DOI: https://doi.org/10.32782/2521-666X/2023-82-15
УДК 336.71

Вощак О.В.
аспірант кафедри фінансів, банківської справи та страхування,
Університет митної справи та фінансів

Voshchak Oleksii
University of Customs and Finance

ДОСЛІДЖЕННЯ ЗМІНИ ПРОФІЛЮ ОПЕРАЦІЙНИХ РИЗИКІВ БАНКІВ

INVESTIGATING THE CHANGE IN THE PROFILE OF OPERATIONAL RISKS IN BANKS

Наукова стаття присвячена дослідженню та аналізу проблем операційного ризику в сучасних умовах. У статті розглянуто становлення поняття «операційний ризик». Висвітлено його трансформацію, під впливом еволюційних процесів та змін. Виявлені та проаналізовані фактори впливу, які найбільше вплинули на якісні і кількісні зміни профілю операційних ризиків банків та запропоновані шляхи їх мінімізації. До переліку основних генераторів зміни профілю ризиків, автор відносить процес цифровізації банківської галузі, швидкі технологічні зрушення, пандемію COVID-19, а також, суттєві зміни в соціально-економічному середовищі, яким передувало розгортання повномасштабної війни, спричиненої військовою агресією з боку Росії. У зв'язку з цим, набуває ще більшої актуальності питання вдосконалення методів та інструментів управління операційним ризиком.

Ключові слова: *банківська система, операційний ризик, цифровізація, військові дії, кіберзахист, пандемія.*

The scientific article is devoted to the research and analysis of operational risk issues in modern conditions. The article examines the emergence of the concept of «operational risk» and its transformation under the influence of evolutionary processes and changes. Due to rapid technological advancements and changes in the socio-economic environment, the profile of operational risks for banks has also undergone significant changes. The identification and analysis of factors that have the greatest impact on qualitative and quantitative changes in the profile of operational risks are important tasks for financial institutions. One of the main drivers of changes in risk profiles is the process of digitization in the banking industry. The use of modern information and communication technologies in the banking sector significantly facilitates operations but also leads to new types of risks such as technological failures, cyber-attacks, and theft of confidential information. Another factor that significantly influences the profile of operational risks is the COVID-19 pandemic. The global pandemic has posed a major challenge to the banking sector as it has resulted in significant changes in the way banking services are provided, leading to the emergence of new operational risks. In particular, the implementation of quarantine restrictions and the transition to remote work have prompted banks to review their operational procedures and ways of interacting with clients. This has increased the risk associated with technological flaws, inadequate cybersecurity, and data storage problems. Additionally, the deployment of full-scale warfare caused by military aggression from Russia has a serious impact on operational risk. In such circumstances, banks face significant difficulties in ensuring the security of their assets, carrying out operations, and ensuring the normal functioning of the financial system as a whole. The military conflict has led to instability in the economic environment, a significant decrease in trust in financial institutions, and threats to the solvency of banks. In light of the growing threats of operational risk, the question of improving methods and tools for managing it becomes even more relevant. Banks need to carefully analyze their operational processes, identify potential risks, and develop effective strategies to minimize these risks.

Key words: *banking system, operational risk, digitization, military actions, cybersecurity, pandemic.*

Постановка проблеми. Зростання цифровізації банківської сфери, призвело до зміни характеру операційних ризиків, пов'язаних з інформаційною безпекою, технічними збоями та шахрайством. Пандемія COVID-19 ще більше посилила цей процес, оскільки банки були змушені прискорено переходити на віддалену роботу та цифрові канали обслуговування, що призвело до збільшення операційних ризиків. Але максимальної загрози з боку операційних ризиків, банківський сектор зазнав з початком повномасштабної війни, розпочатої 24 лютого 2022 року, що призвело до їх суттєвого збільшення і створило додаткові виклики для банків.

Аналіз останніх досліджень і публікацій. Увагу до проблем дослідження операційного ризику банку, його оцінки та управління ним, присвячені роботи таких науковців як: Дмитров О.С. [1, с. 6–23, 52], Коваленко В.В. [2, с. 192–212], Шульга Н.П. [3, с. 7–25], Камінський А. [4, с. 7–11], Набок Р. [5, с. 61–65], Криклій А.О. [6, с. 168–172]. Незважаючи на велику кількість наукових досліджень, сьогодення вимагає проведення подальших теоретико-методологічних досліджень процесу

розширення і трансформації операційних ризиків в сучасних умовах.

Мета статті. Цифрові технології стали невід'ємною частиною банківської сфери, що дозволяє розширювати клієнтську базу, збільшувати частку ринку, підвищувати фінансову стійкість та безпеку з одного боку. А з іншого боку, такий розвиток стає суттєвим джерелом операційного ризику. Метою дослідження є аналіз зміни профілю операційного ризику банків в умовах зростаючої цифровізації.

Виклад основного матеріалу. Сутність поняття «ризик», визначається як можливість настання несприятливої події та, здебільшого, трактується як загроза втрати суб'єктами господарювання частини своїх ресурсів, недоотримання доходів чи виникнення додаткових витрат в результаті здійснення певної виробничої чи фінансової діяльності [7, с. 7].

З-поміж інших банківських ризиків, останнім часом все більше уваги приділяється саме операційному ризику. Увага до нього зумовлена посиленням глобалізації, та значним поширенням новітніх інформаційних технологій. А його важливість зумовлена руйнівними наслідками, до яких може призвести недбале керування цими ризиками, а саме: репутаційні втрати, суттєві збитки, витік конфіденційної інформації тощо.

Не зайвим буде нагадати найяскравіші приклади реалізації операційних ризиків у вітчизняній та світовій практиці. Один із таких випадків трапився у 2017 році. Спочатку комп'ютерний вірус «Wanna Cry», а потім і «Petya.A.» вразив комп'ютерні мережі багатьох державних і комерційних установ України, серед яких була і велика кількість банків (Ощадбанк, ТАС Комерцбанк, Укргазбанк, Південний, ОТП банк, Кредобанк), роботу яких було повністю чи частково заблоковано на деякий час. Ще один приклад – запровадження карантину та запровадження обмежувальних протиепідемічних заходів з метою запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2.

Інший яскравий приклад – початок бойових дій 24 лютого 2022 року на території України та впровадження військового стану, призвели до шокового стану банківську систему України, та змусили суттєво обмежити діяльність багатьох банківських установ. Характерною ознакою цієї події, стало вимушене скорочення кількості відділень та перенавантаження діючих, через зміну розподілу клієнтів, спричинену внутрішнім переселенням. Втрата частини персоналу та зниження бізнес-активності клієнтів, через вимушену міграцію або мобілізацію, обмеження розрахункових операцій з валютою. Блекаути, спричинені ворожими ракетними атаками на енергосистеми країни, які вплинули на можливість надавати безперервний сервіс та роботу внутрішніх систем. Всі перелічені вище обставини, змусили перейти від середньострокових і довгострокових стратегій до короткострокового планування та зміни бізнес-моделі.

В США в 2019 році трапився інцидент з даними клієнтів в Capital One. Відбувся злам даних клієнтів, що призвело до витоку особистої інформації більше 100 мільйонів клієнтів. Інцидент з Danske Bank стався в Данії та пов'язаний з його філією в Естонії у 2017 році. Головною проблемою було те, що банк не здійснював достатньої перевірки клієнтів і не контролював джерела їхніх коштів. Це дозволило пройти через систему банку багатьом злочинцям і корупціонерам.

Отже, для більш глибокого розуміння сутності операційного ризику, потрібно дослідити історію розвитку даного виду ризику. Спираючись на документи Базельського комітету, можна відслідкувати еволюцію поняття «операційний ризик». До 1988 року в документах Базельского комітету, термін «операційний ризик» не фігурував як такий. Але з появою доповіді «Ризики в комп'ютерних і телекомунікаційних системах», як свідчення зростання банківських ризиків в зв'язку з автоматизацією їх діяльності, була виокремлена ціла низка ризиків (ризик втрати даних, неефективний розвиток IT інфраструктури, шахрайські дії з використанням інформаційних систем банку, зупинка бізнесу через збої програм і устаткування та ін.), що в сучасному світі класифікують як операційні. Але одним з найважливіших документів в цьому напрямку, вважається «Належна практика управління і нагляд за операційними ризиками», що розкриває методологію управління операційними ризиками [8, с. 3–5; 9, с. 89]. Незважаючи на відсутність чіткого визначення терміну «операційний ризик», було сформульовано, які саме ризики мають відноситись до операційних. Ці ризики були згруповані в сім категорій:

– внутрішнє шахрайство;
– зовнішнє шахрайство;
– практика зайнятості і безпека праці;
– клієнти, продукти і ведення бізнесу;
– збиток матеріальним активам;
– зупинка бізнесу і збої в системах;
– проблеми з управлінням і виконання операцій.

Відтак з'явилися чітко окреслені межі поняття «операційний ризик».

Наступний суттєвий етап еволюції поняття «операційний ризик», який дозволив остаточно сформувати розуміння операційного ризику в сучасних умовах, завдячує виходу так званого документу Базель II. Згідно цієї угоди, операційний ризик визначається як ризик виникнення збитків в результаті недоліків або помилок в ході здійснення внутрішніх

процесів, допущених з боку персоналу, функціонування інформаційних систем і технологій, а також унаслідок зовнішніх подій [10].

Майже ідентичне формулювання фігурує і у вітчизняному законодавстві – «імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок недоліків або помилок в організації внутрішніх процесів, навмисних або ненавмисних дій працівників банку або інших осіб, збоїв у роботі інформаційних систем банку або внаслідок впливу зовнішніх факторів. Операційний ризик уключає юридичний ризик, однак має виключати ризик репутації та стратегічний ризик» [11]. Що свідчить про використання регулятором, прогресивного міжнародного досвіду.

Розуміючи сутність операційного ризику, можна окреслити основні фактори його виникнення: недосконала побудова бізнес-процесів, некласифіковані дії персоналу, шахрайство, перебої в роботі інформаційних систем та зовнішні чинники. З розвитком інформаційних технологій та збільшенням мобільного доступу до інтернету та цифрових послуг по всьому світу за останні роки, процес надання послуг, включаючи фінансові, значно змінився. З огляду на це, в окремий рядок слід винести інформаційні системи, оскільки з-поміж інших, саме вони стають головним «генератором» операційних ризиків сьогодення. Цей процес зумовлений цифровізацією банківської сфери і дозволяє розширити клієнтську базу, збільшити частку ринку банківських послуг, знизити витрати, підвищити фінансову стійкість та безпеку банку. Цифровізація діяльності банку включає нові методи роботи, банківські продукти та послуги, що допомагає вирішувати поставлені завдання мінімальними затратами [12, с. 3–5]. З одного боку цей процес стимулюється висококонкурентним середовищем. Кожна банківська установа відповідно до своїх особливостей ведення бізнесу, намагається бути сучасною і технологічною, надаючи зручні сервіси, послуги і продукти. З іншого боку, цей процес був значно пришвидшений через настання пандемії COVID-19, яка змусила навіть ті банки, які не схильні до змін, шукати нові рішення, продукти і формати роботи [13, с. 149–158]. В першу чергу це торкнулося персоналу банківських установ, який був вимушений переходити на віддалений режим роботи. Відповідно відбулися зміни у виконанні різних процедур і процесів. Також це потребувало відповідних змін у інформаційних банківських системах – розробка нових продуктів, з метою максимального зсуву в бік надання дистанційних послуг (онлайн банкінг, віртуальні консультанти, дистанційне оформлення платіжних карток тощо). Підсумовуючи вищезазначене, можна констатувати, що в банківському секторі відбулася приоритезація напрямків розвитку цифрової трансформації, серед яких зокрема розвиток платіжно-розрахункових систем, розвиток цифрового банкінгу, дистанційна ідентифікація, масштабне впровадження інноваційних технологій, що використовують новий рівень організації внутрішніх бізнес-процесів банків, включаючи технології bigdata та штучного інтелекту. Цьому процесу всебічно сприяє і держава на рівні керівних органів. Національний банк та Міністерство цифрової трансформації спільно працюють над цифровізацією банківської системи України, метою якої є оптимізація внутрішніх процесів, скорочення бюрократичних процедур, впровадження сучасних послуг, підвищити конкурентоспроможності [14].

Одним з найяскравіших прикладів є monobank – роздрібний продукт АТ «Універсал Банк», який виник у рамках співпраці з командою Fintech Band. Основна мета: «забезпечити клієнтів прогресивним інструментом персонального банкінгу, надзвичайно вигідним і конкурентоспроможним на ринку кредитних послуг». Основною особливістю продукту є обслуговування клієнтів без відділень, де майже всі послуги надаються за допомогою мобільного застосунку.

Аналізуючи закордонний досвід, слід зазначити, що цифрові технології (Digital money, FinTech, BigTech) значно вплинули на банківську галузь ще до початку пандемії COVID-19. Вони дозволили створювати нові продукти та послуги, покращити ефективність роботи банків, але з іншого боку і посилили конкуренцію з традиційними банківськими бізнес-моделями. Протягом десятиліть банки контролювали цифрові форми грошей та платежів, але сучасні технології змінили цю ситуацію. Мова йде про різноманітні цифрові активи, які не знаходяться на балансах банків: криптовалюти, електронні гаманці, стейблкоїни або баланси у телекомунікаційних провайдерів. Конкурентна перевага нових гравців базується не на самому активі, а на технології оплати, пов'язаній з ним. Зручність платежів та зв'язки з іншими частинами зростаючого цифрового життя споживачів та бізнесу, що були прискорені кризою COVID, стали ключем до успіху. Отже, внаслідок швидких технологічних змін та зростаючої конкуренції від нових учасників, банківська галузь може перейти від традиційного олігопольного ринку до системи з декількома домінуючими платформами, що контролюють доступ до клієнтської бази. У такому сценарії, володіння клієнтськими даними, а також сумісність даних між платформами, стануть ключовими факторами для забезпечення низьких витрат на перехід для клієнтів та забезпечення достатньої конкуренції на ринку. Тому Big Tech-компанії, разом з різними платформи, можуть стати домінуючими учасниками ринку. Це створює серйозний виклик

для традиційних банківських бізнес-моделей, та змушує їх трансформуватися, використовуючи інноваційні технології [15].

Досліджуючи звіт компанії ORX (одна з найбільших асоціацій з управління операційними ризиками в секторі фінансових послуг) «Insights into Material Risks» за 2022 рік, можна дійти висновку, що одним з домінуючих факторів ризику є інформаційна безпека. Це зумовлено швидкими технологічними змінами та використання новітніх технологій. З-поміж інших, до основних загроз відносяться: біометрична ідентифікація, загрози, пов'язані із хмарними сервісами та зберіганням даних, загрози пов'язані з використанням штучного інтелекту [16, с.4].

Проведений аналіз, дозволяє зробити впевнені висновки, щодо значимої зміни кількісних і якісних характеристик профілю операційних ризиків банківської системи. Досить суттєвий зсув у бік зовнішніх факторів ризику, відбувся з початком цифровізації банківської галузі, каталізатором пришвидшення якої, стала пандемія COVID-19. А умови повномасштабної війни, суттєво збільшили операційні ризики.

Зважаючи на суттєві зміни профілю операційного ризику, ще більшої актуальності набуває питання вдосконалення методів та інструментів управління операційним ризиком. Сучасні підходи в управлінні операційними ризиками передбачають здійснення цілої низки заходів, які передбачені законодавчо. З-поміж інших, основними є створення політики та процедури управління операційними ризиками і виявлення та вимірювання операційного ризику. В свою чергу, виявлення та оцінка операційного ризику в сучасних умовах є досить складним процесом, обумовленим наступними факторами:

1) недостатність даних – деякі операційні ризики можуть бути не очевидними, та складними для передчасного виявлення. Для оцінки операційного ризику потрібно мати велику кількість достовірних та повних історичних даних, пов'язаних з інцидентами та помилками, що ускладнює оцінку ризиків. Недостатність таких даних, або недостовірна інформація можуть призвести до неправильних рішень;

2) складність оцінки потенційних збитків – операційний ризик може мати безліч потенційних наслідків, включаючи фінансові, репутаційні та юридичні наслідки. Оцінка потенційних збитків може бути складною через багато факторів, які можуть вплинути на кінцеві витрати;

3) недостатня стандартизація -оцінювання операційного ризику може бути складним завданням через недостатню стандартизацію методів та метрик. Це може призвести до того, що різні компанії можуть застосовувати різні підходи до оцінювання ризику, що робить порівняння таких даних важким.

В цілому, законодавство України передбачає порядок створення системи управління ризиками та її архітектуру, але і дає можливість самостійно обирати підходи щодо виявлення, вимірювання, моніторингу, контролю, звітування,вибору критеріїв визначення значних подій операційного ризику, порядку їх дослідження, підходів щодо здійснення стрес-тестування тощо. Тобто законодавством регламентовано які саме процедури мають відбуватися, але за банками лишається можливість обирати спосіб реалізації цих процедур, відповідно до власних потреб і особливостей бізнес-моделі. З одного боку, це дає можливість банкам швидко реагувати на зміни, доналаштовуючи систему управління ризиками відповідно до сучасних викликів. А з іншого боку, це призводить до урізноманітнення підходів, критеріїв оцінки, метрик тощо.

Висновки. Щоб зберегти операційну ефективність, банки мають пристосувати свої бізнес-моделі до роботи в сучасних висококонкурентних умовах. Через це, в банківському секторі відбувається приоритезація напрямків розвитку в бік цифрової трансформації. Основні зусилля спрямовані на розвиток платіжно-розрахункових систем, розвиток цифрового банкінгу та інше. З одного боку це дозволяє розширювати клієнтську базу, збільшувати частку ринку, підвищувати фінансову стійкість та безпеку. А з іншого, цифрові технології, зумовлені недосконалою побудовою бізнес-процесів та перебоями в роботі інформаційних систем, стають вагомим джерелом операційного ризику, який стрімко зростає на тлі військових дій в країні. Враховуючу складну передбачуваність таких ризиків, банкам необхідно приділити особливу увагу вдосконаленню системи управління операційними ризиками, впровадженню нових технології та інструментів для покращення управління ризиками, таких як штучний інтелект та аналіз даних, забезпеченню належного рівня кваліфікації персоналу, вдосконаленню системи кіберзахисту. Особливої актуальності у воєнний час, набуває необхідність підтримки безперервної роботи сервісів та збереження інформації, тому слід звернути увагу на можливість впровадження резервного розгортання всіх електронних процесів банків у хмарних сервісах за межами країни, що в разі руйнування фізичної інфраструктури, дасть можливість швидко відновити штатне функціонування і зберегти всю інформацію. Перспективи подальших досліджень даної теми, полягають у розробці теоретичних та практичних рекомендацій, направлених на створення уніфікованих методики та інструментів раннього виявлення та запобігання операційних ризиків, з метою мінімізації потенційних втрат, створення загальнонаціонального реєстру інцидентів, який надасть можливість використовувати досвід всіх учасників ринку.

Список літератури:

1. Дмитров С.О. Моделювання оцінки операційного ризику комерційного банку. Суми : Українська академія банківської справи Національного банку України, 2010. С. 6–23, 52 с.
2. Коваленко В.В. Система ризик-менеджменту в банках: теоретичні та методологічні аспекти : монографія. Одеса : ОНЕУ, 2017. С. 192–212.
3. Шульга Н.П., Міщенко В.І., Анісімова Л.Л. та ін. Інтегрована система управління ризиками банку : монографія / за заг. ред. Шульги Н.П. Київ : Київ. нац. торг.-екон. ун-т, 2018. С. 7–25.
4. Камінський А., Кияк А. Ідентифікація, аналіз та управління операційними ризиками в українських банках. *Вісник НБУ*. 2005. № 10. С. 7–11.
5. Набок Р. Окремі питання управління операційним ризиком у банках. *Вісник Національного банку України*. 2013. № 1. С. 61–65.
6. Криклій О.А. Інструментарій оцінки операційного ризику банку. *Економічний аналіз*. 2011. № 1(9). С. 168–172.
7. Дмитров С.О. Моделювання оцінки операційного ризику комерційного банку» Суми : Українська академія банківської справи Національного банку України, 2010. С. 8.
8. Тарнавський М. Мінімальні вимоги до капіталу. URL: https://bank.gov.ua/admin_uploads/article/Risks_%D0%A2%D0%B0%D1%80%D0%BD%D0%B0%D0%B2%D1%81%D1%8C%D0%BA%D0%B8%D0%B9_VV.pdf?v=4 (дата звернення: 16.03.2023).
9. Основні принципи ефективного банківського нагляду (Основні Базельські принципи). URL: https://bank.gov.ua/admin_uploads/article/Basel_Core_principles_2012.pdf (дата звернення: 16.03.2023).
10. Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework. Basel Committee on Banking Supervision. URL: https://www.bis.org (дата звернення: 16.03.2023).
11. Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах : Постанова правління НБУ № 64 від 11.06.2018 року.
12. Кльоба Л.Г. Цифровізація – інноваційний напрям розвитку банків. *Ефективна економіка*. 2018. № 12. URL: http://www.economy.nayka.com.ua/?op=1&z=6741 DOI: https://doi.org/10.32702/2307-2105-2018.12.84 (дата звернення: 16.03.2023).
13. Кочума І.Ю. Вплив цифровізації банківського сектору на трансформацію зайнятості за сучасних умов. *Фінансовий простір*. 2021. № 4(44). С. 149–158. DOI: https://doi.org/10.18371/fp.4(44).2021.149158 URL: http://fpnpu.cibs.ubs.edu.ua/article/view/249578
14. НБУ та Мінцифри спільно працюють над цифровізацією банківської системи України. URL: https://bank.gov.ua/ua/news/all/nbu-ta-mintsifri-spilno-pratsyuyut-nad-tsifrovizatsiyeyu-bankivskoyi-sistemi-ukrayini (дата звернення: 16.03.2023).
15. The bank business model in the post-Covid-19 world. URL: https://cepr.org/voxeu/columns/bank-business-model-post-covid-19-world (дата звернення: 16.03.2023).
16. Insights into Material Risks 2022 Public Report. Pdf. URL: https://engage.orx.org/thank-you/download-the-orx-scenarios-insights-into-material-risks-2022?submissionGuid=9996cbee-03e0-456c-b5c6-02789e82592c (дата звернення: 16.03.2023).

References:

1. Dmytrov S.O. (2010) Modeliuvannia otsinky operatsiinoho ryzyku komertsiinoho banku [Modeling the assessment of operational risk in a commercial bank]. Sumy: Ukrainian Academy of Banking of the National Bank of Ukraine, pp. 6–23, 52 p.
2. Kovalenko V.V. (2017) Systema ryzyk-menedzhmentu v bankakh: teoretychni ta metodolohichni aspekty [Risk management system in banks: theoretical and methodological aspects]: monograph. Odesa: ONEU, pp. 192–212.
3. Shulha N.P., Mishchenko V.I., Anisimova L.L. (ed.) (2018) Intehrovana systema upravlinnia ryzykamy banku [Integrated risk management system of a bank]: monohrafiia / ed. by Shulha N.P. Kyiv: Kyiv National Trade and Economic University, pp. 7–25
4. Kaminskii A., Kiiak A. (2005) Identifikatsiia, analiz ta upravlinnia operatsiinymy ryzykamy v ukrainskykh bankakh [Identification, analysis, and management of operational risks in Ukrainian banks]. *Visnyk NBU*, no. 10, pp. 7–11.
5. Nabok R. (2013) Okremi pytannia upravlinnia operatsiinym ryzykom u bankakh. [Specific issues of operational risk management in banks]. *Visnyk Natsionalnoho banku Ukrainy*, no. 1, pp. 61–65.
6. Kryklii O.A. (2011) Instrumentarii otsinky operatsiinoho ryzyku banku. [Toolkit for evaluating bank operational risk]. *Ekonomichnyi analiz,* no. 1(9), pp. 168–172.
7. Dmytrov S.O. (2010) Modeliuvannia otsinky operatsiinoho ryzyku komertsiinoho banku [Modeling the assessment of operational risk in a commercial bank]. Sumy: Ukrainian Academy of Banking of the National Bank of Ukraine, p. 8.
8. Tarnavskyi M. Minimalni vymohy do kapitalu [Minimum capital requirements]. Available at: https://bank.gov.ua/admin_uploads/article/Risks_Tarnavsky_VV.pdf?v=4 (accessed 16 March 2023).
9. Osnovni pryntsypy efektyvnoho bankivskoho nahliadu (Osnovni Bazelski pryntsypy) [Core Principles for Effective Banking Supervision (Basel Core Principles)]. Available at: https://bank.gov.ua/admin_uploads/article/Basel_Core_principles_2012.pdf (accessed 16 March 2023).
10. Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework. Basel Committee on Banking Supervision. Available at: http://www.bis.org (accessed 16 March 2023).

11. Pro zatverdzhennia Polozhennia pro orhanizatsiiu systemy upravlinnia ryzykamy v bankakh Ukrainy ta bankivskykh hrupakh: Postanovy pravlinnia NBU № 64 vid 11.06.2018 roku [On the approval of the Regulation on the organization of risk management systems in banks of Ukraine and banking groups].

12. Klioba L.H. (2018) Tsyfrovizatsiia – innovatsiinyi napriam rozvytku bankiv [Digitization as an innovative direction for the development of banks]. *Efektyvna ekonomika*, no. 12. Available at: http://www.economy.nayka.com.ua/?op=1&z=6741 DOI: https://doi.org/10.32702/2307-2105-2018.12.84 (accessed 16 March 2023).

13. Kochuma I.Yu. (2021) Vplyv tsyfrovizatsii bankivskoho sektoru na transformatsiiu zainiatosti za suchasnykh umov [The impact of digitization on the transformation of employment in the banking sector under modern conditions]. *Finansovyi prostir*, no. 4(44), pp. 149–158. Available at: http://fpnpu.cibs.ubs.edu.ua/article/view/249578 DOI: https://doi.org/10.18371/fp.4(44).2021.149158 (accessed 16 March 2023).

14. NBU ta Mintsifri spilno pratsiuiut nad tsyfrovizatsiieiu bankivskoi systemy Ukrainy [NBU and the Ministry of Digital Transformation work together on the digitalization of the banking system of Ukraine]. Available at: https://bank.gov.ua/ua/news/all/nbu-ta-mintsifri-spilno-pratsyuyut-nad-tsifrovizatsiyeyu-bankivskoyi-sistemi-ukrayini (accessed 16 March 2023).

15. The bank business model in the post-Covid-19 world. Available at: https://cepr.org/voxeu/columns/bank-business-model-post-covid-19-world (accessed 16 March 2023).

16. Insights into Material Risks 2022 Public Report. Pdf. Available at: https://engage.orx.org/thank-you/download-the-orx-scenarios-insights-into-material-risks-2022?submissionGuid=9996cbee-03e0-456c-b5c6-02789e82592c (accessed 16 March 2023).