

DOI: 10.25140/2411-5215-2021-4(28)-186-193

УДК 330.33.012

JEL Classification: G10

Алла Абрамова

кандидат економічних наук, доцент,
доцент кафедри публічних, корпоративних фінансів та фінансового посередництва
Чернівецький національний університет імені Юрія Федьковича (Чернівці, Україна)
E-mail: alla1labramova@ukr.net. **ORCID:** <https://orcid.org/0000-0003-3364-8316>
Scopus ID: [57213158224](https://scopus.com/authid/detail.uri?https://orcid.org/0000-0003-3364-8316). **ResearcherID:** [W-2085-2017](https://pubs.rsos.royalsocietypublishing.org/author/W-2085-2017)

СИСТЕМА РИЗИКІВ ДІЯЛЬНОСТІ КОМЕРЦІЙНИХ БАНКІВ В УМОВАХ ЦИФРОВІЗАЦІЇ

У статті представлено основні тенденції банківської діяльності в сучасних глобалізаційних умовах господарювання. Досліджено теоретичні засади природи ризиків банківської діяльності та здійснено їх класифікацію. Визначено категорії найбільш впливових серед них, зокрема: стратегічні ризики, операційні ризики, зростаючі труднощі у виконанні комплаєнс-вимог та стандартів, комплаєнс-ризик, ризики третіх сторін, кіберризики, ризик ліквідності та ризики, пов'язані з використанням хмарних технологій. Це дало можливість систематизувати та поглибити положення контролінгу та менеджменту діяльності банків. Представлено механізм управління ризиками цифровізації в комерційних банках. Таким чином, лише правильний підхід та підбір елементів та інструментів управління ризиками банківської діяльності в майбутньому може забезпечити стабільність та ефективність функціонування.

Ключові слова: ризики; цифровізація; причини ризиків; види ризиків; контролінг; управління ризиками.

Рис.: 1. Бібл.: 17.

Постановка проблеми. Кризово-пандемійні умови діяльності зумовлюють формування особливого інформаційного забезпечення та застосування нових технологій, які чинять значний вплив на всі сфери господарювання, зокрема сферу банківської діяльності. Зростає важливість стратегічного вибору та пошуку нових пріоритетних моделей розвитку банківського бізнесу в умовах цифровізації. Використовуючи досконаліші технології, банки здатні знижувати витрати та збільшувати доходи, а клієнти, у свою чергу, частіше отримують від використання кращі, ніж раніше, умови.

Одночасно спостерігається значний попит на послуги дистанційного банківського обслуговування. Сьогодні більшість клієнтів комерційних банків користуються мобільним банкінгом, обираючи смартфон як кращий метод для отримання банківських послуг та здійснення банківських операцій. Однак зазнають суттєвих змін характер та масштаби ризиків, до яких схильні банківські інститути в умовах розвитку цифрових технологій. Усе це зумовлює не тільки перетворення банківських бізнес-моделей, а також виникнення нових завдань управління та контролінгу.

Регулювання складної комбінації технологічних та конкурентних змін може адекватно здійснюватися лише в тому випадку, якщо належним чином буде враховано особливості нової фінансової діяльності. Багато нововведень, пов'язаних із цифровізацією, не можуть бути розглянуті через призму традиційних підходів управління. Наглядово-контрольні органи повинні відстежувати такі технологічні проблеми та розробляти відповідні маршрути управлінського реагування. У зв'язку з цим проблема трансформації банківського управління в умовах цифровізації та пошуку ефективних механізмів її здійснення є досить актуальною.

Аналіз останніх досліджень та публікацій. Вплив цифрових технологій на банківську діяльність та трансформацію банківських бізнес-моделей досліджували закордонні автори V. A. Shestak, A. G. Volevodz, V. A. Alizade та інші, а також вітчизняні вчені В. Гончарук, А. Долгушина, М. Івлєва, А. Писарев, О. Соснін та інші. У своїх роботах В. Гончарук, М. Івлєва розглядаються ризики, супутні впровадження цифрових технологій у банківську діяльність.

Виділення недосліджених частин загальної потреби. Аналіз праць науковців та практиків виявив, що досі недостатньо дослідженими залишаються питання трансформації банківського управління та контролю в умовах розвитку цифрових технологій. Зокрема, не встановлено, які законодавчі та практичні заходи необхідно здійснити для забезпечення умов розвитку інновацій у банківському секторі за умов мінімізації управлінських ризиків.

Мета статті. Метою статті є розробка теоретико-методичних положень та практичних рекомендацій щодо управління банківськими ризиками в умовах цифровізації.

Виклад основного матеріалу. У сучасних умовах діяльності комерційних банків цифровізація процесів прийняття рішень та різноманітних операцій допомагає зберегти клієнтську базу та розширити банківський бізнес за допомогою нових електронних каналів та онлайн-кредитування. Це сприяє підвищенню ефективності та конкурентоспроможності банків, а також скороченню часу на обслуговування клієнтів. Створення платформ для банків підвищує їх привабливість для клієнтів та зацікавлених сторін взаємопов'язаного бізнесу, надаючи тим самим можливості для створення екосистеми банків. Соціальні фактори та розвиток нових цифрових інформаційних технологій позитивно впливають на інвестиції в банки.

Перспектива створення нових сервісів, таких як онлайн-облік, оперативний облік, оподаткування, прогнозування прибутку, створення екосистем, дає можливість враховувати потреби клієнтів у майбутньому. Однак оцифрування даних створює близько 70 % цифрових ризиків для банків. За даними аналізу, 22 % банків у всьому світі інвестували понад 25 % свого річного бюджету на оцифрування управління ризиками [1].

Ключовими трендами банківської цифровізації в Україні сьогодні є: оптимізація віддаленої роботи працівників банку, зростання операцій онлайн, спрощення доступу до послуг банку, розвиток каналів дистанційного продажу, боротьба з шахраями та хакерами, широке застосування технологій штучного інтелекту, перехід до управління на основі даних, програми тотальної персоніфікації, імпортозаміщення, розвиток екосистем, розробка власного програмного забезпечення та зростання потреби в ІТ-фахівцях

І хоча інноваційні банківські технології відкривають нові можливості, вони також створюють нові джерела ризиків. Як зазначає у своєму звіті Базельський комітет із банківського нагляду, банки, що покладаються на інноваційні технології, повинні забезпечувати ефективні процеси управління ризиками, а також системи контролю, які ефективно усувають джерела їх виникнення [13; 16].

Характер і масштаби ризиків, яким піддаються банківські інститути в їхній традиційній діяльності, зазнають суттєвих змін за умов розвитку цифрових технологій. Існує тезис, що впровадження цифрових технологій чинить найбільший вплив на категорію нефінансових ризиків, зокрема на кібербезпеку, комплаєнс-ризик, ризик шахрайства, а також ризик, пов'язані зі схильністю банків бути учасниками процесів відмивання коштів, отриманих незаконним шляхом та фінансування тероризму.

Найбільш значущим дослідженням, присвяченим аналізу впливу фінтеху на банківську діяльність (у тому числі трансформації банківських ризиків) є документ Базельського комітету з банківського нагляду [10]. Відповідно до нього, ключовими ризиками, пов'язаними з розвитком цифрових технологій, визначається стратегічний ризик, операційний ризик, кіберризик, комплаєнс-ризик.

Ще одним вагомим дослідженням є глобальний огляд банківського ризик-менеджменту, підготовлений аудиторською та консалтинговою компанією Ernst & Young спільно з Інститутом міжнародних фінансів. Відповідно до нього [8] визначено такий комплекс ризиків банківської діяльності в умовах диджиталізації:

1. Ризики впливу на споживачів: конфіденційність даних, безпека даних, припинення окремих видів банківських послуг та шахрайські маркетингові практики.

2. Ризики впливу на банки та банківську систему: стратегічний ризик та ризик прибутковості, кіберризик, операційний ризик, підвищення взаємозв'язку між учасниками банківського сектору, ризик ліквідності та волатильність джерел банківського фінансування, комплаєнс-ризик (включаючи ризик невідповідності вимогам законодавства про захист персональних даних), ризики фінансових технологій, ризики третіх сторін (або ризик аутсорсингу).

Найбільший вплив на банківську діяльність при впровадженні цифрових технологій чинять такі ризики:

1. Стратегічні ризики. Можливість входу на ринок та швидкого розвитку фінтех-компаній, для яких у багатьох західних країнах уже було змінено законодавство та створено спеціальні регуляторні режими, збільшує ризик втрати прибутковості окремих банків. Діючі фінансові установи можуть втратити значну частину своєї частки ринку, якщо нові учасники зможуть краще використати технології та надавати аналогічні, але менш дорогі послуги, які краще відповідають очікуванням клієнтів. У сучасних умовах погіршення прибутковості через відсутність гнучкості у взаємодії з клієнтами може послабити здатність діючих банківських установ витримувати цикли ділової активності.

2. Операційні ризики. Широке застосування цифрових технологій призводить до збільшення взаємозалежності між учасниками ринку, що використовують ті самі платформи, що може призвести до того, що збій у роботі IT-інфраструктури перетворився у системну кризу. Крім того, розширення складу учасників банківського сектору збільшує складність системи та призводить до появи суб'єктів, які можуть мати обмежений досвід та знання в управлінні ризиками. Як зазначає у своєму дослідженні колектив експертів Європейської ради з системних ризиків, застарілі банківські IT-системи дуже складно адаптувати до нових умов [16]. Крім того, багато банків використовують значну кількість третіх осіб або через аутсорсинг (використання хмарних розрахунків), або через інші партнерські відносини з технологічними компаніями, що підвищує складність управління ризиками та загалом знижує прозорість операцій.

Практика широкого залучення послуг третіх осіб може призвести до збільшення ризиків, пов'язаних із безпекою даних, конфіденційністю, відмиванням грошей та кіберзлочинністю. Зазначені ризики набувають ще більшого характеру, якщо регуляторний режим не забезпечує достатній рівень ефективності в дотриманні нормативних стандартів та забезпеченні засобів контролю для управління цими ризиками. Крім того, використання сторонніх провайдерів послуг може збільшити ризики, пов'язані з неформальними зобов'язаннями банку щодо підтримки контрагентів: банки можуть опинитися в положенні, коли їм доведеться надавати підтримку провайдеру, який має фінансові труднощі, а інакше вони зіткнуться з припиненням надання критично важливих послуг.

3. Зростаючі складнощі у виконанні комплаєнс-вимог та стандартів. Цифровізація породжує нові ризики та проблеми. Нові вразливі області банківської діяльності можуть розвиватися через появи нових фінансових продуктів та технологій. Поширення цифрових технологій призводить до збільшення кількості фінтех-компаній, поява яких у багатьох країнах, з одного боку, полегшила і здешевило транскордонні транзакції, а з іншого – зробила моніторинг транзакцій складнішим. Нарешті, хоча нові учасники фінансового сектору значною мірою здатні змінити банківську систему, вони можуть виходити за рамки регулювання банківського сектору.

Крім того, якщо банки співпрацюють з фінтех-компаніями і здійснюють від імені їх клієнтів транзакції, їм потрібно включити дані операції у периметр своїх систем моніторингу існуючі ризики. Це відрізняється від поточної практики, оскільки в даний час,

ФІНАНСОВІ РЕСУРСИ: ПРОБЛЕМИ ФОРМУВАННЯ ТА ВИКОРИСТАННЯ

коли клієнт здійснює платежі за допомогою банківської картки або рахунку, банк несе відповідальність за належну ідентифікацію клієнта та надання йому можливості провести сумнівні операції [11]. Результатом може стати більш високий рівень автоматизації серед банків та фінтех-компаній, менше прозорості у тому, як виконуються транзакції та хто несе відповідальність за дотримання нормативних вимог. Таким чином, залучення фінтех-компаній збільшує ризики для банків, оскільки вони несуть підвищену відповідальність за їхні дії.

4. Комплаєнс-ризик (включаючи ризик невідповідності вимогам законодавства про захист персональних даних). Ризик недотримання вимог конфіденційності даних багаторазово зростає у випадку, коли банки співпрацюють з великою кількістю третіх сторін, кожна з яких прагне отримати доступ та використовувати персональні дані клієнтів у своїх цілях.

5. Ризики третіх сторін (або ризик аутсорсингу). Банки все частіше вдаються до використання сторонніх постачальників послуг для надання операційної підтримки їх продуктів, заснованих на застосуванні цифрових технологій. Як зазначає міжнародна аудиторська та консалтингова компанія Deloitte, основними драйверами розвитку аутсорсингу в банківському секторі є зниження витрат, експлуатаційна гнучкість та підвищення безпеки та операційної стійкості [9]. Водночас, згідно зі стандартами Базельського комітету з банківського нагляду, хоча частина функціоналу банку може бути передана на аутсорсинг, ризики та зобов'язання, пов'язані з цим, залишаються за банками.

6. Кіберризики – ризики втрати цілісності даних і несанкціонованого доступу до даних клієнта, ризики порушення функціонування технічної системи в інформаційному просторі, ризики кібератак. Зростання кіберризиків було визначено як банками, так і наглядовими органами як одна з основних зон впливу при використанні цифрових технологій, згідно з одним з останніх досліджень Базельського комітету з банківського нагляду [14]. Нові технології та бізнес-моделі значною мірою збільшують схильність банків до кіберризиків, якщо його системи управління є застарілими і не встигають за змінами. Крім того, велика залежність від нових технологій, що підвищують взаємопов'язаність з організаціями та секторами, не охопленими еквівалентними банківськими нормативними вимогами, потенційно може зробити банківську систему більш вразливою до кіберризиків і піддати великі обсяги персональних даних потенційних порушень.

Іншими проблемами, пов'язаними з кіберризиками, є кібератаки на системно значущі фінансові установи або навіть на іншу критично важливу інфраструктурну галузь, таку як телекомунікаційні або хмарні провайдери. Враховуючи злиття проблем забезпечення конфіденційності даних та кібербезпеки, не дивно, що банки найбільше стурбовані втратою даних клієнтів. Разом з тим, банки також переймаються доступом і цілісністю даних – в одному в двох (51%) фінансових інститутах ці проблеми розглядаються як ключові ризики протягом наступних п'яти років.

7. Ризик ліквідності. Використання нових технологій та сучасних мобільних пристроїв дозволяє клієнтам миттєво перемикатися між різними банківськими рахунками, вкладками, інвестувати в різні цінні папери або купувати паї інвестиційних фондів, щоб отримувати більшу прибутковість. Надання широкого вибору інвестиційних продуктів, з одного боку, підвищує лояльність клієнтів, але, з іншого боку, збільшує волатильність коштів, що є на депозитних рахунках банку. Усе це, у свою чергу, може призвести до збільшення ризику ліквідності для банків.

8. Ризики, пов'язані з використанням хмарних технологій. Використання провайдерів хмарних технологій для зберігання конфіденційних банківських даних пов'язане з низкою потенційних впливів, якими є можлива втрата даних, підтримання їх цілісності та доступності в будь-який момент на вимогу. Застосування даних технологій викликає певну зане-

покоєність і серед регуляторів. Водночас, згідно з експертними опитуваннями, банки більше стурбовані репутаційним ризиком, ніж регулятори, тоді як державні органи більше непокоїть географічне розташування даних та серверів, на яких вони зберігаються [8].

Отже, систематизація основних ризиків і загроз, з якими зіштовхуються банки при впровадженні цифрових технологій, дозволяє узагальнити основні положення того, як банки реагують на ризики, що виникають, і керують ними.

На першій стадії цифровізації банківської діяльності (у відповідь реакція на конкуренцію) банки намагаються підтримувати свої застарілі технологічні системи, а також проводити роботу з усунення недоліків у системі ідентифікації особистості як базової технологічної розробки на даному етапі. Оскільки на аналізованому проміжку банками здійснюється розробка основних елементів системи управління ризиками для її подальшого використання, основний фокус робиться на фінансові ризики. З метою їх мінімізації банки розширюють чисельність персоналу, зайнятого у створенні систем ризик-менеджменту.

На стадії технологічної адаптації банки прагнуть цифровізації клієнтського досвіду – переведення більшості банківських продуктів та послуг в онлайн-режим, впровадження системи управління кіберризиками. Основна увага на цій стадії приділяється нефінансовим ризикам, для чого використовується розроблена раніше операційна система ризик-менеджменту.

На завершальній стадії цифровізації (стратегічне позиціонування) банки модернізують свої бек-офіси, впроваджують стандарти кібербезпеки в усі бізнес-процеси (злиття та поглинання, перевірка контрагентів, розробка нових продуктів). На цьому проміжку основний фокус робиться на управлінні та досягненні балансу між фінансовими та нефінансовими ризиками. З метою мінімізації ризиків застосовується система ризик-менеджменту з використанням технологій автоматизації, машинного навчання та штучного інтелекту.

Отже, управління ризиками банків базується на визначенні джерел ризику, ідентифікації ризиків, оцінці операційних ризиків, моніторингу ризиків, а також контролю та мінімізації таких ризиків (рис. 1).

Таким чином, вважаємо, що основними причинами кіберризиків для комерційного банку може бути: відсутність постійного оновлення законодавства та єдиних стандартів безпеки, відсутність власного банківського фінансування, а також відсутність корпоративної культури у сфері кібербезпеки в банку.

Вказані причини зумовлюють застосування таких елементів контролінгу та менеджменту діяльності комерційних банків:

1. Навчання персоналу правилам кібербезпеки у довільному форматі, у будь-який час і в будь-якому місці (навчальні матеріали подавати спрощено для сприйняття: через анімацію, відео та інші «зручні» інструменти). Після кожного етапу навчання має бути організоване формальне та приховане тестування (фішингові листи для перевірки реакції персоналу).

2. Розробка плану на випадок. Обговорення плану дій з професійною модерацією дозволить визначити ключові проблеми. Необхідно вирішити проблему до того, як банківську систему буде зламано. Також важливо створити центри безпеки, які здійснюють кіберрозвідку, відстежують загрози та вчасно реагують на них.

3. Регулярне проведення аудитів кібербезпеки (важливий аспект – кваліфікація аудитора, який повинен мати достатню компетенцію для виявлення вузьких місць у безпеці банку).

4. Навчання клієнтів основним правилам безпеки (це допоможе знизити додаткові ризики несанкціонованого доступу до інформації через одноразові паролі та двофакторну аутентифікацію).

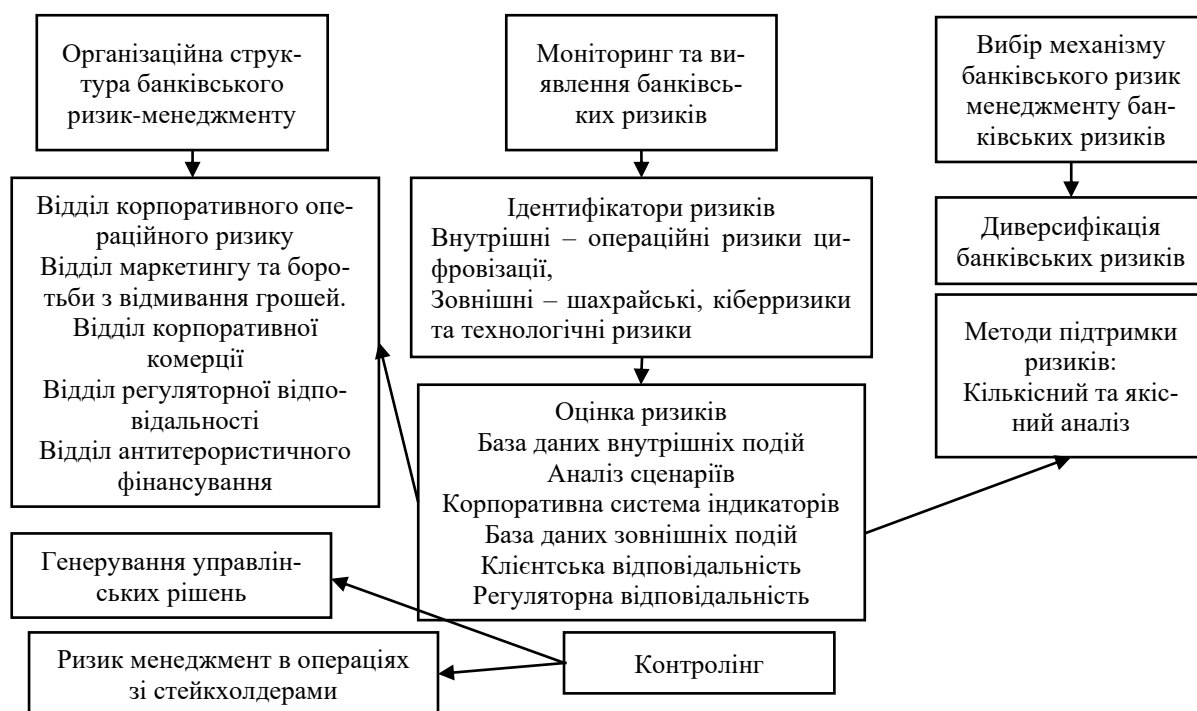


Рис. 1. Механізм управління ризиками цифровізації в комерційних банках
Джерело: розроблено автором на основі [1; 7; 9].

Критично важливим питанням управління банківськими ризиками в умовах цифровізації виступає посилення правових положень, які б регулювали сферу дистанційного банківського обслуговування.

Вважаємо, що комерційним банкам доцільно управляти банківськими ризиками шляхом їх диверсифікації з метою підвищення їх фінансової стійкості. Диверсифікація банківських ризиків при сталому фінансуванні позитивно вплине на капіталізацію банків, дозволить їм збільшити грошові потоки та отримати додатковий дохід. Також, в умовах глобалізації банківським установам необхідно залучати додаткові інвестиції для управління кіберризиками й побудови відносин із зацікавленими сторонами для обміну інформацією та покриття ризиків, пов'язаних з кібератаками, і тим самим сприяти стабільному зростанню фінансових ресурсів.

Список використаних джерел

1. An endurance course: surviving and thriving through 10 major risks over the next decade. Tenth annual EY [Electronic resource]. – Accessed mode: [https://www.ey.com/Publication/vwLUAssets/ey-global-risk-survey2019/\\$FILE/ey-global-risk-survey-2019.pdf](https://www.ey.com/Publication/vwLUAssets/ey-global-risk-survey2019/$FILE/ey-global-risk-survey-2019.pdf).
2. Basel Committee on Banking Supervision: The Joint Forum on Outsourcing in Financial Services [Electronic resource]. – Accessed mode: <https://www.bis.org/publ/joint12.pdf>.
3. Basel Committee on Banking Supervision: Sound Practices – Implications of fintech developments for banks and bank supervisors [Electronic resource]. – Accessed mode: <https://www.bis.org/bcbs/publ/d431.pdf>.
4. Carbó-Valverde S. The Effect of Banks' IT Investments on the Digitalization of their Customers / S. Carbó-Valverde, P.J. Cuadros-Solas, F. Rodríguez-Fernández // Glob. Policy. – 2020. – № 11. – Pp. 9-17.
5. Gilje E. P. Exporting liquidity: Branch banking and financial integration / E. P. Gilje, E. Loutschina, P. E. Strahan // J. Financ. – 2016. – № 71. – Pp. 1159-1184.
6. Ernst & Young: Global FinTech Adoption Index 2019 [Electronic resource]. – Accessed mode: https://www.ey.com/en_gl/ey-global-fintech-adoption-index.
7. ING Bank. Ecosystems: The Future for Banks? 2020 [Electronic resource]. – Accessed mode: <https://view.ingwb.com/ecosystemsthe-future-for-banks>.

8. Institute of International Finance. The Future of Risk Management in the Digital Era; McKinsey&Company Report; 2017 [Electronic resource]. – Accessed mode: <https://www.mckinsey.com/~media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20future%20of%20risk%20management%20in%20the%20digital%20era/Future-of-risk-management-in-the-digital-era-IIF-and-McKinsey.ash>.
9. Outsourcing banking processes – Deloitte research [Electronic resource]. – Accessed mode: <https://www2.deloitte.com/us/en/pages/advisory/articles/outsourcingbanking-processes.html>.
10. Regulatory complexity and the quest for robust regulation: Reports of the Advisory Scientific Committee [Electronic resource]. – Accessed mode: https://www.esrb.europa.eu/pub/pdf/asc/esrb.asc190604_8_regulatorycomplexityquestrobustregulation~e63a7136c7.en.pdf.
11. Shestak V. A. On the possibility of doctrinal perception of artificial intelligence as the subject of crime in the system of common law: using the example of the U.S. / V. A. Shestak, A. G. Volevodz, V. A. Alizade // Criminal legislation. – 2019. – Vol. 13. – Pp. 547-554.
12. The Global Innovation Index 2020. [Electronic resource]. – Accessed mode: <https://www.globalinnovationindex.org/gii-full-report-2020.pdf#>.
13. Гончарук В. В. Інновації фінансової структури в умовах цифрової економіки / В. В. Гончарук // Розвиток банківських послуг та інновацій в цифровій економіці : матеріали наук.-практ. інтерн. конф. студ. аспір. і молод. вчених. Київ, 14 квітня 2019 р. – К. : КНЕУ, 2019. – С. 12-15.
14. Долгушина А. Я. Цифрова модель банківського обслуговування [Електронний ресурс] / А. Я. Долгушина // *π-Economy*. – 2016. – Режим доступу: <https://cyberleninka.ru/article/n/tsifrovaya-model-bankovskogo-obsluzhivaniya>.
15. Івлева М. І. Тенденція цифровізації банківської галузі [Електронний ресурс] / М. І. Івлева // Молодий вчений. – 2020. – № 2 (292). – С. 268-270. – Режим доступу: <https://moluch.ru/archive/292/66194>.
16. Писарев А. Освоили технологии [Электронный ресурс]. – Режим доступа: <https://minfin.com.ua/2019/10/18/39314319>.
17. Соснін О. Цифровізація як нова реальність України [Електронний ресурс]. – Режим доступу: <https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny>.

References

1. An endurance course: surviving and thriving through 10 major risks over the next decade. Tenth annual EY. [https://www.ey.com/Publication/vwLUAssets/ey-global-risk-survey2019/\\$FILE/ey-global-risk-survey-2019.pdf](https://www.ey.com/Publication/vwLUAssets/ey-global-risk-survey2019/$FILE/ey-global-risk-survey-2019.pdf).
2. Basel Committee on Banking Supervision: The Joint Forum on Outsourcing in Financial Services. <https://www.bis.org/publ/joint12.pdf>.
3. Basel Committee on Banking Supervision: Sound Practices – Implications of fintech developments for banks and bank supervisors. <https://www.bis.org/bcb/publ/d431.pdf>.
4. Carbó-Valverde, S., Cuadros-Solas, P.J., Rodríguez-Fernández, F. (2020). The Effect of Banks' IT Investments on the Digitalization of their Customers. *Glob. Policy.*, (11), 9-17.
5. Gilje, E.P., Loutskina, E., Strahan, P.E. (2016). Exporting liquidity: Branch banking and financial integration. *J. Financ.*, (71), 1159-1184.
6. Ernst & Young: Global FinTech Adoption Index 2019. https://www.ey.com/en_gl/ey-global-fintech-adoption-index.
7. ING Bank. Ecosystems: The Future for Banks? 2020. <https://view.ingwb.com/ecosystemsthe-future-for-banks>.
8. Institute of International Finance. The Future of Risk Management in the Digital Era; McKinsey&Company Report; 2017. <https://www.mckinsey.com/~media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20future%20of%20risk%20management%20in%20the%20digit%20era/Future-of-risk-management-in-the-digital-era-IIF-and-McKinsey.ash>.
9. Outsourcing banking processes – Deloitte research. <https://www2.deloitte.com/us/en/pages/advisory/articles/outsourcingbanking-processes.html>.
10. Regulatory complexity and the quest for robust regulation: Reports of the Advisory Scientific Committee. https://www.esrb.europa.eu/pub/pdf/asc/esrb.asc190604_8_regulatorycomplexityquestrobustregulation~e63a7136c7.en.pdf.

11. Shestak, V.A., Volevodz, A.G., Alizade, V.A. (2019). On the possibility of doctrinal perception of artificial intelligence as the subject of crime in the system of common law: using the example of the U.S. *Criminal legislation.*, 13, 547-554.
12. The Global Innovation Index 2020. <https://www.globalinnovationindex.org/gii-full-report-2020.pdf#>.
13. Honcharuk, V.V. (2019). Innovatsii finansovoi struktury v umovakh tsyfrovoy ekonomiky [Innovations of financial structure in terms of digital economy]. *Rozvytok bankivskykh posluh ta innovatsii v tsyfrovii ekonomitsi : materialy nauk.-prakt. intern. konf. stud. aspir. i molod. vchenykh – Development of banking services and innovations in digital economy: materials of scientific practice. intern. conf. stud. aspir. and young. Scientists* (pp. 12-15). KNEU.
14. Dolhushyna, A.Ya. (2016). Tsyfrova model bankivskoho obsluhovuvannya [Digital model of banking services]. *π-Economy*. <https://cyberleninka.ru/article/n/tsifrovaya-model-bankovskogo-obsluzhivaniya>.
15. Ivlieva, M.I. (2020). Tendentsiia tsyfrovizatsii bankivskoi haluzi [Tendency of digitalization of the banking industry]. *Molodyi vchenyi – Young scientist*, (2(292)), 268-270. <https://moluch.ru/archive/292/66194>.
16. Pysarev, A. (2019). *Osvoyly tekhnolohyy [Mastered technologies]*. <https://minfin.com.ua/2019/10/18/39314319>.
17. Sosni, O. (2020). *Tsyfrovizatsiia yak nova realnist Ukrainy [Digitalization as a new reality of Ukraine]*. <https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny>.

Отримано 25.10.2021

UDC 330.33.012

Alla Abramova

PhD in Economics, Associate Professor,
Associate Professor of Department of Public, Corporate Finance and Financial Intermediation
Yuriy Fedkovych Chernivtsi National University (Chernivtsi, Ukraine)
E-mail: alla1labramova@ukr.net. **ORCID:** <https://orcid.org/0000-0003-3364-8316>
Scopus ID: [57213158224](https://scopus.com/authid/detail.uri?https://orcid.org/0000-0003-3364-8316). **ResearcherID:** [W-2085-2017](https://pubs.rsos.royalsocietypublishing.org/author/W-2085-2017)

SYSTEM OF RISKS OF ACTIVITY OF COMMERCIAL BANKS IN THE CONDITIONS OF DIGITALIZATION

The trend of modern commercial banks is the digitalization of decision-making processes and various operations, which ensures the preservation of the customer base and the expansion of the banking business through new electronic channels and online lending. It is established that innovative banking technologies create new sources of risk and should ensure effective processes of their management and control. The complex of risks of banking activity in the conditions of digitalization from the standpoint of consumer interests (data confidentiality, data security, termination of certain types of banking services and fraudulent marketing practices, as well as from the standpoint of banks and the banking system) is identified. , increasing the relationship between participants in the banking sector, liquidity risk and volatility of sources of bank financing, compliance risk, financial technology risks, outsourcing risk.

Among the most influential in the implementation of digital technologies in the implementation of digital technologies are the following: strategic, operational risks, growing difficulties in complying with compliance requirements and standards, compliance risk, third party risks, cyber and liquidity risks, and related risks using cloud technologies. The main causes of cyber risks for a commercial bank are stated, which can be solved by constantly updating legislation and uniform security standards, increasing its own bank financing, as well as cultivating a corporate culture in the field of cybersecurity in the bank. These reasons lead to the use of certain elements of controlling and management of a commercial bank, the system of which includes training staff in cybersecurity rules in any format, developing a fraud plan, regular cybersecurity audits, training customers in basic security rules. A critical issue in the management of banking risks in the context of digitalization is the strengthening of legal provisions governing the field of remote banking.

Keywords: risks, digitalization; causes of risks; types of risks; controlling; risk management.

Fig.: 1. References: 17.