УДК 336.71:004.9
JEL Classification G21, G32, O33, D80
DOI: 10.31767/nasoa.3-4-2025.01

Т. Г. БОНДАРУК,
доктор економічних наук, професор,
завідувач кафедри фінансів, банківської справи та страхування,
Національна академія статистики, обліку та аудиту;
e-mail: bondaruk23@ukr.net
ORCID ID: https://orcid.org/0000-0001-9410-6428
Researcher ID: Q -5166-2016

Використання сучасних цифрових технологій в управлінні процесами інформаційного забезпечення економічної безпеки банків

У статті здійснено комплексний аналіз впливу сучасних цифрових технологій на трансформацію системи інформаційного забезпечення економічної безпеки банків у контексті динамічного розвитку цифрової економіки та зростання фінансових, кібернетичних і операційних ризиків. Обґрунтовано, що цифровізація банківської діяльності виходить за межі технічного оновлення IT-систем і формує передумови для перегляду концептуальних засад моделювання ризиків, формування інформаційних потоків та організації управлінських процедур. Визначено, що ключовими чинниками модернізації інформаційно-аналітичної підсистеми є розвиток технологій Big Data, штучного інтелекту, машинного навчання, хмарних обчислень, відкритого банкінгу, дистанційної ідентифікації та комплексів кіберзахисту.

У дослідженні систематизовано сучасні підходи до трактування цифрової трансформації та розкрито їх значення для формування нової моделі інформаційно-аналітичної діяльності банків, орієнтованої на проактивне виявлення загроз і випереджуюче реагування на зміни зовнішнього середовища. Показано, що цифрові технології забезпечують розширення джерел даних, інтеграцію внутрішніх і зовнішніх інформаційних потоків, підвищення точності прогнозних оцінок і скорочення часових лагів у прийнятті управлінських рішень. Особливу увагу приділено ролі штучного інтелекту у формуванні моделей поведінкової аналітики, систем раннього попередження та автоматизованих механізмів контролю транзакцій.

Запропоновано організаційно-функціональну модель управління процесами інформаційного забезпечення економічної безпеки банку, що охоплює блоки формування, інтеграції, зберігання, аналізу та захисту даних. Доведено, що впровадження такої моделі створює можливості для формування замкненого інформаційного контуру «дані – аналітика – рішення – захист – нові дані». Аргументовано, що технологічне та інституційне підсилення цієї моделі сприяє підвищенню адаптивності банків до зовнішніх шоків, мінімізації інформаційної асиметрії, розширенню контролю за ризиками та зміцненню їх фінансової стійкості.

Ключові слова*: економічна безпека банку; цифрові технології; управління процесами інформаційно-аналітичного забезпечення; Big Data; штучний інтелект; кіберзахист; цифрова трансформація; ризик-менеджмент.*

T. H. BONDARUK,
Dsc in Economics, Professor,
Head of Department for Finance, Banking and Insurance,
National Academy of Statistics, Accounting and Audit
e-mail: bondaruk23@ukr.net
ORCID ID: https://orcid.org/0000-0001-9410-6428
Researcher ID: Q -5166-2016;

Use of Modern Digital Technologies in Managing the Information Support Processes of Banks' Economic Security

The article provides a comprehensive analysis of the impact of modern digital technologies on the transformation of information support systems for banks' economic security in the context of the rapidly developing digital economy and the growing intensity of financial, cyber, and operational risks. It is argued that digitalization in the banking sector goes beyond the technological upgrade of IT infrastructures and creates prerequisites for revisiting the conceptual foundations of risk modelling, information flow management, and organizational decision-making practices. The study identifies Big Data technologies, artificial intelligence, machine learning, cloud computing, open banking, remote identification, and cybersecurity systems as the key drivers of modernization of banks' information and analytical subsystems.

The research systematizes contemporary approaches to interpreting digital transformation and highlights their significance for building a new model of information and analytical activity aimed at proactive threat detection and anticipatory responses to external changes. Digital technologies expand data sources, ensure integration of internal and external information flows, improve the precision of predictive analytics, and significantly shorten decision-making time. Particular attention is paid to the role of artificial intelligence in behavioural analytics, early-warning risk systems, and automated transaction monitoring mechanisms.

An organizational and functional model for managing information processes of economic security is proposed, encompassing data formation, integration, storage, analysis, and protection blocks. The study demonstrates that implementing such a model enables the formation of a closed-loop information cycle "data – analytics – decisions – protection – new data". Strengthening this model technologically and institutionally enhances banks' adaptability to external shocks, minimizes information asymmetry, expands risk-control capabilities, and reinforces financial resilience.

Keywords*: bank's economic security; digital technologies; management of information and analytical support processes; Big Data; artificial intelligence (AI); cybersecurity; digital transformation; risk management.*

Постановка проблеми. В умовах цифровізації фінансового сектору та посилення кіберзагроз економічна безпека банків набуває особливого значення. Сучасні банки функціонують у середовищі, де інформаційні потоки суттєво розширюються та стають більш різнорідними, а швидкість прийняття рішень визначає конкурентоспроможність та стабільність фінансової установи. Традиційні підходи до організації інформаційно-аналітичних процесів дедалі менше відповідають вимогам часу, вони не забезпечують оперативності обробки великих масивів даних, не гарантують достатнього рівня захисту від зовнішніх і

внутрішніх загроз, а також не дають можливості гнучко реагувати на трансформацію структури ризиків банку.

Війна та пов'язані з нею дестабілізаційні чинники суттєво підвищили рівень інформаційних ризиків, зокрема зросла кількість кібератак, ускладнились вимоги до безперервності операцій та достовірності даних. У таких умовах банки змушені переходити до використання сучасних цифрових технологій, таких як big data, штучний інтелект, хмарні сервіси, інтелектуальні системи моніторингу та прогнозування. Проте впровадження цих інструментів потребує методичного обґрунтування, адаптації до специфіки українських банків та розроблення ефективних моделей управління інформаційними процесами.

Отже, виникає потреба у формуванні обґрунтованих підходів до включення сучасних цифрових технологій у процеси управління інформаційним забезпеченням економічної безпеки банків, що дасть змогу гарантувати своєчасність надходження, високу якість, надійність та аналітичну цінність інформації для прийняття управлінських рішень.

Аналіз останніх досліджень та публікацій. Питання економічної та фінансово-економічної безпеки банків ґрунтовно висвітлено в роботах українських дослідників. Класичні підходи до сутності, складових та індикаторів безпеки банківських установ сформовано в монографії під редакцією А. Єпіфанова [1], де економічна безпека банків розглядається як інтегральний стан стійкості та захищеності фінансових та інформаційних ресурсів, також В. Коваленко [2] деталізує інструменти забезпечення фінансово-економічної безпеки банків в умовах трансформації фінансового ринку.

У працях П. Куцика та О. Куцика [3] економічна безпека банків розглядається як складна багаторівнева система, чутлива до глобалізаційних процесів, посилення міжнародної конкуренції, мобільності фінансових потоків та транснаціональних ризиків. Авторами наголошено, що глобалізація формує нові виклики для банків – зростання вразливості до зовнішніх шоків, підвищення залежності від міжнародних ринків капіталу та посилення регуляторного тиску, що потребує переорієнтації методів оцінювання та управління ризиками. У свою чергу, С. Васильчук [4] акцентує увагу на фундаментальних аспектах економічної безпеки банків, розкриваючи методи її забезпечення через систему фінансових, організаційних і правових інструментів. Автор стверджує, що ефективність безпеки визначається не лише якістю ризик-менеджменту, а й здатністю банку формувати життєздатні внутрішні регламенти, здійснювати належний моніторинг операцій і забезпечувати інформаційну прозорість діяльності.

Сучасні дослідження, присвячені цифровізації фінансового сектору, поглиблюють попередні теоретичні підходи та демонструють трансформацію безпекової парадигми. У роботі С. Теслюка, Н. Матвійчук і А. Левчука [5] економічна безпека банків аналізується крізь призму цифрових загроз та нових технологічних можливостей, автори доводять, що цифровізація водночас розширює спектр інструментів захисту і формує нові ризики (кібератаки, технічні збої, вразливість цифрової інфраструктури). Аналіз тенденцій цифрового банкінгу, здійснений М. Tymots [6], підтверджує, що цифрові сервіси стають ключовим елементом конкурентоспроможності банків, а їх розвиток потребує посилення інформаційної безпеки та модернізації моделей управління ризиками. Доповнює цей блок дослідження А. Клочка, Н. Волченко та Н. Клєцової [7], яке підкреслює, що у контексті євроінтеграційних процесів економіко-право-

ві засади банківської безпеки зазнають значної трансформації, зокрема гармонізація з європейськими стандартами вимагає підвищення рівня прозорості, стійкості, кіберзахисту та інформаційної відповідальності фінансових установ. Сукупно ці джерела створюють цілісний науковий фундамент для осмислення економічної безпеки банків у контексті сучасних викликів цифрової економіки.

Отже, наявні наукові напрацювання формують теоретико-методичне підґрунтя для розуміння сутності економічної безпеки банків та окремих аспектів цифрової трансформації банківського сектору. Водночас розгляд сучасних цифрових технологій саме як інструментів управління процесами інформаційного забезпечення економічної безпеки (від збору та інтеграції даних до аналітики, прогнозування й підтримки управлінських рішень) – залишається фрагментарно дослідженим. Це зумовлює необхідність подальших розробок, спрямованих на формування концептуальних і прикладних підходів до побудови цифрово орієнтованих систем інформаційного забезпечення економічної безпеки банків.

Метою статті є обґрунтування теоретичних засад і розробка практичних підходів до використання сучасних цифрових технологій в управлінні процесами інформаційного забезпечення економічної безпеки банків.

Виклад основного матеріалу. Ідентифікація цифрової трансформації фінансового сектору як довгострокового системного процесу, а не як окремого етапу технологічної модернізації, зумовлена сукупністю структурних змін, що протягом останніх двох десятиліть відбуваються у глобальній та національній фінансовій архітектурі [8]. Першою фундаментальною передумовою такого підходу є *зміна природи фінансових посередницьких функцій* під впливом цифрових технологій. Традиційні банківські операції дедалі більше заміщуються цифровими платформами, інтегрованими платіжними сервісами, відкритими API та фінтех-рішеннями [9], що переструктуровують канали створення вартості й руйнують монопольну позицію банків на окремих сегментах ринку. Це не є тимчасовим зрушенням, а свідчить про становлення нової моделі взаємодії фінансових інститутів, клієнтів і технологічних провайдерів.

Наступною передумовою є *глибинна трансформація інформаційних та аналітичних процесів*, через які банк здійснює управління ризиками та ухвалення рішень. Поява технологій Big Data, штучного інтелекту, хмарних обчислень і поведінкової аналітики [10, 11] зумовила поступовий перехід від дискретних, регламентних моделей оцінювання ризиків до адаптивних, безперервних систем моніторингу та прогнозування. У цих умовах інформаційно-аналітичні системи банку перестають бути допоміжними і перетворюються на ядро управлінської архітектури, що безпосередньо визначає економічну безпеку, цінову політику, взаємодію з контрагентами та клієнтами.

Третьою ключовою передумовою є *інституційна перебудова фінансового ринку*, спричинена як цифровими інноваціями, так і регуляторними змінами [12]. Європейські директиви PSD2/PSD3 [13], розвиток open banking, посилення вимог до управління кіберризиками відповідно до стандартів NIST Cybersecurity Framework [14], а також запровадження Європейського Регламенту про цифрову операційну стійкість DORA [15] суттєво модифікують встановлені інституційні межі функціонування банків. Регуляторні рамки більше не розглядають цифровізацію як добровільний вибір банків, а встановлюють її як норму, без якої неможливо забезпечити належний рівень прозорості, безпеки та конкурентоспроможності [16].

Також важливим чинником є те, що цифрова трансформація змінює *структуру та поведінку фінансових ризиків.* Ризики набувають високого ступеня взаємозалежності: інформаційні та кібернетичні фактори безпосередньо впливають на кредитний, операційний, ринковий та комплаєнс-ризики. Водночас зростає швидкість поширення ризикових сигналів у цифровому середовищі, що потребує системного, а не епізодичного характеру цифрових змін.

Отже, у сукупності ці чинники підтверджують системну природу цифрової трансформації та її вирішальну роль у формуванні сучасної архітектури банківської діяльності та економічної безпеки. Цифрову трансформацію фінансового сектору доцільно розглядати не як окремий етап технологічного оновлення, а як довгостроковий системний процес, що модифікує інституційну архітектуру ринку, конфігурацію бізнес-моделей банків і характер функціонування їх інформаційно-аналітичних систем. Для банківських установ України цей процес розгортається в умовах високої турбулентності зовнішнього середовища, воєнних ризиків [17], підвищених вимог до безперервності платежів та захищеності цифрової інфраструктури.

У цьому контексті цифрова трансформація не зводиться до розширення спектра дистанційних каналів обслуговування, а набуває ознак парадигмальної зміни способів формування, обробки та використання інформації в системі управління економічною безпекою банку. Цифрові платформи, мобільний та інтернет-банкінг, відкриті API, хмарні рішення й інструменти штучного інтелекту забезпечують перехід від фрагментарних інформаційних процедур до інтегрованих, ризик-орієнтованих механізмів управління.

З огляду на це, цифровізацію банківського сектору доцільно розглядати як ключову детермінанту модернізації інформаційних процесів, у межах яких інформація набуває статусу стратегічного ресурсу економічної безпеки, а не лише операційного супроводу поточної діяльності.

Загострення фінансових, технологічних та регуляторних викликів у банківському секторі створило сукупність наукових і практичних передумов, що зумовлюють перегляд підходів до тлумачення інформаційного забезпечення економічної безпеки банків. Насамперед, стрімке ускладнення ризикового середовища, таке як зростання частоти кіберінцидентів, посилення волатильності фінансових ринків, збільшення залежності банків від міжсистемних цифрових інтеграцій, сформувало потребу у якісно нових механізмах акумуляції, перевірки та аналітичного узагальнення інформації. У цих умовах інформація перестає виконувати роль допоміжного операційного ресурсу, а трансформується в основу стратегічного управління ризиками та формування фінансової стійкості. Наступним важливим чинником є інтенсивний розвиток цифрових технологій, який розширює спектр джерел даних, підвищує їх різнорідність та прискорює оборот інформаційних потоків, що потребує багаторівневої логістики їх обробки від оперативного моніторингу до сценарного прогнозування. Наукові дослідження останнього десятиріччя демонструють трансформацію статичних моделей аналізу у динамічні цифрові платформи, які здатні підтримувати безперервний контроль та ідентифікацію загроз у режимі реального часу.

Додатковою передумовою стало поступове формування концепції інформаційної стійкості (information resilience), яка в сучасному банківському менеджменті виходить за межі суто технічного захисту даних та охоплює їх цілісність, надійність, верифікованість, аналітичну цінність та здатність забезпечувати

прийняття обґрунтованих управлінських рішень. В свою чергу, інтеграція банків у глобальні фінансові та цифрові екосистеми призвела до появи багатошарової інфраструктури інформаційних взаємодій, таких як: внутрішньобанківські, міжбанківські, міжсекторальні і трансграничні. Така складність об'єктивно потребує структуризації інформаційного забезпечення як підсистеми, що функціонує на декількох рівнях: технологічному (збір і передавання даних), аналітичному (інтерпретація, моделювання, прогнозування), управлінському (прийняття рішень, реагування, формування політики) та безпековому (захист активів і резервування інформаційної стійкості). Узагальнення цих тенденцій дозволяє стверджувати, що інформаційне забезпечення економічної безпеки банків доцільно розглядати як багаторівневу підсистему, інтегровану в загальну архітектуру управління ризиками та здатну забезпечувати цілісний, адаптивний і безперервний цикл обробки інформації в умовах цифрової трансформації.

У традиційній, моделі підсистема інформаційного забезпечення характеризувалася високою фрагментованістю, значною часткою ручних процедур, низьким рівнем інтегрованості даних та часовими лагами між виникненням ризику й управлінською реакцією. Цифрове середовище радикально змінює параметри функціонування інформаційного забезпечення, зокрема істотно зростає обсяг, швидкість і різнорідність даних (операційні, поведінкові, мережеві, кіберінциденти); розширюється коло зовнішніх джерел інформації (фінтех-партнери, платіжні сервіси, маркетплейси, державні реєстри); посилюється взаємозалежність між інформаційними та фінансовими ризиками (кібератаки, витоки даних, маніпуляція інформацією); підвищуються вимоги до режиму реального часу в моніторингу операцій та ризиків.

Внаслідок цього виникає потреба в перегляді концептуальних підходів до організації інформаційного забезпечення економічної безпеки від підсистеми підтримки звітності – до інтегрованої цифрової платформи управління ризиками.

Розвиток цифрових технологій зумовлює формування принципово нової архітектури управління інформаційними потоками у банківському секторі. На відміну від традиційних моделей, що спиралися на ієрархічні та фрагментовані системи обробки даних, сучасні цифрові інфраструктури функціонують як інтегровані середовища, у яких поєднуються аналітичні, комунікаційні та захисні інструменти [8]. Упровадження цифрових платформ, хмарних рішень і технологій Big Data забезпечує можливість одночасної роботи з масштабними обсягами різнорідної інформації, її оперативної інтеграції та побудови глибоких аналітичних моделей, що підвищує точність оцінювання ризиків і швидкість управлінських рішень [10].

Ключовим елементом такої архітектури є аналітичні інструменти – системи штучного інтелекту, машинного навчання, поведінкової аналітики та прогнозних моделей, які перетворюють дані на високоінформативні сигнали для управління економічною безпекою банку. Додатково формуються розширені цифрові канали комунікації, включаючи відкриті API та стандарти open banking, що забезпечують інтеграцію внутрішніх і зовнішніх джерел інформації відповідно до вимог PSD2 та проєкту PSD3 [12, 14]. Завдяки цьому банківська система отримує можливість синхронізувати інформаційні потоки між підрозділами, контрагентами, фінансовими сервісами та регуляторами в режимі реального часу.

Не менш значущою складовою нової архітектури управління інформаційними потоками є захисні інструменти – системи кіберзахисту, інцидент-ме-

неджменту та управління цифровою операційною стійкістю. Регламент DORA установлює обов'язкові вимоги до багаторівневого захисту даних і безперервності цифрових операцій, що робить кіберстійкість невід'ємною частиною інформаційної інфраструктури банку [14]. У свою чергу NIST Cybersecurity Framework і стандарти ISO/IEC 27001:2022 визначають методологічні підходи до побудови захищених інформаційних систем, які охоплюють ідентифікацію загроз, контроль доступу, шифрування, моніторинг інцидентів і протидію кібератакам [11, 13].

Узгоджене функціонування аналітичних, комунікаційних та захисних компонентів формує нову логіку управління інформаційними потоками від лінійної обробки до циклічного, самонавчального та адаптивного контурного управління, у межах якого інформація стає базою для прогнозування, діагностики та мінімізації ризиків. Отже, цифрові технології не лише модернізують технічну інфраструктуру банків, а й трансформують засади економічної безпеки, переводячи її у площину інтегрованих цифрових екосистем, що забезпечують стійкість, прозорість і керованість інформаційного середовища. Цифрові технології формують нову архітектуру управління інформаційними потоками, яка ґрунтується на поєднанні аналітичних, комунікаційних та захисних інструментів.

Так, технології Big Data та машинного навчання забезпечують можливість обробки великих, різнорідних масивів даних щодо клієнтської поведінки, транзакційної активності, структури активів і зобов'язань, інформаційних інцидентів. Застосування сучасних цифрових технологій у банківському секторі забезпечує якісно новий рівень опрацювання інформації, що виявляється у здатності систем розпізнавати нетипові операції та поведінкові відхилення, які можуть свідчити про шахрайські дії чи внутрішні порушення; посилювати точність і адаптивність скорингових моделей та внутрішніх рейтингів за рахунок поглибленої аналітики даних, а також формувати достовірні прогнозні оцінки щодо розвитку ризиків ліквідності, кредитного, ринкового й операційного характеру, враховуючи інформаційну складову та динаміку цифрових потоків у фінансовому середовищі.

Застосування сучасних цифрових технологій у банківському секторі формує якісно новий рівень опрацювання інформації, за якого автоматизовані системи здатні виявляти нетипові операції та поведінкові відхилення, що можуть свідчити про шахрайські дії чи внутрішні порушення, забезпечують підвищення точності й гнучкості скорингових моделей та внутрішніх рейтингів завдяки використанню поглибленої аналітики даних, а також підтримують побудову обґрунтованих прогнозних оцінок щодо динаміки ризиків ліквідності, кредитного, ринкового й операційного характеру з урахуванням інформаційної складової та особливостей циркуляції цифрових потоків у сучасному фінансовому середовищі.

В свою чергу, хмарні обчислення та платформні рішення створюють інфраструктурну основу для масштабування інформаційно-аналітичних систем, гнучкого управління обчислювальними ресурсами, реалізації стійких конфігурацій зберігання даних. Для економічної безпеки це означає підвищення стійкості інформаційних систем до технічних та кібернетичних збоїв.

Також, інструменти дистанційної ідентифікації та біометрії, інтегровані у фронт-офісні процеси, одночасно виконують функцію розширення доступу до послуг і зменшення ймовірності маніпуляцій з ідентифікаційними даними. Вони формують важливий елемент інформаційної бази – надійні дані щодо клієнтів,

які надалі використовуються в аналітиці ризиків. Так, комплекси кіберзахисту (SOC-центри, системи управління подіями інформаційної безпеки – SIEM, багатофакторна аутентифікація, шифрування та токенізація) стають невід'ємною частиною інформаційно-аналітичної підсистеми, дані про інциденти кібербезпеки включаються до загальної картини ризиків, а не розглядаються ізольовано.

Отже, у контексті цифрової трансформації банківського сектору особливої ваги набуває аналіз технологічних інструментів, що забезпечують формування, інтеграцію, обробку та захист інформаційних потоків у системі економічної безпеки банку. Цифрові рішення не лише оптимізують операційну діяльність, а й визначають якість ризик-орієнтованого управління, оскільки саме на їх основі здійснюється моніторинг транзакцій, ідентифікація аномалій, моделювання ризиків та підтримка прийняття управлінських рішень. Водночас інтенсивне поширення відкритих API, хмарних сервісів, інструментів штучного інтелекту, платформ аналітики великих даних і систем кіберзахисту формує нову архітектуру інформаційної взаємодії банків, у межах якої дані набувають статусу стратегічного ресурсу безпеки. З огляду на це у таблиці 1 систематизовано ключові цифрові технології, що забезпечують функціонування інформаційних процесів економічної безпеки банку та визначають їхню ефективність у сучасному цифровому середовищі.

Таблиця 1

Цифрові технології в управлінні інформаційними процесами економічної безпеки банку

Технологічний інструмент	Функціональне призначення у банку	Аналітично-безпекова роль у системі економічної безпеки
Big Data та машинне навчання	Збір і обробка великих масивів транзакційних, поведінкових та зовнішніх даних	Виявлення аномалій, моделювання ризиків, створення профілів клієнтів і контрагентів, прогнозування загроз
Штучний інтелект (AI/ML)	Автоматизований скоринг, динамічне оновлення ризикових моделей, аналітичні рекомендації	Підтримка проактивного управління ризиками, раннє попередження загроз, безперервний моніторинг
Хмарні обчислення (Cloud)	Масштабоване зберігання даних, централізований доступ, стійкість до збоїв	Забезпечення відмовостійкості інформаційної інфраструктури, підвищення доступності даних для аналітики
Open API та відкритий банкінг	Інтеграція з фінтех-платформами і зовнішніми сервісами	Розширення джерел інформації, підвищення точності оцінки ризиків, мінімізація інформаційної асиметрії
Біометрія, e-KYC, дистанційна ідентифікація	Верифікація особи при відкритті рахунків і проведенні операцій	Зниження шахрайства, зменшення ризиків маніпуляції ідентифікаційними даними, формування достовірної клієнтської бази
Системи кіберзахисту (SIEM, SOC, MFA)	Контроль доступу, моніторинг інцидентів, захист від атак	Підвищення стійкості до кібератак, захист критичних інформаційних активів, безперервне виявлення загроз
Блокчейн та смарт-контракти	Прозорі транзакції, токенізація активів, децентралізоване зберігання	Неможливість підробки записів, зниження операційних і репутаційних ризиків, підвищення довіри
RPA та роботизовані системи	Автоматизація бек-офісних процесів, обробки платежів, документів	Зменшення людських помилок, прискорення інформаційних потоків, оптимізація операційної безпеки

Джерело: побудовано автором

В таблиці узагальнено ключові цифрові технології, які вже сьогодні визначають архітектуру інформаційно-аналітичної підсистеми економічної безпеки банків. Аналіз їх функціонального призначення демонструє, що цифровізація змінює роль інформаційних ресурсів – від інструментів супроводу операцій до стратегічного активу, на основі якого приймаються управлінські рішення щодо ризиків, фінансової стійкості та захисту інфраструктури.

Big Data, штучний інтелект та машинне навчання формують основу цифрової аналітики, забезпечуючи безперервний моніторинг транзакцій, поведінкових моделей клієнтів, операційних аномалій і тенденцій у фінансовому середовищі. Це дозволяє банкам переходити до проактивної моделі економічної безпеки, де ризики не лише фіксуються постфактум, а прогнозуються та ідентифікуються на ранніх етапах. Хмарні обчислення і відкриті API радикально змінюють інформаційну інфраструктуру банку, підвищуючи її гнучкість, доступність, масштабованість і здатність інтегрувати зовнішні інформаційні потоки. Це має важливе значення для зниження інформаційної асиметрії та посилення міжсистемної взаємодії в моделі «банк – фінтех – регулятор».

Засоби дистанційної ідентифікації та біометрія забезпечують формування достовірної клієнтської бази – одного з ключових активів у системі контролю ризиків та виявлення шахрайства. Водночас технології кіберзахисту, включаючи SIEM, SOC та MFA, стають критичними для захисту інформаційних активів від зростаючої інтенсивності кібератак. Отже, таблиця 1 демонструє структуроутворюючу роль цифрових технологій у побудові системи управління економічною безпекою, де кожний технологічний інструмент виконує функції як операційної підтримки, так і аналітичної синхронізації ризиків.

З урахуванням викладеного доцільно запропонувати організаційно-функціональну модель управління процесами інформаційного забезпечення економічної безпеки банку на засадах використання сучасних цифрових технологій (рис. 1).

Запропонована модель фіксує перехід від лінійного, «звітно-орієнтованого» розуміння інформаційного забезпечення до контурної, замкненої системи, де цифрові технології забезпечують повний цикл: «дані – аналітика – рішення – захист – нові дані». В ній відображено концепцію багаторівневої та замкненої інформаційної системи економічної безпеки банку, в якій цифрові технології виступають засобами інтеграції, аналізу та захисту даних. Запропонована модель демонструє логіку формування повного циклу інформаційної підтримки управління ризиками – від збирання первинних даних до їх використання у процесах прийняття рішень і повернення в систему як нових інформаційних сигналів. Аналітична інтерпретація моделі дозволяє виділити кілька ключових аспектів. Блок формування даних передбачає мультиканальність цифрових джерел, що розширює спектр інформації, необхідної для оцінювання ризиків. У контексті цифрової економіки саме повнота та різноманітність даних визначає якість моделювання загроз. Інтеграційний блок виконує функцію уніфікації й централізації даних, забезпечуючи їх структурованість, цілісність та доступність. Його значущість зростає в умовах, коли банки оперують масштабними масивами транзакційних, клієнтських та технологічних даних.

Аналітико-моделюючий блок демонструє зміщення від статичних методів аналізу до динамічних, адаптивних моделей, заснованих на AI і машинному навчанні, забезпечує підвищення точності прогнозів і можливість створення інтегральних індикаторів економічної безпеки. Блок підтримки прийняття

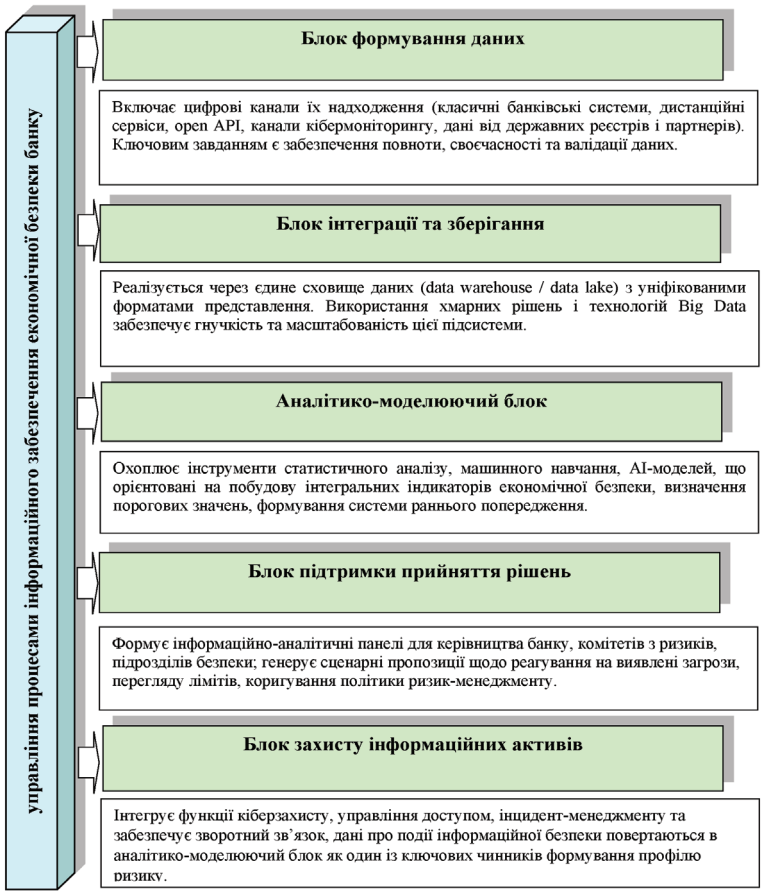

Рис. 1. Організаційно-функціональна модель управління процесами інформаційного забезпечення економічної безпеки банку

Джерело: розроблено автором

рішень забезпечує формування цифрових інформаційних панелей, тригерів і сценаріїв реагування. Цей елемент моделі підсилює стратегічний характер інформаційної підтримки і забезпечує оперативність управлінських дій. Блок захисту інформаційних активів виконує роль «цифрового щита», інтегруючи кіберзахисні засоби у загальний контур економічної безпеки. Він не лише захищає дані, а й формує інформаційні сигнали про інциденти, які повертаються в аналітичну підсистему.

У сукупності елементи моделі відображають якісно новий тип інформаційно-аналітичного забезпечення – інтегрований, адаптивний, ризик-орієнтований, побудований на цифрових технологіях і здатний підтримувати економічну безпеку банків в умовах диджиталізації та зростання загроз.

Висновки. Обгрунтовано, що цифровізація банківської діяльності стає ключовим чинником модернізації системи економічної безпеки банків, визначаючи нову логіку формування, аналізу та використання інформації в управлінських процесах. Цифрові технології не лише оптимізують операційні процедури, а й трансформують архітектуру інформаційних потоків, забезпечуючи можливість переходу від фрагментарних та реактивних механізмів до інтегрованих, проактивних моделей ризик-менеджменту.

Встановлено, що сучасне цифрове середовище формує якісно нові вимоги до інформаційно-аналітичної підсистеми економічної безпеки банку. Система, яка історично виконувала функції підтримки звітності та контролю окремих ризиків, у цифровій економіці перетворюється на стратегічний елемент управління, що забезпечує безперервний моніторинг загроз, високу точність прогнозування та інформаційну синхронізацію між підрозділами банку.

Обґрунтовано, що використання Big Data, штучного інтелекту, хмарних обчислень, інструментів відкритого банкінгу, засобів кіберзахисту та дистанційної ідентифікації створює передумови для формування цілісної цифрової моделі управління інформаційними процесами. Застосування цих технологій забезпечує розширення джерел даних, автоматизацію аналітичних процедур, підвищення стійкості інформаційної інфраструктури, а також мінімізацію операційних та інформаційних ризиків.

Запропонована організаційно-функціональна модель управління процесами інформаційного забезпечення економічної безпеки банку демонструє можливість побудови замкненого інформаційно-аналітичного контуру, у якому цифрові інструменти забезпечують повний цикл «дані – аналітика – рішення – захист – нові дані». Її впровадження спрямоване на підвищення адаптивності банку до зовнішніх шоків, зменшення інформаційної асиметрії та підсилення стратегічного потенціалу системи економічної безпеки.

Узагальнюючи результати дослідження, слід зазначити, що цифровізація є не лише технологічним, а насамперед концептуально-управлінським процесом, який суттєво змінює характер взаємодії між інформаційними ресурсами, ризиками та управлінськими рішеннями. Це зумовлює необхідність подальших досліджень, спрямованих на оцінювання ефективності цифрових інструментів, розроблення методів кількісного вимірювання цифрової стійкості та удосконалення регуляторних механізмів цифрової трансформації фінансового сектору.

Список використаних джерел

1. Єпіфанов А. О., Пластун О. Л., Домбровський В. С. *Фінансова безпека підприємств і банківських установ : монографія* / за заг. ред. А. О. Єпіфанова. Суми: ДВНЗ УАБС НБУ, 2009. 295 с.
2. Коваленко В. В. Філософія безпеки банків в умовах структурних дисбалансів економіки України. *Економічний форум*. 2016. № 2. С. 256–262. URL: http://nbuv.gov.ua/UJRN/ecfor_2016_2_41
3. Куцик П. О., Куцик О. П. Економічна безпека банків в умовах глобалізації. *Економіка та суспільство*. 2017. Вип. 11. URL: https://economyandsociety.in.ua/index.php/journal/article/view/82
4. Васильчук С. В., Моцьо Р. Ю. Економічна безпека банків та методи її забезпечення. *Науковий вісник Львівської політехніки. Серія: Економіка*. 2009. № 19(12). С. 287–294. URL: https://nv.nltu.edu.ua/Archive/2009/19_12/287_Wasylczak_19_12.pdf
5. Теслюк С. А., Матвійчук Н. М., Левчук А. О. Фінансова безпека банківських установ в умовах цифровізації. *Економіка та суспільство*. 2024. Вип. 60. URL: https://economyandsociety.in.ua/index.php/journal/article/view/3646; DOI: 10.32782/2524-0072/2024-60-117
6. Tymots M. Analysis of trends and prospects of digital banking in Ukraine. *ISJMEF – International Scientific Journal of Management, Economics & Finance*. 2025. Vol. 4, № 5. С. 34–47. URL: https://isg-journal.com/isjmef/article/view/1089; DOI: 10.46299/j.isjmef.20250405.03

7. Клочко А. М., Волченко Н. В., Клєцова Н. В. Економіко-правові засади банківської безпеки за умов посилення євроінтеграційних процесів в Україні. *Юридичний бюлетень*. 2021. № 18. С. 164–171. URL: https://lawbulletin.oduvs.od.ua/archive/2021/18/24.pdf; DOI: 10.32850/LB2412-4207.2021.18.22
8. Bank for International Settlements. *Annual Economic Report 2023. Chapter III: Digitalisation and its impact on finance.* URL: https://www.bis.org/publ/arpdf/ar2023e3.htm
9. World Bank. *Digital Financial Services: Challenges and Opportunities.* Washington, DC, 2022. URL: https://www.worldbank.org/en/topic/financialsector
10. International Monetary Fund. *Fintech and Financial Services: Initial Considerations.* IMF Staff Discussion Note, 2017. URL: https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/Fintech-and-Financial-Services-44921
11. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems. URL: https://www.iso.org/standard/82875.html
12. Бондарук Т.Г., Богріновцева Л.М., Бондарук О.С. Методологічні підходи до оптимізації боргової політики України в контексті фінансової безпеки. Статистика України. 2025. №1. С. 13-24. URL: https://su-journal.com.ua/index.php/journal/article/view/460/428; DOI: 10.31767/su.1(108)2025.01.02
13. Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market (PSD2). URL: https://eur-lex.europa.eu/eli/dir/2015/2366/oj
14. National Institute of Standards and Technology. *Cybersecurity Framework* (NIST CSF). Version 1.1, 2018. URL: https://www.nist.gov/cyberframework
15. Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector (DORA). URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj
16. Basel Committee on Banking Supervision. *Principles for Operational Resilience.* BIS, 2021. URL: https://www.bis.org/bcbs/publ/d516.htm
17. Бондарук Т., Чеховська М., Бондарук О. Економічна безпека України під час військових дій: виклики та шляхи протидії. *Економічні горизонти.* 2024. №1(27). С. 129–141. DOI: 10.31499/2616-5236.1(27).2024.299201

References

1. Yepifanov, A. O., Plastun, O. L., & Dombrovskyi, V. S. (2009). *Financial Security of Enterprises and Banking Institutions* (A. O. Yepifanov, Ed.). Sumy: Ukrainian Academy of Banking of the National Bank of Ukraine.
2. Kovalenko, V. V. (2016). Philosophy of bank security under structural imbalances of Ukraine's economy. *Economic Forum*, 2, 256–262. Retrieved from http://nbuv.gov.ua/UJRN/ecfor_2016_2_41
3. Kutsyk, P. O., & Kutsyk, O. P. (2017). Economic security of banks in the context of globalization. *Economy and Society*, 11. Retrieved from https://economyandsociety.in.ua/index.php/journal/article/view/82
4. Vasyltchuk, S. V., & Motso, R. Yu. (2009). Economic security of banks and methods of its assurance. *Scientific Bulletin of Lviv Polytechnic. Economics Series*, 19(12), 287–294. Retrieved from https://nv.nltu.edu.ua/Archive/2009/19_12/287_Wasylczak_19_12.pdf
5. Tesliuk, S. A., Matviichuk, N. M., & Levchuk, A. O. (2024). Financial security of banking institutions under digitalization. *Economy and Society*, 60. Retrieved from https://economyandsociety.in.ua/index.php/journal/article/view/3646; DOI: 10.32782/2524-0072/2024-60-117
6. Tymots, M. (2025). Analysis of trends and prospects of digital banking in Ukraine. *International Scientific Journal of Management, Economics & Finance (ISJMEF)*,

4(5), 34–47. Retrieved from https://isg-journal.com/isjmef/article/view/1089; DOI: 10.46299/j.isjmef.20250405.03
7. Klochko, A. M., Volchenko, N. V., & Klietsova, N. V. (2021). Economic and legal foundations of banking security under strengthened EU integration processes in Ukraine. *Law Bulletin*, 18, 164–171. Retrieved from https://lawbulletin.oduvs.od.ua/archive/2021/18/24.pdf; DOI: 10.32850/LB2412-4207.2021.18.22
8. Bank for International Settlements. (2023). *Annual Economic Report 2023 – Chapter III: Digitalisation and its impact on finance*. Retrieved from https://www.bis.org/publ/arpdf/ar2023e3.htm
9. World Bank. (2022). *Digital Financial Services: Challenges and Opportunities*. Washington, DC: World Bank Group. Retrieved from https://www.worldbank.org/en/topic/financialsector
10. International Monetary Fund. (2017). *Fintech and Financial Services: Initial Considerations* (IMF Staff Discussion Note). Retrieved from https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/Fintech-and-Financial-Services-44921
11. ISO/IEC 27001:2022. (2022). Information security, cybersecurity and privacy protection – Information security management systems. Retrieved from https://www.iso.org/standard/82875.html
12. Bondaruk, T. H., Bohrinovtseva, L. M., & Bondaruk, O. S. (2025). Methodological approaches to optimizing Ukraine's debt policy in the context of financial security. *Statistics of Ukraine*, 1, 13–24. Retrieved from https://su-journal.com.ua/index.php/journal/article/view/460/428; DOI: 10.31767/su.1(108)2025.01.02
13. European Parliament and Council. (2015). *Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*. Retrieved from https://eur-lex.europa.eu/eli/dir/2015/2366/oj
14. National Institute of Standards and Technology. (2018). *NIST Cybersecurity Framework* (Version 1.1). Retrieved from https://www.nist.gov/cyberframework
15. European Parliament and Council. (2022). *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA)*. Retrieved from https://eur-lex.europa.eu/eli/reg/2022/2554/oj
16. Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements. Retrieved from https://www.bis.org/bcbs/publ/d516.htm
17. Bondaruk, T., Chekhovska, M., & Bondaruk, O. (2024). Economic security of Ukraine during wartime: challenges and countermeasures. *Economic Horizons*, 1(27), 129–141. https://doi.org/10.31499/2616-5236.1(27).2024.299201; DOI: 10.31499/2616-5236.1(27).2024.299201

Посилання на статтю:

Бондарук Т. Г. Використання сучасних цифрових технологій в управлінні процесами інформаційного забезпечення економічної безпеки банків. *Науковий вісник Національної академії статистики, обліку та аудиту*: *зб. наук. праць*. № 3–4. 2025. С. 7–19. DOI: 10.31767/nasoa.3-4-2025.01

Link to the article:

Bondaruk, T. H. (2025) Vykorystannia suchasnykh tsyfrovykh tekhnolohii v upravlinni protsesamy informatsiinoho zabezpechennia ekonomichnoi bezpeky bankiv [Use of modern digital technologies in managing the information support processes of banks' economic security]. *Naukovyi visnyk Natsionalnoi akademii statystyky, obliku ta audytu – Scientific Bulletin of the National Academy of Statistics, Accounting and Audit.* 3–4. 7–19. DOI: 10.31767/nasoa.3-4-2025.01 [in Ukrainian].