Шатонська К.Г., студентка ІІ курсу групи ФБСМ-10
Науковий керівник – к.е.н., доц. Литвинчук І.В.,
Доцент кафедри фінансів та цифрової економіки
Державний університет «Житомирська політехніка»

СУЧАСНІ ВИКЛИКИ БАНКІВСЬКОЇ БЕЗПЕКИ ТА УПРАВЛІННЯ РИЗИКАМИ

У контексті сучасної геоекономічної турбулентності, енергетичної волатильності та тотальної цифрової трансформації фінансового сектора банківська безпека України виступає системоцентричним детермінантом макрофінансової стійкості. Імплементація глобальних регуляторних стандартів Basel III, а також нормативних вимог Директиви ЄС NIS2 і Регламенту DORA, зумовлює трансформацію парадигми ризик-менеджменту, акцентуючи на ідентифікації, кваліфікації та моніторингу операційних, кібернетичних і системно-структурних ризиків [1]. Аналітична мета дослідження полягає у детермінації ключових викликів банківської безпеки на основі аналізу діяльності АТ КБ «ПриватБанк» - найбільшої державної фінансово-кредитної корпорації України. Новизна підходу полягає у поєднанні кількісного аналізу ризикової експозиції банку з оцінкою регуляторно-інституційних детермінант його стійкості.

Сучасна архітектоніка банківської безпеки в Україні визначається взаємодією трьох підсистем – фінансової, операційної та кібернетичної. Дослідження АТ КБ «ПриватБанк» показує концентрацію ризиків у фінансовій площині (зростання NPL, ліквідність), операційній (збої в ІТ-системах, кібератаки, кадровий дефіцит у сфері безпеки) та макроекономічній (інфляційно-девальваційні коливання, воєнна нестабільність). За даними НБУ [2], станом на березень 2025 р. рівень непрацюючих кредитів у банківській системі становив 37,4%, тоді як у ПриватБанку він утримувався у межах 170–180 млрд грн, при цьому покриття резервами перевищувало 85% [2]. Можемо, говорити про консервативну, але стійку модель ризик-менеджменту, також посилюються регуляторні вимоги до кіберстійкості, через імплементацію стандартів ISO/IEC 27001:2022 і вимог фінансового моніторингу FATF/AML. Управління ризиками переходить від реактивного до превентивного формату, що вимагає інтеграції аналітичних, цифрових і правових механізмів контролю [3].

Основним викликом є домінування кредитного ризику як базового джерела системної вразливості. Висока частка проблемних активів і залежність від державного фінансування обмежують маневреність банків у сфері ліквідності. ПриватБанк, маючи стратегічний вплив на економіку, забезпечує покриття непрацюючих кредитів резервами у 94–96%, що відповідає вимогам Basel III щодо достатності капіталу [2]. Операційні ризики зумовлені цифровізацією банківських процесів – системи «Приват24», процесингова мережа та мобільні застосунки формують вектор вразливості до кібератак і витоку персональних даних. Регуляторні ризики, спричинені жорстким моніторингом з боку НБУ, призводять до зниження динаміки управлінських рішень, але підвищують прозорість корпоративного управління. Репутаційні загрози посилюються внаслідок судових процесів, інформаційних атак і політичного тиску на державні банки [4-5].

На основі «карти ризиків діяльності АТ КБ «ПриватБанк»» визначено, що найвищі індекси ризиковості мають чинники:

- ескалація воєнних дій;
- зростання NPL;
- кібератаки та технічні збої в системах.

Система управління ризиками банку базується на трирівневій моделі контролю, що включає операційний менеджмент, незалежний підрозділ комплаєнсу та службу внутрішнього аудиту. У поєднанні з державними гарантіями капіталу та впровадженням процедур кіберстійкості відповідно до DORA це забезпечує підтримання стабільності навіть в умовах пікових загроз.

Проведений аналіз засвідчив, що сучасні виклики банківської безпеки в Україні мають мультифакторну природу. Для їхнього подолання потрібна інтегрована модель управління ризиками, що охоплює фінансовий моніторинг, стрес-тестування, кіберзахист і комплаєнс-контроль. Досвід ПриватБанку доводить, що поєднання макрофінансової підтримки, нормативної гнучкості та цифрової трансформації здатне мінімізувати вплив системних ризиків. Теоретична цінність дослідження полягає у формуванні методології кількісної оцінки ризикової експозиції, практична у можливості використання результатів для побудови адаптивної системи банківської безпеки на національному рівні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Директива Європейського Парламенту і Ради (ЄС) 2022/2555 від 14 грудня 2022 р. про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2). *Офіційний вісник Європейського Союзу,* L 333/80, 27.12.2022. URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text (дата звернення: 28.10.2025).

2. Огляд банківського сектору, травень 2025 року. *Національний банк України.* URL: https://bank.gov.ua/ua/news/all/oglyad-bankivskogo-sektoru-traven-2025-roku (дата звернення: 28.10.2025).

3. Оновлено вимоги щодо організації системи внутрішнього контролю в банках та банківських групах. *Національний банк України.* URL: https://bank.gov.ua/ua/news/all/onovleno-vimogi-schodo-organizatsiyi-sistemi-vnutrishnogo-kontrolyu-v-bankah-ta-bankivskih-grupah (дата звернення: 28.10.2025).

4. Кіберзахист під час війни: виклики та рішення. *PROIT*. 11 вересня 2024. URL: https://proit.ua/kiberzakhist-pid-chas-viini-vikliki-ta-rishiennia/ (дата звернення: 28.10.2025).

5. Кльоба Л., Кльоба Т. Кіберзагрози банківського сектора в умовах воєнного стану в Україні. *Financial and Credit Activity: Problems of Theory and Practice.* 2022. Т. 5, № 46. С. 19–28. DOI: https://doi.org/10.55643/fcaptp.5.46.2022.3883.