the Computing Continuum. 2025. P. 1–16. URL: <https://arxiv.org/abs/2506.09559>
7. Singh A. P., Kuzminykh I., Ghita B. Industry Perception of Security Challenges with Identity Access Management Solutions. 2024. P. 1–20. URL: <https://arxiv.org/abs/2408.10634>
8. Сагайдак М. Платформні бізнес-екосистеми та моделі управління доступом до даних. Економіка та суспільство. 2025. № 35. С. 44–55. URL: <https://journal.eae.com.ua/index.php/journal/article/download/599/450>
9. Горбань С. Бізнес-екосистеми в Україні: стратегічні напрями розвитку в умовах цифровізації. Scientific Development and Education. 2025. № 8. С. 77–91. URL: <https://www.eu-scientists.com/index.php/sdel/article/download/173/167>
10. Одношєвна О. О., Міньковська А. В., Саванчук Т. М. Антикризове управління як елемент удосконалення системи економічної безпеки в сучасних умовах. Економіка та суспільство. 2023. Вип. 49. С. 55–60. DOI: <https://doi.org/10.32782/2524-0072/2023-49-9>
11. Горбаньова В. О. Цифрова екосистема як основний елемент клієнтоорієнтованої стратегії управління підприємством. Підприємництво та інновації. 2024. № 31. С. 31–36. DOI: doi.org. URL: <https://ei-journal.in.ua/index.php/journal/article/view/647>
12. Рибалко-Рак Л. А., Гусаковська Т. О., Опришко В. І. Цифровізація та антикризове управління: стратегічні зміни для розвитку конкурентоспроможної екосистеми. Проблеми економіки. 2025. № 1 (63). С. 223–229. DOI: doi.org/10.32983/2222-0712-2025-1-223-229
13. Лаптев М., Лаптев С., Захаров О. Стратегії антикризового управління українськими підприємствами в умовах післявоєнної трансформації економіки. Вчені записки Університету «КРОК». 2025. № 2 (78). С. 193–202. DOI: doi.org/10.31732/2663-2209-2025-78-193-202.
14. Приб К. А. Антикризові стратегії в управлінні підприємствами. Економіка та суспільство. 2024. Вип. 70. С. 661–667. DOI: doi.org 10.32782/2524-0072/2024-70-116. С. 661–667
15. Leendertse J., Schrijvers M., Stam E. Measure twice, cut once: Entrepreneurial ecosystem metrics. Research Policy. 2022. Vol. 51, Issue 9. Article 104336. DOI: <https://doi.org/10.1016/j.respol.2021.104336>
16. Audretsch D., Cruz M., Torres J. Revisiting Entrepreneurial Ecosystems. World Bank Policy Research Working Paper. 2022. No. 10229. DOI: <https://doi.org/10.1596/1813-9450-10229>
17. Сагайдак М. П., Білецький Я. О. Управління бізнес-екосистемою в умовах нової нормальності та трансцендентності. Вчені записки КНЕУ. 2024. № 36. С. 138–144. DOI: https://doi.org/10.33111/vz_kneu.36.24.03.20.138.144
18. Horban S., Bilenko O. Business ecosystems in Ukraine: status and development prospects. Social Development: Economic and Legal Issues. 2025. No. 4. P. 15. DOI: <https://doi.org/10.70651/3083-6018/2025.4.15>
19. Дмитренко А. Діджиталізація бізнес-екосистем в сучасній економічній парадигмі в умовах цифрової трансформації економіки. Економіка і регіон. 2025. № 4 (99). URL: <https://journals.nupp.edu.ua/eir/uk/article/view/4166>
20. Горбаньова В. Вплив цифрової трансформації бізнесу на механізми корпоративного управління. Український економічний часопис. 2024. № 4. С. 5–10. DOI: <https://doi.org/10.32782/2786-8273/2024-4-1>

References:

1. Korobeinikova, T. I., & Kravchenko, O. V. (2024). Kontseptsiiia nulovoi doviry: suchasni metody zabezpechennia kiberbezpeky korporatyvnykh merezh [The zero trust concept: Modern

methods of ensuring cybersecurity of corporate networks]. *Visnyk Lvivskoho Derzhavnogo Universytetu Bezpeky Zhyttiediyalnosti*, (30), 156–165. URL: <https://journal.ldubgd.edu.ua/index.php/Visnuk/article/view/2769>

2. Kapeliushna, T., & Prymachenko, D. (2025). Mechanism for Managing Access to Information Resources at an Enterprise. *Kiberbezpeka: Osvita, Nauka, Tekhnika*, 3(27), 171–183. URL: <https://www.csecurity.kubg.edu.ua/index.php/journal/article/download/743/609>

3. Mankivskiy, B. (2025). Doslidzhennia mozhlivosti realizatsii kontseptsii Zero Trust v ekosystemakh Internetu rechei [Researching the possibility of implementing the Zero Trust concept in Internet of Things ecosystems]. *Kiberbezpeka: Osvita, Nauka, Tekhnika*, (2), 89–101. URL: <https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/864>

4. Horodytskyi, O., & Opirskiy, I. (2025). Pokrokovyi pidkhid do implimentatsii Zero Trust u hibrydnykh arkhitekturakh korporativnoi bezpeky [A step-by-step approach to the implementation of Zero Trust in hybrid enterprise security architectures]. *Kiberbezpeka: Osvita, Nauka, Tekhnika*, 3(31), 38–54. URL: <https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/864>

5. Skladannyi, P. M. (2026). Bezperervna otsinka dostupu v Zero Trust Access Management na osnovi podiiivnykh syhnaliv bezpeky ta dynamichnoho keruvannya sesiiamy [Continuous access evaluation in Zero Trust Access Management based on event-driven security signals and dynamic session management]. *Matematychni Mashyny i Systemy*, (1), 5–18. URL: https://www.immsp.kiev.ua/publications/articles/2026/2026_1/01_26_Skladannyi.pdf

6. Kyriakidou, C. D. N., Papathanasiou, A. M., Siris, V. A., & Fotiou, N. (2025). *Identity and access management for the computing continuum* (pp. 1–16). URL: <https://arxiv.org/abs/2506.09559>

7. Singh, A. P., Kuzminykh, I., & Ghita, B. (2024). *Industry perception of security challenges with identity access management solutions* (pp. 1–20). URL: <https://arxiv.org/abs/2408.10634>

8. Sahaidak, M. (2025). Platformni biznes-ekosystemy ta modeli upravlinnia dostupom do danykh [Platform business ecosystems and data access management models]. *Ekonomika ta Suspilstvo*, (35), 44–55. URL: <https://journal.eae.com.ua/index.php/journal/article/download/599/450>

9. Horban, S. (2025). Biznes-ekosystemy v Ukraini: stratehichni napriamy rozvytku v umovakh tsyfryzatsii [Business ecosystems in Ukraine: Strategic development directions in the context of digitalization]. *Scientific Development and Education*, (8), 77–91. URL: <https://www.eu-scientists.com/index.php/sdel/article/download/173/167>

10. Odnosheva, O. O., Minkovska, A. V., & Savanchuk, T. M. (2023). Antykryzove upravlinnia yak element udoskonalennia systemy ekonomichnoi bezpeky v suchasnykh umovakh [Crisis management as an element of improving the economic security system in modern conditions]. *Ekonomika ta Suspilstvo*, (49), 55–60. URL: DOI: <https://doi.org/10.32782/2524-0072/2023-49-9>

11. Horbanova, V. O. (2024). Tsyfrova ekosistema yak osnovnyi element kliientoorientovanoi stratehii upravlinnia pidpriemstvom [Digital ecosystem as a fundamental element of customer-oriented strategy of enterprise management]. *Pidpriemnytstvo ta Innovatsii*, (31), 31–36. URL: DOI: <https://doi.org/10.32782/2415-3583/31.5>

12. Rybalko-Rak, L. A., Husakovska, T. O., & Opryshko, V. I. (2025). Tsyfryzatsiia ta antykryzove upravlinnia: stratehichni zminy dla rozvytku konkurentospromozhnoi ekosystemy [Digitalization and crisis management: Strategic changes for the development of a competitive ecosystem]. *Problemy Ekonomiky*, 1(63), 223–229. URL: DOI: <https://doi.org/10.32983/2222-0712-2025-1-223-229>

13. Laptiev, M., Laptiev, S., & Zakharov, O. (2025). Stratehii antykryzovoho upravlinnia ukraïnskymy pidpriemstvamy v umovakh pisliavoiennoi transformatsii ekonomiky [Strategies of crisis management of Ukrainian enterprises in the conditions of post-war economic transformation]. *Vcheni Zapysky Universytetu KROK*, 2(78), 193–202. URL: <https://doi.org/10.31732/2663-2209-2025-78-193-202>

14. Prib, K. A. (2024). Antykryzovi stratehii v upravlinni pidpriemstvamy [Crisis strategies in enterprise management]. *Ekonomika ta Suspilstvo*, (70), 661–667. URL:

<https://doi.org/10.32782/2524-0072/2024-70-116>.

15. Leendertse, J., Schrijvers, M., & Stam, E. (2022). Measure twice, cut once: Entrepreneurial ecosystem metrics. *Research Policy*, 51(9), Article 104336 URL: <https://doi.org/10.1016/j.respol.2021.104336>.

16. Audretsch, D., Cruz, M., & Torres, J. (2022). Revisiting Entrepreneurial Ecosystems. *World Bank Policy Research Working Paper*, (10229). URL: <https://doi.org/10.1596/1813-9450-10229>.

17. Sahaidak, M. P., & Biletskyi, Ya. O. (2024). Upravlinnia biznes-ekosystemoi v umovakh novoi normalnosti ta transtsendentnosti [Business ecosystem management under the new normality and transcendence]. *Vcheni Zapysky KNEU*, (36), 138–144. URL: https://doi.org/10.33111/vz_kneu.36.24.03.20.138.144.

18. Horban, S., & Bilenko, O. (2025). Business ecosystems in Ukraine: Status and development prospects. *Social Development: Economic and Legal Issues*, (4), 15. URL: <https://doi.org/10.70651/3083-6018/2025.4.15>.

19. Dmytrenko, A. (2025). Didzhitalizatsiia biznes-ekosistem v suchasni ekonomichni paradymy v umovakh tsyfrovoy transformatsii ekonomiky [Digitalization of business ecosystems in the modern economic paradigm under conditions of digital economic transformation]. *Ekonomika i Rehion*, 4(99). URL: <https://journals.nupp.edu.ua/eir/uk/article/view/4166>.

20. Horbanova, V. (2024). Vplyv tsyfrovoy transformatsii biznesu na mekhanizmy korporatyvnoho upravlinnia [The impact of digital business transformation on corporate governance mechanisms]. *Ukrainskyi Ekonomichnyi Chasopys*, (4), 5–10. URL: <https://doi.org/10.32782/2786-8273/2024-4-1>.

OLGA GUSEVA, ARSENI BOYKO. ACCESS MANAGEMENT IN DIGITAL ECOSYSTEMS AS AN ELEMENT OF THE ANTI-CRISIS STRATEGY OF ENTERPRISE.

The article substantiates the theoretical, methodological, and practical foundations of forming an anti-crisis strategy for enterprises operating within digital ecosystems. The leading trends in the development of ecosystem entrepreneurship under conditions of large-scale digitalization are identified, including business platformization, co-opetition, and technological hyper-integration, which cause the erosion of the classical network perimeter and the emergence of permeable inter-organizational boundaries.

The essence of anti-crisis management transformation is investigated, shifting from the isolated protection of an individual economic entity to ensuring the collective resilience of the entire partner network. The author's architecture of the anti-crisis strategy is developed, integrating sequential functional stages of response (contours of economic security, platform technology stack, network interaction, and socio-ethical contour) with radial closure of all processes on a single coordination center — the core of dynamic access management.

The feasibility of deploying this core based on the Zero Trust Architecture with the application of continuous adaptive user rights assessment mechanisms based on security event signals and real-time contextual session management is proven. The strategic role of access management as a fundamental coordination lever ensuring deep resource microsegmentation, the legitimacy of inter-organizational transactions, and the general economic security of enterprises in a turbulent digital environment is defined.

Ключові слова: *access management, digital ecosystem, ecosystem entrepreneurship, anti-crisis strategy, Zero Trust, economic security, platformization, co-opetition, resilience*

Надійшла до редакції: 12.06.2026

Прийнято до друку: 22.06.2026

Опубліковано: 30.06.2026

© 2026 Гусєва О.Ю., Бойко А.О.

Цей матеріал ліцензовано за умовами CC BY 4.0. <https://creativecommons.org/licenses/by/4.0/>