

Економічні наслідки цифровізації: трансформація ризиків і показників ефективності підприємства

З економічної точки зору, цифровізація стимулює підвищення продуктивності праці, зменшення транзакційних витрат, оптимізацію ланцюгів постачання та пришвидшення обороту капіталу. Вона змінює структуру витрат підприємств, трансформує моделі створення доданої вартості та сприяє формуванню нових ринкових ніш. Проте одночасно із цим посилюється залежність бізнесу від цифрових інфраструктур і платформ, що підвищує рівень вразливості до зовнішніх та внутрішніх шоків, у тому числі кіберзагроз, регуляторних обмежень і технологічної монополізації.

Цифровізація змінює саму природу економічних ризиків: на перший план виходять ризики інформаційної асиметрії, втрати даних, збоїв у функціонуванні цифрових платформ і мереж, що здатні паралізувати фінансові потоки та підірвати стійкість підприємств і державних інституцій. Наявні механізми забезпечення безпеки дедалі менше відповідають потребам економіки, оскільки новітні ризики не зводяться лише до технічних чи операційних загроз, а мають стратегічний характер і прямо впливають на конкурентоспроможність, інвестиційну привабливість і макроекономічну стабільність.

Подана у таблиці 1 систематизація демонструє взаємозв'язок між ключовими цифровими ризиками та показниками ефективності й ризику, що дозволяє розглядати цифровізацію не лише як технологічний, а й як економічний феномен.

Таблиця 1

Цифрові ризики та їх кореляція з KPI/KRI підприємства

Вид цифрового ризику	Механізм впливу на бізнес-процеси	Економічні наслідки	KPI (ключові показники ефективності)	KRI (ключові показники ризику)
Ризики кібербезпеки	Порушення безперервності діяльності; зупинка виробництва; втрата даних клієнтів	Прямі фінансові збитки; зростання витрат на відновлення; падіння ринкової капіталізації; зниження довіри інвесторів; зростання страхових премій	EBITDA; рентабельність продажів; продуктивність праці	Частота кіберінцидентів; середній час відновлення (MTTR); частка IT-бюджету, спрямованого на безпеку
Регуляторні ризики	Необхідність перебудови бізнес-процесів, забезпечення системи внутрішнього контролю за дотриманням регуляторних вимог	Зростання транзакційних витрат; ризик штрафів і санкцій; зниження інвестиційної привабливості; обмеження доступу до міжнародних ринків; зростання собівартості продукції	Доступ до нових ринків; коефіцієнт фінансової стійкості; обсяг інвестицій	Кількість випадків невідповідності регуляторним вимогам; витрати на комплаєнс у % від доходу
Залежність від цифрових платформ	Високі витрати на зміну провайдера; ефект технологічної залежності; ризик збоїв у глобальних хмарних сервісах	Зростання собівартості; падіння маржинальності; ризик зупинки критичних процесів; підвищення вартості капіталу; обмеження стратегічної гнучкості	Операційна рентабельність; коефіцієнт оборотності активів; питома вага доходів, сформованих цифровими каналами збуту та обслуговування	Витрати на підтримку IT-інфраструктури у % від виручки; рівень диверсифікації цифрових постачальників

Джерело: авторська розробка.

Отже, систематизація цифрових ризиків демонструє, що цифровізація є амбівалентним фактором економічної безпеки: вона одночасно відкриває нові можливості зростання та створює нові виклики для підприємств. З одного боку, впровадження цифрових технологій сприяє зниженню транзакційних витрат, прискорює обіг капіталу та підвищує продуктивність праці. З іншого – цифрові ризики у вигляді кібератак, регуляторної нестабільності та залежності від платформ формують додаткові витрати на захист інформаційних активів, дотримання нормативних вимог та страхування ризиків. Це породжує необхідність моделювання причинно-наслідкових зв'язків між процесами цифрової трансформації та ключовими економічними показниками, що дозволяє комплексно оцінити як позитивні ефекти, так і загрози для економічної безпеки підприємства.

Цифрові ризики становлять комплекс загроз і вразливостей, що виникають у процесі цифровізації економіки та можуть істотно впливати на конкурентоспроможність підприємств, інвестиційну привабливість і загальний рівень економічної безпеки.

Особливої уваги заслуговує міжнародний досвід управління ризиками бізнес-процесів у цифровій економіці, де визначальним є поєднання стратегічного бачення та використання сучасних цифрових інструментів. Практика зарубіжних країн підтверджує ефективність моделей, що базуються на інтеграції ризик-менеджменту у стратегічне управління, а також на впровадженні механізмів моніторингу й адаптивного реагування [1]. Українські науковці наголошують на потребі ризик-орієнтованого стратегічного управління як ключового

напряму забезпечення економічної безпеки у цифровому середовищі, що вимагає поєднання теоретико-методологічних основ та практичних інструментів [2].

На державному рівні визначальним орієнтиром залишається Стратегія економічної безпеки України на період до 2025 року, де цифровізація прямо розглядається як один із ключових чинників стійкості національної економіки та інституційної спроможності протидіяти ризикам [3]. Проте існують суттєві інституційні прогалини, зокрема: низький рівень гармонізації національного законодавства з європейськими нормами, обмежена кількість секторальних методик та кадровий дефіцит у сфері цифрової безпеки.

Системний аналіз зарубіжних і вітчизняних практик цифрового ризик-менеджменту дає можливість виявити сильні та слабкі сторони існуючих підходів, окреслити критичні «зони ризику» та визначити напрями адаптації міжнародних стандартів в український економічний простір. Це створить підґрунтя для розробки інтегрованої моделі цифрового ризик-менеджменту, здатної забезпечити економічну стійкість і відповідати стратегічним цілям євроінтеграції України.

Моніторинг та раннє попередження цифрових загроз необхідно розглядати не лише як технічний захід, а передусім як економічний інструмент, що зменшує очікувану величину можливих втрат підприємства. Йдеться про запобігання простою виробничих чи фінансових процесів, уникнення штрафних санкцій, а також стабілізацію ринкової вартості бізнесу та довіри інвесторів.

У країнах із високим рівнем інституційної зрілості система протидії цифровим загрозам вибудовується за принципом інтегрованого контуру, де поєднуються кілька ключових елементів:

1. центри моніторингу подій (операційні підрозділи, що забезпечують цілодобовий нагляд за інформаційними системами);
2. системи аналізу та кореляції даних про інциденти (програмні комплекси, які збирають і співставляють інформацію про можливі атаки для своєчасного виявлення закономірностей);
3. команди реагування на інциденти (спеціалізовані групи, що здійснюють координацію дій під час кризових ситуацій);
4. платформи обміну інформацією про загрози між підприємствами та державними органами, які знижують інформаційну асиметрію на ринку [4].

Такі інтегровані системи дають змогу суттєво знизити економічні ризики невизначеності, які виникають унаслідок раптових кіберінцидентів.

Цифровізація сучасної економіки формує нову парадигму управління ризиками, в якій ключового значення набуває взаємозв'язок між технологічними інноваціями та економічною безпекою. Проведена систематизація цифрових ризиків і показників KPI/KRI засвідчує необхідність комплексного підходу до оцінювання впливу цифрових трансформацій на стійкість підприємств. Визначено, що ефективне управління цифровими ризиками потребує інтеграції ризик-менеджменту у стратегічне планування та використання інструментів моніторингу, адаптованих до умов цифрової економіки. Запозичення кращих міжнародних практик та розроблення національної моделі цифрового ризик-менеджменту сприятиме підвищенню конкурентоспроможності підприємств і забезпеченню економічної безпеки України в умовах євроінтеграційних процесів.

Список використаних джерел:

1. Климчук М. М., Ачкасов І. А., Климчук С. А., Поляк О. П. Вплив ризик-менеджменту на формування стратегії управління бізнес-процесами підприємства в умовах цифрової економіки: міжнародний досвід. Бізнес-Інформ. 2021. № 1 (516). С. 272–278. DOI: 10.32983/2222-4459-2021-1-272-278
2. Богуславська С., Бондар Ю., Фесун С. Теоретико-методологічні основи наукових досліджень ризик-орієнтованого стратегічного управління в умовах цифровізації. Цифрова економіка та економічна безпека. 2024. № 3 (12). С. 3–7. DOI: <https://doi.org/10.32782/dees.12-1>
3. Про Стратегію економічної безпеки України на період до 2025 року: Указ Президента України від 11.08.2021 № 347/2021. URL: <https://zakon.rada.gov.ua/laws/show/347/2021#Text>
4. European Union Agency for Cybersecurity (ENISA). How to Set Up CSIRT and SOC: Good Practice Guide. December 2020. 57 p. ISBN 978-92-9204-410-7; DOI 10.2824/056764.