

ТРАНСФОРМАЦІЙНА ПРИРОДА ОПЕРАЦІЙНИХ РИЗИКІВ КОМЕРЦІЙНИХ БАНКІВ

TRANSFORMATIONAL NATURE OF OPERATIONAL RISKS OF COMMERCIAL BANKS

Абрамова А. С.

кандидат економічних наук, доцент,
Чернівецький національний університет
імені Юрія Федьковича,
м. Чернівці, Україна
ORCID: 0000-0003-3364-8316

Alla Abramova

PhD (Economics), Associate Professor,
Yuri Fedkovych National University of Chernivtsi,
Chernivtsi, Ukraine

Нові явища в економіці, її інформаційне забезпечення та застосування нових технологій чинять значний вплив на сферу банківської діяльності. Зростає значимість стратегічного вибору та пошуку нових пріоритетних моделей розвитку банківського бізнесу в умовах цифровізації. Використовуючи досконаліші технології, банки здатні знижувати витрати реалізації основних продуктів, послуг та збільшувати доходи за ними, а клієнти отримують кращі умови обслуговування та вищий ступінь гарантій. Спостерігається значний попит на послуги дистанційного банківського обслуговування. Зазначають суттєвих змін характер та масштаби ризиків банківської діяльності. Зазначені обставини визначають необхідність перетворення банківських бізнес-моделей у відповідності вимог середовища та реалізації нових завдань для регуляторів даних процесів. У статті досліджено природу операційних ризиків та процеси їх цифровізації. Встановлено коло нових видів ризиків, пов'язаних з цифровізацією: кіберризик як результат цифрових атак, ризики функціональної моделі банківського обслуговування та ризики зараження і пошкодження персональних даних клієнтів та звітних даних діяльності комерційних банків. Представлено авторське бачення напрямків мінімізації їх негативних впливів шляхом удосконалення операційної діяльності, швидкого реагування на підозрілі процеси у банківських операціях та підвищення стійкості бізнес-процесів комерційних банків, поглиблення систем внутрішньої аналітики та миттєвого звітування про визначені види ризиків в режимі on-line на основі використання великих сховищ даних, блок-чейн, а також посилення контролю за ризиками людського фактору як зі сторони банківського персоналу, так і клієнтської аудиторії.
Ключові слова: операційні ризики, цифровізація, кіберризик, цифрова модель, ризик зараження, сховище даних, блокчейн.

New phenomena in the economy, its information support and the use of new technologies have a significant impact on the sphere of banking activity. The importance of strategic choice and the search for new priority models of banking business development in the conditions of digitalization is increasing. By using more advanced technologies, banks are able to reduce the cost of selling basic products and services and increase their revenues, while clients receive better service conditions and a higher degree of guarantees. There is a significant demand for remote banking services. The nature and scale of banking risks are undergoing significant changes. The specified circumstances determine the need to transform banking business models in accordance with the requirements of the environment and to implement new tasks for the regulators of these processes. The article examines the nature of operational risks and processes of their digitalization. A range of new types of risks associated with digitalization has been established: cyber risk as a result of digital attacks, risks of the functional model of banking services, and risks of infection and damage to personal data of clients and reporting data of commercial banks. The author's vision of ways to minimize their negative effects by improving operational activities, quickly responding to suspicious processes in banking operations and increasing the stability of business processes of commercial banks, deepening internal analytics systems and instant reporting on certain types of risks in online mode based on the use of large data warehouses, block chain, as well as strengthening control over the risks of the human factor both on the part of the bank staff and the client audience.
Key words: operational risks, digitization, cyber risk, digital model, infection risk, data storage, blockchain.

Постановка проблеми. Швидкоплинність та мінливість ділового середовища вимагає нових підходів до управління операційними ризиками комерційних банків. Новітні технології, розширений доступ до баз даних, нові види бізнесу спонукають до перегляду методик та підходів обслуговування потенційних клієнтів, визначають особливі умови банківської діяльності, застосування специфічних засобів контролю та ефективних підходів в мінімізації операційних ризиків.

Операційний ризик є молодого галуззю сфери управління банку, однак, потребує розробки та застосування специфічного інструментарію його мінімізації. Сьогодні зупиняться лише на контролі банківської звітності та простій оцінці ризиків недостатньо. І хоча значні інвестиційні вкладення в ідентифікацію, оцінку та боротьбу з операційними ризиками вже дали позитивні результати, проте збитки від ризиків залишаються високими. Ситуація ускладнюється тим, що сучасні операційні ризики включають десятки підвидів (ризики кібербезпеки, IT-ризики, кіберураження, упередженості рішень штучного інтелекту та етичного використання клієнтської інформації), управління ними вимагає нагляду і прозорості всіх організаційних та бізнес-процесів. І хоча діджиталізація та автоматизація банківських операцій змінюють характер роботи банків, показники рівня їх операційних ризиків продовжують зростати.

Вказані аргументи визначають актуальність дослідження та необхідність прийняття відповідних результативних управлінських рішень. Відповідно існує потреба у проведенні додаткових наукових досліджень за вказаною тематикою, особливо у напрямку застосування інструментарію мінімізації цифрових операційних ризиків.

Аналіз останніх досліджень і публікацій. Питання цифровізації банківської діяльності присвячені праці широкого кола науковців, зокрема: Козляченко О. М., Коваленко В. В., Корнівської В. О., Онищенко Ю. І., Романовської Ю. А., Холявко Н. І., Шелудько С. А. та ін. Серед авторів, які вивчають питання сучасних проблем управління операційними ризиками комерційних банків, відзначено Бойко А. О., Дмитрова О. С., Гончарова К. Г., Коваленко В. В., Олійник А. В., Юдіна С. В., Нагорнюк Г. О. та ін.

Виділення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття. Вивчаючи заявлені проблеми, постає необхідність удосконалення інструментарію та підходів до управління операційними ризиками банків відповідно до трансформаційного середовища ведення банківського бізнесу.

Формулювання цілей статті (постановка завдання). Мета дослідження визначена необхідністю удосконалення процесів управління

операційними ризиками банків за принципами партнерства з бізнесом у режимі реального часу та швидкої реакції на виникаючі проблеми чи стійкі загрози.

Виклад основного матеріалу дослідження. Операційні ризики притаманні всім банківським продуктам, видам діяльності, процесам і системам, відповідно ними потрібно ретельно керувати. Традиційно процес управління операційними ризиками спрямований на захист комерційних банків від потенційних втрат, а також збільшення економічної цінності їх діяльності. Досліджуючи практичні аспекти діяльності встановлено, що у процесі управління операційними ризиками банків виділено шість головних кроків, зокрема: ідентифікація, оцінка, вимірювання, контроль та згладжування наслідків, моніторинг та створення плану безперервності мінімізації негативного впливу.

Сьогодні більшість банків пропонують послуги електронного банкінгу, за допомогою яких клієнти можуть отримати доступ до своїх рахунків, оплачувати їх та переказувати кошти. З появою цифровізації, еволюції суспільства та технологій загалом, клієнти вимагають вищого рівня обслуговування, цінності та довіри. Це змушує банки переосмислити свої бізнес-моделі, процеси і системи та працювати з новими операційними ризиками.

Детальніше наголосимо на сутності «операційного ризику» та «цифровізації». Так, згідно положень Базелі III це: «Ризик прямих або непрямих збитків виникають у результаті неадекватних або невдалих внутрішніх процесів, людей і систем, або через зовнішні події» [1]. Згідно тверджень словника: «Цифровізація – це використання цифрових технологій для зміни бізнес-моделі з метою створення нових можливостей отримання доходу та створення вартості» [10].

Використання цифрових каналів банківських продуктів та послуг спричиняє розвиток ризиків і виникнення нових. Тому ризик-менеджери витрачають більше часу на їх виявлення, оцінку та мінімізацію їх впливу. Ці ризики не є по-справжньому «новими», вони еволюціонують і збільшуються у результаті структурних змін у зв'язку з цифровізацією бізнес-моделей. Проте виникли і нові ризики, пов'язані з цифровізацією: кіберризик, ризики функціональної моделі та ризики зараження.

1. Кіберризик – відноситься до будь-якого ризику фінансових втрат, руйнування або шкоди репутації організації через збій її системи інформаційних технологій [3]. Він є найбільш важливим з огляду на велику кількість даних, які обробляються. Він є дороговартісним для банків, а атаки не лише порушують їх роботу, але й призводять до ризику втрати і розголошення даних клієнтів.

Враховуючи нинішній геополітичний контекст, не дивно, що в наступні роки рівень кібербезпеки банків буде тільки зростати. Це може відбуватися не лише на інституційному рівні, а й у всій галузі між банками.

2. Ризик цифрової функціональної моделі – визначається як потенційна втрата, з якою може зіткнутися банк через неправильне використання або помилки, що мають місце при розробці або впровадженні функціональної цифрової моделі, які, в основному, використовуються для обробки даних та прийняття рішень. Так, модель підходу до розподілу збитків або модель інтеграції може використовуватися для регулювання, управлінських та бухгалтерських цілей. Кількість моделей у великих банках зростає, стають складнішими і керувати цими ризиками важче. Причинами є ненадійні дані, погана їх якість, технічні дефекти та помилки впровадження.

3. Ризик зараження – відноситься до можливості того, що негативні події в одному файлі поширюються на інші та впливають на фінансові результати та вимоги до капіталу. Цифрові та автоматизовані процеси будуть діяти як каталізатори і збільшуватимуть швидкість їх поширення. Комерційні банки повинні розуміти шляхи зараження та застосовувати ефективні засоби мінімізації негативних наслідків впливу.

Вважаємо, що кіберризик, ризик функціональної моделі та ризик зараження не обов'язково є «новими», однак їхнє зростаюче значення та вплив на діяльність банківських установ значно змінився. За таких обставин надійний процес управління ними має важливе значення для гарантії раннього виявлення та впровадження найкращих процедур мінімізації збитків.

На нашу думку, процеси цифровізації у системі управління операційними ризиками, реалізуючи стратегію та тактику, повинні враховувати наступні засади:

1. Дані, які банки генерують і мають під своїм контролем, постійно зростають та диференціюються (стенограми чатів або кліки). Тому процес управління ризиками повинен мати стійкий підхід і чітко визначений процес для обробки та використання інформації. Необхідно, щоб менеджери з ризиків визначали, оцінювали та вибирали правильний тип даних для прийняття своєчасних і точних рішень. Розгортання процесів цифровізації спричинить нові ризики, а банкам потрібно буде їх вимірювати, що створить потребу в нових типах даних.

2. Використання автоматизованого технологічного процесу – за рахунок роботизації зменшує потребу у ручному втручанні у ризикові види діяльності за рахунок зменшення кількості неточностей і тривалості процесу, які можуть використовувати менеджери операційних ризиків. Оптичне

розпізнавання символів зможе читати та розуміти документи в цифровому вигляді для вилучення даних.

3. Результативною сьогодні є технологія блокчейн (Blockchain) – як форма непідкупної децентралізованої розподіленої книги зі списком транзакцій, яка тиражується, підтримується та перевіряється одночасно кількома зацікавленими сторонами. Ця технологія надзвичайно цікава для ризик-менеджерів з трьох причин:

1) це безпечна система завдяки своєму технологічному шифруванню та підтримці смарт-контрактів;

2) завдяки високому рівню безпеки ризик-менеджерам простіше встановлювати автоматизований контроль і впроваджувати вбудований рівень управління ризиками безпосередньо в Blockchain;

3) це дозволить ризик-менеджерам знизити свої витрати (завдяки автоматичному виконанню або звірці).

Збільшення обсягу даних створює тиск на інфраструктуру банків через велику кількість джерел таких даних. Перебудова інфраструктури даних є ключовою метою для банків, які прагнуть цифровізувати свою бізнес-модель, включаючи процес управління ризиками. Гібридне середовище даних на основі обробки в режимі реального часу та меншої вартості зберігання даних за принципом єдиного сховища є шляхом вирішення проблем управління ризиками.

4. «Розумна» візуалізація та інтерфейси дозволяють користувачам отримувати доступ до інформації та даних легшим і персоналізованим способом. Такими технологіями можуть бути інформаційні панелі – реалізують взаємозв'язок між інструментами або доповнену реальність. Менеджери операційних ризиків можуть персоналізувати дані та інформацію, щоб покращити прийняття рішень. Ці інструменти дозволяють користувачам приймати більш точні та швидші рішення. Зважаючи на те, що управління ризиками в банках загалом є консервативним, ці інструменти допоможуть змінити та модернізувати процес.

Невід'ємною складовою процесів діджиталізації банківських процесів, відповідно, операційних ризиків, є зовнішня екосистема, яка забезпечує доступ до зовнішніх постачальників інформаційних даних та рекомендаційних схем управління, зокрема, альтернатива управлінських рішень у різних сферах банківської діяльності (підтримка даних про ризики, розробка технологій або зменшення ризику операційних втрат).

Сьогодні між комерційними банками все більше посилюється співпраця з питань ризику та регулювання – банки можуть мати доступ до даних, які зберігаються на спільних платформах. Такі утиліти можуть бути корисними для протидії

таким ризикам, як кіберризик, і дозволять банкам обмінюватися аналітикою та даними, пов'язаними з ними, щоб відповідати вимогам нагляду за дотриманням вимог. Однак банки повинні уважно проаналізувати потенційний розвиток ІТ та кіберризику, а також ризики, які можуть виникнути у ході такої співпраці – вони також повинні перевірити, чи ці альянси не ставлять під загрозу будь-які конкурентні переваги для банку.

5. Корпоративна культура, яка вимагатиме від співробітників потужних аналітичних навичок. Доведеться змінити методи найму персоналу, запровадити специфічний процес навчання, який дозволить нинішнім працівникам вдосконалюватися у цій галузі.

Вважаємо, що систему удосконалення боротьби та мінімізації операційних ризиків в умовах цифровізації банківської діяльності необхідно розвивати за наступними напрямками:

1) удосконалення операційної діяльності та підвищення стійкості бізнес-процесів банків шляхом побудови дорожньої карти процесів, ризиків та засобів контролю, визначення допоміжних технологій виявлення ризиків, встановлення ресурсів та засобів контролю та нагляду;

2) поглиблення систем внутрішньої аналітики та звітування про ризики в режимі on-line на основі використання великих сховищ даних. Індикатори ризику включають діагностику операційних процесів і засобів контролю, зони стресу операційної діяльності, стрибки в обсягах транзакцій та інші показники рівнів ризику (незаконні банківські операції, кіберризик, кібератаки, електронне шахрайство та поведінкові ризики, відмивання грошей);

3) посилені контроль за ризиками людського фактору – співробітники банку є потенційним джерелом операційного ризику. Розробка ефективної системи нагляду за ризиками

людського фактору є непростим завданням. Деякі пов'язані з поведінковими порушеннями серед працівників; інші передбачають зловживання внутрішніми організаційними знаннями та пошук шляхів обходу статичного контролю. Комерційні банки повинні інтегрувати персонал та роботу служби операційного ризику у напрямку забезпечення гнучкості розробки, дослідження даних і міждисциплінарної командної роботи.

Висновки. Розвиток технологій та цифровізація глибоко інтегрувалися у банківську діяльність. Досліджуючи практичні аспекти функціонування банків встановлено шість головних кроків управління їх операційними ризиками, зокрема: ідентифікація, оцінка, вимірювання, контроль та згладжування наслідків, моніторинг та створення плану безперервності мінімізації негативного впливу. Через призму вивчення природи «операційного ризику» та «цифровізації» визначено такі нові важливі ризики операційної діяльності банків, як: кіберризик, ризики функціональної моделі та ризики зараження.

Запропоновано авторське бачення процедур управління операційними ризиками в умовах діджиталізації на основі засад стійкого підходу і чітко визначеного процесу обробки та використання інформаційних банківських даних, посилення автоматизації технологічних банківських процесів на основі роботизації, технологій блокчейн, «розумної» візуалізації та інтерфейсів, співпраці комерційних банків з питань операційних ризиків та їх регулювання, а також контролю за реалізацією банківської культури працівників банків.

Перспективи подальших досліджень вбачаємо у поглибленні підходів щодо деталізації інструментарію управління банківськими операційними ризиками в умовах цифровізації та автоматизації банківських процесів.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Коваленко В.В. Розвиток FinTech: загрози та перспективи для банків України. *Приазовський економічний вісник*. 2018. № 4(9). URL : http://pev.kpu.zp.ua/journals/2018/4_09_uk/24.pdf.
2. Корнівська В.О. Цифровий банкінг: ризики фінансової дигіталізації. *Проблеми економіки*. 2017. № 3. С. 254-261.
3. Олійник А.В. Інструменти управління операційним ризиком банку. URL: http://elar.khmnmu.edu.ua/jspui/bitstream/123456789/9760/1/tz_oliinyk_a_v.pdf.
4. Онищенко Ю.І. Банківська діяльність в умовах розвитку цифрових технологій. *Вісник ОНУ ім. І.І. Мечникова*. 2018. Т. 23. Вип. 8(73). С. 160-165.
5. Романовська Ю.А. Діджиталізація банківського сектору в умовах пандемії. *Економіка та суспільство*. 2022. Випуск № 36. URL: <https://webcache.googleusercontent.com/search?q=cache:x6aNemQLd44J:https://economyandsociety.in.ua/index.php/journal/article/download/1120/1077+&cd=4&hl=uk&ct=clnk&gl=ua>. DOI: <https://doi.org/10.32782/2524-0072/2022-36-4>.
6. Холявко Н.І., Козляниченко О.М. Світові тенденції діджиталізації банківського сектору. *Проблеми економіки*. 2021. № 2 (48). С. 217-224. DOI: <https://doi.org/10.32983/2222-0712-2021-2-217-224>.
7. Шелудько С.А., Браткевич П.П. Вплив цифровізації на банківський бізнес в Україні. *Приазовський економічний вісник*. 2019. Вип. 5(16). С. 334-339. DOI: <https://doi.org/10.32840/2522-4263/2019-5-57>.
8. Юдіна С.В., Нагорнюк Г.О. Проблеми визначення та управління операційними ризиками комерційних банків. *Науковий вісник Ужгородського національного університету*. 2019. Випуск 26. Ч. 2. С. 125-130.
9. Basel III: international regulatory framework for banks. URL : <https://www.bis.org/bcbs/basel3.htm>.
10. Gartner it glossary. Digitalization - Gartner IT Glossary. URL: <https://www.gartner.com/it-glossary/digitalization>.

REFERENCES:

1. Kovalenko, V.V. (2018). Rozvytok FinTech: zahrozy ta perspektyvy dlia bankiv Ukrainy [Development of FinTech: threats and prospects for Ukrainian banks]. *Pryazovskyi ekonomichnyi visnyk – Pryazovsky Economic Bulletin*, 4(9). URL: http://pev.kpu.zp.ua/journals/2018/4_09_uk/24.pdf.
2. Kornivska, V.O. (2017). Tsyfrovyyi bankinh: ryzyky finansovoi dyhitalizatsii [Digital banking: risks of financial digitization]. *Problemy ekonomiky – Problems of the economy*, 3, 254-261.
3. Oliinyk, A.V. (2018). Instrumenty upravlinnia operatsiinym ryzykom banku [Bank operational risk management tools]. URL: http://elar.khmnu.edu.ua/jspui/bitstream/123456789/9760/1/tz_oliinyk_a_v.pdf.
4. Onyshchenko, Yu.I. (2018). Bankivska diialnist v umovakh rozvytku tsyfrovoykh tekhnolohii [Banking activity in the conditions of the development of digital technologies]. *Visnyk ONU im. I.I. Mechnykova – Bulletin of ONU named after I.I. Mechnikova*, 8(73), 160-165.
5. Romanovska, Yu.A. (2022). Didzhitalizatsiia bankivskoho sektoru v umovakh pandemii [Digitization of the banking sector in the conditions of the pandemic]. *Ekonomika ta suspilstvo – Economy and society*, 36. URL: <https://webcache.googleusercontent.com/search?q=cache:x6aNemQLd44J:https://economyandsociety.in.ua/index.php/journal/article/download/1120/1077+&cd=4&hl=uk&ct=clnk&gl=ua>. DOI: <https://doi.org/10.32782/2524-0072/2022-36-4>.
6. Kholiavko, N.I., Kozlianchenko, O.M. (2021). Svitovi tendentsii didzhitalizatsii bankivskoho sektora [World trends of digitization of the banking sector]. *Problemy ekonomiky – Problems of the economy*, 2 (48), 217-224. DOI: <https://doi.org/10.32983/2222-0712-2021-2-217-224>.
7. Sheludko, S.A., Bratkevych, P.P. (2019). Vplyv tsyfrovizatsii na bankivskyi biznes v Ukraini [The impact of digitization on the banking business in Ukraine]. *Pryazovskyi ekonomichnyi visnyk – Pryazovsky Economic Bulletin*, 5(16), 334-339. DOI: <https://doi.org/10.32840/2522-4263/2019-5-57>.
8. Iudina, S.V., Nahorniuk, H.O. (2019). Problemy vyznachennia ta upravlinnia operatsiinymy ryzykamy komertsiiinykh bankiv [Problems of determining and managing operational risks of commercial banks]. *Naukovyi visnyk Uzhhorodskoho natsionalnogo universytetu – Scientific Bulletin of the Uzhhorod National University*, 26, 125-130.
9. Basel III: international regulatory framework for banks. URL: <https://www.bis.org/bcbs/basel3.htm>.
10. Gartner it glossary. Digitalization - Gartner IT Glossary. URL: <https://www.gartner.com/it-glossary/digitalization>.