

УДК 005.35:004.9:336.71(477)
DOI: 10.31732/2663-2209-2026-83-256-265

Дата надходження: 18.08.2026
Дата прийняття до друку: 21.09.2026
Дата публікації: 30.09.2026



Ця робота ліцензується відповідно до [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/)

КОМУНІКАЦІЙНІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В СИСТЕМІ КОРПОРАТИВНОГО УПРАВЛІННЯ БАНКІВСЬКИХ УСТАНОВ УКРАЇНИ

Анна Пазєєва¹

¹Канд. екон. наук, доцент кафедри управлінських технологій Університету «КРОК», Київ, Україна, e-mail: PazeevaA@krok.edu.ua, ORCID: <https://orcid.org/0000-0002-6557-6890>

COMMUNICATION AND INFORMATION TECHNOLOGIES IN THE CORPORATE GOVERNANCE SYSTEM OF UKRAINIAN BANKING INSTITUTIONS

Anna Pazeieva¹

¹PhD in Economics, Associate Professor of the Department of Managerial Technologies, «KROK» University, Kyiv, Ukraine, e-mail: PazeevaA@krok.edu.ua, ORCID: <https://orcid.org/0000-0002-6557-6890>

Анотація. Цифрова трансформація банківського сектору змінює не лише технології надання фінансових послуг, а й механізми корпоративного управління, оскільки якість управлінських рішень дедалі більше залежить від своєчасності інформації, захищеності корпоративних комунікацій, доступності аналітичних даних та цифрової операційної стійкості банку. Метою дослідження є розвиток теоретико-методичних засад використання комунікаційних та інформаційних технологій у корпоративному управлінні банківських установ України та формування структурно-функціональної моделі їх інтеграції в управлінські процеси. Об'єктом дослідження є інформаційно-комунікаційне забезпечення корпоративного управління банківськими установами. Методологічну основу становлять системний і структурно-функціональний підходи, методи аналізу та синтезу, порівняння, систематизації, контент-аналізу нормативно-правових документів та міжнародних стандартів корпоративного й IT-управління. Обґрунтовано необхідність переходу від розуміння цифрових технологій як операційного інструменту банку до їх трактування як складової корпоративного управління. Запропоновано трирівневу модель інформаційно-комунікаційного забезпечення, що включає комунікаційний, інформаційно-аналітичний та контрольний-безпековий рівні. Систематизовано технології за п'ятьма функціональними напрямками: підтримка управлінських рішень; корпоративна комунікація; управління ризиками та внутрішній контроль; розкриття інформації й регуляторна взаємодія; цифрова операційна стійкість. Визначено шість критеріїв оцінювання ефективності такого забезпечення: своєчасність, повнота, достовірність, простежуваність, захищеність та стійкість інформаційних потоків. Практичне значення отриманих результатів полягає у можливості використання запропонованої моделі радами та правліннями банків для формування політики цифрового корпоративного управління, удосконалення систем внутрішнього контролю та підвищення якості управлінських рішень.

Ключові слова: корпоративне управління, банківська установа, інформаційні технології, комунікаційні технології, цифровізація, IT governance, інформаційна безпека, цифрова операційна стійкість, управління ризиками.

Формул: 0; рис.: 0; табл.: 3; бібл.: 17.

Abstract. Digital transformation of the banking sector is changing not only the technologies used to provide financial services but also corporate governance mechanisms, as the quality of managerial decisions increasingly depends on timely information, secure corporate communications, availability of analytical data, and banks' digital operational resilience. The study aims to develop theoretical and methodological foundations for using communication and information technologies in the corporate governance of Ukrainian banking institutions and to construct a structural-functional model for their integration into governance processes. The object of the study is the information and communication support of corporate governance in banking institutions. The methodological framework combines systemic and structural-functional approaches with analysis and synthesis, comparison, systematisation, and content analysis of regulatory documents and international corporate and IT governance standards. The study substantiates the transition from considering digital technologies primarily as operational banking tools towards recognising them as an integral component of corporate governance. A three-level model of information and communication support is proposed, comprising communication, information-analytical, and control-security levels. Technologies are systematised across five functional areas: management decision support; corporate communication; risk management and internal control;

disclosure and regulatory interaction; and digital operational resilience. Six criteria for assessing the effectiveness of information and communication support are identified: timeliness, completeness, reliability, traceability, security, and resilience of information flows. The proposed approach integrates IT governance into the overall corporate governance architecture and clarifies the responsibilities of the supervisory board, management board, risk management, compliance, internal audit, and IT functions. The practical significance of the findings lies in the possibility of applying the proposed model by supervisory and management boards of Ukrainian banks when developing digital governance policies, improving internal control systems, managing ICT-related risks, and increasing the quality and transparency of corporate decision-making.

Keywords: corporate governance, banking institution, information technology, communication technology, digitalisation, IT governance, information security, digital operational resilience, risk management.

Formulas: 0; **fig.:** 0; **tab.:** 3; **bibl.:** 17.

Вступ. Цифрова трансформація банківського сектору протягом останніх років набула системного характеру. Інформаційні технології вже не виконують виключно допоміжну функцію, пов'язану з автоматизацією банківських операцій, дистанційним обслуговуванням клієнтів або обробленням значних масивів фінансових даних. Вони дедалі більше визначають способи формування, передачі та аналізу управлінської інформації, характер взаємодії між органами корпоративного управління, ефективність систем ризик-менеджменту та внутрішнього контролю, а також здатність банку підтримувати безперервність діяльності в умовах зовнішніх шоків.

Для банківських установ ця трансформація має особливе значення. На відміну від більшості нефінансових компаній, банки функціонують в умовах високої регуляторної інтенсивності, значної інформаційної асиметрії, системних ризиків та підвищених вимог до захисту інформації. Тому цифровізація корпоративного управління в банку не може обмежуватися електронним документообігом або використанням сучасних засобів комунікації. Вона має охоплювати весь інформаційний цикл управлінського рішення, починаючи від отримання та верифікації даних і завершуючи їх аналізом, передачею органам управління, документуванням рішення та подальшим контролем його виконання.

Міжнародні стандарти корпоративного управління також дедалі чіткіше пов'язують відповідальність ради компанії з управлінням цифровими

ризиками. G20/OECD Principles of Corporate Governance наголошують на необхідності використання цифрових технологій у корпоративному управлінні та одночасного контролю пов'язаних із ними ризиків. До обов'язків ради віднесено нагляд за системами управління ризиками, включаючи цифрову безпеку, захист даних та інформаційні процеси (OECD, 2023). У банківській сфері такий підхід посилюється принципами Basel Committee on Banking Supervision, відповідно до яких ефективне корпоративне управління має забезпечувати якісне управління ризиками, функціонування незалежних контрольних функцій та доступ органів управління до релевантної інформації (BCBS, 2015).

В Україні значення інформаційно-комунікаційного компонента корпоративного управління додатково посилюється необхідністю забезпечення безперервності роботи банківської системи в умовах воєнних загроз, кібератак, фізичного пошкодження інфраструктури, територіальної розосередженості персоналу та прискореної інтеграції українського фінансового сектору до нормативного середовища Європейського Союзу. Впровадження відкритого банкінгу, регулювання хмарних технологій, удосконалення вимог до інформаційної безпеки та кіберзахисту суттєво розширюють відповідальність органів корпоративного управління за технологічні рішення банку.

За цих умов виникає необхідність системного визначення ролі комунікаційних та інформаційних технологій у корпоративному управлінні банківських установ та формування моделі,

яка поєднувала б цифрові інструменти з функціями ради банку, правління, ризик-менеджменту, комплаєнсу, внутрішнього аудиту та інших суб'єктів корпоративного управління.

Аналіз останніх досліджень. Теоретичні основи корпоративного управління традиційно формувалися навколо проблем розподілу повноважень між власниками, радою директорів і виконавчим менеджментом, забезпечення підзвітності, контролю та захисту інтересів стейкхолдерів. У банківській сфері до цих завдань додається необхідність забезпечення фінансової стабільності, ефективного управління ризиками та захисту інтересів вкладників.

У попередньому дослідженні А. Пуша, І. Мігус та Н. Наконечної було систематизовано основні цілі, принципи, функції та суб'єкти корпоративного управління банківськими установами. Серед функціональних напрямів корпоративного управління авторами було виокремлено, зокрема, комунікацію, контроль, управління ризиками, стратегічне планування та інноваційний розвиток (Пуш та ін., 2024). Водночас подальша цифровізація банківської діяльності потребує окремого дослідження технологічної інфраструктури реалізації цих функцій.

Концепція IT governance сформувалася як відповідь на зростання стратегічної ролі інформаційних технологій в організаціях. У сучасному трактуванні IT governance не зводиться до технічного управління IT-підрозділом, а передбачає визначення повноважень, відповідальності та механізмів прийняття рішень щодо використання інформаційних технологій на рівні організації. Weill and Ross (2004) пов'язують ефективність IT governance з чітким розподілом прав прийняття рішень та відповідальністю за використання IT-ресурсів.

De Haes and Van Grembergen (2009) розглядають IT governance як складову корпоративного управління, яка забезпечує стратегічну відповідність бізнесу й

інформаційних технологій, створення вартості та контроль технологічних ризиків. Подальші дослідження підтверджують посилення ролі ради директорів у цьому процесі. Caluwe and De Haes (2019) виявили, що цифрова трансформація підвищує значення участі ради в управлінні цифровими активами та IT-ризиками. У новішому дослідженні Caluwe et al. (2024) доведено необхідність інтегрувати IT governance безпосередньо в корпоративне управління, а не залишати відповідні питання виключно в компетенції IT-підрозділів або спеціалізованих комітетів.

Для банків ця проблема має особливий характер, оскільки інформаційні технології одночасно виступають ресурсом, каналом комунікації, основою бізнес-процесів і джерелом операційного ризику. Принципи Basel Committee on Banking Supervision наголошують на відповідальності ради за стратегію банку, систему управління ризиками та контрольні функції (BCBS, 2015). Принципи операційної стійкості додатково вимагають формування здатності банку підтримувати критичні операції під час технологічних відмов, кіберінцидентів та інших деструктивних подій (BCBS, 2021).

Подібна логіка покладена в основу європейського Регламенту DORA. Його принципове значення для корпоративного управління полягає в закріпленні відповідальності органу управління фінансової установи за систему управління ІСТ-ризиком, затвердження стратегії цифрової операційної стійкості, визначення відповідальності за IT-функції та забезпечення інформаційної взаємодії між ними (European Parliament & Council of the European Union, 2022).

В українському нормативному середовищі відповідні елементи формуються через Положення про організацію системи управління ризиками в банках України та банківських групах, Положення про організацію системи внутрішнього контролю, нормативні вимоги з інформаційної безпеки й

кіберзахисту, а з 2025 року також через регулювання відкритого банкінгу та використання технології хмарних обчислень (Національний банк України, 2018, 2019, 2021, 2025a, 2025b, 2025c).

Отже, наукові та нормативні джерела підтверджують тенденцію до зближення корпоративного управління та IT governance. Водночас недостатньо дослідженням залишається питання систематизації комунікаційних та інформаційних технологій саме відповідно до функцій і суб'єктів корпоративного управління банківської установи. Це створює методологічний розрив між дослідженнями цифровізації банківських послуг та дослідженнями корпоративного управління, що визначає необхідність подальшого наукового опрацювання проблеми.

Постановка завдання. Метою дослідження є розвиток теоретико-методичних засад використання комунікаційних та інформаційних технологій у корпоративному управлінні банківських установ України шляхом формування структурно-функціональної моделі їх інтеграції в управлінські процеси.

Для досягнення поставленої мети необхідно уточнити місце інформаційних та комунікаційних технологій у системі корпоративного управління банком; систематизувати технологічні інструменти відповідно до функцій та суб'єктів корпоративного управління; визначити взаємозв'язок між цифровізацією управління та технологічними ризиками; сформулювати критерії оцінювання ефективності інформаційно-комунікаційного забезпечення корпоративного управління.

Методологічною основою дослідження є системний та структурно-функціональний підходи. Системний підхід дає змогу розглядати корпоративне управління як сукупність взаємопов'язаних суб'єктів, процесів, інформаційних потоків та механізмів контролю. Структурно-функціональний підхід використано для встановлення відповідності між окремими

групами цифрових технологій і функціями корпоративного управління.

Застосовано методи аналізу і синтезу для узагальнення наукових підходів до corporate governance та IT governance, порівняльний аналіз для зіставлення українських регуляторних вимог із міжнародними підходами, контент-аналіз нормативно-правових документів, а також систематизацію та класифікацію для побудови авторської моделі інформаційно-комунікаційного забезпечення корпоративного управління.

Інформаційну базу дослідження сформовано з міжнародних стандартів OECD, Basel Committee on Banking Supervision, European Banking Authority, законодавства Європейського Союзу, нормативно-правових актів Національного банку України та сучасних академічних публікацій з корпоративного та IT-управління.

Результати дослідження. Цифровізація банківського сектору традиційно аналізується переважно через призму розвитку дистанційного банкінгу, мобільних застосунків, автоматизації платежів, використання Big Data, штучного інтелекту та фінансових технологій. Проте такий підхід характеризує насамперед цифрову трансформацію банківських продуктів і операцій, а не корпоративного управління.

Корпоративне управління створює інший технологічний запит. Його ключовим ресурсом є достовірна інформація, доступна відповідним органам та посадовим особам у час, достатній для прийняття обґрунтованого рішення. Тому інформаційні технології у корпоративному управлінні виконують передусім функції збору, оброблення, верифікації, інтеграції, аналізу, збереження та представлення даних. Комунікаційні технології забезпечують передачу цієї інформації, взаємодію між учасниками корпоративного управління, колективне обговорення рішень, документування позицій та передачу управлінських сигналів.

На цій основі пропонуємо розмежовувати інформаційні технології корпоративного управління як цифрові засоби формування, оброблення, аналізу, зберігання та контролю управлінської інформації та комунікаційні технології корпоративного управління як цифрові засоби забезпечення захищеного

інформаційного обміну та взаємодії між органами управління, контрольними функціями та стейкхолдерами банку.

Водночас практично ці дві групи технологій формують єдину інформаційно-комунікаційну інфраструктуру. Її значення для окремих суб'єктів корпоративного управління представлено у таблиці 1.

Таблиця 1

Інформаційно-комунікаційне забезпечення основних суб'єктів корпоративного управління банку

Суб'єкт корпоративного управління	Інформаційна потреба	Основні технологічні інструменти	Управлінський результат
Акціонери та загальні збори	Інформація про результати діяльності, структуру власності, суттєві корпоративні рішення	електронні корпоративні портали, цифрове розкриття інформації, електронне голосування, захищений документообіг	реалізація корпоративних прав, прозорість і підзвітність
Рада банку та її комітети	Стратегічна, фінансова, ризикова та нефінансова інформація	board portals, BI-панелі, системи управлінської звітності, захищені відеоконференції, електронний документообіг	стратегічне керівництво, моніторинг правління та ризиків
Правління	Операційна й аналітична інформація у режимі, наближеному до реального часу	MIS, DSS, ERP, BI, сховища даних, корпоративні комунікаційні платформи	оперативне управління та реалізація стратегії
Ризик-менеджмент і комплаєнс	Дані про ризикові позиції, транзакції, ліміти, порушення, санкції	GRC-системи, risk dashboards, AML/KYC-системи, data analytics, автоматизований моніторинг	раннє виявлення ризиків та контроль відповідності
Внутрішній аудит	Дані про бізнес-процеси, контрольні процедури та цифрові сліди	audit management systems, process mining, data analytics, електронні журнали подій	незалежна оцінка системи внутрішнього контролю
Регулятор та інші стейкхолдери	Регуляторна, фінансова та нефінансова звітність	RegTech, API, системи автоматизованої звітності, захищені канали обміну	регуляторна відповідність і зовнішня прозорість

Джерело: розроблено авторами на основі BCBS (2015), OECD (2023), Caluwe et al. (2024)

Таблиця 1 демонструє, що одна й та сама технологічна система може одночасно обслуговувати кілька ланок корпоративного управління. Наприклад, інтегроване сховище даних може використовуватися правлінням для операційного управління, радою для стратегічного моніторингу, ризик-менеджментом для оцінювання ризиків, а внутрішнім аудитом для незалежної перевірки. Тому ключовим питанням стає не кількість цифрових систем, а якість їх інтеграції та відповідність правам доступу,

функціональним повноваженням і відповідальності користувачів.

Особливого значення набувають технології підтримки роботи ради банку. Дослідження Caluwe et al. (2024) показує, що в умовах цифровізації управління інформаційними технологіями не може залишатися делегованим виключно виконавчому менеджменту та ІТ-підрозділам. Рада має розуміти стратегічне значення технологічних активів, контролювати пов'язані з ними ризики та

володіти достатньою колективною цифровою компетентністю.

Для українських банків ця теза отримує регуляторне підкріплення. Підхід НБУ до наглядової оцінки корпоративного управління передбачає аналіз ефективності систем управління ризиками і внутрішнього контролю, а також функціонування інформаційних систем, необхідних для контролю реалізації стратегії банку. Таким чином, якість ІТ-

архітектури фактично стає одним із факторів оцінювання загальної життєздатності та керованості банку.

Розвиток нормативного середовища України протягом 2025–2026 років особливо чітко демонструє перехід від технологій як операційної категорії до технологій як об'єкта корпоративного управління. Основні напрями цієї трансформації наведено у таблиці 2.

Таблиця 2

Регуляторні напрями цифрової трансформації та їх вплив на корпоративне управління банків

Регуляторний напрям	Технологічний компонент	Наслідки для корпоративного управління
Управління банківськими ризиками	інтегровані інформаційні системи, ризикові бази даних, аналітичні панелі	необхідність своєчасного забезпечення ради та правління інформацією про ризики
Внутрішній контроль	цифрове документування процедур, журнали подій, автоматизовані контрольні механізми	підвищення простежуваності рішень та відповідальності
Інформаційна безпека і кіберзахист	SOC, SIEM, системи керування доступом, моніторинг кіберінцидентів	включення ICT-ризиків до загальної системи управління ризиками
Відкритий банкінг	API, електронна ідентифікація, управління згодами, обмін даними у режимі реального часу	розширення зовнішнього цифрового контуру банку та відповідальності за третіх осіб
Хмарні технології	cloud computing, віддалене зберігання й оброблення даних	посилення управління аутсорсинговим та third-party ICT risk
SREP та пруденційний нагляд	інтегровані управлінські інформаційні системи	оцінювання здатності інформаційної інфраструктури підтримувати стратегію, ризик-менеджмент і внутрішній контроль

Джерело: систематизовано авторами на основі нормативно-правових актів Національного банку України (2018, 2019, 2021, 2025a, 2025b, 2025c, 2026)

Особливої уваги потребує відкритий банкінг. Його впровадження змінює традиційну архітектуру інформаційного середовища банку, оскільки частина інформаційної взаємодії здійснюється через стандартизовані API із зовнішніми постачальниками послуг. Це створює додаткову управлінську площину, що охоплює питання авторизації доступу, захисту даних, ідентифікації контрагентів, управління згодою клієнтів, відповідальності третіх сторін і безперервності технологічної взаємодії.

Аналогічний управлінський ефект має використання хмарних технологій. Положення НБУ № 99 від 25 серпня 2025

року регламентує використання хмарних послуг банками та іншими учасниками фінансового ринку, включаючи вимоги до управління ризиками, договірних відносин із постачальниками та інформування регулятора. Внаслідок цього рішення про перенесення певних інформаційних ресурсів до хмарної інфраструктури не може розглядатися лише як технічне рішення ІТ-департаменту. Воно має враховувати ризик-апетит банку, критичність процесів, концентраційний ризик, можливість виходу з відносин із постачальником, захист даних та забезпечення безперервності діяльності.

З урахуванням визначених тенденцій пропонуємо структурно-функціональну модель інформаційно-комунікаційного забезпечення корпоративного управління банківської установи, що складається з трьох взаємопов'язаних рівнів.

Перший рівень, комунікаційний, забезпечує захищену взаємодію між акціонерами, радою банку, правлінням, комітетами, контрольними функціями, регулятором та іншими стейкхолдерами. До нього належать корпоративні портали, системи електронного документообігу, захищені платформи відеоконференцій, електронне голосування, корпоративні месенджери та канали регуляторної взаємодії.

Другий рівень, інформаційно-аналітичний, забезпечує формування інформаційної основи управлінського рішення. Він включає системи управлінської інформації, Business Intelligence, Decision Support Systems, інтегровані сховища даних, аналітичні платформи, інструменти сценарного моделювання, ризикові панелі та технології аналізу значних масивів даних.

Третій рівень, контрольнo-безпековий, забезпечує достовірність, захищеність, простежуваність і стійкість інформаційного середовища. До нього належать GRC-платформи, автоматизовані системи внутрішнього контролю, SIEM і SOC, управління ідентифікацією та доступом, моніторинг кіберінцидентів, системи резервування та відновлення, а також засоби управління технологічними ризиками третіх сторін.

Принциповою ознакою запропонованої моделі є те, що зазначені рівні не функціонують автономно. Управлінське рішення має пройти повний цифровий цикл: дані → аналітична інформація → комунікація → рішення → документування → виконання → контроль → зворотний інформаційний зв'язок. Порушення будь-якої ланки цього циклу знижує якість корпоративного управління незалежно від технологічної розвиненості інших компонентів.

На основі проведеної систематизації доцільно виділити п'ять функціональних напрямів використання інформаційно-комунікаційних технологій у корпоративному управлінні банку: підтримку управлінських рішень; корпоративну комунікацію; управління ризиками та внутрішній контроль; розкриття інформації та регуляторну взаємодію; забезпечення цифрової операційної стійкості.

Водночас сам факт упровадження відповідних технологій не означає підвищення ефективності корпоративного управління. Надмірна автоматизація може створювати інформаційне перевантаження, технологічну залежність, концентрацію ризиків у постачальників ІТ-послуг, непрозорість алгоритмічних рішень та нові можливості несанкціонованого доступу. Тому оцінювання цифрової зрілості корпоративного управління має базуватися не на кількості використаних технологічних продуктів, а на характеристиках інформації й інформаційних потоків.

Пропонуємо використовувати шість базових критеріїв такого оцінювання, представлених у таблиці 3.

Запропоновані критерії утворюють основу для подальшої розробки інтегрального індексу цифрової зрілості корпоративного управління банківських установ. Такий підхід дає змогу змістити фокус із формального контролю наявності цифрових систем на оцінювання їх реального внеску в якість управління.

При цьому важливо розмежовувати цифровізацію менеджменту та цифровізацію корпоративного управління. Перша спрямована передусім на підвищення ефективності бізнес-процесів і операційної діяльності. Друга має забезпечувати інформаційні потреби органів корпоративного управління, прозорість процесів прийняття рішень, незалежність контрольних функцій, підзвітність менеджменту, управління конфліктами інтересів та контроль системних ризиків.

Таблиця 3

Критерії ефективності інформаційно-комунікаційного забезпечення корпоративного управління банку

Критерій	Зміст	Приклад управлінського індикатора
Своєчасність	надходження інформації до моменту прийняття рішення	частка звітів, наданих органам управління у встановлені строки
Повнота	охоплення суттєвих фінансових і нефінансових факторів	частка ключових ризиків, інтегрованих у управлінську звітність
Достовірність	точність і верифікованість даних	кількість істотних коригувань управлінської інформації
Простежуваність	можливість встановлення джерела даних, автора та історії рішення	частка управлінських рішень з повним цифровим audit trail
Захищеність	конфіденційність, цілісність та контроль доступу	кількість суттєвих інцидентів несанкціонованого доступу
Стійкість	здатність підтримувати інформаційні та комунікаційні процеси під час збоїв	фактичний час відновлення критичних управлінських систем

Джерело: розроблено автором

Звідси випливає принципова зміна ролі ради банку. В умовах цифрового банкінгу рада не повинна здійснювати оперативне керівництво інформаційними технологіями, однак вона має визначати стратегічні засади їх використання, контролювати відповідність ІТ-стратегії загальній стратегії банку, затверджувати прийнятний рівень ІСТ-ризиків, отримувати регулярну інформацію про суттєві технологічні інциденти та контролювати цифрову операційну стійкість.

Для практичного впровадження такого підходу доцільним є формування в банку *політики цифрового корпоративного управління*, яка має узгоджувати корпоративну стратегію, ІТ strategy, risk appetite, політики інформаційної безпеки, data governance, використання хмарних послуг та управління зовнішніми технологічними постачальниками. При цьому не обов'язково створювати додаткові органи управління. Цифрові питання можуть бути інтегровані у роботу чинних комітетів ради, якщо забезпечено достатній рівень цифрової компетентності їх членів.

Наукова новизна запропонованого підходу полягає в інтеграції інформаційно-комунікаційного та корпоративного контурів управління банком. На відміну від підходів, у яких інформаційні технології розглядаються переважно як інструмент автоматизації банківських операцій, запропонована модель трактує їх як

інфраструктуру корпоративного управління, що одночасно забезпечує інформаційне підґрунтя управлінських рішень, комунікацію між суб'єктами управління та контроль цифрових ризиків.

Таким чином, ІТ governance доцільно розглядати не як автономний технологічний сегмент, а як функціональну складову загальної системи корпоративного управління банківської установи. Така інтеграція набуває особливого значення в умовах переходу до відкритого банкінгу, використання хмарних технологій, розширення цифрових екосистем та посилення кіберризиків.

Висновки. Проведене дослідження засвідчило, що сучасна цифрова трансформація банківського сектору змінює функціональну природу інформаційних і комунікаційних технологій. Вони переходять із категорії переважно операційних інструментів до складу інфраструктури корпоративного управління, від якої залежать якість стратегічних рішень, ефективність нагляду за виконавчим менеджментом, управління ризиками, внутрішній контроль та підзвітність.

Комунікаційні та інформаційні технології в корпоративному управлінні банківських установ утворюють єдиний цифровий контур, який забезпечує рух управлінської інформації між акціонерами, радою банку, правлінням, ризик-

менеджментом, комплаєнсом, внутрішнім аудитом, регулятором та іншими стейкхолдерами.

За результатами дослідження запропоновано трирівневу структурно-функціональну модель, що включає комунікаційний, інформаційно-аналітичний та контрольно-безпековий рівні. У межах моделі систематизовано п'ять функціональних напрямів застосування технологій: підтримка управлінських рішень; корпоративна комунікація; управління ризиками та внутрішній контроль; розкриття інформації і регуляторна взаємодія; забезпечення цифрової операційної стійкості.

Обґрунтовано, що ефективність інформаційно-комунікаційного забезпечення корпоративного управління доцільно оцінювати за шістьма характеристиками: своєчасністю, повнотою, достовірністю, простежуваністю, захищеністю та стійкістю інформаційних потоків. Це дає

змогу перейти від формального оцінювання факту впровадження цифрових технологій до визначення їх фактичного внеску в якість корпоративного управління.

Подальша цифровізація банківської діяльності потребує інтеграції IT governance до загальної системи корпоративного управління, посилення цифрової компетентності членів рад банків, удосконалення механізмів управління ICT-та third-party risk, а також узгодження практик українських банків із принципами цифрової операційної стійкості Європейського Союзу.

Перспективи подальших досліджень пов'язані з емпіричною апробацією запропонованої моделі на вибірці банків України, розробленням системи кількісних показників та інтегрального індексу цифрової зрілості корпоративного управління, а також дослідженням впливу рівня цифрової зрілості на фінансову стійкість, операційні ризики та результативність банківських установ.

Конфлікт інтересів. Автор заявляє про відсутність конфлікту інтересів, який міг би вплинути на результати дослідження або їх інтерпретацію.

Фінансування. Дослідження виконано без зовнішнього фінансування.

Етична заява. Дослідження ґрунтується на аналізі відкритих наукових, нормативно-правових та статистичних джерел і не передбачало проведення досліджень за участю людей або тварин, тому окреме етичне схвалення не вимагалось.

Декларація про використання ШІ. Під час підготовки рукопису інструменти генеративного штучного інтелекту не використовувалися. Автор несе повну відповідальність за зміст рукопису.

Внесок авторів. Концептуалізація, методологія, аналіз джерел, формування результатів, написання та редагування рукопису будуть належать автору одноосібно.

Література:

1. Basel Committee on Banking Supervision. (2015). *Corporate governance principles for banks*. Bank for International Settlements. <https://www.bis.org/bcbs/publ/d328.htm>

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

3. Caluwe, L., & De Haes, S. (2019). Board level IT governance: A scoping review to set the research agenda. *Information Systems Management*, 36(3), 262–283. <https://doi.org/10.1080/10580530.2019.1620505>

4. Caluwe, L., Wilkin, C. L., De Haes, S., & Huygh, T. (2024). Board roles required for IT

governance to become an integral component of corporate governance. *International Journal of Accounting Information Systems*, 54, 100694. <https://doi.org/10.1016/j.accinf.2024.100694>

5. De Haes, S., & Van Grembergen, W. (2009). An exploratory study into IT governance implementations and its impact on business/IT alignment. *Information Systems Management*, 26(2), 123–137. <https://doi.org/10.1080/10580530902794786>

6. European Banking Authority. (2021). *Guidelines on internal governance under Directive 2013/36/EU*. <https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/internal-governance/guidelines-internal-governance>

7. European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/2554 of 14 December 2022 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>

8. OECD. (2023). *G20/OECD principles of corporate governance* 2023. OECD Publishing. <https://doi.org/10.1787/ed750b30-en>

9. Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business School Press.

10. Національний банк України. (2018). *Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах*: Постанова Правління Національного банку України від 11.06.2018 № 64. <https://zakon.rada.gov.ua/laws/show/v0064500-18>

11. Національний банк України. (2019). *Про затвердження Положення про організацію системи внутрішнього контролю в банках України та банківських групах*: Постанова Правління Національного банку України від 02.07.2019 № 88. <https://zakon.rada.gov.ua/laws/show/v0088500-19>

12. Національний банк України. (2021). *Про затвердження Положення про захист інформації та кіберзахист учасниками платіжного ринку*: Постанова Правління Національного банку України від 19.05.2021 № 43. <https://zakon.rada.gov.ua/laws/show/v0043500-21>

13. Національний банк України. (2025a). *Про затвердження Змін до деяких нормативно-правових актів Національного банку України з питань інформаційної безпеки та кіберзахисту*: Постанова Правління Національного банку України від 25.02.2025 № 24. https://bank.gov.ua/admin_uploads/law/25022025_24.pdf

14. Національний банк України. (2025b). *Про затвердження Положення про відкритий банкінг в Україні*: Постанова Правління Національного банку України від 25.07.2025 № 80. <https://bank.gov.ua/ua/payments/open-banking>

15. Національний банк України. (2025c). *Про затвердження Положення про порядок застосування технології хмарних обчислень*: Постанова Правління Національного банку України від 25.08.2025 № 99. <https://zakon.rada.gov.ua/laws/show/v0099500-25>

16. Національний банк України. (2026). *Про затвердження Положення про встановлення підвищених значень пруденційних нормативів для банків України*: Постанова Правління Національного банку України від 28.05.2026 № 57. <https://zakon.rada.gov.ua/laws/show/v0057500-26>

17. Пуш, А., Мігус, І., & Наконечна, Н. (2024). Основні моделі корпоративного управління в банківських установах. *Вчені записки Університету «КРОК»*, 2(74), 204–216. <https://doi.org/10.31732/2663-2209-2024-74-204-216>