https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/05/impacts-of-the-russian-invasion-of-ukraine-on-financial-market-conditions-and-resilience_a29d11b1/879c9322-en.pdf

2. World Bank. Remittances Slowed in 2023, Expected to Grow Faster in 2024 : прес-реліз, 26.06.2024 р. – Washington, DC : World Bank, 2024. URL: https://www.worldbank.org/en/news/press-release/2024/06/26/remittances-slowed-in-2023-expected-to-grow-faster-in-2024

3. Bank for International Settlements. Streamlining Cross-Border Transaction Compliance : BIS Working Paper [Електронний ресурс]. Basel: BIS, 2024. URL: https://www.bis.org/publ/work1234.htm

4. Lubold G. Needing Dollars, Iran-Backed Militias Turn to Visa and Mastercard [Електронний ресурс] // The Wall Street Journal. – 31 May 2025. URL: https://www.wsj.com/articles/iran-backed-militias-visa-mastercard-11686000000

5. KPMG. Pulse of FinTech 2021: Record Investment Year [Електронний ресурс]. – London: KPMG International, 2022. URL: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2022/02/pulse-of-fintech-h2-2021.pdf

6. KPMG. Pulse of FinTech 2022: Full-Year Review [Електронний ресурс]. – London: KPMG International, 2023. URL: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2023/02/pulse-of-fintech-2022.pdf

7. KPMG. Global FinTech Investment Fell from $119.8 bn in 2023 to $95.6 bn in 2024 : Press Release, 17 Feb 2025 [Електронний ресурс]. London: KPMG International, 2025. – Режим доступу: https://home.kpmg/xx/en/home/media/press-releases/2025/02/global-fintech-investment-2024.html

8. KPMG. Pulse of FinTech H2’24: Global Analysis of FinTech Funding [Електронний ресурс]. London: KPMG International, 2024. URL: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2024/02/pulse-of-fintech-h2-2024.pdf

**Івасів І.Б.,**
д.е.н., проф., професор кафедри банківської справи та страхування,
Київський національний економічний університет імені Вадима Гетьмана

## ОПЕРАЦІЙНА СТІЙКІСТЬ БАНКІВ: ПРОБЛЕМИ ТА ВИКЛИКИ

З часу світової фінансової кризи та пандемії COVID-19 і, особливо, зараз в період геополітичної нестабільності та відкритого військового вторгнення в Україну, банки стикаються з комплексом взаємопов’язаних проблем: від масового переходу до віддалених послуг до зростання кібератак. Ті, хто вистояв, мали дещо спільне – операційну стійкість. Операційна стійкість – це здатність банку забезпечувати безперебійну роботу, адаптуватися до криз і швидко відновлюватися, зберігаючи довіру клієнтів.

Базельський комітет з банківського нагляду у своїх «Принципах операційної стійкості» [1] наголошує, що банки з розвиненою цифровою інфраструктурою та

ефективними системами управління ризиками краще підготовлені до протистояння, адаптації та відновлення після серйозних збоїв, таких як кібератаки, технологічні збої чи пандемії.

Сучасні наукові дослідження виділяють ключові виклики, зокрема інфраструктурні недоліки, проблеми в управлінні ризиками та регуляторні бар'єри. Так, технологічна інфраструктура є одночасно ключовим фактором підтримки та викликом для операційної стійкості банків. Технологічні обмеження, зокрема використання застарілих систем, недостатня підготовка персоналу та операційні ризики (включаючи кібератаки та недоступність систем), були визнані серйозними викликами у дослідженнях К. Демма та ін. [2], О. Берг та К. Крістоферсен [3], Ф. Пессі [4]. К. Демма та ін. надали кількісні докази того, що банки з вищим рівнем цифровізації виявилися більш стійкими під час пандемії COVID-19, оскільки могли швидко перейти на онлайн-обслуговування та підтримувати клієнтів дистанційно. В. Галловей [5] стверджує, що ефективне управління ризиками, фінансова стійкість та інновації у сфері штучного інтелекту є ключовими стратегіями операційної стійкості. Ш. Бі та Ю. Ліан [6] та Р. Стюарт та М. Чоудхурі [7] відзначають, що нормативне регулювання необхідне для стабільності, але непослідовні або надто жорсткі норми можуть ускладнювати адаптивне реагування.

Підсумовуючи сучасні наукові дослідження, до основних проблем можна віднести:

- Технологічні загрози: застарілі системи, нерівномірна цифровізація, вразливість до кіберзагроз і технічних збоїв ускладнюють забезпечення дистанційного обслуговування.
- Організаційні та у сфері ризик-менеджменту: недостатня підготовка до різних сценаріїв, слабке управління ліквідністю та недоліки у стрес-тестуванні стали особливо помітними під час глобальної фінансової кризи 2008 року та пандемії COVID-19.
- Регуляторні: суперечливі або надто суворі нормативні вимоги часто перешкоджають ефективному управлінню в кризових ситуаціях.
- Економічні: нестача ліквідності, дефіцит капіталу та системні ризики є найкритичнішими проблемами, зазначеними у більшості досліджень.

Також, дослідження свідчать, що великі банки з потужними цифровими технологіями та ефективними системами управління ризиками виявляють більшу стійкість до криз, тоді як менші або менш розвинені установи стикаються зі значними труднощами.

В умовах затяжного воєнного конфлікту та супутньої економічної турбулентності, операційний ризик виступає одним із ключових викликів для банківської системи України. Незважаючи на високу інтенсивність загроз, банківські установи продемонстрували високий рівень адаптивності, забезпечивши ефективне управління ризиками та підтримання фінансової стабільності. На початковому етапі повномасштабного вторгнення відбулося різке зростання оцінок операційного ризику, проте з часом, у міру стабілізації безпекової ситуації в більшості регіонів, ці оцінки поступово знижувалися.

Наразі операційний ризик не класифікується як критичний, хоча продовжує залишатися важливим чинником системної уразливості.

До основних джерел операційного ризику належать випадки шахрайства, кіберактивність, порушення безперервності бізнес-процесів внаслідок воєнних дій, а також деградація людського капіталу. З метою протидії таким загрозам банки здійснюють покриття операційного ризику за рахунок капіталу. Станом на березень 2025 р. сукупний обсяг резервів, сформованих для цих цілей, перевищує 40 млрд. грн. [8], що є значно вищим порівняно з аналогічними показниками у низці інших країн. У процесі внутрішньої оцінки адекватності капіталу (ICAAP) банки враховують ширший спектр ризиків, включаючи потенційні стресові сценарії. Варіативність методологічного підходу серед банків призводить до суттєвих відмінностей у частці капіталу, зарезервованого під операційний ризик — від 1% до 50%, що зумовлено особливостями внутрішньої системи аналізу кожної установи.

Попри масштабні виклики, обсяги фактичних втрат від реалізації операційного ризику виявилися нижчими за очікувані. Станом на середину 2023 року сукупні операційні втрати банків становили близько 15 млрд грн. [8]. Значну роль у стримуванні негативних наслідків відіграє управління ризиками, пов’язаними з контрагентами, зокрема постачальниками критично важливих фінансових послуг. У цьому контексті НБУ впроваджує нові регуляторні вимоги, спрямовані на посилення операційної стійкості банків та їх здатності функціонувати в умовах надзвичайних ситуацій.

Таким чином, ефективне управління операційним ризиком виступає ключовим елементом забезпечення довгострокової фінансової стабільності банківського сектору та формує підґрунтя для його відновлення у посткризовий період.

Операційна стійкість банківського сектору України є фундаментальним елементом забезпечення фінансової стабільності держави, особливо в контексті тривалого збройного конфлікту та супровідної економічної нестабільності. Згідно з підходом, що застосовується Національним банком України, операційна стійкість охоплює п’ять взаємопов’язаних компонентів: безперервність операційної діяльності, кадрову спроможність, стійкість інфраструктури, рівень інформаційної безпеки, а також ефективність управління ризиками взаємодії з критично важливими контрагентами. Сукупна дія цих чинників визначає здатність банківських установ ідентифікувати, попереджати та мінімізувати операційні ризики.

Оцінювання рівня операційної стійкості здійснюється в межах наглядового процесу SREP, що передбачає самооцінку банками власної готовності реагувати на дестабілізуючі фактори, зокрема військові загрози, кібератаки та збої у функціонуванні критичних бізнес-процесів. Відповідно до результатів досліджень, належний рівень операційної стійкості забезпечено у 67% системно важливих банків і лише у 22% банків, які не належать до цієї категорії [9]. Однією з основних загроз залишається недостатній контроль за діяльністю критичних контрагентів: більшість банків не вимагає від них наявності планів

безперервності діяльності та не здійснює повноцінного процесу due diligence, що підвищує ймовірність збоїв під час кризових ситуацій.

Стрес-тестування свідчить про наявність у банків резервів для подолання операційних ризиків, хоча й виявляє суттєві прогалини. Особливої уваги потребує проблема кадрової мобілізації: низький рівень бронювання працівників, які підлягають призову, та відсутність апробації сценаріїв функціонування ключового персоналу в умовах надзвичайних ситуацій. Додатково, 19 банків не мають альтернативних засобів зв'язку для критичних працівників [9], що унеможливлює ефективну комунікацію в умовах відключення електроенергії або втрати інтернет-доступу.

Зростає актуальність ризиків, пов'язаних із кібератаками. Хоча більшість банків декларують високу здатність до оперативного відновлення критичних функцій після атак, частина установ не має резервних дата-центрів і запасних каналів зв'язку, що істотно обмежує їхню реальну стійкість. Поточні технічні можливості мобільних операторів дозволяють забезпечити безперервність банківських сервісів за умов блекауту лише протягом восьми годин, що є недостатнім для підтримання стабільної інфраструктури.

Підвищення рівня операційної стійкості вимагає комплексного підходу, зокрема: впровадження механізмів ідентифікації та управління ризиками критичних контрагентів, актуалізації та регулярного тестування планів безперервності діяльності (BCP), урахування стандартів Базельського комітету з банківського нагляду (BCBS) та нових вимог цифрової операційної стійкості (DORA). Водночас необхідно посилити аналітику щодо впливу зовнішніх ризиків на бізнес-процеси, розробити детальні сценарії реагування та оптимізувати моніторинг ризиків.

НБУ рекомендує фінансовим установам здійснювати поглиблену оцінку операційної стійкості з урахуванням можливих кризових сценаріїв — включаючи військові ризики, мобілізаційні виклики та потенційні збої в роботі критичних сервісів. Підвищення якості BCP-планів сприятиме зміцненню механізмів кризового реагування, зниженню системних ризиків та загальній фінансовій стабільності банківського сектору.

Таким чином, ефективне управління операційними ризиками та розвиток системи операційної стійкості становить основу стабільного функціонування банківського сектору України в умовах воєнного конфлікту та подальшого економічного відновлення. Запровадження інтегрованих заходів реагування на кризові ситуації сприятиме збереженню довіри з боку клієнтів і інвесторів, а також посиленню загальної економічної безпеки держави.

## Список використаних джерел

1. Basel Committee on Banking Supervision. Principles for Operational Resilience [Electronic resource] / Bank for International Settlements. — Basel : Bank for International Settlements, 2021. 20 p. URL: https://www.bis.org/bcbs/publ/d516.htm. (дата звернення: 15.04.2025).

2. Demma C., Ferri G., Orame A., Pesic V., Vacca V. P. Banks' Operational Resilience During Pandemics [Електронний ресурс] / C. Demma, G. Ferri, A. Orame,

V. Pesic, V. P. Vacca. – Social Science Research Network, 2024. — URL: https://www.bancaditalia.it/pubblicazioni/qef/2024-0833/QEF_833_24.pdf. (дата звернення: 10.04.2025).

3. Berge T., Christophersen C. Operational Problems In Banks – Effects On The Settlement Of Payments In Norges Bank / T. Berge, C. Christophersen. – 2012. – Norges Bank. – 24 p. — URL: https://norges-bank.brage.unit.no/norges-bank-xmlui/bitstream/handle/11250/2503645/operational_problems_in_banks.pdf?sequence=1&isAllowed=y (дата звернення: 07.04.2025).

4. Passey, Fi (2018, March 1). A customer-insight led approach to building operational resilience. In the *Journal of Business Continuity & Emergency Planning*, Volume 11, Issue 3. https://doi.org/10.69554/YUPV3902. Holloway V. G. Bank executives' strategies for operational resilience amidst crisis [Електронний ресурс] / V. G. Holloway. – Social Science Research Network, 2023.

5. Bi Shuochen, Lian Yufan. Green Finance in Banks: Addressing Climate Risks and Enhancing Economic Resilience // International Journal of Scientific Research in Science and Technology. 2024. Vol. 11, Iss. 3. P. 389–399. URL: https://ijsrst.com/paper/18972.pdf. (ата звернення: 5.04.2025).

6. Stewart R., Chowdhury Murshed. Banking Sector Distress and Economic Growth Resilience: Asymmetric Effects // The Journal of Economic Asymmetries. 2021. Vol. 24. P. 226. URL: https://doi.org/10.1016/j.jeca.2021.e00226.

7. Дадашова П. Вплив операційного ризику на фінансовий сектор України на четвертий рік війни : виступ на XIII Щорічній конференції «Операційна стійкість та управління операційними ризиками», 7 березня 2025 р. [Вадим Дадашов]. Організатор: компанія Extra Consulting. 2025.

8. Паламарчук Л. Оцінка операційної стійкості банків: виклики, результати та подальші кроки : виступ на XIII Щорічній конференції «Операційна стійкість та управління операційними ризиками», 7 березня 2025 р. Лариса Паламарчук. Організатор: компанія Extra Consulting. 2025.

**Ільїна В.О.,**
студент ОПП «Митна справа», 4 курс,
Київський національний економічний університет імені Вадима Гетьмана
Науковий керівник – к.е.н., доцент кафедри фінансів імені В. Федосова
Бороденко.Т. М.

## ОСОБЛИВОСТІ МИТНО-ТАРИФНОГО РЕГУЛЮВАННЯ ЗОВНІШНЬОЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ В УКРАЇНІ

Митно-тарифне регулювання є одним із основних джерел поповнення державного бюджету. Цей механізм передбачає стягнення митних зборів із товарів, що імпортуються та експортуються. Внаслідок цього державна скарбниця поповнюється коштами, а вітчизняні виробники отримують захист від зовнішньої конкуренції.

Митне регулювання відіграє важливу роль у системі зовнішньоторговельної політики, яка спрямована на захист економічних інтересів держави, виконання