



УДК 336.7

JEL E50, G21

Сергій Сергійович ЗАДВОРНИХ

кандидат економічних наук,

доцент кафедри фінансів,

Приватний заклад вищої освіти

«Східноєвропейський університет імені Рауфа Аблязова»,

м. Черкаси, Україна

 <https://orcid.org/0000-0002-7025-4116>

zadvornykh.s@gmail.com

БАНКІВСЬКИЙ МЕНЕДЖМЕНТ: ВИКЛИКИ І ПЕРСПЕКТИВИ СУЧАСНОСТІ

Анотація. У статті досліджено сучасні виклики банківського менеджменту в умовах цифровізації, зростання ролі FinTech, економічних криз та глобальної нестабільності. Низка глобальних потрясінь, зокрема пандемія, війна та поширення цифрових валют актуалізували потребу у нових підходах до управління банками з акцентом на кібербезпеку, гнучкість, стійкість та клієнтоорієнтованість. Основними проблемами визначено залежність від цифрових технологій, загрози кібератак, потребу в управлінні великими даними та використанні штучного інтелекту. У дослідженні доведено важливість розробки нових стандартів безпеки, адаптації продуктів до потреб різних категорій клієнтів, автоматизації та персоналізації послуг. Також обґрунтовано необхідність впровадження комплексної системи моніторингу, навчання персоналу та клієнтів, а також стратегії ризик-менеджменту як засобів підвищення стійкості банків і конкурентоспроможності у динамічному цифровому середовищі.

Ключові слова: банківський менеджмент, FinTech, фінансова стійкість, кібербезпека, ризик-менеджмент.



Постановка проблеми. Банківський сектор, його стабільність перебувають у центрі інтересів, а також уваги з точки зору фінансової безпеки кожної держави. Однак, зважаючи на складність та актуальність цієї сфери, її тісний зв'язок з персональними даними користувачів, психологією людей та аспектом традицій, глобальним характером наслідків від прийнятих управлінських рішень, трансформації в банківському секторі та зміни у банківському менеджменті відбуваються дуже повільно. Проте цей прогрес неминучий, і банки не стануть винятком. З метою забезпечення своєчасної адаптації банківської системи до потреб сучасності і забезпечення її стабільності, стійкості і підтримки належного рівня фінансової безпеки, необхідним є з'ясування викликів сучасності, які постають перед банківським менеджментом, а також формування на їх основі підходів до побудови нової, більш ефективної системи управління.

Аналіз останніх досліджень і публікацій. Питанням, пов'язаним із трансформацією банківської системи і системи банківського менеджменту у відповідності до викликів сучасності присвячені дослідження вітчизняних і зарубіжних вчених, а також спеціалізованих міжнародних організацій. Серед них можна виокремити роботи Т. Болейна, В. Ванга, Ф. Гаррідо, П. Гріффіна, З. Донга, Дж. Маркеса, Б. Меггесона, Х. Стюарта, М. Такі, А. Фанта, П. Шнайдера та ін. і дослідження, проведені ЄЦБ, МВФ, НБУ, S&P Global та ін. Проте, незважаючи на численну кількість праць, проблематика комплексної адаптації банківського менеджменту з врахуванням потреб клієнтів і викликів глобальної цифровізації є недостатньо дослідженою.

Формулювання мети статті. Метою даного дослідження є виявлення основних тенденцій на ринку банківських послуг, з'ясування залежності необхідності трансформацій у підходах в банківському менеджменті від сприйняття клієнтами тих чи інших рішень, а також з'ясування перспектив розвитку банківської сфери на сучасному етапі.

Методи і методологія здійснення дослідження. Методологічною та теоретичною основами даного дослідження слугували наукові праці зарубіжних і вітчизняних вчених, аналітична та статистична інформація стосовно тенденцій розвитку сфери фінансових та банківських послуг, впливу безпеки на сприйняття клієнтом банківських установ, а також нормативні акти, створені для регулювання банківського сектору і безпеки фінансових послуг. У процесі проведення дослідження використовувались методи порівняльного й емпіричного аналізу та синтезу, системний підхід.

Виклад основного матеріалу дослідження. Різноманітні зрушення в суспільному житті формують нові запити від користувачів. Так, пандемія коронавірусу показала, що люди відчують значну потребу в дистанційному обслуговуванні і можливості отримання щонайменше частини послуг в цифровому форматі. Початок війни в Україні лише поглибив цю потребу, а також показав, що банки потребують більшої автономності, стресостійкості, а на глобальному рівні – підвищення рівня безпеки як мереж, послуг, так і управління, щоби відповідати сучасним реаліям і викликам сьогодення.

Іншим викликом для сучасної банківської системи став швидкий розвиток FinTech стартапів, які нерідко пропонують більш зручні та інклюзивні рішення, а також зростаюча кількість цифрових валют, зокрема і плани урядів багатьох країн щодо впровадження цифрових національних валют (CBDC) [1]. Все це ставить нові вимоги до банків. Підсилює напруженість і все частіше висловлення позиції з боку критиків щодо того, що сучасна банківська система не сприяє прогресу, є архаїчною, не пропонує достатньо інклюзивних рішень, а також націлена більше на отримання прибутку, ніж на комфорт споживачів фінансових послуг і здешевлення самих послуг [2].

Крім вищезазначеного, суттєве занепокоєння викликає і те, що становище самих банків, зокрема глобальних і системоутворюючих, лише підтверджує потребу в зміні підходів щодо банківського менеджменту і ситуація, що сталась з Commerzbank і Deutsche Bank [3] якнайкраще ілюструє це. Статистичні дані та висновки міжнародних організацій також свідчать на користь цієї тези. Зокрема за даними S&P Global в 2023 р. у фінансовому секторі спостерігалось зростання кількості заяв про банкрутство і їх показник перевищив найвище до цього значення 2010 р. [4]. Зростає і загальний рівень банкрутства компаній в ЄС, хоча і не власне банків, проте воно значною мірою пов'язано з банківською діяльністю, а саме – підвищенням процентної ставки на кредитні кошти [5], що, в свою чергу, певною мірою стабілізує банківську систему, допомагає банкам сформувати достатньо резервного капіталу, але в довгостроковій перспективі призводить до формування суттєвої залежності банків від великих установ, які тримають на рахунках значні суми чи беруть кредити [3]. Якщо така установа стає неплатоспроможною, стійкість банку опиняється під загрозою. Саме тому необхідним є формування нових підходів до банківського менеджменту і коригування існуючих у відповідності до актуальної ситуації з врахуванням основних ризиків.

Ризики, які виникають в фінансовій і банківській сфері визначають потреби



в рішеннях в банківському менеджменті. До основних із них на сучасному етапі належать:

- кібербезпека і діджиталізація;
- використання інструментів на основі штучного інтелекту;
- корпоративне управління і стандарти;
- управління даними;
- системний ризик.

Розглянемо кожен із зазначених викликів і те, як вони можуть позначитись на банківському менеджменті, а також як зміни у підходах до банківського менеджменту можуть пом'якшити їх негативний вплив (рис. 1.).

Перший з викликів пов'язаний зі швидкою цифровізацією банківських послуг. З одного боку, виникає потреба у зміні стратегії управління банками шляхом певного зниження фізичної доступності банків через скорочення в них персоналу, оптимізацію географії і чисельності самих відділень, а також трансформації існуючих фінансових послуг у відповідності до сучасних потреб, чи створення нових, адже дослідження показують, що цифровізація призводить до суттєвих змін в потребах користувачів [6].

З іншого боку – цифровізація формує певну залежність як користувача, так і фінансових і банківських установ від цифрових технологій, підвищує рівень загроз, традиційних для цифрових мереж – загроз у сфері кібербезпеки з боку користувача і постачальника послуг, фішингу, витоків даних і несанкціонованого доступу до масиву даних банківської установи.

Результати досліджень показують, що фішинг і шкідливе ПЗ залишаються найчастіше використовуваними видами атак у банківському секторі. Іншим методом шахрайства, який належить до найбільш популярних, є використання програм-вимагачів [7].

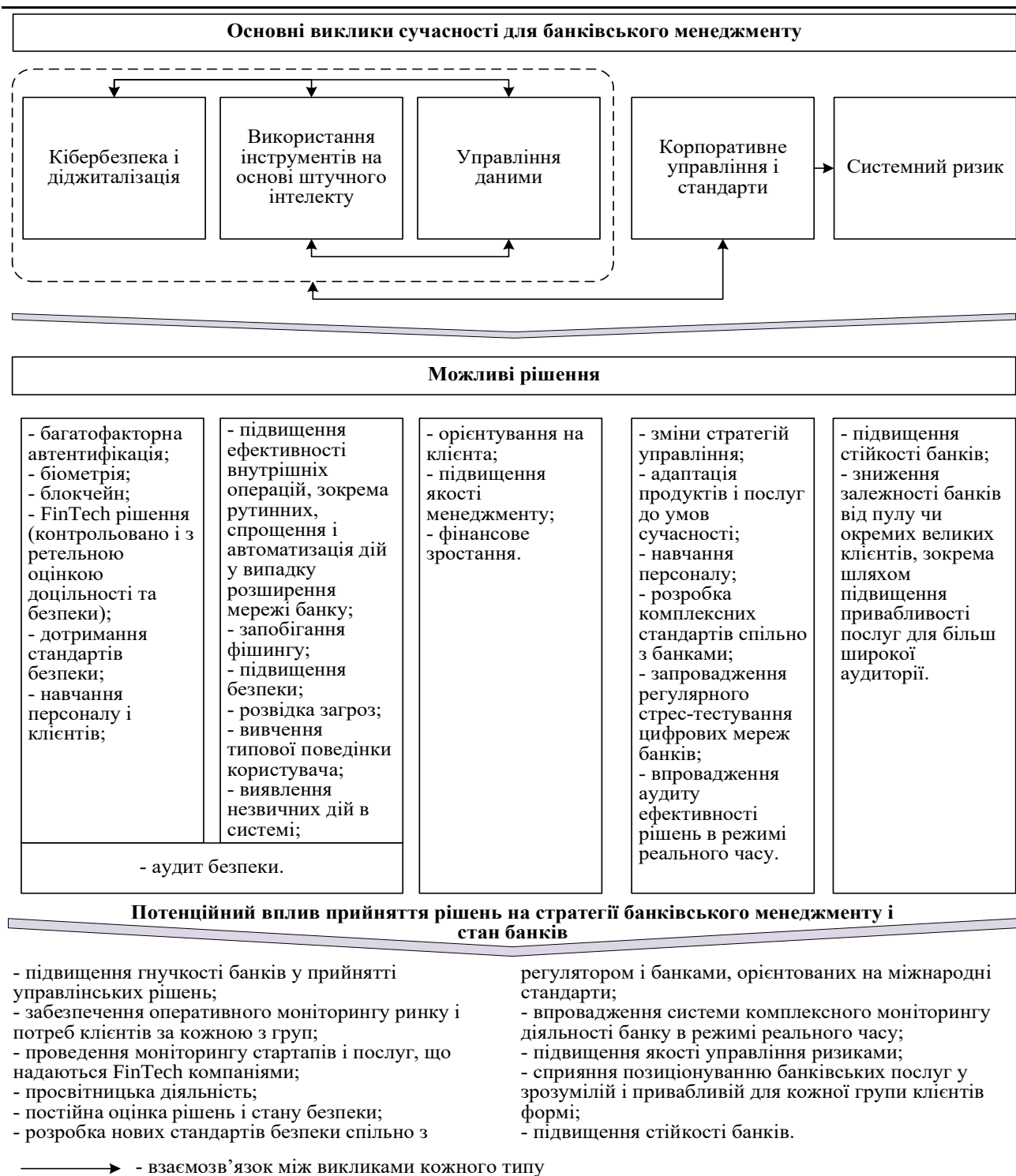


Рис. 1. Основні виклики в банківському управлінні сучасності і їх потенційний вплив на стратегії банківського менеджменту

Джерело: розроблено автором.



Такі програми не лише призводять до фінансових втрат, але і до суттєвих перебоїв в роботі, що особливо негативно позначається на корпоративних клієнтах. Інколи вони можуть спричинити навіть тривалі збої у роботі установи [8].

Ця проблема набуває дедалі більшої актуальності і з огляду на те, що за результатами досліджень, користувачі ставляться з великим рівнем недовіри до тих банківських установ, з якими в них чи їх близьких були пов'язані випадки втрати коштів або даних внаслідок шахрайства [9; 10], навіть якщо ці втрати були зумовлені їх власною необачністю. Такі користувачі нерідко мігрують до більш зрозумілих і інколи краще захищених фінансових стартапів чи установ. Це призводить, окрім загроз безпеки, до зниження довіри клієнтів і скорочення клієнтської бази банку. Також для корпоративних клієнтів проблеми безпеки можуть становити загрози, пов'язані не лише зі втратою коштів, даних, а також розкриттям потенційно важливої стратегічної інформації про діяльність компанії, але скомпрометовані фінансові дані можуть мати і довгострокові наслідки, включаючи пониження кредитного рейтингу та юридичні ускладнення, що виникають внаслідок шахрайської діяльності, як для самої компанії, так і для її клієнтів [11; 12].

З метою запобігання негативним наслідкам від цих загроз, необхідною є зміна у підходах в управлінні. Перш за все, важливим є моніторинг потреб і поведінки клієнтів, а також адаптація послуг у відповідності до виявлених тенденцій. Хоча банківська сфера є доволі суворо регульованою і не передбачає значної свободи у прийнятті управлінських рішень, в межах, де це доступно, необхідною є адаптація продуктів до реалій і до потреб окремих груп користувачів. Доцільним є, зокрема, розподіл таких продуктів за групами орієнтування на користувачів різних категорій – корпоративний сегмент, стартапи, молоді люди, працюючі люди середнього віку і люди похилого віку. В даному випадку адаптація і позиціонування продукту дозволить не лише підвищити його привабливість і зручність для конкретної категорії користувачів, релевантність до їх потреб, але і за рахунок правильного маркетингу банк отримає змогу залучити більш широке коло користувачів. Також такий підхід в управлінні дозволить краще зрозуміти потреби клієнтів. У цьому випадку банк отримає змогу проводити ненав'язливе інформування і безпосередні навчання клієнтів щодо фінансової грамотності, а також щодо цифрової безпеки банківських послуг і базових способів уникнення шахрайства зрозумілою для конкретної групи користувачів мовою з врахуванням найбільш притаманних саме їй загрозам. Такий підхід в стратегії управління дозволить наблизити банк психологічно до користувача і зробити його послуги більш привабливими у порівнянні з FinTech стартапами.

Іншим важливим елементом стратегії банківського управління в цьому контексті є власне підвищення безпеки внутрішнього середовища банку і його систем. В цьому напрямі банку необхідно розробити комплексний підхід до безпеки як операцій, здійснюваних самим банком, так і безпеки взаємодії клієнта з цифровим банком.

Дослідження дозволили виявити низку найбільш ефективних рішень в цьому контексті. Так, наприклад, було доведено, що використання двоетапної автентифікації та біометрії дозволяє більш ніж на 70% скоротити рівень спроб шахрайського доступу до рахунків клієнтів [13]. Проте при впровадженні таких рішень необхідно також зважати на цільову аудиторію цифрового продукту банку, оскільки іноді підвищення безпеки для окремих груп клієнтів означає також надмірне підвищення складності у доступі до послуг банку, і, як наслідок, – або пошук більш зручних рішень в іншому банку чи фінансовій установі, або ж розчарування і спроби знайти можливість обійти систему безпеки, розроблену банком.

Щодо безпеки самого банку, доцільною є зміна підходу до проведення транзакцій. Так, дослідження показують, що криптографічне хешування блокчейну та функції розподіленого реєстру дозволяють надійно захистити цифрові транзакції від несанкціонованих модифікацій і кібератак [14]. Дослідження дозволяють зробити висновок про те, що фінансові установи, які впроваджують системи транзакцій на основі блокчейну, відчують зниження операційних витрат та підвищення безпеки завдяки функціям перевірки в режимі реального часу і прозорості. Крім того, такі рішення допоможуть банкам пристосуватись до нових реалій в контексті здійснення платежів, а саме – підвищити швидкість транзакцій і знизити операційні витрати при проведенні самої транзакції. Це набуває актуальності, зокрема, в контексті міжнародних розрахунків, а також поступової підготовки до можливості впровадження національних цифрових валют – CBDC. Крім того, смарт-контракти покращують автоматизацію та усувають потребу в посередниках, що ще більше зменшує потенціал для фінансового шахрайства [15]. Проте оцінка ефективності впровадження того чи іншого рішення для конкретного банку повинна проводитись ретельно та регулярно. Хоча такі рішення і є ефективними, але було виявлено, що при їх реалізації можуть виникати проблеми з масштабованістю і регулюванням, які пов'язані з децентралізацією самого рішення [16]. Тому, у випадку їх впровадження, оцінка доцільності повинна обов'язково бути регулярною, адже розширення мережі банку чи вихід його на новий ринок, впровадження нового цифрового продукту можуть не вкластись повною мірою в цифрову модель, яка була ефективною до того. Саме для запобігання подібним ситуаціям і супроводжуваним ними ризиків необхідно є система комплексного



моніторингу діяльності банку загалом і всіх його систем зокрема в режимі реального часу.

В налагодженні такого моніторингу може допомогти впровадження управлінських інструментів на основі штучного інтелекту. Ці інструменти доводять свою ефективність в аналізі великих обсягів даних про банківські транзакції для виявлення незвичайних патернів, що вказують на зараження шкідливим програмним забезпеченням [17]. Також вони дозволяють в режимі реального часу отримувати інформацію щодо кіберзагроз, що дає змогу певною мірою випередити розвиток нових шкідливих програм, а також допомагає автоматизувати значну частку процесів в управлінні банку. Такі інструменти, окрім безпеки, дають можливість пришвидшити та оптимізувати рутинні завдання, оцінку клієнта, прогнозування його фінансової поведінки. Якщо банк має розгалужену структуру і, зокрема, закордонні відділення, інструменти на основі штучного інтелекту дозволяють оптимізувати обмін даними між відділеннями, пришвидшити доступ до інформації, що міститься в різних структурних підрозділах, а також спростити процедуру заповнення документів у відповідності до стандартів і законодавства різних країн, навіть забезпечити автоматизацію надання необхідної інформації працівникам з відділень банку у різних юрисдикціях мовою, яка є вживаному саме в їх країні.

Щодо користувачів – стратегія банку щодо впровадження інструментів на базі штучного інтелекту також може допомогти як в підвищенні зручності отримання послуги, наприклад, за рахунок інтеграції асистента, який допоможе у більш зручний і швидкий спосіб вирішити проблеми клієнта, так і в контексті безпеки. Такі інструменти допомагають виявити спроби несанкціонованого входу до облікових записів, вивчаючи особливості поведінки користувача при самій аутентифікації, а також безпосередньо при взаємодії з цифровим банком.

Проте, незважаючи на численні переваги, цей напрям тісно пов'язаний з роботою з великими даними. З огляду на їх стратегічну важливість для будь-якої фінансової установи, в цьому контексті необхідною є розробка комплексної стратегії роботи з такими даними і їх захисту. Робота з великими даними потребує не лише їх перевірки і обробки, але і їх верифікації, адже значною мірою інструменти управління, що ґрунтуються на штучному інтелекті, вимагають тренування і, у випадку використання хибних даних, виправлення сформованого алгоритму потребуватиме значних затрат часу і ресурсів. Також великі дані стають предметом інтересу для шахраїв та злочинців, саме тому робота з ними потребує значного рівня захисту, що, зважаючи на обмежений обсяг даного дослідження, буде відображено в майбутніх працях. Проте потенційно інтеграція великих даних в управління саме в банківській сфері, незважаючи на ризики, є одним з найбільш перспективних напрямів і, за

оцінками експертів, до кінця 2025 р. може глобально сприяти зростанню банківського сектору на 62,1 млрд. дол. [18].

Сприяють підвищенню безпеки використання цифрових інструментів і великих даних в банківському секторі також інші фактори. Зокрема, одним з найбільш ефективних є дотримання стандартів, розроблених відповідними регуляторними органами [19]. Прикладами таких дієвих стандартів є Загальний регламент Європейського Союзу про захист даних (GDPR), Директива про платіжні послуги 2 (PSD2), Закон Грамма-Ліча-Блайлі (GLBA). На жаль, в Україні немає чіткого законодавства чи стандартів, які б регламентували ці питання, окремі елементи містяться в різних нормативно-правових актах та постановах НБУ. Також суттєвою прогалиною є те, що вітчизняне законодавство хоча і запроваджує проведення стрес-тестів банків і винесення на основі їх результатів рекомендацій щодо управління у банківському секторі в цілому та підвищення стійкості окремо взятих банків, проте Концепція оцінки стійкості не передбачає розробки чітких стандартів, а також не встановлює ані вимог, ані дає рекомендацій банкам щодо проведення регулярних перевірок на стресостійкість і вразливість саме електронних систем [20]. З огляду на те, що в Україні на сучасному етапі банківські системи перебувають у особливому фокусі зловмисників, розробка таких стандартів, адаптованих до вимог міжнародного законодавства, передусім ЄС, є важливою і необхідною. Зокрема, впровадження таких дієвих стандартів дозволить запобігти частині проблем, пов'язаних з масштабованістю управлінських моделей. Зважаючи на те, що кожна банківська установа має свій унікальний досвід і свої потреби, при формуванні таких стандартів доцільним є спільна робота регулятора і банків. Це допоможе уникнути прогалин в сформованих рішеннях і зробити їх оптимальними для всіх акторів ринку.

Проте не лише розробка стандартів стає одним з першочергових завдань для оптимізації системи управління банками. Дослідження показують, що інтеграція навчальних програм до системи управління на регулярній основі як для персоналу, так і для клієнтів банку дозволяє не лише підвищити привабливість банківської установи, зробити її і фінансові послуги більш зрозумілими і доступними, але і суттєво підвищити рівень обізнаності працівників і клієнтів щодо цифрової безпеки [21]. Це доцільно і з огляду на те, що регулярне навчання персоналу дозволить в подальшому заощадити кошти на спеціальних тренінгах, які будуть необхідними поруч із залученням висококваліфікованих фахівців в галузі ІТ при впровадженні нових стандартів безпеки [22]. Також це допомагає суттєво знизити ризик шахрайства внаслідок фішингових атак і соціальної інженерії, а отже – підвищити довіру до банківської установи.



При обранні нового підходу в банківському менеджменті важливим є також дотримання балансу між потребами, конкретними рішеннями, безпекою і інвестиціями. Регулярна оцінка доцільності і спроможності впровадження того чи іншого рішення дозволить знизити ризики і оптимізувати власні процеси, а також підвищити довіру користувачів до банку. Більше того, проведення такого моніторингу повинне бути включеним до стандартів безпеки і стандартів з оцінки стійкості банків. Це пов'язано ще й з тим, що нерідко прийняття невірною управлінського рішення призводить не лише до прямих втрат, але і необхідності значних інвестицій. При цьому, завжди існує системний ризик, який лише поглиблюється внаслідок таких дій. Як уже зазначалось раніше, банки часто задля нарощування капіталу чи підвищення власної стійкості фокусуються на клієнтах, які є або вкладниками значного за обсягом капіталу, великих корпоративних клієнтах, або ж намагаються отримати значні за обсягом кредити [3]. Така залежність підвищує системний ризик, ставлячи банки в залежність від певного пулу клієнтів. Якщо вони бажають змінити обслуговуючий банк чи провести трансфер капіталу, або якщо такі клієнти припиняють свою діяльність чи банкрутують – стійкість банку опиняється під загрозою. В той же час, ці рішення банки приймають нерідко задля того, щоби покрити інвестиції, необхідні для підвищення власної кібербезпеки чи розробки нових продуктів.

Зазначена стратегія стає дедалі більш ризиковою, особливо в Україні, коли з прийняттям закону 4015-IX [23] доходи банків суттєво скоротились, а інвестиції в технології та системи безпеки зростають у зв'язку з прийняттям того ж закону і коливанням курсів валют, адже значна частка обладнання виробляється за кордоном. Саме тому в таких умовах банки повинні скоригувати свої стратегії управління таким чином, щоби включити до них комплексну оцінку ризиків, яка виходитиме за межі існуючої стандартної. Також банки повинні переглянути розпочаті проєкти і повторно оцінити їх доцільність та вплив продовження реалізації такого проєкту на стійкість банку задля уникнення погіршення ситуації і загострення системного ризику. Тобто, управління ризиками, яке включає комплексну оцінку безпеки і доцільності впровадження нових рішень, в т.ч. цифрових, нових продуктів і спроможності банку, як інституційної, так і кадрової та фінансової, реалізувати такі проєкти є ключовою.

Висновок. Система банківського менеджменту, як і вся галузь загалом, потребує певних змін у відповідь на виклики сучасності. У період активних трансформацій, виникнення нових загроз, відкриття нових перспектив, виявлення потреб в нових продуктах і рішеннях потреба у таких змінах і адаптації до нових реалій набуває особливої ваги. Горизонти стратегії банківського менеджменту виходять за межі класичного банківського управління

і повинні враховувати нові, нехарактерні раніше для галузі, елементи, а також враховувати глобальні тенденції, коригувати вже існуючі рішення з огляду на їх масштабованість. Дослідження дозволило виявити прямий зв'язок між основними напрямками, в яких виникає потреба в розробці додаткових рішень, як і те, що кожне з них за умови неналежним чином оціненого та спланованого підходу може підсилити негативний вплив іншого, або ж допомогти вирішити проблему в іншій сфері при належному плануванні. Це лише підтверджує необхідність комплексного підходу і оцінки як поточного становища банку, так і кожного окремо взятого рішення, а також змін в загальній стратегії банківського менеджменту. Також було виявлено, що банки і їх послуги стають дедалі більш залежними від настроїв і сприйняття користувача, а також його зручності. Значна кількість фінансових установ і стартапів пропонує користувачам нерідко більш зручні рішення, в той же час, як регулятори часто спонукають банки до того, що вони, як і їх послуги, стають дедалі більш подібними одне до одного, деперсоніфікованими. Це означає, що банки у своїх стратегіях потребують все більшого фокусування на користувачі, його потребах, потребах кожної цільової групи, безпеці, яка не буде надто обтяжливою для клієнта, проте надійною, а також на розробці стратегій позиціонування продукту у зрозумілій для клієнта формі. Динаміка сфери фінансових і банківських послуг також свідчить про необхідність розробки нових стандартів безпеки, орієнтованих на міжнародні і розроблених з врахуванням практичного досвіду і перспективи самих банків. Таким чином, на сучасному етапі виникла нагальна потреба у формуванні нової комплексної системи банківського менеджменту. І лише в умовах ефективних і своєчасних змін класична банківська система має і далі надійні перспективи до існування, в той же час відсутність адекватної відповіді з боку банків в системі управління призведе до поступової заміни їх більшістю користувачів на більш прості, інклюзивні, зрозумілі і доступні рішення FinTech установ чи стартапів.

Список використаних джерел:

1. Central Bank Digital Currency Tracker. *Atlantic Council*. URL: <https://www.atlanticcouncil.org/cbdctracker/>.
2. Fanta A., Bollein T. European banks are scared of the digital euro. Here's how their secret lobbying could torpedo it. *Follow the money*. URL: <https://www.ftm.eu/articles/banks-fear-digital-euro-secret-lobby>.
3. Schneider P. Fusion: Commerzbank-Kunden überzeugt als Deutsche-Bank-Kunden. *WirtschaftsWoche*. URL: <https://www.wiwo.de/unternehmen/banken/brandindex-fusion-commerzbank-kunden-ueberzeugter-als-deutsche-bank-kunden/24164234.html>.



4. Meggeson B., Garrido F., Taqi M. Europe's banks brace for more bad loans. *S&P Global*. URL: https://www.spglobal.com/market-intelligence/en/news-insights/articles/2023/6/europe-s-banks-brace-for-more-bad-loans-75917936?utm_source=chatgpt.com.
5. European Union Bankruptcies. *Trading Economics*. URL: <https://tradingeconomics.com/european-union/bankruptcies>.
6. Policy report on FinTech data gaps / Marqués J. et al. *Latin American Journal of Central Banking*. 2021. 2(3), 100037-NA. <https://doi.org/10.1016/j.latecb.2021.100037>.
7. Ahmad I., Khan S., Iqbal S. Guardians of the vault: unmasking online threats and fortifying ebanking security, a systematic review. *Journal of Financial Crime*. 2024. 31(6), P. 1485-1501. <https://doi.org/10.1108/jfc-11-2023-0302>.
8. Assessment of Machine Learning Approaches for the Predictive Modeling of Plasma-Assisted Ignition Kernel Growth / Bhuiyan S.M.Y et al. *Proceedings of the ASME 2024 International Mechanical Engineering Congress and Exposition November 17–21, 2024*. 2024. Volume 9: Heat Transfer and Thermal Engineering. Portland, Oregon, USA. V009T11A049. <https://doi.org/10.1115/IMECE2024-1459068>.
9. Javaid M. A. Cyber Security: Challenges Ahead. *SSRN Electronic Journal*. 2013.
10. Cyber security threats: A never-ending challenge for e-commerce / Liu X. et al. *Frontiers in psychology*. 2022. 13(NA), P. 927398-NA. <https://doi.org/10.3389/fpsyg.2022.927398>.
11. Stewart H., Jürjens J. Data security and consumer trust in FinTech innovation in Germany. *Information & Computer Security*. 2018. 26(1), P. 109-128. <https://doi.org/10.1108/ics-06-2017-0039>.
12. Data privacy and cybersecurity challenges in the digital transformation of the banking sector / Wang S. et al. *Computers & Security*. 2024. 147, P. 104051-104051. <https://doi.org/10.1016/j.cose.2024.104051>.
13. Mbama C. I., Ezepue P. Digital banking, customer experience and bank financial performance: UK customers' perceptions. *International Journal of Bank Marketing*. 2018. 36(2), P. 230-255. <https://doi.org/10.1108/ijbm-11-2016-0181>.
14. Gomathi C., Jayasri K. Rain Drop Service and Biometric Verification Based Blockchain Technology for Securing the Bank Transactions from Cyber Crimes Using Weighted Fair Blockchain (WFB) Algorithm. *Cybernetics and Systems*. 2022. 54(4), P. 550-576. <https://doi.org/10.1080/01969722.2022.2103229>.
15. Dong Z. Y., Luo F., Liang G. Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems. *Journal of Modern Power Systems and Clean Energy*. 2018. 6(5), P. 958-967. <https://doi.org/10.1007/s40565-212>

018-0418-0.

16. Duran R., Griffin P. Smart contracts: will Fintech be the catalyst for the next global financial crisis? *Journal of Financial Regulation and Compliance*. 2020. 29(1), P. 104-122. <https://doi.org/10.1108/jfrc-092018-0122>.
17. Customers' perceptions of FinTech adaptability in the Islamic banking sector: comparative study on Malaysia and Saudi Arabia / Oladapo, I. A. et al. *Journal of Modelling in Management*. 2021. 17(4), P. 1241-1261. <https://doi.org/10.1108/jm2-10-2020-0256>.
18. Rayaprolu A. 25+ Impressive BD Statistics for 2024. *TechJury*. <https://techjury.net/blog/big-data-statistics/>.
19. Calderaro A., Craig A. J. S. Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*. 2020. 41(6), P. 917-938. <https://doi.org/10.1080/01436597.2020.1729729>.
20. Концепція оцінки стійкості банків у 2025 році. *Національний банк України*. URL: https://bank.gov.ua/admin_uploads/article/Stability_assessment_pr_2025.pdf?v=13.
21. Mugarura N., Ssali E. Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. *Journal of Money Laundering Control*. 2020. 24(1), P. 10-28. <https://doi.org/10.1108/jmlc-112019-0092>.
22. Huawei Pakistan Providing Cloud Solutions for Banking Industry: A Data Driven Study / Nawaz H. et al. *The Asian Bulletin of Big Data Management*. 2024. 4(1), P. 89-107. <https://doi.org/10.62019/abbdm.v4i1.122>.
23. Про внесення змін до Податкового кодексу України та інших законів України щодо забезпечення збалансованості бюджетних надходжень у період дії воєнного стану: Закон України від 10.10.2024 р. № 4015-IX: станом на 9 трав. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/4015-IX>.

Serhii ZADVORNYKH

Ph.D. in Economic Sciences,
Associate Professor of the Department of Finance,
Private Higher Education Institution
«Rauf Ablyazov East European University»,
Cherkasy, Ukraine
 <https://orcid.org/0000-0002-7025-4116>
zadvornykh.s@gmail.com



BANKING MANAGEMENT: MODERN CHALLENGES AND PROSPECTS

Abstract. *Purpose.* The article explores the modern challenges of banking management in the context of digital transformation, the rise of FinTech, economic crises, and global instability. It aims to identify key trends and risks shaping the banking sector and assess how these factors necessitate the evolution of banking management strategies. The study specifically focuses on cybersecurity, artificial intelligence, big data management, and customer-oriented service adaptation as essential components of a new, resilient management model.

Methods. The research is grounded in a comprehensive review of domestic and international academic literature, regulatory documents, and statistical data. It employs a comparative and empirical analysis approach, utilizing synthesis and systems thinking to evaluate trends in banking services, technological risks, and customer behavior. The study integrates case analysis of notable institutions and data from global organizations to contextualize challenges in digital banking environments.

Results. The findings highlight that digitalization, while offering operational efficiency and convenience, introduces systemic risks including increased exposure to cyber threats, dependence on large clients, and structural vulnerabilities. The rise of FinTech and digital currencies has amplified the urgency for banks to modernize their management strategies, emphasizing resilience, flexibility, and customer-centricity. Key recommendations include: implementing AI-powered monitoring tools for real-time threat detection and service personalization; developing adaptive products targeted at specific categories of clients; integrating blockchain for transaction security and efficiency; establishing comprehensive training programs for staff and clients; creating new security standards aligned with international regulations taking into account the experience of banks and with their direct involvement in the development of such standards; regularly reassessing the scalability and financial feasibility of digital initiatives.

The study concludes that traditional banks must transit toward a more agile and technologically integrated management framework. Failing to adapt may result in loss of competitiveness to FinTech firms that offer simpler, more inclusive, and user-friendly financial services.

Keywords: bank management, FinTech, financial stability, cybersecurity, risk management.