УДК 336.71:004.9:005.21
JEL Classification: G21; G28; C88; O33; M15

АРХІТЕКТУРА ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ ПІДТРИМКИ АДАПТИВНОГО УПРАВЛІННЯ БАНКІВСЬКОЮ СИСТЕМОЮ

ГРАБАРЄВ Андрій
Київський національний економічний університет імені Вадима Гетьмана
https://orcid.org/0000-0001-6165-0996
e-mail: hrabariev_andrii@kneu.edu.ua

Фрагментарність інформаційних джерел, моделей і засобів візуалізації ускладнює відтворення підстав управлінського рішення та посилює ризик використання несинхронних даних, застарілих моделей або непрозорих аналітичних сигналів. Метою дослідження є розроблення референтної архітектури інформаційно-аналітичної системи підтримки адаптивного управління банківською системою, у якій шлях від джерела даних до рішення організовано як керований доказовий цикл. Запропоновано шестирівневу функціональну архітектуру, доповнену чотирма наскрізними контурами управління і контролю та трьома контрольними шлюзами Data Gate, Model Gate і Decision Gate. Функціональні рівні охоплюють отримання даних і метаданих, інтеграцію та контроль якості, семантичний і ознаковий шар, аналітичний і модельний шар, оркестрацію управлінських рішень, представлення та взаємодію. Наукова новизна полягає у формалізації безперервності доказового ланцюга «джерело – дані – трансформація – модель – сигнал – пояснення – рішення – результат – зворотний зв'язок» із версійністю, трасованістю, поясненістю за задумом, безпечною відмовою аналітики та обов'язковою участю фахівця. Мінімальний шлюз якості даних апробовано на 84 місячних спостереженнях інтегрального індексу адаптивного розвитку банківської системи (IAR) та п'яти функціональних компонентів за 2019M01-2025M12: середній і мінімальний коефіцієнти повноти дорівнюють 1, максимальна похибка математичного узгодження становить близько 2,22×10-16, усі записи отримали статус PASS. Синтетичні негативні сценарії використано окремо для перевірки реакції CHECK/STOP. Запропонована архітектура є платформонезалежною та орієнтованою на відтворювану, підзвітну й керовану інформаційно-аналітичну підтримку. Практичне значення архітектури полягає у зменшенні інформаційного та модельного ризику без ототожнення автоматизованого сигналу з автоматичним управлінським рішенням.

Ключові слова: адаптивне управління; банківська система; інформаційно-аналітична система; управління даними; управління моделями; безперервність доказового ланцюга; human-in-the-loop; SupTech.

https://doi.org/10.31891/mdes/2026-22-9

This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

Стаття надійшла до редакції / Received 06.09.2026
Прийнята до друку / Accepted 27.10.2026
Опубліковано / Published 12.11.2026

© ГРАБАРЄВ Андрій

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Сучасне адаптивне управління банківською системою здійснюється в умовах високої динамічності макрофінансового, регуляторного, технологічного та інформаційного середовища. Зростання обсягів даних, різночастотність інформаційних потоків, регулярні перегляди статистики, поширення автоматизованої аналітики та одночасне використання різних класів моделей суттєво підвищують вимоги не лише до швидкості отримання аналітичного результату, а й до його відтворюваності, часової коректності, пояснюваності та підзвітності. За таких умов окремий прогноз, індикатор або інформаційна панель самі по собі не забезпечують достатньої якості управлінської підтримки. Необхідним стає формування цілісного інформаційно-аналітичного контуру, у межах якого можна простежити весь шлях від первинного джерела даних до аналітичного сигналу, його інтерпретації та остаточного управлінського рішення.

Особливої актуальності ця проблема набуває через неоднорідність інформаційної бази банківського аналізу. Макрофінансові, монетарні, регуляторні, банківські, технологічні та поведінкові дані характеризуються різною періодичністю, часовими лагами публікації, правилами перегляду та методологічними межами. За відсутності єдиного архітектурного контуру автономні моделі можуть використовувати різні статистичні зрізи, неузгоджені версії показників і відмінні правила трансформації, що ускладнює відтворення підстав управлінського висновку та підвищує інформаційний ризик. Вимоги до точності, повноти, своєчасності та адаптивності агрегації ризикових даних системно закріплено у BCBS 239, а сучасні оцінки його імплементації додатково акцентують на якості архітектури даних, lineage та здатності відтворювати інформаційний стан, на якому ґрунтувалося рішення [1; 2]. Це означає, що в сучасній ІАС показник має розглядатися не лише як числове значення, а як керований інформаційний об'єкт із визначеним джерелом, версією, часовою міткою, нативною частотою та історією трансформацій.

Другим чинником актуальності є зростання залежності аналітичного процесу від цифрової інфраструктури, програмних сервісів та автоматизованих каналів оброблення даних. Недоступність критичного сервісу, несанкціонована зміна конфігурації, втрата первинної версії даних або використання частково оновленого інформаційного пакета можуть безпосередньо впливати на якість і своєчасність управлінського реагування. Тому інформаційно-аналітична підтримка повинна бути стійкою не лише з економічного, а й з операційного та кібербезпекового погляду. Принципи операційної стійкості Basel Committee та вимоги DORA передбачають керованість критичних функцій, розмежування доступу, журналювання подій, резервування, відновлення та визначені режими функціонування у випадку порушення штатної роботи [3; 4]. Для архітектури IAC це означає необхідність формалізації умов, за яких аналітичний продукт може бути використаний, обмежений або заблокований.

Не менш важливою є проблема модельного ризику, що посилюється внаслідок паралельного використання економетричних, прогнозних, сценарних, класифікаційних та AI/ML-моделей. Технічна доступність моделі не гарантує її придатності до поточного інформаційного стану: необхідно враховувати її версію, область застосовності, валідаційний статус, стан калібрування, ознаки дрейфу, дату перегляду та сумісність із поточними даними. Вимоги до керованого життєвого циклу AI та системного контролю модельного ризику сформульовано у NIST AI RMF і сучасних рекомендаціях щодо моніторингу розгорнутих AI-систем [5; 6]. Водночас автоматизація не усуває потреби у професійному судженні. Модельно орієнтовані системи підтримки рішень передбачають взаємодію користувача з даними, моделями та альтернативами, а не делегування системі остаточного управлінського вибору [7; 8]. У сфері фінансового нагляду аналогічна логіка реалізується в межах SupTech, де технології підвищують швидкість і масштаб аналітики, але потребують чіткої відповідальності, контролю якості, трасованості та участі людини [9; 10].

Отже, актуальність дослідження визначається необхідністю переходу від фрагментарного використання окремих джерел даних, моделей і засобів візуалізації до цілісної інформаційно-аналітичної системи, у якій якість управлінської підтримки забезпечується безперервністю доказового ланцюга, часовою та версійною узгодженістю даних, контролем модельного ризику, операційною стійкістю та збереженням професійної відповідальності. Наукова проблема полягає у визначенні такої архітектури IAC, за якої автоматизація підвищує швидкість і масштаб аналізу, але не послаблює його доказовість, відтворюваність, підзвітність і керованість.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є розроблення та концептуально-емпірична перевірка референтної архітектури інформаційно-аналітичної системи підтримки адаптивного управління банківською системою. Наукова новизна полягає у формалізації наскрізного циклу **«джерело → дані → трансформація → модель → сигнал → пояснення → рішення → результат → зворотний зв'язок»** у межах шестирівневої функціональної структури, чотирьох наскрізних контурів управління і контролю та трьох контрольних шлюзів Data Gate, Model Gate і Decision Gate.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ВИДІЛЕННЯ НЕВИРІШЕНИХ АСПЕКТІВ ПРОБЛЕМИ

Теоретичні засади систем підтримки рішень ґрунтуються на розмежуванні аналітичної підтримки та власне управлінського вибору. **Power і Sharda** розглядають model-driven DSS як середовище інтеграції даних, моделей і процедур аналізу, у якому алгоритм має підтримувати структурування рішення, а не замінювати користувача [7]. У фінансовій сфері **Zopounidis, Doumpos і Niklis** акцентують на багатокритеріальності, невизначеності та необхідності пояснюваності аналітичного результату у контексті конкретного управлінського завдання [8]. Це особливо важливо для банківської системи, де окрема модель не може замінити повний цикл контролю даних, ризиків, сценаріїв і відповідальності.

У напрямі SupTech **Broeders і Prenio**, аналізуючи досвід ранніх користувачів наглядових технологій, показують, що автоматизація збору, оброблення та пріоритизації інформації підвищує швидкість нагляду, але одночасно потребує формалізованих процедур контролю якості, governance та ескалації [9]. Для України Національний банк також визначає SupTech і RegTech як важливий напрям цифровізації фінансового нагляду [10]. Проте ці підходи переважно спрямовані на автоматизацію окремих функцій і не формалізують наскрізний доказовий шлях від первинного джерела даних до зафіксованого управлінського рішення.

Проблематика управління даними системно розкрита в документах **Basel Committee on Banking Supervision**, де BCBS 239 пов'язує надійність ризикової аналітики з точністю, повнотою,

своєчасністю, походженням і відтворюваністю даних [1]. Подальша оцінка імплементації цих принципів посилює акцент на архітектурі даних, lineage та здатності відтворити інформаційний стан, на якому ґрунтувалося рішення [2]. Для багаточастотного банківського середовища це означає необхідність збереження нативної частоти, версій і методологічного контексту показників, а не їх механічного приведення до єдиного формату.

Операційний вимір розширює ці вимоги до доступності та стійкості аналітичного контуру. **Basel Committee** трактує операційну стійкість як спроможність підтримувати критичні операції та відновлюватися після порушень [3], а **European Parliament і Council of the European Union** у DORA закріплюють вимоги до управління цифровими операційними ризиками, контролю доступу, відновлення та журналювання [4]. У контексті IAC це означає, що недоступність джерела або моделі не повинна призводити до прихованого використання застарілого результату; система має явно маркувати такий стан і блокувати недопустимий перехід до управлінського висновку.

Проблему управління AI та модельним ризиком розвивають **Tabassi**, який у NIST AI RMF формалізує ризик-орієнтований підхід до життєвого циклу AI-систем [5], та **Rao та співавтори**, які акцентують на постійному моніторингу вже розгорнутих AI-моделей, зміні середовища та необхідності контролю їх фактичної поведінки [6]. **Batool, Zowghi і Bano** у систематичному огляді AI-governance підкреслюють важливість відповідальності, прозорості та постійного контролю моделей [11], тоді як **Raji та співавтори** пропонують наскрізну логіку внутрішнього алгоритмічного аудиту, що охоплює не лише модель, а й процес її розроблення, застосування та документування рішень [12]. У фінансовому контексті **Černevičienė і Kabašinskas** показують, що XAI має розглядатися спільно з вимогами governance, а не як ізольований інструмент інтерпретації моделі [16]. Наглядова практика **ECB Banking Supervision** також пов'язує цифрову трансформацію з необхідністю сильного управління та контролю [17].

Методологічно близькою до такого завдання є Design Science Research. **Hevner, March, Park і Ram** визначають науковий внесок через створення та оцінювання артефакта, здатного розв'язувати практично значущу проблему [13]. **Peffers та співавтори** формалізують послідовність DSR від ідентифікації проблеми до проєктування, демонстрації та оцінювання рішення [14], **а Gregor і Hevner** наголошують, що новизна артефакта має визначатися через його співвідношення з наявною базою знань [15]. Саме така логіка є релевантною для побудови референтної архітектури IAC як наукового артефакта.

Отже, наявні дослідження достатньо глибоко розкривають окремі складові — DSS, SupTech, data governance, операційну стійкість, model governance, AI-governance та XAI, однак їх інтеграція в єдину доказово орієнтовану архітектуру адаптивного управління банківською системою залишається неповною. BCBS 239 не формалізує Decision Gate; DSS не забезпечують наскрізної версійності доказового пакета; SupTech не встановлює універсального зв'язку Data Gate – Model Gate – Decision Gate; AI-governance концентрується переважно на життєвому циклі моделей, а не на повному statistical vintage управлінського рішення [1; 5–17]. Відтак дослідницька прогалина полягає у необхідності поєднати семантично й версійно узгоджені дані, контроль придатності моделей та трасований перехід від сигналу до рішення в одному керованому доказовому циклі.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ ТА ПРОЄКТНІ ПОЛОЖЕННЯ

Дослідження виконано в парадигмі Design Science Research, де референтна архітектура IAC розглядається як науковий артефакт, призначений для розв'язання класу проблем доказової та відтворюваної інформаційно-аналітичної підтримки [13-15]. Об'єктом є інформаційно-аналітичні процеси підтримки управління адаптивним розвитком банківської системи; предметом - принципи, функціональні рівні, інформаційні артефакти, контрольні механізми, рольова взаємодія та наскрізні контури управління і контролю IAC. Методологічну логіку структуровано за послідовністю DSR: ідентифікація проблеми та ризиків; визначення цілей архітектурного рішення; проєктування і формування референтної архітектури; демонстрація через операціоналізацію вимог у контрольні шлюзи та статуси; оцінювання мінімального Data Gate на контрольному інформаційному пакеті; комунікація результатів і меж застосовності. Така побудова відокремлює наукове оцінювання артефакта від опису конкретного програмного продукту.

Дослідницькі питання сформульовано наступним чином: RQ1 – які функціональні рівні необхідні для перетворення автономних даних і моделей на керовану IAC; RQ2 – як забезпечити безперервність доказового ланцюга від первинного джерела до рішення та ex post оцінювання; RQ3 – як Data Gate, Model Gate і Decision Gate мають запобігати поширенню непридатного аналітичного результату; RQ4 - як поєднати автоматизацію з human-in-the-loop, рольовою відповідальністю і

принципом least privilege; RQ5 – чи може мінімальний data-quality gate бути формально та емпірично перевірений; RQ6 – як зберегти платформонезалежність архітектури при достатній конкретності для інституційної реалізації.

Замість статистичних гіпотез використано три проєктні положення. Перше: надійність управлінського рішення залежить від безперервності доказового ланцюга, а не лише від точності окремої моделі. Друге: критичний збій контрольного шлюзу має блокувати або маркувати подальше використання аналітичного продукту незалежно від технічної можливості продовжити розрахунок. Третє: автоматизований сигнал не повинен бути тотожним автоматичному рішенню; для високоризикового фінансового середовища human-in-the-loop є обов'язковою властивістю архітектури.

Емпіричну частину побудовано на контрольному пакеті з 84 місячних спостережень за період 2019M01-2025M12 інтегрального індексу адаптивного розвитку банківської системи (IAR) та п'яти його функціональних компонентів CAP, LIQ, CREDIT, RISK і PROF. Вихідна дослідницька база сформована на основі офіційної статистики Національного банку України щодо показників фінансової стійкості, наглядової статистики та доступних інтерфейсів даних [18-20]. Емпірична перевірка у цій статті стосується виключно логіки контрольного шлюзу і не підміняє повномасштабну валідацію виробничої IAC. Систематизацію відповідних архітектурних ризиків і вимог наведено в табл. 1, а логіку обґрунтування референтної архітектури IAC — на рис. 1.

Таблиця 1.

Архітектурні ризики та вимоги до інформаційно-аналітичної системи

Проблема середовища	**Потенційний збій**	**Архітектурна вимога**	**Контрольний механізм**
Неоднорідність джерел, частот і лагів	Несинхронний статистичний зріз	Єдина модель метаданих і часової узгодженості	Каталог даних, native frequency, release timestamp
Перегляди статистики та методології	Невідтворюваність попереднього результату	Версійність і lineage	Source/version ID, методологічний прапорець, change log
Паралельне використання моделей	Суперечливі результати без визначення придатності	Model governance та керована оркестрація	Model registry, validation status, owner, execution log
Висока швидкість зміни середовища	Використання застарілого аналітичного продукту	Контроль свіжості даних і подій	Freshness flag, policy update, event trigger, SLA
Кібер- та операційні залежності	Втрата критичного аналітичного контуру	Операційна стійкість і сегментація доступу	Role-based access, backup, degraded mode, audit trail
Висока ціна помилкового висновку	Непрозора автоматизація та відсутність відповідальності	Explainability, human-in-the-loop, decision log	Reason code, approval, rationale, ex post review

Джерело: систематизовано автором на основі [1-17].

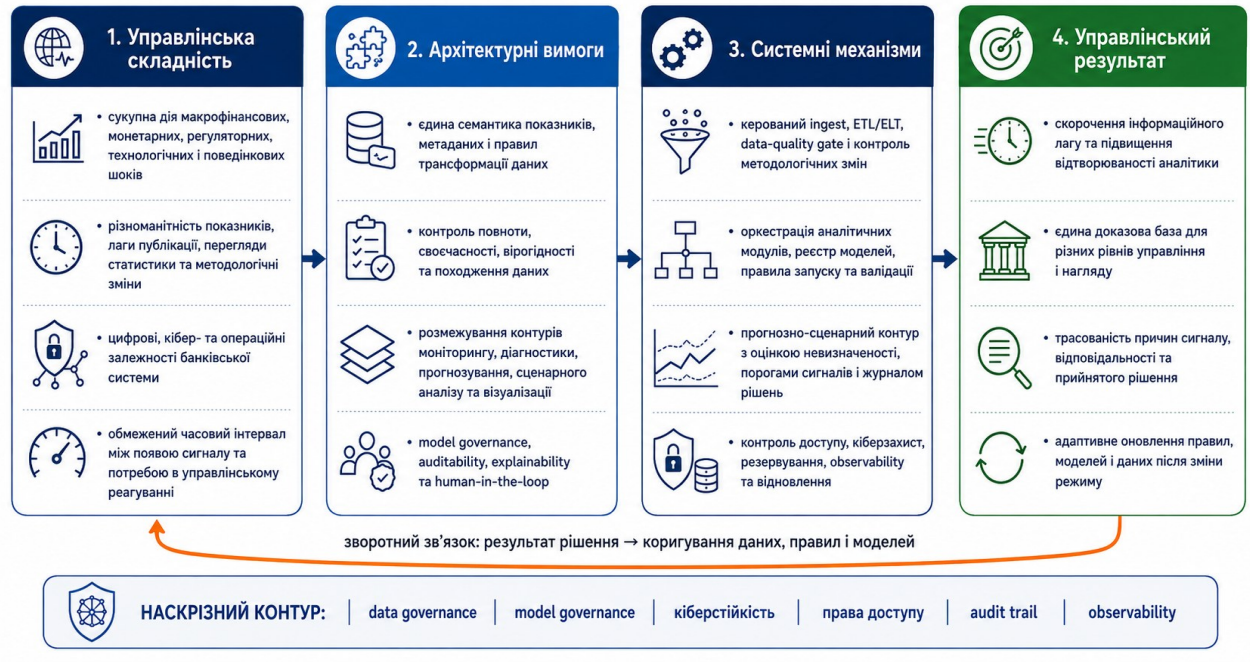


Рис. 1. Логіка обґрунтування референтної архітектури IAC

Джерело: розроблено автором.

Запропонована архітектура виходить із того, що архітектурне рішення має починатися не з вибору програмної платформи, а з формалізації управлінських ризиків і вимог до доказовості. У цьому розумінні ІАС є логічно впорядкованою сукупністю інформаційних, аналітичних, модельних, управлінських і контрольних компонентів, між якими визначено потоки даних, відповідальність, правила валідації, права доступу та механізми зворотного зв'язку. Архітектура повинна бути нейтральною до конкретної програмної реалізації, але достатньо конкретною, щоб встановлювати обов'язкові функції, інформаційні артефакти й контрольні точки.

Базовим проєктним правилом є розмежування відповідальності (separation of concerns). Джерело даних не визначає економічну інтерпретацію показника; модуль інтеграції не підміняє модельну валідацію; прогнозний сервіс не формує автоматично управлінський вплив; інтерфейс не має приховувати невизначеність або обмеження моделі. Водночас функціональне розділення не повинно розривати трасованість: для будь-якого показника, сигналу або рекомендації має зберігатися можливість відновити джерело, версію, трансформації, застосовану модель, припущення та факт погодження.

Центральним поняттям авторської конструкції є безперервність доказового ланцюга (evidence continuity). Управлінський продукт містить не лише числовий результат, а й дату статистичного зрізу, статус джерел, версію моделі, оцінку невизначеності, reason code, сценарні припущення та обмеження. Версійність забезпечує відтворення аналітичного стану на конкретну дату, а збереження нативної частоти запобігає прихованому змішуванню часових горизонтів. Пояснення формується разом із сигналом, а не як факультативний post hoc-додаток.

Принцип безпечної відмови аналітики (fail-safe analytics) передбачає, що порушення критичної передумови змінює статус аналітичного продукту, а не маскується технічною доступністю розрахунку. Неповний пакет, невідома версія, прострочена валідація або розрив lineage мають приводити до CHECK/STOP або REVIEW/BLOCK залежно від рівня контролю. Модульна розширюваність, своєю чергою, дає змогу підключати нові інформаційні й модельні сервіси через стандартизовані контракти без зміни правил якості, трасованості та відповідальності. Узагальнення принципів архітектури, відповідних контрольних артефактів та управлінських ефектів наведено в табл. 2.

Таблиця 2.

Принципи архітектури та контрольні артефакти

Принцип	Зміст	Контрольний артефакт	Управлінський ефект
Єдине джерело (single source of truth)	Для кожної версії показника визначено авторитетне джерело	Registry of sources, source ID	Усунення конкуренції неузгоджених копій
Нативна частота (native frequency first)	Первинна частота і дата релізу не втрачаються	Frequency field, release timestamp	Часова коректність
Версійність і lineage	Кожна зміна data/method/model має version ID	Version ID, lineage graph, change log	Відтворюваність попереднього стану
Розмежування відповідальності	Дані, моделі, рішення та presentation мають різні контракти	Layer/data contract	Зменшення прихованих залежностей
Evidence continuity	Сигнал зберігає повний контекст формування	Evidence package	Аудитованість управлінської підстави
Explainability by design	Пояснення формується одночасно із сигналом	Reason code, explanation field	Можливість обгрунтування рішення
Human-in-the-loop	Автоматизований сигнал не дорівнює рішенню	Approval status, user ID, timestamp	Підзвітність високоризикових рішень
Fail-safe analytics	Критичний збій блокує або маркує результат	PASS/CHECK/STOP; VALID/REVIEW/BLOCK	Запобігання використанню непридатного продукту
Модульна розширюваність	Нові модулі підключаються через стандартні інтерфейси	Module registry, interface specification	Масштабованість без руйнування ядра

Джерело: розроблено автором.

Функціональна частина референтної архітектури складається з шести рівнів:

Перший рівень – отримання даних і метаданих (Acquisition & Metadata) – реєструє джерело, source ID, статистичний період, release timestamp, vintage/version, native frequency та source status. Його виходом є зареєстрований інформаційний об'єкт, а не просто файл.

Другий рівень – інтеграція та якість даних (Integration & Data Quality) – розмежовує raw і curated zones, виконує типізацію, правила валідації, перевірки пропусків і дублікатів, узгодженості та свіжості й фіксує transformation ID.

Третій рівень – семантичний та ознаковий шар (Semantic & Feature Layer) – забезпечує словник економічних понять, одиниці виміру, частоти, власників методології, контроль структурних залежностей і витоку даних (data leakage).

Четвертий рівень – аналітичний і модельний шар (Analytical & Model Layer) – містить діагностичні, прогнозні та сценарні сервіси й реєстр моделей. Для кожної моделі фіксуються версія і статус, область застосовності, власник, дата наступного перегляду, показники якості й дрейфу та правила повторної валідації.

П'ятий рівень – оркестрація управлінських рішень (Decision Orchestration Layer) – перетворює валідований аналітичний результат на керований сигнал, код причини, пріоритет, маршрут ескалації та пакет пояснення, зберігаючи правило «сигнал не дорівнює рішенню».

Шостий рівень – представлення та взаємодія (Presentation & Interaction) – реалізує рольові представлення та навігацію «status – reason – evidence – lineage», мінімізуючи когнітивну відстань між агрегованим статусом і доказовою основою.

Чотири наскрізні контури управління і контролю мають однаковий пріоритет із функціональними рівнями. Управління даними (Data Governance) визначає власників, правила якості, каталог, пріоритет джерел, lineage та порядок методологічних змін. Управління моделями (Model Governance) регламентує життєвий цикл design – validation – deployment – monitoring – review – decommissioning. Контур кіберзахисту й доступу (Cyber/Access) забезпечує authentication, authorization, least privilege, segmentation, backup/recovery та межі доступу до чутливих bank-level даних. Аудит і спостережуваність (Audit/Observability) фіксують системні події, запуски моделей, зміни конфігурації, генерацію сигналів, дії користувачів, відмови та SLA. Саме їх наявність перетворює багаторівневий потік даних на керовану систему підтримки рішень, а не на технологічний pipeline. Взаємозв'язок шести функціональних рівнів із наскрізними контурами управління і контролю відображено на рис. 2.

Статична структура рівнів доповнюється повторюваним операційним циклом. Він починається з фіксації статистичного зрізу та версії джерел. Data Gate перевіряє completeness, reconciliation, duplicate keys, source freshness, version validity і schema changes. Лише пакет зі статусом, що дозволяє використання, передається до семантичного й модельного рівнів. Така логіка переводить data quality з технічної характеристики у формалізовану передумову управлінського використання.

Model Gate запускає лише модулі, статус яких у model registry дозволяє застосування на поточному зрізі. Контроль охоплює validation status, drift, applicability, calibration status, data compatibility та scenario suitability. Результат має містити не лише point estimate, а й контекст невизначеності та валідаційного статусу. Якщо критична умова не виконана, діагностичний результат може зберігатися для аналізу, але не повинен автоматично отримувати статус доказової основи рішення.

Decision Gate перевіряє повноту explanation package, повноваження користувача, маршрут ескалації, human approval і наявність decision log. Відхилення уповноваженого користувача від рекомендації системи не є помилкою, але має фіксуватися із rationale. Журнал рішення повинен зберігати timestamp, user ID, signal ID, explanation snapshot, рішення, коментар і результат ex post перегляду. Це забезпечує можливість аналізувати корисність сигналів, систематичні помилки, обґрунтованість експертних override та потребу в перекалібруванні правил.

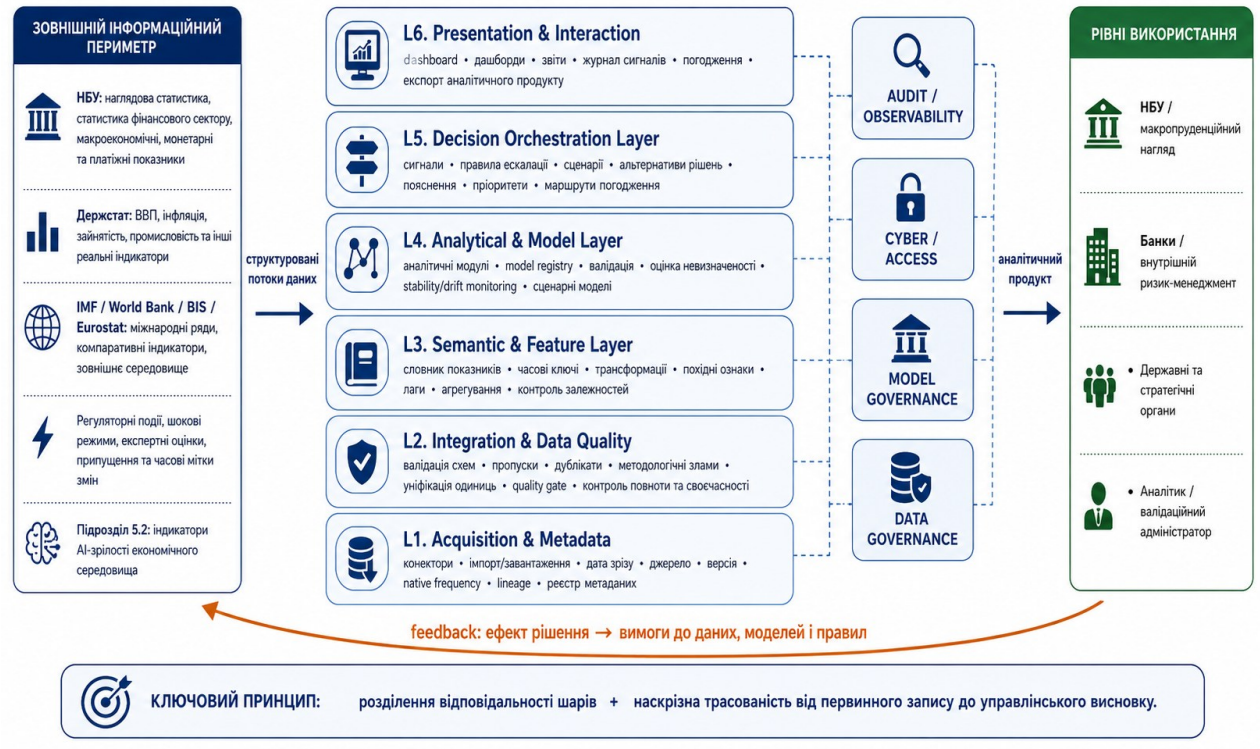


Рис. 2. Референтна шестирівнева архітектура IAC та наскрізні governance-контури
Джерело: розроблено автором.

Зворотний зв'язок реалізує адаптивність архітектури: результат рішення повертається до нового циклу як інформація для зміни вимог до даних, активного складу моделей, сценарних припущень і правил реагування. Принципово, що таке оновлення не змінює заднім числом інформаційний стан попереднього рішення; historical vintage та explanation snapshot зберігаються для коректної ex post оцінки. Узагальнену послідовність операційного циклу з Data Gate, Model Gate, Decision Gate та зворотним зв’язком наведено на рис. 3.

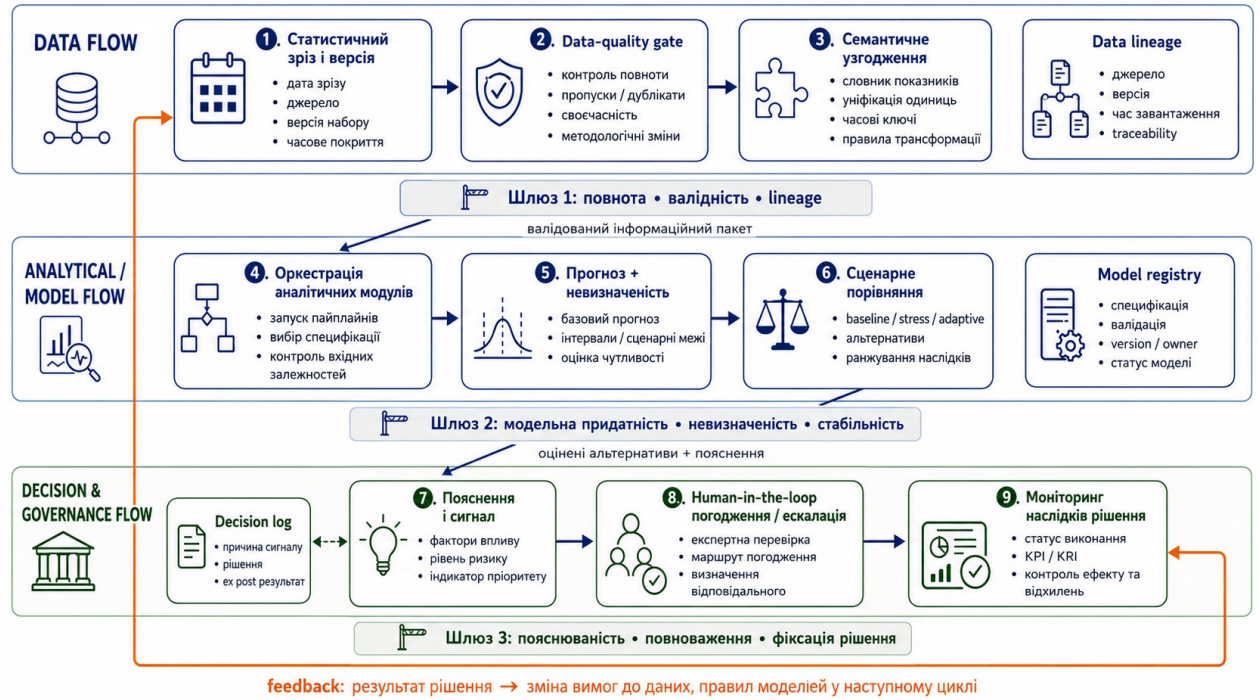


Рис. 3. Операційний цикл із Data Gate, Model Gate, Decision Gate та зворотним зв'язком
Джерело: розроблено автором.

Рольове розмежування реалізує least privilege, але не повинно руйнувати evidence continuity. Агрегований висновок, доступний управлінцю, має зберігати технічний шлях до джерел, трансформацій і моделі для уповноваженого валідатора. Водночас глибина пояснення адаптується до ролі: валідатор бачить специфікацію, дані та stability diagnostics; управлінець - причину сигналу, сценарні альтернативи й обмеження; адміністратор - стан сервісів і журнал подій. Така багаторівнева пояснюваність відповідає принципу explainability at the point of use. Рольову модель використання ІАС систематизовано в табл. 3.

Таблиця 3.

Рольова модель використання ІАС

Роль	Управлінське завдання	Гранулярність	Основний інформаційний продукт
Макропруденційний рівень / НБУ	Системна вразливість, наглядові пріоритети, сценарна оцінка	System-level + authorized drill-down	System cockpit, early-warning queue, scenario report, decision log
Банк / risk management	Капітальні, ліквіднісні, кредитні та операційні рішення	Internal bank-level + system context	Risk panel, forecast, stress/scenario view, factor explanation
Стратегічний державний рівень	Узгодження фінансової, цифрової та інституційної політики	Агреговані дані без чутливих bank-level деталей	Strategic panel, scenario effects, structural constraints
Аналітик / валідатор	Якість даних, моделі, стабільність і відтворюваність	Максимальний technical drill-down у межах прав	Data quality monitor, model registry, validation report, lineage
Адміністратор ІАС	Доступність, версійність, резервування, доступ	System metadata та журнали	Service status, access log, backup/recovery status, observability

Джерело: розроблено автором з урахуванням концепцій DSS і SupTech [7-10].

Типологія сигналів має важливий методологічний наслідок: не кожне спрацювання ІАС означає погіршення економічного стану. Сигнал може стосуватися якості даних, модельного ризику, кіберподії або порушення governance. Зведення таких різнорідних подій до одного індикатора створювало б хибну однозначність; тому архітектура спочатку локалізує джерело проблеми, а вже потім визначає маршрут реагування. На рівні інтерфейсу це реалізується через ієрархію «status – reason – evidence – lineage». Основні класи сигналів, реакції ІАС та маршрути їх ескалації наведено в табл. 4.

Щоб архітектура не залишалася лише концептуальною схемою, мінімальне ядро Data Gate формалізовано та перевірено на контрольному пакеті з 84 спостережень. Контрольованими полями є IAR і п'ять функціональних компонентів CAP, LIQ, CREDIT, RISK та PROF, отже $\boldsymbol{J = 6}$. Перша метрика – коефіцієнт повноти $\mathbf{C}_{\boldsymbol{t}}$, що визначає частку наявних обов'язкових значень. Друга – абсолютна похибка reconciliation $\boldsymbol{\varepsilon_t}$, яка перевіряє, чи переданий між шарами IAR відповідає саме тій версії п'яти компонентів, з якої він мав бути сформований.

Таблиця 4.

Класи сигналів і маршрути ескалації

Клас сигналу	Типова причина	Реакція ІАС	Маршрут ескалації
Data-quality signal	Пропуск, дубль, stale source, unknown version, methodology break	Зупинка/маркування залежних розрахунків; reason code	Data owner / administrator / analyst
Model-risk signal	Expired validation, drift, degradation, out-of-domain	REVIEW/BLOCK; блокування прогнозного статусу	Model owner / independent validator
System-state signal	Матеріальна зміна адаптивного стану	Аналітичний пакет і відкриття decision case	Analyst -> authorized manager/regulatory level
Scenario-divergence signal	Висока розбіжність сценаріїв або невизначеність	Підвищення пріоритету scenario analysis; фіксація припущень	Strategic / macroprudential level
Governance/access signal	Unauthorized access, config change, missing decision log	Security/audit event; блокування критичної дії	Cybersecurity / compliance / administrator

Джерело: розроблено автором.

Reconciliation не є повторною економічною валідацією методики IAR. Її функція суто архітектурна: виявити порушення цілісності або версійної узгодженості інформаційного пакета. Якщо інтегральний показник і компоненти походять із різних версій або трансформацію змінено без оновлення залежностей, ε_t перестає бути машинно нульовою і пакет не повинен автоматично переходити до наступного шару.

Мінімальне ядро Data Gate використовує три стани. PASS присвоюється за повної комплектності полів та $\varepsilon_t <= 10^{-8}$; CHECK – за повної комплектності, але порушення арифметичної узгодженості; STOP – за відсутності хоча б одного обов'язкового поля. Порогове значення 10^{-8} не є економічним нормативом або межею системного ризику, а використовується виключно як технічний допуск машинної точності.

$$C_t = 1 - M_t / J \quad (1)$$

$$\varepsilon_t = \left| IAR_t - \frac{(CAP_t + LIQ_t + CREDIT_t + RISK_t + PROF_t)}{5} \right| \quad (2)$$

$$G_t = \{ PASS, C_t = 1 \wedge \varepsilon_t \leq 10^{-8};\ CHECK, C_t = 1 \wedge \varepsilon_t > 10^{-8};\ STOP, C_t < 1 \} \quad (3)$$

де C_t – коефіцієнт повноти контрольованого пакета; M_t – кількість відсутніх обов'язкових значень у момент t; $J = 6$ – кількість контрольованих полів (IAR та п'ять функціональних компонентів); ε_t – абсолютна похибка математичного узгодження між переданим IAR і середнім значенням його п'яти компонентів; G_t – статус проходження Data Gate. Модуль у формулі (2) забезпечує симетричний контроль відхилення незалежно від його знака.

За результатами контрольної апробації середній і мінімальний коефіцієнти повноти дорівнюють 1; максимальна похибка математичного узгодження становить приблизно $2{,}22 \times 10^{-16}$; усі 84 записи отримали статус PASS. Отриманий результат підтверджує працездатність мінімального ядра gate на коректному інформаційному пакеті, але не означає повномасштабної операційної валідації системи.

Окремо сформовано синтетичні негативні контрольні сценарії: пропуск обов'язкового поля, навмисне порушення reconciliation, дублювання ключа, прострочення джерела та невідома версія. Вони не є емпіричними спостереженнями банківської системи і використовуються виключно для перевірки логіки реакції CHECK/STOP та розширених правил унікальності, свіжості й валідності версії. Для production-рівня Data Gate має додатково контролювати допустимі діапазони, монотонність дат, одиниці виміру, методологічні розриви та неочікувані зміни схеми джерела. Результати емпіричної та негативної перевірки Data Gate узагальнено в табл. 5.

Обговорення результатів та практичні імплікації. Отриманий результат доцільно трактувати як governance-архітектуру, а не як опис конкретної IT-платформи. Головним продуктом є контроль цілісності доказу, а не сама інформаційна панель. Порівняно з BCBS 239 запропонована конструкція продовжує lineage від даних до модельного й управлінського рівнів; порівняно з DSS - додає формальні Data Gate і Model Gate; порівняно з SupTech - вводить універсальний Decision Gate та збереження explanation snapshot; порівняно з AI-governance - включає статистичний vintage, семантичну узгодженість і рольове перетворення сигналу на рішення [1; 5-17]. Така постановка змінює критерій якості IAC: система є корисною не тому, що містить більше моделей або графіків, а тому, що дає змогу встановити, які дані та версії були доступні, яка модель сформувала сигнал, який її валідаційний статус, чому було запропоновано певну дію і хто прийняв остаточне рішення.

Versioning і statistical vintage мають окреме значення для ex post оцінювання. Якщо після рішення статистичний ряд або методологію переглянуто, повторний розрахунок за новою версією не повинен підміняти інформацію, фактично доступну в момент рішення. Тому архітектура розрізняє поточний перерахований стан та історичний evidence snapshot. Це створює умови для коректної оцінки якості управління і для навчання системи на наслідках попередніх рішень.

Fail-safe analytics є сильнішою вимогою, ніж безумовна технічна безперервність. У високоризиковому середовищі безпечніше тимчасово зупинити або обмежити використання аналітичного продукту, ніж непомітно підставити stale data, кешований прогноз або модель із простроченою валідацією. Для недоступного модельного сервісу доцільним є degraded mode: відображення останнього валідованого стану з явним попередженням про прострочення та блокування нового автоматизованого висновку.

Human-in-the-loop не є обмеженням автоматизації. Автоматизація скорочує час виявлення, стандартизує перевірки, прискорює сценарний аналіз та формує пояснювальний пакет; відповідальність за високоризиковий управлінський вплив залишається людською та

інституційною. Саме decision log перетворює цю взаємодію на об'єкт подальшого аналізу: можна оцінювати частоту override, якість рекомендацій, причини відхилення і наслідки рішень.

Таблиця 5.

Результати емпіричної та негативної перевірки Data Gate

Контроль	**Правило**	**Фактичний результат**	**Статус**	**Негативний контроль**
Completeness	$C_t = 1$	Mean = 1; min = 1	PASS, 84/84	Пропуск critical field -> STOP
Reconciliation	$\varepsilon_t <= 10^{-8}$	max $\varepsilon \approx 2{,}22\times10^{-16}$	PASS, 84/84	Навмисне порушення -> CHECK
Unique key	Відсутність дубльованого ключа	У базовому пакеті порушення не зафіксовано	Придатний пакет	Synthetic duplicate: спрацювання розширеного gate
Source freshness	Джерело актуальне для заданого зрізу	Базовий пакет сформовано на узгодженому зрізі	Придатний пакет	Synthetic stale source: маркування/блокування
Version validity	Версія відома та узгоджена з lineage	Базовий пакет має визначену версійну залежність	Придатний пакет	Synthetic unknown version: маркування/блокування

Джерело: розраховано автором за контрольним інформаційним пакетом; негативні сценарії є синтетичними тестами логіки шлюзу.

Практична реалізація може здійснюватися поетапно. Research prototype забезпечує контрольоване сховище, source map, формули перевірки та ручний запуск модулів. Institutional pilot додає централізований каталог, автоматизоване надходження даних, model registry, role-based access і журнал сигналів. Production decision-support доповнює відмовостійкість, SLA, резервування, інтеграцію з внутрішніми системами та workflow погодження. Конкретний технологічний стек не є складовою наукової новизни і може змінюватися без порушення архітектурних правил.

Обмеження дослідження пов'язані з тим, що запропонована конструкція є референтною, а не готовою production platform. Апробація на 84 спостереженнях перевіряє контрольну логіку Data Gate, але не продуктивність, доступність чи стійкість повномасштабної системи. Конкретні SLA, security controls, escalation thresholds та юридичні режими доступу мають визначатися інституційно. Model Gate також потребуватиме різних метрик для різних класів розгорнутих моделей.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У результаті дослідження розроблено та концептуально-емпірично перевірено референтну архітектуру інформаційно-аналітичної системи підтримки адаптивного управління банківською системою. Запропонована архітектура формує цілісний доказовий контур, у якому послідовно поєднано отримання і версіювання даних, контроль їх якості, семантичну узгодженість, використання аналітичних і модельних сервісів, формування керованого сигналу, його пояснення, погодження управлінського рішення та подальший зворотний зв’язок. Це дозволяє перейти від фрагментарного використання окремих джерел даних і моделей до керованої системи, у якій кожний аналітичний результат має відтворюване походження, визначений статус придатності та зафіксований зв’язок із прийнятим рішенням.

Науковий результат полягає у формалізації шестирівневої функціональної архітектури, доповненої чотирма наскрізними контурами управління і контролю та трьома контрольними шлюзами Data Gate, Model Gate і Decision Gate. Їх поєднання забезпечує безперервність доказового ланцюга, версійність і lineage, контроль придатності даних і моделей, пояснюваність результатів, рольову відповідальність та принцип human-in-the-loop. Важливо, що автоматизований сигнал у запропонованій IAC не ототожнюється з управлінським рішенням: система формує доказову основу, визначає статус, причину та маршрут ескалації, тоді як остаточне рішення залишається за уповноваженим користувачем.

Емпірична апробація мінімального Data Gate на контрольному пакеті з 84 місячних спостережень IAR та п’яти функціональних компонентів за 2019M01–2025M12 підтвердила працездатність базової логіки контролю якості та версійної узгодженості. Середній і мінімальний коефіцієнти повноти дорівнюють 1, максимальна похибка математичного узгодження становить приблизно 2,22×10−162{,}22\times10^{-16}, усі записи отримали статус PASS. Окремі синтетичні негативні сценарії продемонстрували спроможність архітектури ідентифікувати пропуски,

порушення reconciliation, дублювання, прострочення джерел і невідомі версії та переводити відповідні пакети у режими CHECK або STOP. Водночас така перевірка характеризує саме контрольну логіку Data Gate і не підміняє повномасштабної операційної валідації всієї IAC.

Практичне значення запропонованої архітектури полягає у зменшенні інформаційного та модельного ризику, підвищенні відтворюваності аналітичних висновків і створенні умов для підзвітного адаптивного управління в умовах різночастотних даних, зміни моделей та цифрово-операційної невизначеності. Платформонезалежність архітектури дає змогу реалізовувати її поетапно — від дослідницького прототипу до інституційної системи підтримки рішень — без зміни базових правил доказовості, контролю та відповідальності. Подальші дослідження доцільно спрямувати на повномасштабну апробацію Model Gate і Decision Gate, кількісне тестування SLA та операційної стійкості, формалізацію метрик якості зворотного зв'язку й пілотне впровадження архітектури в інституційному середовищі.

ЛІТЕРАТУРА:

1. Basel Committee on Banking Supervision. (2013). *Principles for effective risk data aggregation and risk reporting (BCBS 239)*. Bank for International Settlements. URL: https://www.bis.org/publ/bcbs239.htm
2. Basel Committee on Banking Supervision. (2026, January 6). *Implementation of the principles for effective risk data aggregation and risk reporting (BCBS 239 principles)*. BCBS Newsletter. Bank for International Settlements. URL: https://www.bis.org/publ/bcbs_nl36.htm
3. Basel Committee on Banking Supervision. (2021). *Principles for operational resilience*. Bank for International Settlements. URL: https://www.bis.org/bcbs/publ/d516.htm
4. European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector. *Official Journal of the European Union, L 333*, 1-79. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj
5. Tabassi, E. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1
6. Rao, A., Keller, A., Kalra, N., Steed, R., Kwegyir-Aggrey, K., Klyman, K., Staheli, D., & Bergman, A. (2026). *Challenges to the monitoring of deployed AI systems (NIST AI 800-4)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.800-4
7. Power, D. J., & Sharda, R. (2007). Model-driven decision support systems: Concepts and research directions. *Decision Support Systems, 43*(3), 1044-1061. https://doi.org/10.1016/j.dss.2005.05.030
8. Zopounidis, C., Doumpos, M., & Niklis, D. (2018). Financial decision support: An overview of developments and recent trends. *EURO Journal on Decision Processes, 6*(1-2), 63-76. https://doi.org/10.1007/s40070-018-0078-3
9. Broeders, D., & Prenio, J. (2018). *Innovative technology in financial supervision (SupTech): The experience of early users (FSI Insights No. 9)*. Bank for International Settlements. URL: https://www.bis.org/fsi/publ/insights9.htm
10. Національний банк України. (n.d.). *Впровадження SupTech та RegTech*. URL: https://bank.gov.ua/ua/supervision/suptech-regtech
11. Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: A systematic literature review. *AI and Ethics, 5*, 3265-3279. https://doi.org/10.1007/s43681-024-00653-w
12. Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 33-44. https://doi.org/10.1145/3351095.3372873
13. Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75-105. https://doi.org/10.2307/25148625
14. Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302
15. Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly, 37*(2), 337-355. https://doi.org/10.25300/MISQ/2013/37.2.01
16. Černevičienė, J., & Kabašinskas, A. (2024). Explainable artificial intelligence (XAI) in finance: A systematic literature review. *Artificial Intelligence Review, 57*, 216. https://doi.org/10.1007/s10462-024-10854-8

17. European Central Bank Banking Supervision. (2023, May 17). *Digital transformation requires strong governance and steering*. Supervision Newsletter. URL: https://www.bankingsupervision.europa.eu/press/supervisory-newsletters/newsletter/2023/html/ssm.nl230517_3.en.html

18. Національний банк України. (n.d.). *Грошово-кредитна та фінансова статистика: показники фінансової стійкості*. URL: https://bank.gov.ua/ua/statistic/sector-financial

19. Національний банк України. (n.d.). *Наглядова статистика*. URL: https://bank.gov.ua/ua/statistic/supervision-statist

20. Національний банк України. (n.d.). *API для розробників*. URL: https://bank.gov.ua/ua/open-data/api-dev

REFERENCES:

1. Basel Committee on Banking Supervision. (2013). *Principles for effective risk data aggregation and risk reporting (BCBS 239)*. Bank for International Settlements. https://www.bis.org/publ/bcbs239.htm

2. Basel Committee on Banking Supervision. (2026, January 6). *Implementation of the principles for effective risk data aggregation and risk reporting (BCBS 239 principles)*. BCBS Newsletter. Bank for International Settlements. https://www.bis.org/publ/bcbs_nl36.htm

3. Basel Committee on Banking Supervision. (2021). *Principles for operational resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.htm

4. European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector. *Official Journal of the European Union, L 333*, 1–79. https://eur-lex.europa.eu/eli/reg/2022/2554/oj

5. Tabassi, E. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1

6. Rao, A., Keller, A., Kalra, N., Steed, R., Kwegyir-Aggrey, K., Klyman, K., Staheli, D., & Bergman, A. (2026). *Challenges to the monitoring of deployed AI systems (NIST AI 800-4)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.800-4

7. Power, D. J., & Sharda, R. (2007). Model-driven decision support systems: Concepts and research directions. *Decision Support Systems, 43*(3), 1044–1061. https://doi.org/10.1016/j.dss.2005.05.030

8. Zopounidis, C., Doumpos, M., & Niklis, D. (2018). Financial decision support: An overview of developments and recent trends. *EURO Journal on Decision Processes, 6*(1–2), 63–76. https://doi.org/10.1007/s40070-018-0078-3

9. Broeders, D., & Prenio, J. (2018). *Innovative technology in financial supervision (SupTech): The experience of early users (FSI Insights No. 9)*. Bank for International Settlements. https://www.bis.org/fsi/publ/insights9.htm

10. National Bank of Ukraine. (n.d.). *Vprovadzhennia SupTech ta RegTech* [Implementation of SupTech and RegTech]. https://bank.gov.ua/ua/supervision/suptech-regtech [in Ukrainian].

11. Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: A systematic literature review. *AI and Ethics, 5*, 3265–3279. https://doi.org/10.1007/s43681-024-00653-w

12. Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 33–44. https://doi.org/10.1145/3351095.3372873

13. Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105. https://doi.org/10.2307/25148625

14. Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

15. Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly, 37*(2), 337–355. https://doi.org/10.25300/MISQ/2013/37.2.01

16. Černevičienė, J., & Kabašinskas, A. (2024). Explainable artificial intelligence (XAI) in finance: A systematic literature review. *Artificial Intelligence Review, 57*, 216. https://doi.org/10.1007/s10462-024-10854-8

17. European Central Bank Banking Supervision. (2023, May 17). *Digital transformation requires strong governance and steering*. Supervision Newsletter. https://www.bankingsupervision.europa.eu/press/supervisory-newsletters/newsletter/2023/html/ssm.nl230517_3.en.html

18. National Bank of Ukraine. (n.d.). *Hroshovo-kredytna ta finansova statystyka: pokaznyky finansovoi stiikosti* [Monetary and financial statistics: Financial stability indicators]. https://bank.gov.ua/ua/statistic/sector-financial [in Ukrainian].

19. National Bank of Ukraine. (n.d.). *Nahliadova statystyka* [Supervisory statistics]. https://bank.gov.ua/ua/statistic/supervision-statist [in Ukrainian].

20. National Bank of Ukraine. (n.d.). *API dlia rozrobnykiv* [API for developers]. https://bank.gov.ua/ua/open-data/api-dev [in Ukrainian].

ARCHITECTURE OF AN INFORMATION-ANALYTICAL SYSTEM FOR ADAPTIVE BANKING SYSTEM MANAGEMENT

HRABARIEV Andrii
Kyiv National Economic University named after Vadym Hetman

Fragmentation of information sources, analytical models, and visualization tools complicates reproduction of the evidence underlying a managerial decision and increases the risk of using asynchronous data, outdated models, or opaque analytical signals. The study aims to develop a

reference architecture of an information-analytical system for adaptive banking system management in which the path from a data source to a decision is organized as a governed evidence cycle. A six-layer functional architecture is proposed, complemented by four cross-cutting governance domains and three control gates: Data Gate, Model Gate, and Decision Gate. The functional layers cover acquisition and metadata, integration and data quality, a semantic and feature layer, an analytical and model layer, decision orchestration, and presentation and interaction. The scientific contribution consists in formalizing evidence continuity along the chain "source – data – transformation – model – signal – explanation – decision – outcome – feedback", with versioning, lineage, explainability by design, fail-safe analytics, and mandatory human-in-the-loop control. The minimum data-quality gate is empirically verified on 84 monthly observations of the integral index of adaptive development of the banking system (IAR) and five functional components for 2019M01-2025M12. The mean and minimum completeness coefficients equal 1, the maximum reconciliation error is approximately 2.22×10-16, and all records receive PASS status. Synthetic negative-control scenarios are treated separately to test CHECK/STOP responses. The architecture is platform-independent and supports reproducible, accountable, governed, and auditable analytical decision support across heterogeneous information sources and model services. Its practical value lies in reducing information and model risk without equating an automated signal with an automated managerial decision.

Keywords: adaptive management; banking system; information-analytical system; data governance; model governance; evidence continuity; human-in-the-loop; SupTech.