3. Students, Computers and Learning: Making the Connection. OECD Report Digest. – 15th of September 2015. URL: http://copilotpartners.com/wp-content/uploads/CP_EI_Students-Computers-and-Learning-OECD-Report-Digest-150915.pdf
4. Індекс глобальної залученості за версією компанії Huawei – Global Connectivity Index. URL: https://www.huawei.com/minisite/gci/en/country-profile.html
5. Рейтинг цифрової конкурентоспроможності світу – World Digital Competitiveness Ranking. 2018. URL: https://www.ceda.com.au/CEDA/media/General/Publication/PDFs/WCYdigitalranking2018.pdf

Архірейська Н.В.
к.е.н., доцент
Губа М.О.
к.е.н., доцент
Університет митної справи та фінансів, м. Дніпро

УПРАВЛІННЯ БАНКІВСЬКИМИ РИЗИКАМИ В УМОВАХ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ

На сучасному етапі цифрові технології активно впроваджуються у стратегічний процес діяльності банку, оскільки майже весь бізнес підпадає під вплив цифрових трансформацій. Цифрові переваги з точки зору споживача, зокрема його доходів і витрат, є очевидними та дуже переконливими. Адаптація нових технологій і операційних моделей є запорукою зростання цих вигід. У цьому плані не повинно бути винятком й управління ризиками у банку, витрати на яке протягом останнього десятиліття суттєво зросли. Цифрові технології дозволяють банкам збільшити ефективність і покращити якість прийняття рішень на підставі оцінки ризиків, а також якісніше здійснювати моніторинг і контроль, забезпечивши більш ефективне дотримання нормативних вимог.

Управління ризиками у банківській справі трансформувалося протягом останнього десятиріччя у відповідь, насамперед, на

нове банківське регулювання, спричинене глобальною фінансовою кризою, а також – на розвиток цифрових технологій у суспільстві [1].

Розвиток технологічних інновацій, застосування передових засобів аналізу даних і поглиблена аналітика дозволить забезпечити розвиток нових технік управління ризиками, що сприятиме прийняттю кращих рішень за скорочених витрат. На сьогоднішній день найпоширенішими технологіями, що впливають на рівень ризик-менеджменту в банках, є такі:

− великі дані (big data), які дозволяють використовувати значний обсяг інформації щодо споживача при прийнятті рішень стосовно рівня цього ризику, переглядати його портфелі, визначати можливість фінансового злочину, прогнозувати операційні збитки;

− комп'ютерне (само)навчання (machine learning), яке дозволяє підвищити точність моделей ризиків (моделей дії факторів ризику, risk models), визначаючи складні, нелінійні тренди у великих масивах даних;

− краудсорсинг (crowdsourcing) – залучення до вирішення проблем ризик-менеджменту широкого кола осіб, з використанням їхніх знань, досвіду та навичок на добровільних засадах із використанням інформаційно-комунікаційних технологій [2].

Проте, використання подібних технологій у процесі управління банківським ризиками потребує високого рівня захисту інформації. На сьогодні основними прикладами цих ризиків є такі.

Ризики моделі (model risk) – зростаюча залежність банків від використання моделей в управлінні ризиками потребує від керівництва та персоналу кращого розуміння та керування цими моделями. В іншому випадку можуть виникнути втрати від помилок моделі. Яскравим прикладом є Азіатсько-Тихоокеанський банк (Asia-Pacific bank), що втратив $1,4 млрд. внаслідок застосування моделей ризику зміни процентної ставки (interest-rate models), які містили некоректні припущення та помилки введення даних. Зменшення такого ризику можливе через дотримання чітких методичних вказівок стосовно побудови й оцінки подібних моделей, а також у пос-

тійному їх моніторингу й удосконаленні.

Кіберризики (cybersecurity risk). Ймовірність кібератак збільшується, оскільки зростає обсяг даних, яким оперують банки [3]. У 2018 р. в Україні сталося кілька масштабних кібератак. Від них постраждала низка компаній, банків, органів влади. Головними цілями таких кібератак є захоплення даних з інформаційних систем економічних агентів, отримання повного контролю над ресурсами їх комп'ютерів або виведення систем із ладу. Це призводить до таких негативних наслідків, як прямі фінансові втрати банків і підприємств, вихід із ладу їх ІТ-систем, перерви в роботі, втрата інтелектуальної власності та репутації, шкода інтересам третіх осіб (клієнтів, акціонерів, співробітників). За оцінками МВФ, непрямі збитки зазвичай становлять близько 90% від загальної суми. Так, щорічні втрати від реалізації кіберризиків у світі складають $0,25–1,0 трлн. [4, с.54].

Ризик ланцюгової реакції (contagion risk) – банки є вразливими до ланцюгової реакції на глобальних ринках. Негативний розвиток ринку може швидко поширюватись на банки. Тому банки мають виміряти та відслідковувати власну схильність до ланцюгової реакції та її потенційний вплив на діяльність банку. Заходи, спрямовані на скорочення загального банківського ризику можуть скорочувати його вимоги до капіталу, оскільки ризик ланцюгової реакції є одним із головних чинників класифікації банку як глобального системно значимого банку (global systemically important bank, G-SIB) [5; 6].

В умовах розвитку цифрової економіки ефективне управління ризиками в банку має враховувати управління різними типами ризиків, у координації із чинними регуляторними нормами та приготуванням до нових стандартів. У цих умовах відповідність очікуванням споживачів починає відігравати ключову роль у досягненні кінцевого результату. Проте, на сьогодні якість функції управління ризиками в багатьох банках досить далека від перелічених вимог. Оптимальна функція управління ризику в умовах цифровізації економіки повинна мати такі якості та можливості:

− повна автоматизація рішень і процесів із мінімальним руч-

ним втручанням;

− зростаюче використання моделей із використанням поглибленої аналітики;

− тісна взаємодія з бізнесом задля підвищення ступеня задоволеності клієнта якістю обслуговування (customer experience), прийняття збалансованих однозначних рішень і покращення готовності до регуляторних змін;

− переконливий захист корпоративних цінностей і принципів, підтримуваний обґрунтованою, чітко визначеною та підкріпленою банком культурою ризиків (risk culture), цінність якої полягає у відмові від прийняття невиправданих, високих ризиків;

− висококваліфіковані спеціалісти з аналітичними здібностями.

Отже можна зробити висновок, що перехід від традиційної організації управління ризиками в банку до цифрової є фундаментальним викликом у сучасних умовах цифровізації економіки.

Список використаних джерел

1. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації, 2018. Розпорядження КМУ від 17 січня 2018 р., № 67-р.

2. Saxton, G. D., Onook, Oh. & Kishore, R., 2013. Rules of Crowdsourcing: Models, Issues, and Systems of Control Pages 2-20, [Published online: 22 Jan 2013] Information Systems Management 30(1) https://doi.org/10.1080/10580530.2013.739883.

3. 2016 Accenture Technology Vision for Banking Digital Trust: Erase the trust paradox in banking.
URL: https://www.accenture.com/t20160529T211723__w__/us-en/_acnmedia/PDF-20/Accenture-Banking-Tech-Vision-Digital-Trust.pdf.

4. Звіт про фінансову стабільність, 2017. Національний Банк України, 4, грудень, 75 с.

5. Schoenmaker, D., 1996. Contagion Risk in Banking. L.S.E. Financial Markets Group Discussion Paper, 239, London: London School of Economics, March. pp.86-104.

6. Financial Contagion in the Era of Globalised Banking?. 2012. OECD Economics Department Policy Notes, 14, June. 10 p.