АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Менеджмент

УДК 005.334:004.9:658

DOI https://doi.org/10.5281/zenodo.19075600

Інформаційно-аналітичні системи моніторингу ризиків у діяльності підприємств

Лопатка Сергій

доктор економічних наук, доцент,

професор кафедри економіки підприємств та інформаційних технологій

ЗВО «Львівський університет бізнесу та права»

https://orcid.org/0009-0008-7941-368X

Лопатка Оксана

кандидат економічних наук, доцент кафедри економіки підприємств та інформаційних технологій

ЗВО «Львівський університет бізнесу та права»

https://orcid.org/0009-0006-7501-5022

Прийнято: 12.12.2025 | Опубліковано: 30.12.2025

Анотація. *У статті досліджено теоретичні та прикладні аспекти побудови інформаційно-аналітичних систем (ІАС) моніторингу ризиків у діяльності підприємств. Обґрунтовано, що в умовах нелінійності, крихкості та каскадних взаємодій ризиків, характерних для BANI-середовища, традиційні статичні підходи до управління ризиками (періодичні аудити, ризик-матриці, разові оцінки) втрачають управлінську релевантність і потребують заміни на безперервний моніторинг із використанням випереджувальних індикаторів, порогових значень та ескалаційних процедур. Проаналізовано еволюцію підходів від реактивної до проактивної та предиктивної парадигми ризик-менеджменту*

з урахуванням стандартів ISO 31000 і COSO ERM. Розглянуто архітектуру IAC як соціотехнічної системи, що інтегрує чотири ядрових контури: збір внутрішніх і зовнішніх даних, інтеграцію та узгодження довідників, аналітичне ядро (від кількісних і якісних методів до машинного навчання та систем раннього попередження), а також візуальну й процедурну підтримку управлінських рішень (дашборди, тригери, ескалації). Визначено межі автоматизації моніторингу ризиків та ідентифіковано ключові «сліпі зони» IAC, що мають переважно інституційний, а не технічний характер: розмитість відповідальності, формальність KRI, відсутність зв'язку між прогнозом і управлінською дією. Досліджено можливості та обмеження ML/AI у ризик-скорингу, зокрема модельний ризик, зміщення даних та ефект «чорної скриньки». Особливу увагу приділено українському контексту, де повномасштабна війна трансформувала ризик-профіль підприємств і створила потребу в IAC як інструменті не лише контролю, а й адаптивності та стратегічної стійкості. Проаналізовано євроінтеграційні чинники (CSRD, DORA, ESRS), що формують зовнішній попит на формалізований ризик-моніторинг, та здійснено порівняння з практиками країн ЄС (Польща, Чехія, Естонія). Визначено перспективи подальших досліджень у напрямі емпіричної верифікації ефективності IAC та розробки типових архітектурних рішень для підприємств із обмеженими ресурсами.

Ключові слова: *інформаційно-аналітична система, моніторинг ризиків, ризик-менеджмент, ключові індикатори ризику, система раннього попередження, безперервний моніторинг, машинне навчання, цифрова трансформація, євроінтеграція, BANI-середовище.*

АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Information and analytical systems for risk monitoring in enterprise activities

Serhii Lopatka
Doctor of Economic Sciences, Associate Professor,
Professor of the Department of Enterprise Economics and Information Technologies,
Lviv University of Business and Law,
https://orcid.org/0009-0008-7941-368X

Oksana Lopatka
Candidate of Economic Sciences, Associate Professor of the Department of Enterprise Economics and Information Technologies,
Lviv University of Business and Law,
https://orcid.org/0009-0006-7501-5022

Abstract. *The article examines theoretical and applied aspects of building information-analytical systems (IAS) for enterprise risk monitoring. It is substantiated that in conditions of non-linearity, fragility, and cascading risk interactions characteristic of the BANI environment, traditional static approaches to risk management (periodic audits, risk matrices, one-off assessments) lose their managerial relevance and require replacement with continuous monitoring using leading indicators, threshold values, and escalation procedures. The evolution of approaches from reactive to proactive and predictive risk management paradigms is analysed with reference to ISO 31000 and COSO ERM standards. The IAS architecture is considered as a sociotechnical system integrating four core circuits: collection of internal and external data, integration and reconciliation of reference data, an analytical core (from quantitative and qualitative methods to machine learning and early warning systems), and visual and procedural support for managerial decision-making (dashboards, triggers, escalations). The limits of risk monitoring automation are defined, and key IAS "blind spots," which are predominantly institutional rather*

than technical in nature, are identified: diffused accountability, formalistic KRIs, and the absence of a link between forecasts and managerial action. The capabilities and limitations of ML/AI in risk scoring are explored, including model risk, data bias, and the "black box" effect. Particular attention is paid to the Ukrainian context, where full-scale war has transformed the risk profile of enterprises and created a need for IAS as a tool not only of control but also of adaptability and strategic resilience. EU integration factors (CSRD, DORA, ESRS) that shape external demand for formalised risk monitoring are analysed, and a comparison with EU country practices (Poland, Czech Republic, Estonia) is conducted. Prospects for further research in the direction of empirical verification of IAS effectiveness and the development of standard architectural solutions for resource-constrained enterprises are outlined.

Keywords: *information-analytical system, risk monitoring, risk management, key risk indicators, early warning system, continuous monitoring, machine learning, digital transformation, European integration, BANI environment.*

Постановка проблеми/ У менеджменті підприємств ризик дедалі менше сприймається як побічний ефект планування і дедалі більше – як структурний параметр середовища, що формує обмеження та можливості для досягнення цілей. Ця зміна посилюється трьома взаємопов'язаними трендами: цифровізацією процесів і рішень, яка збільшує швидкість економічних взаємодій і водночас множить точки відмови; переходом до середовища з крихкістю й нелінійністю причинно-наслідкових зв'язків, що описується концепцією BANI як розвитком логіки VUCA [17]; українськими воєнними викликами, що радикально змінюють структуру операційних, енергетичних, логістичних і фінансових ризиків, перетворюючи їх на каскади взаємопосилень [24; 25]. У цих умовах базовою одиницею управління ризиком стає не «ризикова подія» як така, а інформаційний сигнал про зміну експозиції та траєкторії ризику. Тому в центрі сучасного ризик-менеджменту опиняється моніторинг ризиків – як безперервна аналітична функція.

Під ризиком у діяльності підприємства доцільно розуміти вплив невизначеності на цілі (ефект може бути як негативним, так і позитивним), що відповідає визначенню в ISO 31000 [21]. Ризик-менеджмент, своєю чергою, – це скоординовані дії щодо спрямування і контролю організації стосовно ризику, тобто логіка «governance + процеси + дані + рішення», а не лише набір інструментів оцінювання [20; 21]. Саме тут виникає предмет дослідження: інформаційно-аналітичні системи (IAC) моніторингу ризиків. Під IAC у межах менеджменту варто розуміти соціотехнічну систему, яка здійснює збір та інтеграцію внутрішніх і зовнішніх даних, їхню аналітичну обробку в інтересах управління, а також візуальну й процедурну підтримку управлінських рішень через пороги, ескалації та сценарії.

Проблема полягає в тому, що наявні підходи до ризик-менеджменту часто працюють у режимі статичних оцінок і періодичних аудитів, що не відповідає динамічному й каскадному характеру сучасних ризиків. Це створює розрив між декларованою аналітичною спроможністю організацій та їхньою реальною здатністю перетворювати дані на випереджувальні управлінські дії. Відтак актуальним стає дослідження IAC як механізму безперервного моніторингу, що має подолати зазначений розрив і забезпечити перехід від реактивної до предиктивної парадигми управління ризиками.

Аналіз останніх досліджень і публікацій. Проблематика моніторингу ризиків та інформаційно-аналітичного забезпечення ризик-менеджменту активно досліджується у зарубіжній науковій літературі. Концепцію безперервного моніторингу та оцінки ризиків (Continuous Risk Monitoring and Assessment) як нового компонента системи безперервного забезпечення обґрунтовано у роботі D. Moon та J. P. Krahel [1], де акцент робиться на перетворенні статичних систем контролю на динамічні конструкції, що реагують на зміни бізнес-ризиків через релевантні індикатори й тригери. Розвиток цього підходу в технологічному вимірі запропоновано Z. Zhang та співавторами [2], які досліджують можливості Інтернету речей і блокчейн-смартконтрактів для

«вбудованого» безперервного моніторингу ризиків у P2P-кредитуванні, демонструючи потенціал автоматизованого контролю на рівні окремих транзакцій і подій.

Роль аналітики даних в операційному ризик-менеджменті систематизовано в оглядовому дослідженні N. Cornwell та співавторів [3], де підкреслено, що традиційні практики часто залишаються ручними, статичними та схильними до упереджень, тоді як аналітика даних створює основу для об'єктивнішого й динамічного керування ризиками. У подальшій роботі ця група авторів [4] запропонувала модернізований підхід до управління операційними ризиками у фінансових інституціях на основі data-driven каузального аналізу, зокрема із застосуванням байєсівських мереж для моделювання імовірності операційних втрат і встановлення критичних порогів. Питання практичної дієвості ключових індикаторів ризику (KRI) досліджено G. J. van den Brink та M. Leipoldt [5], які констатують втрату релевантності KRI у випадках, коли вони не вбудовані у відповідальність першої лінії управління і не перетворюються на управлінську дію.

Автоматизацію управління ризиками ланцюгів постачання (SCRM) комплексно проаналізовано в огляді S. K. Das та M. Perona [6], де зафіксовано, що ризикові дані є онлайн і динамічними, а фаза моніторингу отримала найменше уваги серед усіх етапів управління ризиками ланцюга через складність різнорідних даних і потребу в гібридних підходах. Вплив впровадження корпоративного ризик-менеджменту (ERM) на ризик і результативність підприємств досліджено у кількох емпіричних роботах: L. Otero González та співавтори [7] на прикладі іспанських лістингових компаній встановили зв'язок між ERM і зниженням рівня ризику та покращенням фінансових результатів; D. J. Jurdi та S. M. AlGhnaimat [8] проаналізували ефекти впровадження ERM у європейських страхових компаніях, зафіксувавши позитивний вплив на продуктивність і зниження сукупного ризику. Роль ERM у забезпеченні організаційної стійкості досліджено A. Monazzam та J. Crawford [9] на кейсі

шведської гірничодобувної промисловості, де ERM-практики продемонстрували здатність підтримувати адаптивність підприємства в умовах зовнішніх шоків.

S. Grishunin, S. Suloeva та E. Burova [10] запропонували механізм розвитку системи ризик-метрик для оцінювання й підвищення довгострокової орієнтованості стратегій нефінансових компаній, обґрунтувавши взаємозв'язок між KRI, стратегічними цілями та операційними рішеннями. У сфері прогностичної аналітики A. Samitas, E. Kampouris та D. Kenourgios [11] продемонстрували потенціал машинного навчання як системи раннього попередження для прогнозування фінансових криз, поєднуючи мережевий аналіз із ML-алгоритмами. Аналогічну логіку розвинуто W. Zhu та співавторами [12], які оптимізували метод раннього попередження корпоративних фінансових ризиків на основі моделі DS-RF, забезпечуючи вищу точність прогнозування та інтерпретацію причинних факторів. Вплив цифрової трансформації на схильність підприємств до ризику (risk-taking) досліджено W. Luo, Y. Yu та M. Deng [13] на масиві китайських компаній, де встановлено, що цифровізація може одночасно підвищувати продуктивність і чутливість до збоїв.

Бібліометричний аналіз тематики GRC (governance, risk, compliance) здійснено I. Avianti та S. Handoyo [14], які зафіксували фрагментарність розвитку дисциплін і підкреслили потребу в реальній інтеграції аналітики, кіберризиків і комплаєнсу. Регіональний вимір ERM досліджено в роботах L. Syrová [15] та D. Macek і S. Vitásek [16] для Чехії: перша робота аналізує вплив іноземного капіталу на рівень ERM у малих і середніх підприємствах, друга – готовність чеських компаній до інтеграції ESG-ризиків як факторів управлінської стійкості. Вплив BANI-середовища на інноваційну активність малого бізнесу оцінено E. Mieszajkina та K. Ostapińska [17], які наголошують на неадекватності традиційних інструментів VUCA-епохи в умовах нелінійності й крихкості нового контексту. B. Buczkowski [29] описав еволюцію практик ERM у Польщі в контексті європейських рамок і корпоративного управління, підтвердивши зростаючий попит на системні інструменти ризик-моніторингу.

Попри значний масив досліджень, невирішеною залишається проблема інтеграції технологічного, аналітичного та управлінського вимірів IAC моніторингу ризиків у єдину концептуальну рамку, адаптовану до умов каскадних ризиків і специфіки країн з обмеженою інституційною зрілістю ризик-менеджменту, зокрема України в умовах воєнного часу та євроінтеграційних вимог.

Формулювання цілей статті (постановка завдання). Метою статті є дослідження теоретичних і прикладних аспектів побудови інформаційно-аналітичних систем моніторингу ризиків у діяльності підприємств. Завдання дослідження включають: обґрунтування каскадного характеру сучасних ризиків і його наслідків для управлінської практики; розкриття концептуальної моделі безперервного моніторингу як якісно нової управлінської функції; аналіз архітектури IAC та меж автоматизації моніторингу ризиків; характеристику методів і моделей аналітики ризиків у IAC (від скорингу до машинного навчання); дослідження бар'єрів, драйверів та євроінтеграційного виміру впровадження IAC на українських підприємствах у порівнянні з практиками країн ЄС.

Виклад основного матеріалу. Класична систематизація ризиків у менеджменті зазвичай розрізняє фінансові, операційні, стратегічні, комплаєнс-ризики та ризики, пов'язані з інформаційними технологіями і кібербезпекою; у сучасних умовах окремої ваги набувають геополітичні ризики як першопричина дисрупцій, що проходить через логістику, фінанси, персонал і регуляторні режими [21; 24]. Категоризація сама по собі не є проблемою – проблемою стає те, що у практиці вона часто працює як набір ізольованих «полиць» у ризик-реєстрі, а не як модель взаємодій. У BANI-логіці важливі не стільки назви ризиків, скільки механізми нелінійності та крихкості: одна подія може викликати непропорційно великі втрати, а слабкі сигнали здатні акумулюватися до порогового зламу [17].

Цифрова трансформація не лише додає кіберризики, а й змінює поведінкові параметри підприємств. Емпіричні дослідження показують, що цифрова трансформація може підвищувати рівень схильності до ризику (risk-taking) компаній, змінюючи механізми управлінських рішень, інвестиційної поведінки та використання активів [13]. Управлінський висновок із цього парадоксальний: цифровізація може підсилювати одночасно здатність до контролю і здатність до ризикової експансії, тобто робити систему більш продуктивною, але й більш чутливою до збоїв. Це ще один аргумент, чому статичні ризик-матриці без моніторингу стають управлінськи слабкими.

Найхарактерніша ознака сучасної специфіки ризиків – їхній каскадний (ланцюговий) характер. Зрив постачання або руйнування логістичного вузла може трансформуватися в операційний ризик (недопоставка, простій), потім у фінансовий (розрив грошових потоків, зростання вартості капіталу), далі у комплаєнс-ризик (невиконання контрактних зобов'язань, санкційні обмеження) і зрештою у репутаційний ризик. Огляд літератури з автоматизації управління ризиками ланцюгів постачання підкреслює, що ризикові дані є онлайн і динамічними, а рішення на основі офлайнових і статичних підходів є обмежувальними; водночас технологізація моніторингу залишається недостатньо розвиненою через складність різнорідних даних і потребу в гібридних підходах [6]. Ілюстрацією каскадної логіки може слугувати типова ситуація для українського підприємства, наведена у табл. 1.

Як видно з табл. 1, у міру проходження каскаду горизонт реакції розтягується від діб до місяців, а готовність до автоматизації моніторингу різко знижується: якщо логістичні й фінансові KRI спираються на структуровані дані (GPS, ERP, облік), то комплаєнс- і репутаційні індикатори потребують гібридних моделей із залученням експертного судження. Отже, якщо ризики взаємозалежні й рухаються у часі як система, то управління ними не можна зводити до переліку ризиків і планів реагування – потрібна концептуальна модель моніторингу, яка працює з динамікою експозицій, порогами, ранніми сигналами та ескалаціями.

Таблиця 1

Каскадна трансформація логістичного ризику: етапи, індикатори та вимоги до IAC

Етап каскаду	Категорія ризику	Горизонт реакції	Приклади KRI для моніторингу	Автоматизо-ваність
I. Тригер	Логістичний	0–3 доби	– Затримка поставки > 48 год – Обстріл логістичного вузла (бінарний сигнал) – Кількість альтернативних маршрутів < 2	*Висока – GPS-трекінг, API-інтеграція з перевізниками*
II. Операцій-ний ефект	Операційний	3–14 днів	– % виробничих замовлень без сировини – Завантаження виробничих ліній < 60 % – Кількість інцидентів простою/добу	*Середня – ERP-дані доступні, але тригери потребують калібрування*
III. Фінан-совий удар	Фінансовий	2–8 тижнів	– Відхилення операційного CF від плану > 15 % – Коефіцієнт поточної ліквідності < 1,1 – Зростання вартості залученого капіталу	*Висока – облікові дані структуровані, VaR-моделі автоматизуються*
IV. Комплаєнс-тиск	Комплаєнс / регуляторний	1–3 місяці	– Кількість контрактних дефолтів – Кількість відкритих претензій / позовів – Статус у санкційних реєстрах контрагентів	*Низька – дані неструктуровані, залежність від юридичної експертизи*
V. Системний резонанс	Репутаційний / стратегічний	3–6 місяців	– Тональність медіа-згадок (NLP-скор) – Зміна рейтингу / скорингу контрагентами – Відтік ключового персоналу > норми	*Низька – NLP-аналітика потребує гібридних моделей; суб'єктивні оцінки*

Джерело: складено авторами на основі [1; 5; 6].

ISSN 3041-2129

Визначивши каскадну природу сучасних ризиків, доцільно перейти до аналізу моделі моніторингу, здатної працювати з такою динамікою. Еволюцію підходів до контролю ризиків можна описати як перехід від reactive до proactive і далі до predictive-логіки. У reactive-парадигмі підприємство реагує на факт інциденту; у proactive – на випереджувальні операційні сигнали; у predictive – на прогностичні оцінки й сценарні траєкторії, побудовані на даних. Концепція Continuous Risk Monitoring and Assessment демонструє цей зсув як перетворення статичних систем контролю на динамічні конструкції, що підлаштовуються під зміни бізнес-ризиків через релевантні індикатори [1]. Паралельно систематичний огляд застосування аналітики даних в operational risk management наголошує, що аналітика створює основу для більш об'єктивного й динамічного керування ризиками [3].

З управлінської точки зору, моніторинг є ефективним лише тоді, коли він спроєктований як ланцюг дій, а не як потік звітів. По-перше, потрібна безперервність і частота, співмірна зі швидкістю зміни ризику: для кіберризиків або платіжних ризиків – майже реальний час; для стратегічних – можливий інший ритм, але з чіткими тригерами на перегляд припущень. По-друге, потрібна автоматизація збору даних і правило «одного джерела істини» для ключових показників експозиції, інакше моніторинг деградує до дискусії про якість даних. По-третє, необхідні порогові значення, найчастіше реалізовані через KRI (Key Risk Indicators), які мають бути прив'язані до ризик-апетиту та процедур ескалації. Принципова проблема полягає в тому, що KRI часто існують як формальний атрибут звітності, але рідко запускають управлінську дію; у професійній літературі це прямо описано як втрата релевантності KRI, якщо їх не зробити практичними й такими, що належать першій лінії управління [5].

Відмінність моніторингу від статичного ризик-аудиту та періодичного risk assessment полягає в об'єкті уваги. Аудит і оцінка, навіть виконані якісно, зазвичай фіксують імовірність і вплив у «середньому» сценарії та оцінюють наявність контрольних процедур. Моніторинг же працює з відхиленнями від

очікуваної траєкторії, з аномаліями та з сигналами зміни режиму функціонування системи. Тут виникає місток до систем раннього попередження (EWS): раннє попередження – це моніторинг плюс правило прийняття рішення «коли сигнал стає дією». У фінансових дослідженнях EWS демонструють, що поєднання індикаторів із машинним навчанням може давати високоточні попередження про кризові режими або фінансові ризики [11; 12]. Для підприємства ключове – не повторити типову помилку «передбачили, але не відреагували», тобто не замінити управління прогнозом. Концептуальна модель моніторингу ризиків неминуче ставить вимогу до інфраструктури: потрібна система, яка інтегрує дані, формує KRI та тригери, забезпечує ескалацію та робить аналітику операційною.

Описана концептуальна модель моніторингу становить управлінську рамку, проте для її реалізації необхідна відповідна технологічна інфраструктура. Функціонально IAC моніторингу ризиків складається з чотирьох ядрових контурів. Перший – збір даних: внутрішні джерела (облік, виробництво, продажі, інциденти, втрати) і зовнішні (ринкові індикатори, логістичні сигнали, санкційні списки, новинні потоки, дані контрагентів). Другий – інтеграція та узгодження довідників: без цього підприємство отримує паралельні «правди» про одного й того ж постачальника чи актив. Третій – аналітичне ядро, де дані перетворюються на оцінки експозиції, сценарії, попередження й рекомендації; у підходах continuous monitoring акцент робиться на поєднанні випереджальних і запізнілих індикаторів для відстеження змін ризику [1]. Четвертий – візуалізація і процедурна надбудова: дашборди, heat maps, risk radar, а також журнал ескалацій, відповідальності та рішень, адже без останнього візуалізація стає вітриною без управління. У дослідженнях з автоматизації SCRM підкреслено, що цифровізація може поєднувати реальний час і predictive analytics, але моніторинговий етап є одним із найскладніших для автоматизації через різнорідність і динамічність даних [6].

На ринку рішення зазвичай групуються у три класи: GRC-платформи, які інтегрують governance, risk і compliance як набір процесів, контролів, реєстрів і workflow; спеціалізовані модулі в межах ERP/корпоративних платформ; кастомні рішення на базі BI, які сильні у візуалізації, але потребують окремого проєктування ризик-логіки (пороги, ескалації, реєстри, ризик-апетит). На рівні наукових оглядів GRC-літератури важливо зафіксувати: інтеграція «ризик + комплаєнс + контроль» – не лише технологічна, а й інституційна проблема, бо дисципліни й практики часто розвивалися ізольовано; сучасний зсув до штучного інтелекту і кіберризиків лише посилює вимогу до реальної інтеграції, а не до суміщення модулів [14].

Критичне питання полягає в тому, що саме автоматизується добре, а що залишається «сліпими зонами». Добре автоматизуються задачі з високою структурованістю даних і формалізованими правилами: контрольні тести, тригери на порогові значення, класифікація інцидентів, збір доказів для комплаєнсу, базова аналітика втрат. Набагато гірше автоматизуються задачі, де домінують неструктуровані дані, причинність є нелінійною, спостереження неповне, а зміни відбуваються швидше, ніж оновлюються моделі. Література з SCRM-автоматизації прямо вказує, що фаза моніторингу отримала менше уваги, а її автоматизація є особливо складною через потребу в гібридних підходах і через низьку надійність частини зовнішніх джерел; це – системна межа навіть для найбільш розвинених технологічних стеків [6]. Практика KRI демонструє іншу сліпу зону: індикатори можуть бути побудовані коректно, але залишатися недієвими, якщо вони не вбудовані у відповідальність першої лінії та не перетворюються на управлінську дію [5].

Узагальнюючи архітектуру IAC як конструкцію про здатність зшивати дані, моделі та управлінську відповідальність, доцільно перейти до аналізу конкретних методів і моделей аналітики ризиків, що становлять інтелектуальне ядро таких систем. Аналітика ризиків у корпоративних IAC є багаторівневою. Перший рівень – кількісні методи, які добре працюють там, де ризик має

вимірюваний розподіл і достатньо історичних даних: моделі на кшталт VaR, Monte Carlo, стрес-тестування, сценарне моделювання ліквідності й попиту. Другий рівень – якісні методи, що залишаються незамінними для стратегічних, геополітичних або регуляторних ризиків, де дані неповні або події є рідкісними: експертні оцінки, матриці ризиків, аналіз ключових припущень стратегії. Третій рівень – гібридні підходи, які поєднують кількісні моделі з експертним контекстуванням і політиками прийняття рішень [21] [20].

Формалізація моніторингу ризиків у ІАС потребує кількісного апарату, що забезпечує перехід від описових оцінок до операційних тригерів. Базовим інструментом є агрегований індикатор ризикової експозиції, який зважує окремі KRI з урахуванням їхньої значущості та поточного стану:

$$R_c = \frac{\sum_{i=1}^{n} w_i \cdot KRI_i \cdot \alpha_i}{\sum_{i=1}^{n} w_i}, \qquad (1)$$

де R_c – композитний індекс ризикової експозиції; w_i – вагові коефіцієнти, визначені експертно або на основі історичних втрат; KRI_i – нормалізоване значення i-го ключового індикатора ризику; α_i – коефіцієнт актуальності, що відображає швидкість старіння даних (для щоденно оновлюваних KRI $\alpha_i \to 1$, для квартальних – зменшується між оновленнями).

Для детектування дрейфу ризикової експозиції (зміни режиму, що потребує перегляду моделі або ескалації) доцільно використовувати нормалізоване відхилення:

$$\delta(t) = \frac{|E(t) - E(t-\Delta)|}{\sigma_E}, \qquad (2)$$

де $E(t)$ – поточне значення агрегованої експозиції; $E(t-\Delta)$ – значення на попередньому контрольному горизонті (Δ може дорівнювати одному тижню, місяцю тощо залежно від типу ризику); σ_E – історичне стандартне відхилення експозиції за референтний період. Значення $\delta(t) > 2$ сигналізує про нетипову зміну і запускає верифікацію в ІАС.

Нарешті, тригер системи раннього попередження (EWS) формалізується як порогове правило:

$$S(t) = 1, \text{ якщо } R_c(t) > R_{app} + k \cdot \sigma_R, \quad (3)$$

де *S(t)* – бінарний сигнал тривоги; R_{app} – встановлений ризик-апетит організації; k – параметр чутливості (типово k = 1,5…2,5 залежно від толерантності до помилки першого роду); σ_R – волатильність композитного індексу. Формули (1)–(3) утворюють замкнутий цикл: агрегація KRI → детектування дрейфу → генерація сигналу → ескалація. Саме цей цикл відрізняє IAC від пасивного дашборду.

Роль ML/AI в IAC полягає у розширенні прогнозної частини моніторингу. Для фінансових ризиків існують моделі раннього попередження, що поєднують машинне навчання з підходами до багатовимірного злиття інформації, підвищуючи точність і надаючи менеджменту інтерпретацію причин [12]. Для макро- і системних ризиків раннє попередження може будуватися як мережевий аналіз плюс ML для виявлення режимів нестабільності [11]. Для операційних ризиків у фінансових інституціях демонструється, що data-driven підходи, зокрема байєсівські мережі, можуть моделювати імовірність операційних втрат і встановлювати критичні пороги, важливі саме для моніторингових процедур [4]. У технологічно-орієнтованих кейсах continuous monitoring може бути підсилений IoT і смартконтрактами для вбудованого контролю ризику на рівні транзакцій і подій [2].

Однак у менеджменті не менш важливою є «темна сторона» ML/AI в ризик-скорингу. По-перше, виникає model risk: модель може бути статистично точною на історії, але нестабільною при зміні режиму, що типово для воєнної економіки і BANI-середовища. По-друге, data bias і нерівномірність даних: системи раннього попередження часто «карають» ті сегменти, де дані гірші або де події рідші, що породжує управлінську несправедливість і стратегічні помилки. По-третє, ефект «чорної скриньки»: коли система дає сигнал, але менеджмент не розуміє причин, він або ігнорує попередження, або діє надмірно жорстко, що породжує вторинні втрати. Систематичний огляд data analytics в operational risk management підкреслює, що ключові теми для практиків – це не

тільки prediction, але й risk decision-making та причинні фактори; тобто аналітика має переходити від точності до управлінської придатності [3]. Це пояснює, чому інтеграція ML у ризик-менеджмент потребує процедур управління моделями (валідації, версіонування, пояснюваності), а не лише підключення алгоритму.

Зазначений висновок безпосередньо пов'язаний із питанням комплаєнсу, кіберризику і регуляторної відповідальності. NIST прямо виводить ризикові реєстри як механізм документування та комунікації ризикових рішень і підкреслює необхідність інтегрувати кіберризики у портфель ризиків підприємства, а не ізолювати їх на рівні IT-підрозділу [22]. Для європейського фінансового сектору аналогічна логіка посилюється вектором цифрової операційної стійкості (DORA), який формалізує вимоги до ICT risk management, тестування та інцидент-репортингу, тобто робить безперервність і доказовість компонентами регуляторної норми [19].

Після уточнення методів аналітики стає зрозуміло, що вибір моделей для IAC невіддільний від контексту підприємства й країни, тому доцільно зосередитися на українських реаліях. Повномасштабна війна трансформувала ризик-профіль українських підприємств не як «додатковий ризик», а як метаризик, що переструктурував більшість операційних ланцюгів. Оцінки збитків і потреб відновлення підкреслюють масштаб руйнувань інфраструктури та енергетики, що прямо конвертується у ризики простоїв, збоїв постачання, втрати активів і зростання транзакційних витрат [24]. На рівні приватного сектору огляди стану бізнесу фіксують пошкодження, обмеження фінансування, проблеми кадрів і логістики, що є типовими мультиплікаторами операційних і фінансових ризиків [25]. Для фінансової системи публічні звіти Національного банку України структурують ризики стійкості, включно з операційними та іншими шоками, що створює додатковий тиск на підприємства через кредитні умови, платіжну дисципліну та очікування прозорості [23].

У таких умовах «вимушене прискорення» цифровізації моніторингу має подвійний характер. З одного боку, підприємства прагнуть автоматизувати те,

що прямо впливає на виживання: контроль ліквідності, дебіторки та кредиторки, надійність контрагентів, логістичну видимість, енергетичні режими. З іншого боку, сама війна робить дані більш фрагментарними (релокації, зміни процесів, втрата історичних рядів), що знижує ефективність чисто алгоритмічних підходів і підвищує роль гібридних моделей, де аналітика доповнюється експертним контекстом. Це добре узгоджується з висновком про те, що BANI-умови вимагають нових управлінських механізмів і що традиційні інструменти VUCA-епохи можуть бути недостатніми [17].

Структурний бар'єр для впровадження IAC ризик-моніторингу в Україні проявляється як розрив зрілості між великим бізнесом і МСП. Великі компанії частіше мають ERP-ядро, розвиненіші функції комплаєнсу і можливість інвестувати в інтеграцію даних; МСП часто змушені балансувати між вартістю рішення і потребою в простій управлінській видимості. На цьому тлі особливо критичною стає правильна постановка KRI та відповідальності: якщо індикатори існують лише для звіту, система не стане механізмом попередження, навіть якщо технічно дашборд побудований коректно [5]. Головний дефіцит часто не технологічний, а управлінський: здатність перетворювати дані на дії.

Євроінтеграційний вимір змінює ситуацію через зовнішній примус до стандартизації ризик-експлікації. CSRD розширює вимоги до корпоративної звітності, зокрема щодо значущих ризиків і їхнього управління в контексті сталості, а Європейські стандарти звітності зі сталого розвитку (ESRS) деталізують структуру розкриттів, роблячи ризики та впливи частиною формалізованого управлінського наративу [18; 19]. DORA задає для фінансового сектору вимоги до цифрової операційної стійкості, що підсилює потребу в моніторингу ICT-ризиків, тестуванні й керованості інцидентів [19]. Для українських підприємств це означає, що ризик-моніторинг поступово стає не лише внутрішнім інструментом менеджменту, а й елементом сумісності з європейськими вимогами та очікуваннями партнерів.

Порівняння з Польщею, Естонією та Чехією доцільно будувати не як перелік кращих практик, а як аналіз інституційних умов. Країни ЄС мають більш формалізоване регуляторне середовище і вищу зрілість цифрових публічних сервісів, що відбивається у рамках моніторингу цифрового розвитку Європейською Комісією (DESI та споріднені інструменти) [26]. З боку цифрової держави порівнювану рамку дає Світовий банк через GovTech Maturity Index, який вимірює розвиток ключових аспектів цифрової трансформації публічного сектору [27]. Додаткове порівняння можна здійснити за даними Eurostat щодо цифровізації у Європі [28]. Емпіричні дослідження для Чехії показують специфіку впровадження ERM у МСП і вплив структури капіталу та власності на рівень ERM-підходів [15], а також зміщення ризик-оптики у бік інтеграції ESG-параметрів як факторів управлінської стійкості [16]. Польський контекст у спеціалізованих оглядах ERM наголошує еволюцію практик у зв'язку з європейськими рамками й корпоративним управлінням, що опосередковано підсилює попит на системні інструменти ризик-моніторингу [29].

У підсумку для України ключовим є не «наздогнати технології», а створити керовану траєкторію впровадження: починати з ризиків, де дані вже є (фінансові потоки, контрагенти, логістика), далі – розширювати зовнішні джерела та вводити гібридні моделі прогнозування, паралельно будуючи управління даними, модельний ризик і процедури ескалації. IAC у такій рамці стає інструментом не тільки контролю, а й адаптивності підприємства – тобто фактично компонентом стратегічної стійкості.

Висновки. Інформаційно-аналітичні системи моніторингу ризиків у діяльності підприємств слід трактувати як соціотехнічний механізм перетворення невизначеності на керовані рішення, а не як «пакет модулів» чи «дашборд ризиків». Ризик у BANI-середовищі відзначається нелінійністю, крихкістю та каскадними взаємодіями, тому стандартні таксономії ISO 31000 і COSO ERM залишаються необхідною рамкою, але вимагають доповнення

практиками безперервного моніторингу, які працюють із сигналами дрейфу й режимними зламами.

Головна суперечність сучасного ризик-моніторингу пролягає не між «старими» і «новими» технологіями, а між декларованою аналітичною спроможністю та реальною управлінською поведінкою. Системи можуть формувати KRI, будувати моделі й попередження, але організація продовжуватиме зазнавати непередбачуваних втрат, якщо KRI не стають тригерами рішень першої лінії, якщо ескалації не мають політичної ваги, а модельні припущення не переглядаються при зміні режиму. У цьому сенсі «сліпі зони» IAC часто є не технічними, а інституційними: відповідальність розмита, власник ризику не має повноважень, а ризик-комунікація зводиться до звітності.

Прогнозна аналітика є необхідною, але не достатньою умовою сучасного моніторингу. Дослідження раннього попередження демонструють потенціал ML у прогнозуванні фінансових кризових режимів і корпоративних фінансових ризиків, однак управлінська цінність з'являється лише тоді, коли прогноз підкріплений пояснюваністю, управлінням модельним ризиком і процедурною перетворюваністю сигналу на дію. Запропонований у статті формалізований цикл «агрегація KRI → детектування дрейфу → генерація сигналу → ескалація» (формули (1)–(3)) забезпечує операціоналізацію цього переходу.

Український контекст робить IAC ризик-моніторингу не розкішшю sophisticated management, а інструментом виживання і відновлення. Масштаб руйнувань, енергетична нестабільність, логістичні розриви й фінансові обмеження формують ризик-портфель, який неможливо стабільно управляти без структурованих даних, індикаторів і ескалацій. Євроінтеграційні чинники (CSRD, ESRS, DORA) додають вимір формалізованої доказовості й порівнюваності управління ризиками, що підштовхує підприємства до системного ризик-моніторингу як елемента конкурентоспроможності на європейських ринках.

Перспективи подальших досліджень пов'язані з емпіричною верифікацією ефективності IAC моніторингу ризиків на українських підприємствах різних розмірів і секторів, розробкою типових архітектурних рішень для МСП з обмеженими ресурсами, а також із дослідженням впливу регуляторних вимог CSRD/DORA на трансформацію практик ризик-менеджменту в умовах євроінтеграції.

Список використаних джерел

1. Moon D., Krahel J. P. Continuous Risk Monitoring and Assessment: New Component of Continuous Assurance. *Journal of Emerging Technologies in Accounting*. 2020. Vol. 17, No. 2. P. 173–200. DOI: https://doi.org/10.2308/JETA-18-01-09-1

2. Zhang Z., Gu Y., Jiang L., Yu W., Dai J. Internet of Things and Blockchain-Based Smart Contracts: Enabling Continuous Risk Monitoring and Assessment in Peer-to-Peer Lending. *Journal of Emerging Technologies in Accounting*. 2023. Vol. 20, No. 2. P. 181–194. DOI: https://doi.org/10.2308/JETA-2022-003

3. Cornwell N., Bilson C. M., Gepp A., Stern S., Vanstone B. J. The Role of Data Analytics within Operational Risk Management: A Systematic Review from the Financial Services and Energy Sectors. *Journal of the Operational Research Society*. 2023. Vol. 74, No. 1. P. 374–402. DOI: https://doi.org/10.1080/01605682.2022.2041373

4. Cornwell N., Bilson C., Gepp A., Stern S., Vanstone B. J. Modernising operational risk management in financial institutions via data-driven causal factors analysis: A pre-registered study. *Pacific-Basin Finance Journal*. 2023. DOI: https://doi.org/10.1016/j.pacfin.2023.102011

5. van den Brink G. J., Leipoldt M. Key Risk Indicators reloaded. *Maandblad voor Accountancy en Bedrijfseconomie*. 2022. Vol. 96, No. 5/6. P. 165–171. DOI: https://doi.org/10.5117/mab.96.80730

6. Das S. K., Perona M. Supply chain risk management automation: A literature review. *Electronic Markets*. 2025. Vol. 35. Article 104. DOI: https://doi.org/10.1007/s12525-025-00844-1

7. Otero González L., Durán Santomil P., Tamayo Herrera A. The effect of Enterprise Risk Management on the risk and the performance of Spanish listed companies. *European Research on Management and Business Economics*. 2020. Vol. 26, No. 3. P. 111–120. DOI: https://doi.org/10.1016/j.iedeen.2020.08.002

8. Jurdi D. J., AlGhnaimat S. M. The Effects of ERM Adoption on European Insurance Firms Performance and Risks. *Journal of Risk and Financial Management*. 2021. Vol. 14, No. 11. Article 554. DOI: https://doi.org/10.3390/jrfm14110554

9. Monazzam A., Crawford J. The role of enterprise risk management in enabling organisational resilience: a case study of the Swedish mining industry. *Journal of Management Control*. 2024. Vol. 35. P. 59–108. DOI: https://doi.org/10.1007/s00187-024-00370-9

10. Grishunin S., Suloeva S., Burova E. Development of Risk Management Mechanism and the System of Risk Metrics to Evaluate and Enhance the Long-Term Orientation of the Strategies of Non-Financial Companies. *Risks*. 2022. Vol. 10, No. 9. Article 182. URL: https://www.mdpi.com/2227-9091/10/9/182

11. Samitas A., Kampouris E., Kenourgios D. Machine learning as an early warning system to predict financial crisis. *International Review of Financial Analysis*. 2020. Vol. 71. Article 101507. DOI: https://doi.org/10.1016/j.irfa.2020.101507

12. Zhu W., Zhang T., Wu Y., Li S., Li Z. Research on optimization of an enterprise financial risk early warning method based on the DS-RF model. *International Review of Financial Analysis*. 2022. Vol. 81. Article 102140. DOI: https://doi.org/10.1016/j.irfa.2022.102140

13. Luo W., Yu Y., Deng M. The impact of enterprise digital transformation on risk-taking: Evidence from China. *Research in International Business and Finance*. 2024. Vol. 69. Article 102285. DOI: https://doi.org/10.1016/j.ribaf.2024.102285

14. Avianti I., Handoyo S. A bibliometric analysis of governance, risk, and compliance (GRC): trends, themes, and future directions. *Humanities and Social Sciences Communications*. 2025. Vol. 12. Article 1945. URL: https://www.nature.com/articles/s41599-025-06194-9

15. Syrová L. The Impact of Foreign Capital on the Level of ERM (Evidence from SMEs in the Czech Republic). *Journal of Risk and Financial Management*. 2022. Vol. 15, No. 2. Article 83. URL: https://www.mdpi.com/1911-8074/15/2/83

16. Macek D., Vitásek S. ESG Risk Analysis and Preparedness of Companies in the Czech Republic. *International Journal of Economic Sciences*. 2024. Vol. XIII, No. 2. DOI: https://doi.org/10.52950/ES.2024.13.2.003

17. Mieszajkina E., Ostapińska K. Evaluation of the Impact of the BANI World on Small Business Innovation Activities. *European Research Studies Journal*. 2024. Vol. XXVII, Special Issue 3. P. 272–288. URL: https://ersj.eu/journal/3489

18. Directive (EU) 2022/2464 of the European Parliament and of the Council (Corporate Sustainability Reporting Directive, CSRD). URL: https://eur-lex.europa.eu/eli/dir/2022/2464/oj

19. Regulation (EU) 2022/2554 of the European Parliament and of the Council (Digital Operational Resilience Act, DORA). URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj

20. Committee of Sponsoring Organizations of the Treadway Commission (COSO). Enterprise Risk Management – Integrating with Strategy and Performance (Executive Summary). 2017. URL: https://www.coso.org/Pages/erm.aspx

21. ISO 31000:2018 Risk management – Guidelines. International Organization for Standardization. URL: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100426.pdf

22. Stine K. M. et al. NISTIR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM). National Institute of Standards and Technology. 2020. DOI: https://doi.org/10.6028/NIST.IR.8286. URL: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf

23. National Bank of Ukraine. Financial Stability Report, December 2024. URL: https://bank.gov.ua/admin_uploads/article/FSR_2024-H2_eng.pdf?v=9

24. World Bank Group, Government of Ukraine, European Commission, United Nations. Fourth Rapid Damage and Needs Assessment (RDNA4). 2025. URL: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099022025114040022

25. Kyiv School of Economics. Ukraine: Firms through the War. 2023. URL: https://kse.ua/wp-content/uploads/2024/03/Ukraine.-Firms-through-the-War-Paper-Nov-2023.pdf

26. European Commission. Digital Economy and Society Index (DESI). 2024. URL: https://digital-strategy.ec.europa.eu/en/policies/desi

27. World Bank. GovTech Maturity Index 2022. URL: https://documents1.worldbank.org/curated/en/099035001132365997/pdf/P1694820bcef0903e091160315d2050d03b.pdf

28. Eurostat. Digitalisation in Europe – 2024 edition. URL: https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2024

29. Buczkowski B. Enterprise Risk Management in Poland. Enterprise Risk Management in Europe. Emerald Publishing. 2021. DOI: https://doi.org/10.1108/978-1-83867-245-420211009