



Фінанси, банківська справа, страхування та фондовий ринок

УДК: 338.14:658.52.011

DOI <https://doi.org/10.5281/zenodo.15540326>

Концептуальна модель оцінки економічної безпеки підприємства в умовах цифрової трансформації

Біличенко Максим Миколайович

аспірант кафедри економіки

Державного університету «Київський Авіаційний Інститут», м. Київ, Україна,

<https://orcid.org/0000-0003-4657-1039>

Прийнято: 18.05.2025 | Опубліковано: 29.05.2025

***Анотація.** Метою статті є розроблення та обґрунтування концептуальної моделі економічної безпеки підприємства в умовах цифрової трансформації, яка враховує особливості впливу цифрових ризиків на ключові підсистеми функціонування підприємств. У роботі підкреслюється необхідність переосмислення класичних підходів до забезпечення економічної безпеки в контексті зростаючих викликів цифрової епохи, зокрема з урахуванням кіберзагроз, технічної вразливості та поведінкових ризиків персоналу. Методологічною основою дослідження є комплексне застосування системного підходу, методів моделювання, аналізу ризиків, інтелектуальних алгоритмів виявлення аномалій, прогнозування фінансової стійкості, а також інструментів нечіткої логіки та багатокритеріального прийняття рішень. Для формалізації інтегрального показника економічної безпеки використано комплементарну математичну модель, яка об'єднує результати оцінки фінансової, кадрової та техніко-технологічної підсистем.*



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

У процесі дослідження виявлено, що цифрова трансформація найбільшою мірою впливає саме на ці три підсистеми, змінюючи як можливості розвитку підприємства, так і вектори нових загроз. Показано, що фінансова безпека у цифровому середовищі тісно пов'язана з ризиками використання цифрових сервісів та шахрайства. Кадрова безпека потребує нових методів оцінювання через ризики інсайдерської активності та цифрової неетичності. Техніко-технологічна підсистема демонструє зростаючу залежність від IT-інфраструктури, що вимагає використання адаптивних моделей оцінювання з урахуванням багатофакторності. На основі аналізу та узагальнення даних запропоновано інтегральний індекс економічної безпеки підприємства, побудований з урахуванням ймовірності банкрутства, кількості аномальних дій персоналу та рівня техніко-технологічного захисту. Проведено візуалізацію залежності рівня безпеки від зміни зазначених факторів, що дозволяє підвищити якість управлінських рішень у реальному часі. Практична цінність моделі полягає у її здатності до адаптації, автоматизації моніторингу та інтеграції у стратегічне планування.

Ключові слова: економічна безпека підприємства, цифрова трансформація, кадрові ризики, техніко-технологічна безпека, фінансова стійкість, цифрові ризики, інформаційна система.

A conceptual framework for assessing enterprise economic security in the context of digital transformation

Maksym Bilychenko

Postgraduate Student of the Department of Economy of the State University

«Kyiv Aviation Institute», Kyiv, Ukraine,

<https://orcid.org/0000-0003-4657-1039>



Abstract. *The purpose of this article is to develop and substantiate a conceptual model of enterprise economic security in the context of digital transformation, taking into account the impact of digital risks on key functional subsystems. The study emphasizes the need to revise classical approaches to economic security in light of growing digital-era challenges, including cyber threats, technical vulnerabilities, and staff behavioral risks. The research methodology is based on a comprehensive systems approach, incorporating modeling methods, risk analysis, intelligent anomaly detection algorithms, financial stability forecasting, as well as fuzzy logic and multi-criteria decision-making tools. To formalize the integrated economic security indicator, a complementary mathematical model is proposed, which aggregates the results of assessing the financial, personnel, and techno-technological subsystems.*

The study reveals that digital transformation has the greatest impact on these three subsystems, simultaneously creating development opportunities and introducing new threats. The analysis shows that financial security in a digital environment is closely linked to risks associated with digital services and fraud. Personnel security requires new evaluation methods due to insider threats and issues of digital ethics. The techno-technological subsystem demonstrates increasing dependence on IT infrastructure, necessitating the use of adaptive assessment models that account for multi-factor uncertainty. Based on the analysis and generalization of empirical data, the article proposes an integrated index of enterprise economic security, which combines the probability of bankruptcy, the number of anomalous employee actions, and the level of techno-technological protection. The practical value of the proposed model lies in its adaptability, capacity for automated monitoring, and applicability in strategic planning for enterprises operating in digital environments.



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

Keywords: *enterprise economic security, digital transformation, personnel risks, techno-technological security, financial stability, digital threats, information system.*

Постановка проблеми. В умовах стрімкого розвитку цифрових технологій підприємства дедалі активніше впроваджують інформаційно-комунікаційні технології, штучний інтелект, інтернет речей та хмарні сервіси. Це сприяє формуванню інтегрованого цифрового середовища, в межах якого бізнес-процеси реалізуються з мінімальними витратами часу, ресурсів та з підвищеним рівнем ефективності. Цифровізація включає не лише автоматизацію рутинних операцій, а й розширення можливостей аналітики великих даних для прийняття управлінських рішень, розвиток електронної комерції та вдосконалення механізмів взаємодії з клієнтами.

Ключовими напрямками цифрової трансформації підприємств є оптимізація виробничих і управлінських процесів, розроблення нових цифрових продуктів і сервісів, а також впровадження гнучких, адаптивних бізнес-моделей. Відповідно до наукових досліджень [1], цифрові технології мають найбільший вплив на такі стратегічно важливі елементи бізнесу, як побудова ціннісної пропозиції, взаємодія з клієнтами та управління внутрішніми бізнес-процесами.

Підприємства, які здійснюють стратегічне впровадження цифрових технологій у свої бізнес-процеси та ІТ-інфраструктуру, отримують значні конкурентні переваги. Результати емпіричних досліджень [2] свідчать, що ефективна цифрова трансформація дозволяє не лише підвищити ефективність внутрішніх операційних процесів, а й покращити координацію та інформаційний обмін в рамках бізнес-екосистеми – зокрема, між постачальниками, партнерами та клієнтами. Завдяки цьому формується додаткова цінність для кінцевого споживача, зміцнюється



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

конкурентоспроможність підприємства та зростає його економічна стійкість в умовах цифрової економіки.

Разом із тим, цифрова трансформація супроводжується не лише відкриттям нових можливостей, а й появою специфічних ризиків та загроз, зумовлених цифровою природою нових процесів. Ці ризики можуть проявлятися як на етапі впровадження цифрових рішень, так і під час їхньої експлуатації. Особливу увагу необхідно приділяти питанням кібербезпеки, збереження конфіденційності даних, захисту цифрової інфраструктури. Так, згідно з результатами дослідження, проведеного корпорацією Microsoft, 62 % малих і середніх підприємств у світі вважають кіберзагрози одним із головних бар'єрів на шляху до цифрової трансформації [3]. Найбільш поширеними побоюваннями є витоки персональних та комерційних даних, зловмисне втручання у цифрові системи, атаки на інфраструктуру. Такі загрози істотно стримують готовність компаній до повноцінної цифрової інтеграції та підкреслюють необхідність врахування цифрових ризиків у системі економічної безпеки підприємства.

Аналіз останніх досліджень і публікацій. Проблематика формування системи економічної безпеки підприємства залишається актуальною як у вітчизняному, так і в зарубіжному науковому дискурсі. У класичних підходах акцент робиться переважно на аналізі внутрішніх загроз та стабільності функціонування підприємства, однак сучасні виклики, пов'язані з цифровою трансформацією, зумовлюють потребу в оновленні концептуального апарату та методологічного інструментарію.

Оглядовий аналіз літератури, здійснений у роботі Ю. Шутяк, О. Даниленко і Д. Ван Цайлліє [4], базується на дослідженні понад 50 українських дисертацій, присвячених економічній безпеці підприємств у пострадянських країнах. Було узагальнено основні підходи до її концептуалізації, зокрема у вітчизняній економічній науці.



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

Однак нові підходи, що виникли на тлі цифровізації, пропонують переосмислення самої структури економічної безпеки. Так, у дослідженні Ю. Самойленка та інших [5] було запропоновано заміну застарілого поняття «інформаційна безпека» на «цифрову безпеку підприємства» як окремий компонент економічної безпеки. Автори здійснили аналіз взаємозв'язку рівня цифрової безпеки підприємств із особливостями інституційного середовища та масштабами компаній у країнах Європейського Союзу, тим самим розширивши традиційні рамки оцінювання безпеки.

У свою чергу, системну класифікацію цифрових ризиків у структурі економічної безпеки промислових підприємств запропоновано у роботі Н. Касьянкової, Н. Кравчук та Ю. Коваль [6], де акцентовано увагу на багаторівневому розподілі ризиків, а також на їх впливі на ключові підсистеми підприємства.

Проблема адаптації системи економічної безпеки до цифрових умов більш детально розглянута у праці К. Полупанова, О. Кхаджунова та З. Сіманавіціене [7]. У статті здійснено узагальнення принципів адаптації та представлено структурну модель адаптованої системи безпеки, що враховує вплив цифрової трансформації на внутрішні процеси підприємств. В той же час, ця модель розкриває лише загальні принципи роботи такої системи, в той час як в ній відсутня інформація про будь-які методи оцінки чи кількісного вираження рівня економічної безпеки підприємства.

У дослідженні А. Гарагуліа, В. Суслов та О. Горової [8] розглянуто сучасні інструменти управління економічною безпекою в умовах цифровізації та глобальних викликів, включно з війною в Україні. Особливу увагу приділено таким практичним інструментам як страхування ризиків, прогнозування, аналітичне моделювання, що інтегруються у систему стратегічного менеджменту безпеки.



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

Узагальнюючи, слід зазначити, що сучасні наукові дослідження поступово переходять від фрагментарного аналізу до комплексних моделей, які враховують вплив цифрових технологій на всі основні підсистеми підприємства.

Виділення невирішених раніше частин загальної проблеми. Водночас на основі узагальнення сучасних досліджень та практики цифрової трансформації можна виокремити низку проблем і ризиків, які супроводжують підприємства в процесі цифровізації. Ці ризики мають комплексний характер і охоплюють як технічну, так і організаційно-управлінську сфери, що істотно впливає на загальний рівень економічної безпеки підприємства в цифрову епоху. Основними типами ризиків, характерними для цифрового середовища, є кіберризики, ризики конфіденційності, інсайдерські ризики, технічні збої, шахрайство у цифровому середовищі, ризики некомпетентності, ризики старіння технологій.

Залишаються невизначеними підходи до інтеграції цифрових ризиків у систему оцінювання економічної безпеки підприємства, зокрема в аспектах, що стосуються взаємозв'язку між цифровою трансформацією та функціонуванням окремих підсистем економічної безпеки. Окрім того, недостатньо досліджено практичні механізми формалізації впливу цифрових ризиків на загальний рівень економічної безпеки, зокрема через відсутність уніфікованих моделей, здатних поєднувати кількісні та якісні характеристики ризиків, притаманних цифровому середовищу.

Зазначені аспекти актуалізують необхідність подальших наукових досліджень, зосереджених на формалізації цифрових ризиків у контексті економічної безпеки підприємств, розробці інтегрованих моделей оцінювання, здатних враховувати як кількісні, так і якісні параметри, а також створенні інструментарію, що забезпечує адаптивність і гнучкість систем безпеки в умовах цифрової трансформації.



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

Формулювання цілей статті (постановка завдання). Метою статті є розроблення та обґрунтування концептуальної моделі економічної безпеки підприємства в умовах цифрової трансформації, яка враховує необхідність *оцінки та інтеграції фінансової, кадрової та техніко-технологічної підсистем* в контексті нових цифрових викликів.

Виклад основного матеріалу дослідження. Сучасна система безпеки має бути адаптивною, динамічною та здатною до швидкого реагування на нові загрози, породжені цифровими змінами. Як слушно зазначено у новітніх дослідженнях [9], у структурі економічної безпеки доцільно виокремлювати цифрову безпеку підприємства як окремий компонент. Цей підхід замінює застарілу категорію «інформаційна безпека», оскільки цифрове середовище охоплює значно ширший спектр ризиків, які потребують специфічних механізмів реагування. У зв'язку з цим постає необхідність переосмислення традиційних підходів до моделювання економічної безпеки підприємства. Серед усіх елементів системи економічної безпеки підприємства найбільш значущий вплив цифрова трансформація чинить на фінансову, кадрову та техніко-технологічну підсистеми. Це зумовлено як фундаментальним значенням зазначених компонентів для функціонування підприємства, так і високим рівнем їх чутливості до цифрових змін.

1. У цифрову епоху фінансова підсистема підприємства зазнає істотної трансформації під впливом впровадження інформаційно-комунікаційних технологій. Цифровізація відкриває нові можливості для зростання доходів, оптимізації витрат і підвищення ефективності фінансового управління, але водночас супроводжується появою нових ризиків, які ускладнюють забезпечення фінансової безпеки.

Серед позитивних аспектів цифрового впливу на фінансову систему підприємства можна виділити:



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

- створення нових каналів продажів через електронну комерцію, що сприяє розширенню ринків збуту, підвищенню обороту та зменшенню транзакційних витрат;

- використання цифрового маркетингу забезпечує персоналізацію пропозицій і таргетовану взаємодію з цільовими аудиторіями, що підвищує коефіцієнт конверсії та рентабельність інвестицій у комунікації;

- монетизація цифрових активів і послуг (зокрема програмних продуктів, онлайн-сервісів, цифрових платформ), яка створює нові джерела доходу та підвищує фінансову гнучкість підприємства.

Однак негативний вплив цифровізації також має вагомe значення у контексті фінансової безпеки:

- залежність від цифрових сервісів (зокрема платіжних платформ, хмарних бухгалтерських систем або аналітичних сервісів) робить фінансову систему вразливою до технічних збоїв, збоїв у постачанні сервісів та змін у політиках провайдерів;

- шахрайство у цифрових каналах продажів, включаючи фішингові атаки, підміну платіжних реквізитів і маніпуляції з електронними транзакціями, призводить до фінансових втрат та знижує довіру клієнтів і партнерів до цифрових інструментів.

Таким чином, формування сучасної фінансової безпеки передбачає збереження фінансової стійкості підприємства в умовах цифрової економіки. З огляду на це, оцінювання фінансової підсистеми економічної безпеки дедалі частіше базується на інструментах моделювання та прогнозування, орієнтованих на виявлення кризових станів і побудову систем фінансового раннього попередження. Основу таких рішень становлять дві ключові групи моделей:

- моделі прогнозування банкрутства, що оцінюють ймовірність втрати платоспроможності на основі історичних та поточних фінансових даних [10];



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

- моделі фінансового попередження, які дозволяють завчасно виявляти сигнали майбутніх проблем і формувати управлінські дії для їх уникнення.

Сучасні методології охоплюють як традиційні статистичні підходи (дискримінантний аналіз, логістична регресія), так і методи штучного інтелекту (нейронні мережі, дерева рішень, SVM), а також алгоритми машинного навчання, які значною мірою покладаються на аналітику великих даних [11]. Зокрема, використання технологій deep learning дозволяє моделювати складні, нелінійні взаємозв'язки між фінансовими та нефінансовими змінними, що значно підвищує точність оцінок. У міжнародній практиці все більшого поширення набуває використання ансамблевих методів, таких як XGBoost та Random Forest, які демонструють високу точність і стійкість до шумів у даних [12].

У цифровому контексті фінансова безпека вже не може розглядатися відірвано від технологічних і поведінкових змін – саме тому результатом оцінювання фінансової підсистеми все частіше виступає не лише класичні фінансові змінні, а й використання індикаторів цифрової чутливості та цифрового розвитку. Можна стверджувати, що інтеграція цифрових факторів у моделі прогнозування банкрутства та фінансової безпеки є обов'язковою умовою ефективного управління ризиками підприємства у цифрову добу.

2. Кадрова підсистема економічної безпеки в умовах цифрової трансформації зазнає істотної еволюції, оскільки цифрові технології докорінно змінюють умови праці, вимоги до компетентностей персоналу та систему управління людськими ресурсами. З одного боку, цифровізація створює нові можливості для підвищення ефективності використання трудових ресурсів, з іншого – породжує специфічні ризики, що загрожують стабільності кадрового потенціалу.

Серед позитивного впливу цифровізації на кадрову систему підприємства варто виділити такі аспекти:



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

- підвищення продуктивності праці за рахунок автоматизації рутинних операцій, що дозволяє працівникам зосередитися на стратегічно важливих функціях і підвищує загальну ефективність бізнес-процесів;

- гнучкі умови праці, включаючи дистанційну та гібридну зайнятість, що сприяє зростанню лояльності персоналу, зниженню витрат на утримання офісів та можливості залучення висококваліфікованих фахівців.

Проте цифровізація породжує також ризики, що негативно впливають на кадрову безпеку, зокрема:

- витік конфіденційної інформації з боку працівників, які мають доступ до даних або комерційної таємниці, що створює загрозу інсайдерських атак;

- порушення конфіденційності персональних даних через неналежний захист цифрових кадрових систем;

- кадровий дефіцит, зумовлений високим попитом на IT-фахівців, фахівців з кібербезпеки та цифрових аналітиків, що ускладнює швидку адаптацію підприємства до нових технологічних вимог.

У цьому контексті забезпечення кадрової безпеки в умовах цифрової трансформації повинно передбачати управління цифровими компетентностями персоналу, впровадження політик цифрової етики та інформаційної гігієни, а також організацію внутрішнього контролю та моніторингу поведінки працівників у цифрових середовищах.

Таким чином, оцінювання рівня безпеки кадрової підсистеми має здійснюватися з урахуванням нових загроз і можливостей, які постають у цифровому середовищі. Зважаючи на це, актуальним є використання інтелектуальних моделей для оцінювання кадрової безпеки, що дозволяють аналізувати поведінкові шаблони персоналу в інформаційному середовищі.

Значну увагу в оцінюванні рівня безпеки кадрової підсистеми в умовах цифровізації приділяють методам інтелектуального аналізу даних, а одним із перспективних підходів до виявлення внутрішніх загроз є побудова моделей



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

аномальної поведінки персоналу. Наприклад, в роботі [13] запропоновано мультиперспективну систему моніторингу працівників, яка використовує алгоритм One-Class SVM для виявлення нетипових дій у корпоративній мережі. Такий підхід дозволяє мінімізувати кількість хибнопозитивних сигналів та фокусуватися на дійсно ризикованих сценаріях. Альтернативне рішення представлено у дослідженні [14], де застосовано приховані марковські моделі для аналізу поведінки персоналу в часовому вимірі. Завдяки здатності ідентифікувати відхилення від типових шаблонів дій працівників, ці моделі ефективно виявляють потенційно небезпечну активність.

Отже, комплексна оцінка кадрової підсистеми економічної безпеки в умовах цифровізації повинна ґрунтуватися на визначенні кількості та інтенсивності виявлених аномалій, що сигналізують про ризиковану поведінку працівника. Такий підхід дає змогу сформулювати інтегральний показник безпеки, який враховує як технічні аспекти захисту інформації, так і поведінкові характеристики персоналу.

3. Цифрова трансформація значною мірою змінює техніко-технологічну основу функціонування підприємств, сприяючи переходу до інтелектуальних виробничих систем, автоматизованих процесів управління та підвищеної технологічної гнучкості. Саме техніко-технологічна підсистема є критичною для підтримання стійкості підприємства в умовах динамічних змін ринкового середовища, оскільки вона забезпечує операційну ефективність і здатність до швидкої адаптації.

До ключових позитивних ефектів цифровізації цієї підсистеми належать:

- створення адаптивних і гнучких виробничих систем, що завдяки застосуванню цифрових технологій (інформаційно-комунікаційних технологій, цифрових двійників, SCADA-систем) дозволяють швидко перебудовувати виробничі процеси відповідно до змін у попиту та ресурсних умовах;



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

- оптимізація використання ресурсів, включаючи енергію, матеріали та час, що забезпечується за рахунок автоматизованого моніторингу, предиктивного аналізу та алгоритмів машинного навчання, що знижує загальні виробничі витрати й підвищує конкурентоспроможність.

Утім, цифровізація технічної бази підприємства супроводжується і новими ризиками, що суттєво ускладнюють забезпечення техніко-технологічної безпеки:

- вразливість до кібератак на системи управління через появу доступу до великих обсягів даних;

- тимчасова зупинка виробництва через помилки програмного забезпечення, втрату зв'язку або відмову окремих цифрових елементів;

- прискорене моральне старіння технологій, яке зумовлює постійну потребу в оновленні, що в свою чергу потребує додаткових інвестицій.

У підсумку, цифровізація кардинально змінює техніко-технологічну основу функціонування підприємств, що, з одного боку, сприяє зростанню продуктивності та ефективності, а з іншого – породжує нові технічні та кіберризики. У такому складному та динамічному середовищі оцінка стану техніко-технологічної підсистеми економічної безпеки підприємства набуває особливої ваги, адже саме від неї залежать стабільність виробництва, технологічна стійкість та здатність адаптуватися до змін.

Враховуючи те, що виробничі підприємства суттєво відрізняються за рівнем технологічного розвитку, структурою основних фондів, інтенсивністю використання цифрових технологій та рівнем ІТ-захисту, створення універсальної моделі оцінювання техніко-технологічної підсистеми економічної безпеки є проблематичним. До того ж, численні параметри цієї підсистеми не піддаються однозначному кількісному вимірюванню, особливо в умовах невизначеності, властивій цифровому середовищу. Саме тому



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

доцільним є застосування методів, здатних враховувати нечіткість, багатфакторність і експертні судження.

Одним із найбільш ефективних підходів є застосування методів нечіткої логіки, що дозволяє формалізувати як кількісні, так і якісні характеристики, зокрема: рівень ризику цифрових збоїв, стан технічного парку, ступінь автоматизації виробництва чи цифрову компетентність персоналу. Нечітке моделювання забезпечує можливість використання лінгвістичних змінних та побудову правил типу «якщо – то», що, у свою чергу, дає змогу оцінити потенційні загрози на основі функцій належності до відповідних класів ризику чи рівнів технологічної готовності [15]. Сучасні дослідження підтверджують ефективність інтегративних підходів, які поєднують нечітку логіку з методами багатокритеріального прийняття рішень. Зокрема, такі методи як Fuzzy AHP, Fuzzy Best-Worst Method, Fuzzy TOPSIS чи Fuzzy VIKOR дозволяють не лише визначати вагомість окремих факторів ризику, але й враховувати їхню взаємозалежність і вплив у контексті цифрової трансформації [16].

Таким чином, поєднання експертних методів з нечіткими моделями та цифровими індикаторами є науково обґрунтованим підходом до оцінювання техніко-технологічної підсистеми економічної безпеки підприємства. Це дозволяє здійснити комплексний аналіз, що охоплює цифрові ризики, ступінь автоматизації, інноваційний потенціал обладнання, рівень ІТ-захисту та кваліфікацію персоналу, який працює з цифровими системами.

Для узагальнення результатів оцінювання широко застосовується інтегральний показник, який виступає комплексною мірою техніко-технологічної підсистеми економічної безпеки підприємства. Такий показник може бути основою для стратегічного планування технічної модернізації, підвищення кіберстійкості або оптимізації інвестицій у технологічну інфраструктуру в умовах цифрової економіки.



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

На підставі здійсненого оцінювання фінансової, кадрової та техніко-технологічної підсистем економічної безпеки доцільним є формування єдиної інтегральної оцінки, яка слугуватиме кількісною характеристикою загального рівня безпеки підприємства. Такий підхід дозволяє не лише узагальнити вплив окремих факторів ризику, а й забезпечити уніфіковану основу для прийняття стратегічних і тактичних управлінських рішень. В умовах цифрової трансформації, коли підприємства функціонують у багатофакторному, динамічному та часто непередбачуваному середовищі, побудова узагальненого інтегрального показника економічної безпеки набуває особливого значення. Зростання кількості ризиків, пов'язаних з інформаційною, кібернетичною та технологічною вразливістю, обумовлює потребу в створенні агрегованого інструменту оцінювання, який враховує особливості цифрового контексту.

З огляду на це, в межах дослідження запропоновано формальну модель інтегрального показника економічної безпеки підприємства в умовах цифровізації I_s , який об'єднує результати оцінювання трьох ключових підсистем:

$$I_s = w_1 \cdot (1 - K_f) + w_2 \cdot \left(1 - \frac{K_k}{K_k + 1}\right) + w_3 \cdot K_t$$

де:

K_f – прогнозована ймовірність банкрутства як оцінка фінансової підсистеми.

K_k – кількість аномальних дій працівників як оцінка кадрової підсистеми.

K_t – інтегральний індекс техніко-технологічної безпеки як оцінка техніко-технологічної підсистеми.

w_1, w_2, w_3 – вагові коефіцієнти кожного компонента, які відображають відносну значущість відповідної підсистеми.



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

Запропонована структура індексу базується на комплементарній формі оцінювання. Зокрема, показник $1 - K_f$ інтерпретується як зростаюча функція фінансової стійкості: чим нижчою є ймовірність банкрутства, тим вищим є внесок цього компонента у загальну оцінку безпеки. Для кадрової складової використано асимптотичну залежність типу $\left(1 - \frac{K_k}{K_k + 1}\right)$, яка зменшується із ростом кількості аномальних дій, забезпечуючи нелінійність та чутливість до кадрових ризиків. Техніко-технологічна складова K_t має лінійний позитивний вплив: її значення варіюється в межах $[0;1]$, де 1 означає повну технологічну захищеність.

Інтегральний індекс економічної безпеки дозволяє надати керівництву підприємства узагальнений стан безпеки з урахуванням трьох критично важливих напрямів: фінансів, персоналу та технологій. Цей показник враховує ризики, що виникають у цифровому середовищі, та дозволяє оперативно виявляти тенденції, які загрожують стабільності підприємства.

Практична цінність інтегрального індексу полягає не лише у формальному оцінюванні, а й у можливості візуалізації його поведінки залежно від зміни ключових ризиків. У межах дослідження була побудована тривимірна візуалізаційна модель (рис. 1), яка відображає залежність інтегрального показника I_s , від змін рівня ймовірності банкрутства (K_f), кількості аномальних дій працівників (K_k) та рівня технологічної безпеки (K_t). Такий підхід дозволяє наочно продемонструвати чутливість інтегральної безпеки до кожного типу ризиків та сприяти прийняттю обґрунтованих управлінських рішень. У даному випадку для візуалізації були обрані наступні вагові коефіцієнти $w_1 = 0.4, w_2 = 0.3, w_3 = 0.3$, що відображає домінуючий вплив фінансової стійкості на загальний рівень економічної безпеки в умовах цифрової економіки.

Заключним етапом функціонування запропонованої інформаційної системи є формування управлінських рекомендацій на основі розрахованого



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

значення інтегрального індексу економічної безпеки. Ці рекомендації повинні мати адаптивний характер і бути спрямовані на усунення або мінімізацію виявлених слабких місць у відповідних підсистемах – фінансовій, кадровій чи техніко-технологічній. Таким чином, рішення щодо управління безпекою приймаються не інтуїтивно, а на основі структурованої аналітики та об'єктивних індикаторів.

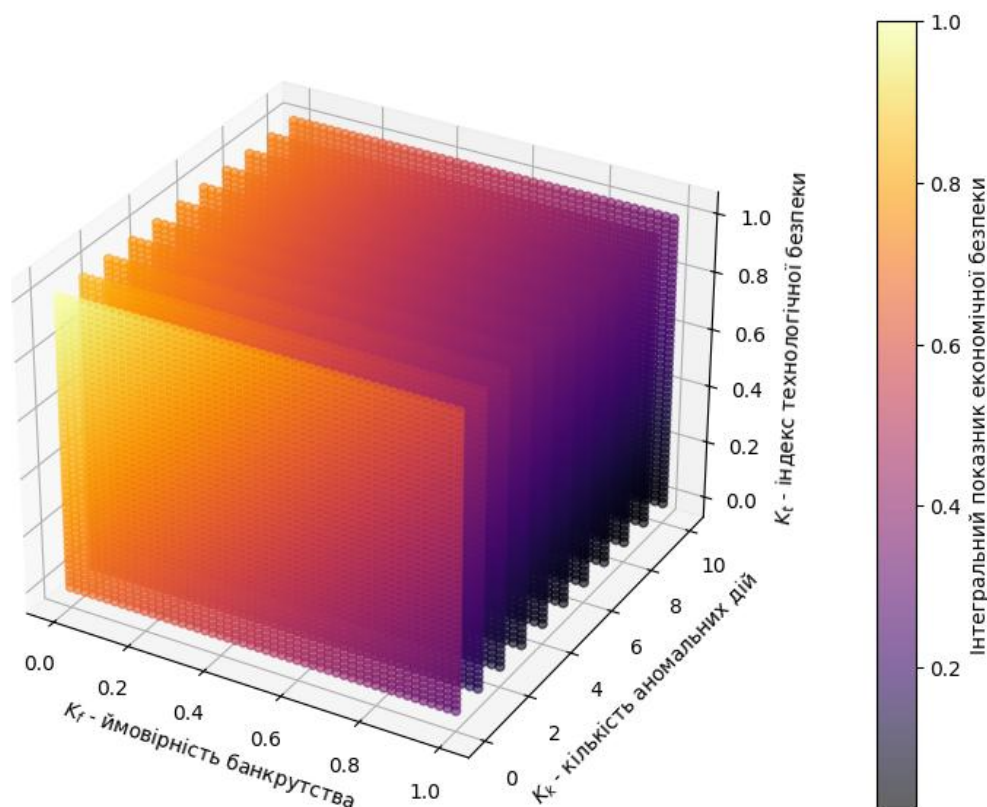


Рис. 1. Візуалізація інтегрального індексу економічної безпеки підприємства залежно від значень компонентів.

Джерело: власна розробка автора

Отже, у результаті проведеного дослідження була сформована концептуальна модель системи економічної безпеки підприємства в умовах цифрової трансформації (рис. 2). Модель структурована за трьома базовими підсистемами – фінансовою, кадровою та техніко-технологічною – які є



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

найбільш чутливими до цифрових змін і водночас визначальними для загального рівня економічної стійкості.

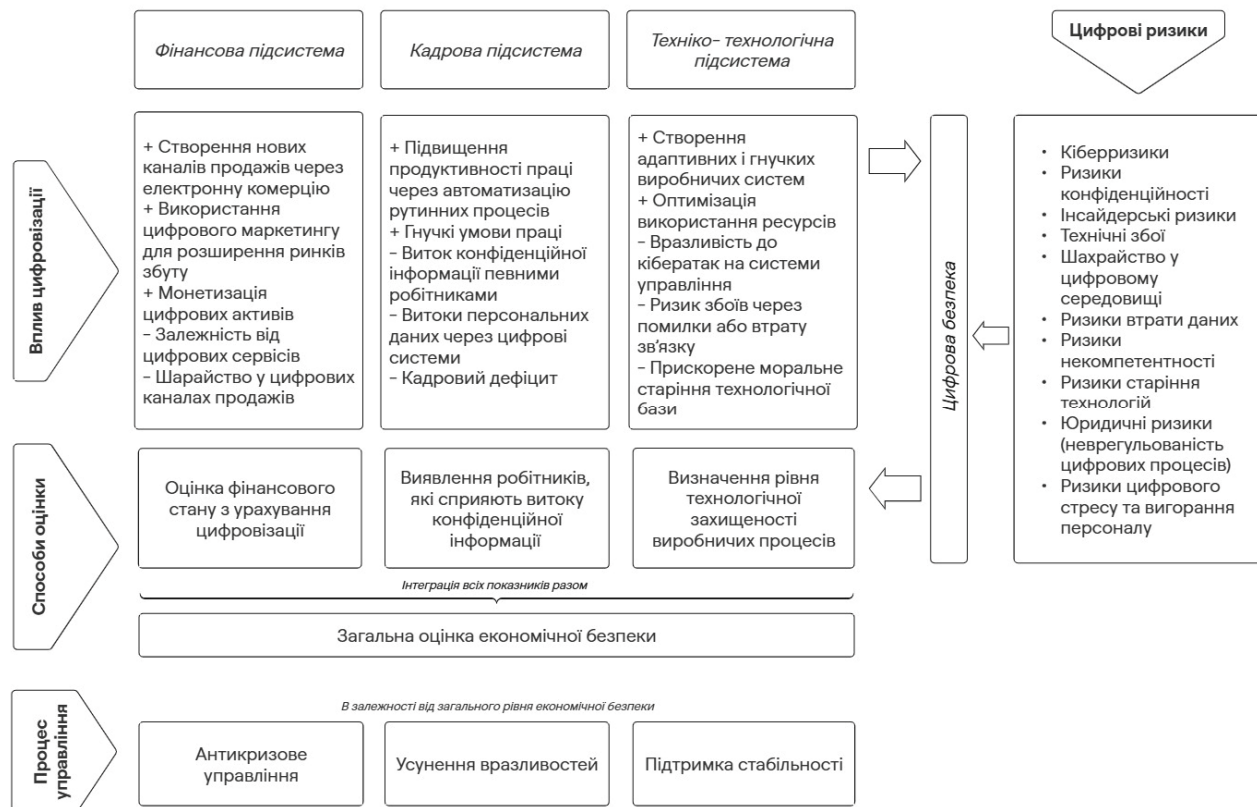


Рис. 2. Загальна схема системи економічної безпеки підприємства в умовах цифрової трансформації.

Джерело: власна розробка автора

Висновки. Розроблена модель має високу прикладну цінність для підприємств різних галузей, які впроваджують цифрові технології або функціонують у цифровізованому середовищі. Її практичне застосування дозволяє:

- системно оцінювати стан економічної безпеки підприємства з урахуванням цифрових ризиків, індикаторів і впливів;
- автоматизувати моніторинг ключових параметрів за допомогою інформаційної системи, що базується на сучасних алгоритмах аналізу;



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

- підтримувати стратегічне планування завдяки можливості оперативного виявлення критичних точок у системі безпеки;
- забезпечити адаптивність рішень через зворотний зв'язок і регулярне оновлення даних.

Таким чином, запропонована концептуальна модель економічної безпеки підприємства в умовах цифрової трансформації не лише забезпечує комплексне бачення внутрішніх і зовнішніх загроз, але й формує надійний інструментарій для прийняття рішень у реальному часі. Її впровадження сприяє підвищенню адаптивності, зниженню вразливості до цифрових ризиків і збереженню стійкості підприємства в умовах турбулентного цифрового середовища.

Список використаних джерел

1. Зуб П., Калач Г. Цифровізація бізнес-процесів промислових підприємств // Економіка та суспільство. 2021. Вип. 26. URL: <https://doi.org/10.32782/2524-0072/2021-26-52>
2. Christian M., Thomas H., Benlian A. Digital Transformation Strategies // Business & Information Systems Engineering. 2015. Vol. 57, Iss. 5. P. 339–343. URL: <https://aisel.aisnet.org/bise/vol57/iss5/5>
3. The Future of the Medium-Sized Business: 7 Trends Driving SMEs' Digital Transformation [Електронний ресурс]. – Microsoft, 2019. – URL: <https://info.microsoft.com/rs/157-GQE-382/images/eBook%20SMB%20of%20the%20Future%20FINAL%202019-07-29.pdf>
4. Shutyak Y., Danylenko O., Van Caillie D. Conceptualization of economic security of the enterprise: a literature review // Proceedings of the 3rd REDETE Conference “Economic Development and Entrepreneurship in Transition Economies”, 10 April 2014, Banja Luka, Bosnia and Herzegovina. P. 145–152.



5. Samoilenko Y., Britchenko I., Levchenko I., Lošonczi P., Bilichenko O., Bodnar O. Economic Security of the Enterprise Within the Conditions of Digital Transformation // *Economic Affairs*. 2022. Vol. 67, No. 4. P. 619–629. URL: <https://ssrn.com/abstract=4260470>

6. Касьянова Н. В., Кравчук Н. М., Коваль Ю. Л. Безпека підприємства в умовах цифрової трансформації економіки // *Modern Economics*. 2020. № 20. С. 124–129. DOI: [https://doi.org/10.31521/modecon.V20\(2020\)-20](https://doi.org/10.31521/modecon.V20(2020)-20)

7. Polupanova K., Khadzhynova O., Simanavičienė Ž. Influence of digital transformation on economic security of enterprises // *Public Security and Public Order*. 2022. No. 31. URL: <https://doi.org/10.13165/PSPO-22-31-17>

8. Harahulia A., Suslov V., Horovoy O. Management of economic security of enterprises in the context of digital transformation // *Baltic Journal of Economic Studies*. 2023. Vol. 9, No. 5. P. 87–93. DOI: <https://doi.org/10.30525/2256-0742/2023-9-5-87-93>

9. Касьянова Н. В., Біличенко М. М., Севериненко А. О. Моделювання цифрової безпеки підприємства // *Modern Economics*. 2023. № 39. С. 54–61. DOI: [https://doi.org/10.31521/modecon.V39\(2023\)-08](https://doi.org/10.31521/modecon.V39(2023)-08)

10. Харчук Т. В., Кредісов В. А., Мельник В. В., Пурденко О. А. Удосконалення методів оцінювання рівня фінансової безпеки підприємств в Україні // *Фінансова та кредитна діяльність: проблеми теорії і практики*. 2021. № 1 (32). С. 213–222. DOI: <https://doi.org/10.18371/fcaptp.v1i32.200300>

11. Peng Y., Wang G., Kou G., Shi Y. An empirical study of classification algorithm evaluation for financial risk prediction // *Applied Soft Computing*. 2011. Vol. 11, No. 2. P. 2906–2915. DOI: <https://doi.org/10.1016/j.asoc.2010.11.028>

12. Shi Y., Li X. An overview of bankruptcy prediction models for corporate firms: A systematic literature review // *Intangible Capital*. 2019. Vol. 15, No. 2. P. 114–127. DOI: <https://doi.org/10.3926/ic.1354>



13. Raissi-Dehkordi M., Carr D. A multi-perspective approach to insider threat detection // MILCOM 2011 Military Communications Conference, 7–10 November 2011, Baltimore, MD, USA. – IEEE, 2011. – P. 1164–1169. – DOI: 10.1109/MILCOM.2011.6127457

14. Rashid T., Agrafiotis I., Nurse J. A new take on detecting insider threats: exploring the use of hidden Markov models // 8th ACM CCS International Workshop on Managing Insider Security Threats. 2016. [Електронний ресурс]. URL: <https://www.cs.ox.ac.uk/files/8364/MIST2016-RAN-AuthorFinal.pdf>

15. Кочетков О. В., Гаур Т. О., Машін В. М. Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки // Наукові праці Одеської національної академії зв'язку ім. О. С. Попова. 2019. № 1. С. 97–104. – URL: http://nbuv.gov.ua/UJRN/Nponaz_2019_1_14

16. Rani P., Mishra A. R., Alrasheedi A. F., et al. Digital transformation project risks assessment using hybrid picture fuzzy distance measure-based additive ratio assessment method // Scientific Reports. 2025. Vol. 15. Article 3286. DOI: <https://doi.org/10.1038/s41598-025-86598-4>