DOI: https://doi.org/10.26642/ema-2026-1(115)-179-186
УДК 336.7

Н.Г. Виговська, д.е.н., проф.
Т.П. Остапчук, д.е.н., проф.
І.В. Литвинчук, к.е.н., доц.
О.С. Новак, к.е.н., доц.
К.Г. Шатонська, магістр
Державний університет «Житомирська політехніка»

Особливості фінансової політики системно важливих банків (на прикладі АТ КБ «ПриватБанк»)

Стаття комплексно висвітлює особливості фінансової політики системно важливих банків крізь призму фінансової, операційної та кібернетичної стійкості на матеріалах АТ КБ «ПриватБанк» (далі – ПриватБанк) і банківської системи загалом. Актуальність зумовлена воєнно-економічною турбулентністю, зростанням частоти та складності кібератак, а також посиленням регуляторних вимог до управління ризиками. Методологічно дослідження спирається на аналіз офіційних документів банку (статут, структура управління, капітал), публічної фінансової звітності за 2022–2024 рр., оглядів НБУ (травень 2025) і порівняльний аналіз міжнародних рамок. Показано, що стратегія українських банків, зокрема ПриватБанку, тяжіє до консервативного управління ризиком – домінування інвестицій у державні цінні папери, високі буфери ліквідності та резервування під NPL (покриття 83–96 %) поєднуються з обмеженою кредитною активністю в умовах підвищеної невизначеності. Інтегральна карта ризиків підтверджує середньо-високий профіль загроз – сукупний індекс 2483,33 формується домінацією макро- та форс-мажорних чинників, підсилених кредитними й операційно-кібернетичними ризиками, а також репутаційно-регуляторними впливами. На цій основі обґрунтовано модель цільового посилення безпеки: (1) імплементація функцій NIST CSF у процесах IT- та бізнес-континуїтету; (2) регулярне тестування операційної стійкості у форматі британських SS1/21/CBEST-підходів; (3) гармонізація з DORA/NIS2 до 2025 р. з акцентом на управління ICT-ризиками й нагляд за критичними провайдерами; (4) розбудова національної платформи обміну кіберзагрозами за аналогією FS-ISAC та розширення взаємодії з CSIRT-NBU. Наукова новизна полягає в інтеграції фінансових метрик стійкості з операційно-кібернетичними індикаторами в єдиній ризик-матриці, а практичне значення у формуванні дорожньої карти для НБУ та системно важливих банків щодо масштабованого впровадження resilience-контурів і комплаєнс-процедур в умовах війни.

Ключові слова: *фінансова політика; системно важливий банк; банківська безпека; операційна стійкість; кібербезпека; DORA; NIS2; CSIRT-NBU; FS-ISAC; NPL; ризик-менеджмент; комплаєнс; стрес-тестування; ПриватБанк; Національний банк України.*

Актуальність теми. Сучасний стан банківської системи України визначається поєднанням воєнно-економічних шоків, різко зростаючих кіберзагроз і глибокої цифровізації фінансових послуг. На тлі переходу банків до дистанційних каналів, мобільних застосунків і віддаленої ідентифікації пріоритетом формування фінансової політики стають операційна стійкість, кіберзахист і регуляторний комплаєнс за вимогами НБУ та європейського права [1–4]. Аналітика НБУ засвідчує відновлення ліквідності й одночасно посилення залежності системи від безперервності IT-сервісів та протидії кіберінцидентам [5–6]. У цих умовах системно важливі установи, зокрема АТ КБ «ПриватБанк», виконують роль фінансових стабілізаторів, поєднуючи внутрішньоринкову надійність із підвищеною чутливістю до зовнішніх ризиків і кібератак [7–11]. Актуальність дослідження зумовлена необхідністю зіставити національну модель безпеки з провідними міжнародними підходами США та Великої Британії і прискорити регуляторну конвергенцію з ЄС.

Аналіз останніх досліджень та публікацій, на які спираються автори. Українські напрацювання фокусуються на зростанні кіберзагроз у банківському секторі, впровадженні інтегрованих AML/KYC-процедур і формуванні зрілої комплаєнс-функції. Зокрема, Л.Кльоба та Т.Кльоба ідентифікують спектр кіберризиків воєнного періоду й підкреслюють роль превентивних технічних і організаційних протоколів захисту [11]. Дослідження У.-Я. Грудзевич, С.Пилипенка та С.Огінок розкриває сучасну архітектуру комплаєнсу в банках України й акцентує на необхідності постійної актуалізації політик та навчання персоналу [12]. Регуляторний контур і галузеві сервіси підтримки кіберстійкості деталізовані в офіційних матеріалах НБУ і CSIRT-NBU, що інституціоналізують обмін індикаторами компрометації, вимоги до системи внутрішнього контролю й моделі «трьох ліній захисту» [3; 6]. Зарубіжні фреймворки формують

© Н.Г. Виговська, Т.П. Остапчук, І.В. Литвинчук, О.С. Новак, К.Г. Шатонська, 2026

еталон для порівняння: рамка NIST CSF, міжвідомчі керівництва FDIC та огляд Федеральної резервної системи репрезентують ризик-орієнтований підхід до кіберстійкості фінсектору США [13–14], у Великій Британії PRA/FCA запровадили регламентовану «операційну стійкість» із тестуванням CBEST і картографуванням критичних послуг [15–16]. Європейський курс закріплюється нормативами цифрової операційної стійкості та NIS2, що підвищують вимоги до моніторингу інцидентів, тестування, управління IT-постачальниками й аудиту [4]. Однак бракує емпіричних українських досліджень, які б досліджували фінансову політику системно важливих банків, яка б поєднувала регуляторні вимоги, ризик-метрики та фактичні кіберподії – прогалину, яку ми частково заповнюємо кейсом АТ КБ «ПриватБанк».

Постановка завдання. Метою дослідження є комплексна оцінка особливостей формування фінансової політики системно важливих банків, яка створюється на перетині трьох вимірів – регуляторного, операційно-технологічного та ризик-фінансового. Емпіричною основою є кейс АТ КБ «ПриватБанк», для якого здійснюється аналіз ліквідності, структури активів / зобов'язань, динаміки NPL і резервування та оцінка елементів внутрішнього контролю й інформаційної безпеки на підставі офіційних документів банку і секторальних оглядів НБУ. Поставлена мета деталізується в таких завданнях: систематизація національних нормативних вимог до внутрішнього контролю, комплаєнсу та кіберзахисту; зіставлення їх із рамкою NIST CSF і підходом PRA/FCA до операційної стійкості (на прикладі ПриватБанку); формування рекомендацій щодо пріоритетів імплементації.

Викладення основного матеріалу. АТ КБ «ПриватБанк» є не лише домінантним фінансово-кредитним інститутом держави, а й системним індикатором банківської безпекової конвергенції України, від якого залежить стійкість фінансової архітектоніки національної економіки. Його фінансово-організаційні та техно-економічні параметри надають можливість здійснювати індикативну оцінку рівня стійкості банківського сектору в умовах воєнно-економічної турбулентності, кібернетичних загроз і макрофінансової волатильності.

Первинною детермінантою системної ваги ПриватБанку є його публічно-державна форма власності, що забезпечує інституційну транспарентність корпоративного управління та регуляторний оверсайт із боку уряду й Національного банку України [1–2]. Внаслідок націоналізації 2016 р. 100 % акцій консолідовано у власності держави, тому діяльність банку функціонально корелює з реалізацією фіскально-монетарної політики держави. Згідно з аналітичними звітами НБУ [5–6], саме державні банки виконують стратегічну функцію фінансової безпекової стабілізації – гарантують платіжну дисципліну, депозитну захищеність та бюджетну ліквідність. Отже, ефективність фінансової політики ПриватБанку є своєрідним барометричним показником результативності державного фінансового регулювання.

Другим параметром системного значення є масштаб операційної інфраструктури, що обумовлює його роль соціально-економічного стабілізатора. Банк обслуговує понад 19 млн клієнтів, має понад 1 тис. структурних підрозділів і понад 10 тис. терміналів самообслуговування, формуючи національну мережу фінансової інклюзії [7; 17]. У фазі енергетичних кризових шоків 2022–2023 рр. банк забезпечив операційну стійкість завдяки диверсифікації дата-центрів, впровадженню автономних IT-рішень і резервному живленню інфраструктури. Як зазначає Л.Кльоба [11], у кризових сценаріях саме операційна резильєнтність є ключовим чинником функціональної стійкості критичної фінансової інфраструктури від систем електронних платежів до соціальних трансферів і заробітних виплат.

З позиції безпекової складової фінансової політики ПриватБанк репрезентує модель консервативного ризик-менеджменту, що ґрунтується на принципах капітальної адекватності та ліквідної диверсифікації. Упродовж 2022–2024 рр. активи банку збільшилися з 540,6 до 761,5 млрд грн, при цьому частка інвестицій у суверенні боргові інструменти зросла з 44,4 до 49,3 % [5], що говорить про стратегічну орієнтацію на низькоризикові активи та бюджетну підтримку макрофінансової стабільності. Сукупні зобов'язання банку досягли 662,3 млрд грн, з яких понад 93 % становлять депозитні пасиви клієнтів, що підтверджує високий рівень довірчої капіталізації серед домогосподарств і корпоративного сектору, навіть у період воєнної економіки. Як наголошує НБУ [5], депозитна концентрація в державному секторі є індикатором довіри до державних гарантій і чинником системної ліквідності.

Важливим елементом фінансової стабільності є капіталізаційна спроможність банку. Власний капітал зріс із 57,8 млрд грн у 2022 р. до 99,1 млрд грн у 2024 р., а резервні фонди з 11,4 до 14,8 млрд грн, що засвідчує поступове акумулювання фінансових буферів [5]. Рівень резервування непрацюючих активів перевищує 85 %, що відповідає стандартам Базельського комітету з банківського нагляду. За оцінками Fitch Ratings і Moody's, банк поєднує високу внутрішню кредитоспроможність із екзогенною вразливістю до геополітичних ризиків, що є типовим для системно важливих фінансових інститутів у конфліктних економіках [8].

У площині кібернетичної безпеки ПриватБанк утримує позиції галузевого лідера. Інституція інтегрувала NIST Cybersecurity Framework, запровадила багатофакторну автентифікацію, end-to-end шифрування та системи раннього детектування аномалій [13–14]. Співпраця з CSIRT-NBU забезпечує реальний тайминг обміну індикаторами компрометації та оперативне реагування на атаки [3; 6]. Як підкреслюють У.Я. Грудзевич, С.М. Пилипенко та С.В Огінок [12], інтероперабельність фінансових

установ із національними центрами кіберреагування формує основу кіберрезильєнтності фінансової екосистеми й мінімізує каскадні ризики. Окрім того, участь ПриватБанку в інформаційних ініціативах FS- ISAC свідчить про його інтегрованість у глобальну систему обміну кіберінцидентами [15–16].

З позиції організаційної перспективи ПриватБанк формує власну фінансову політику на засадах моделі трьох ліній захисту, що забезпечує інституційну сегментацію відповідальності та функціональну автономність контрольних контурів. Наявність департаментів комплаєнсу, ризик-менеджменту, IT-безпеки та внутрішнього аудиту формує комплексну систему внутрішнього контролю [9]. Згідно з методологічними рекомендаціями НБУ [3], у банку діє багаторівнева вертикаль управління ризиками (рис. 1).

Операційна	**Ризик-менеджмент і комплаєнс**	**Внутрішній аудит**
• Бізнес-підрозділи банку (відділення, департаменти кредитування, обслуговування тощо)	• Департамент управління ризиками, відділ комплаєнсу, служба безпеки, IT-департамент	• Підрозділ внутрішнього аудиту

Рис. 1. Банківська система внутрішнього контролю АТ КБ «ПриватБанк» за моделлю трьох ліній захисту

Банківська система внутрішнього контролю функціонує відповідно до концепції трьох ліній захисту, яка є загальновизнаним міжнародним стандартом корпоративного управління ризиками. У структурі АТ КБ «ПриватБанк» модель реалізована у класичному форматі, що забезпечує функціональне розмежування відповідальності та незалежність контролюючих суб'єктів. Перша лінія захисту – операційна, до якої належать бізнес-підрозділи банку (відділення, департаменти кредитування, роздрібного обслуговування, касових операцій тощо), які безпосередньо здійснюють фінансово-господарські операції та первинний контроль за їх коректністю. Основна функція цього рівня полягає в ідентифікації та мінімізації базових операційних ризиків у процесі повсякденної діяльності. Працівники першої лінії несуть персональну відповідальність за дотримання процедур, лімітів і внутрішніх нормативів.

Друга лінія захисту – ризик-менеджмент і комплаєнс, які організаційно представлені департаментом управління ризиками, відділом комплаєнсу, службою безпеки, IT-департаментом та іншими контрольними функціями. На відміну від операційних підрозділів, вони не генерують прибуток і не створюють операцій, а забезпечують розроблення політик ризик-контролю, формування регламентів KYC/AML, моніторинг лімітів ліквідності, процентних і ринкових ризиків, а також відповідність нормативним вимогам регулятора. Підрозділ Compliance у ПриватБанку має незалежний статус, підпорядковується члену правління з комплаєнсу, не входить до складу бізнес-напрямів і не бере участі у формуванні доходів. Його ключові функції включають моніторинг змін законодавства, верифікацію клієнтів, запобігання конфліктам інтересів і фінансовим злочинам, а також нагляд за дотриманням політик етичної поведінки.

Третя лінія захисту – внутрішній аудит – це незалежна контрольна функція, яка підпорядковується Наглядовій раді банку та звітує виключно перед нею. Підрозділ внутрішнього аудиту здійснює періодичні перевірки ефективності першої та другої ліній, проводить оцінку зрілості та ефективності системи внутрішнього контролю, а також формує аудиторські звіти з рекомендаціями для підвищення операційної надійності та відповідності регуляторним стандартам.

Наглядова рада та її комітети з ризиків та аудиту виконують функції стратегічного нагляду, забезпечуючи координацію між лініями захисту та контроль за реалізацією рекомендацій внутрішнього аудиту. Згідно з офіційними документами ПриватБанку, до єдиної системи внутрішнього контролю також входять правління та його комітети (з операційних ризиків і інформаційної безпеки), департамент ризиків, служба бухгалтерського обліку, відділ комплаєнсу, управління захисту персональних даних та інформаційної безпеки. Впроваджена структура повністю відповідає вимогам Постанови НБУ «Про організацію системи внутрішнього контролю в банках України», що передбачає застосування моделі трьох ліній захисту як обов'язкової рамкової конструкції [3]. Підхід, який використовує АТ КБ «ПриватБанк», забезпечує інституційну прозорість, чітке розмежування контрольних повноважень і багаторівневу незалежність нагляду, що підвищує здатність банку своєчасно реагувати на ризики, виявляти порушення та підтримувати сталу комплаєнс-культуру.

АТ КБ «ПриватБанк» формує власну фінансову політику відповідно до принципів правової конформності та міжнародних стандартів регуляторного комплаєнсу, інтегруючи їх у внутрішню систему управління ризиками. Основними документами, що формують культуру етики та комплаєнсу в банку, є Кодекс етики, Політика запобігання конфлікту інтересів, Політика з протидії відмиванню коштів і фінансуванню тероризму, а також низка внутрішніх регламентів, гармонізованих із вимогами

Національного банку України, Групи з розробки фінансових заходів боротьби з відмиванням грошей та нормативно-правових актів Європейського Союзу.

Усі працівники банку зобов'язані дотримуватися високих стандартів професійної етики, прозорості та належної поведінки, що передбачає недопущення зловживань посадовими повноваженнями, розголошення конфіденційної інформації або участі у корупційних схемах.

В цілому підрозділ комплаєнсу виконує роль другої лінії захисту у системі внутрішнього контролю. Його діяльність охоплює реалізацію процедур KYC/AML, а саме: ідентифікацію та верифікацію клієнтів, виявлення незвичних або об'ємних транзакцій, моніторинг підозрілих операцій і формування звітності для НБУ та фінансової розвідки, так званого фінмоніторингу. Департамент комплаєнсу забезпечує моніторинг законодавчих змін, оцінку комплаєнс-ризиків нових банківських продуктів, а також інформування Наглядової ради про виявлені відхилення від політик чи потенційні порушення принципів належного врядування.

Фінансова політика AML/CFT ПриватБанку визначає як стратегічне завдання запобігання використанню банківських послуг для відмивання доходів, одержаних злочинним шляхом, або фінансування тероризму. Антикорупційна програма банку передбачає верифікацію конфліктів інтересів, систему внутрішнього повідомлення та механізми реагування на факти порушень етичного кодексу. Важливим індикатором ефективності комплаєнс-функції є зниження регуляторних, операційних і репутаційних ризиків, що підтверджується результатами незалежних аудитів фінансового моніторингу та перевірок НБУ. ПриватБанк регулярно оновлює свої політики, внутрішні регламенти і тренінгові програми, забезпечуючи безперервну освіту персоналу з питань AML/KYC, санкційного комплаєнсу та етичного лідерства. Розглянемо інструменти системи контролю банку (табл. 1).

Таблиця 1

Система контролю фінансових, операційних та інформаційних ризиків у ПриватБанку

Напрям контролю	Зміст і механізми реалізації	Відповідальні підрозділи / Інструменти	Очікуваний результат
Контроль фінансової звітності	Щорічна перевірка окремої та консолідованої звітності незалежним аудитором; підтвердження відповідності МСФЗ	Незалежний зовнішній аудитор	Підвищення достовірності звітності, довіра інвесторів і регуляторів
Внутрішній аудит	Перевірка точності обліку кредитів, депозитів, ліквідності; застосування принципу подвійного контролю для великих операцій	Підрозділ внутрішнього аудиту	Зменшення операційних помилок і зловживань; підвищення прозорості процесів
Автоматизований контроль операцій	Системи моніторингу транзакцій, двоступенева авторизація, перевірка лімітів ліквідності та процентних ризиків у режимі реального часу	Операційні IT-системи банку, департамент ризик-менеджменту	Оперативне виявлення відхилень і ризикових операцій
Запобігання шахрайству	Аналітика транзакцій, виявлення аномалій, блокування підозрілих операцій, розслідування інцидентів	Служба безпеки, департамент комплаєнсу	Мінімізація шахрайських ризиків і втрат
Інформаційна безпека	Використання антивірусних систем, файрволів, IDS/IPS, шифрування, SIEM-моніторинг, двофакторна автентифікація; політика ІБ за ISO/IEC 27001:2022–2023; програма Bug Bounty	IT-департамент, служба інформаційної безпеки	Захист конфіденційності, цілісності та доступності даних
Моніторинг і вдосконалення контролю	Проведення внутрішніх аудитів; регулярна звітність до НБУ; обмін інформацією з CSIRT-НБУ; оновлення політик (ІБ, КСЗІ, AML)	Внутрішній аудит, НБУ, служба кіберзахисту	Безперервне підвищення ефективності системи контролю та відповідність законодавчим вимогам

Аналіз функціонування АТ КБ «ПриватБанк» ідентифікує наявність як контрольованих, так і латентно-критичних ризикових детермінант, що мультивекторно впливають на фінансову резильєнтність і стратегічну стабільність інституції. Найбільш релевантними є кредитні, операційні, регуляторні, репутаційні та макроекономічні ризики (табл. 2).

Таблиця 2

Матриця оцінки ризиків діяльності АТ КБ «ПриватБанк»

Важливість ризикового фактора	[0–1]	[2–4]	5	[6–8]	[9–10]
0,8					
0,4				R1, O2, R3, R2, C1, E1, O3, F2, F3, M1, F1	M3, O1
0,2				M2, F4	
0,1					
0,05					

Тоді загальна ризикованість діяльності становитиме:

$$W = \frac{3{,}6+\cdots+4}{15} \times 1000 = 2483{,}33.$$

Інтегральна ризикованість операційної діяльності АТ КБ «ПриватБанк» характеризується як середньо-висока та логічно корелює із результатами побудованої ризик-матриці. Структурну домінацію у ризиковому профілі формують макроекономічні та форс-мажорні детермінанти (кластер M3, M1), інтенсифіковані фінансовими ризиками (F1 – надмірна частка NPL, F2, F3 – висока еластичність депозитної бази та чутливість ліквідності). Суттєво впливають також операційні загрози цифрової інфраструктури (O1 – кібератаки, O2 – порушення безперервності мережевих процесів, O3 – кадровий дефіцит у сфері IT-безпеки) та репутаційно-регуляторні чинники (R1, R2, E1), що відображають підвищену вразливість банку до публічних інформаційних ризиків і жорсткого нормативного комплаєнсу. Агреговане значення ризикового індексу, сформоване за методикою зваженої суми, демонструє домінування «верхніх» ризиків із коефіцієнтами вагомості 0,35–0,40 та оцінками 8–10, що в сукупності дає інтегральний показник 2483,33. Можемо говорити про наявність помірної, але контрольованої експозиції до системних загроз. Ризик-баланс підтримується завдяки діючим буферним механізмам – адекватному резервуванню під кредитні втрати, державній підтримці капіталу та диверсифікації активів у суверенні боргові інструменти. Звичайно, що збереження поточної фінансової стійкості вимагає перманентного стрес-тестування ліквідності, посилення кіберстійкості банківської інфраструктури та розвитку адаптивних антикризових сценаріїв управління.

Порівняльний аналіз фінансових політик банків США, Великої Британії та Естонії демонструє, що ключовою тенденцією сучасного фінансового нагляду є інтеграція регуляторних, технологічних і організаційних компонентів у єдину архітектуру фінансової та кібернетичної стійкості. Для України цей досвід є стратегічно релевантним, оскільки воєнно-економічна турбулентність та зростання кіберзагроз потребують системного посилення операційної стійкості національної банківської системи. У цьому контексті АТ КБ «ПриватБанк» є не лише найбільшим фінансовим оператором країни, а й пілотним майданчиком для імплементації міжнародних стандартів кіберзахисту й управління ризиками.

Модель США може бути використана як еталон для побудови інституційно стратифікованої системи банківського супервізорства. Запровадження в Україні національного центру обміну інформацією про кіберінциденти, аналогічного FS-ISAC, дозволить посилити кооперацію між банками, НБУ та урядовими структурами у сфері інформаційної безпеки. Крім того, адаптація NIST Cybersecurity Framework, заснованої на функціях Identify, Protect, Detect, Respond, Recover, сприятиме інтеграції кіберзахисту у внутрішні контури ризик-менеджменту банків, забезпечуючи їхню адаптивну кіберстійкість [13–14]. Британський досвід демонструє необхідність переходу до регуляторної парадигми операційної стійкості, яку реалізує Банк Англії та Управління з фінансового регулювання [15]. Український ПриватБанк уже має технічну базу для імплементації аналогічної системи – регулярне стрес-тестування IT-інфраструктури, картографування критичних процесів і розробку планів безперервності діяльності. Запровадження наглядової політики НБУ за зразком Supervisory Statement SS1/21 дозволило б підвищити контроль за відновлюваністю банків після кіберінцидентів і енергетичних збоїв.

Естонська модель демонструє переваги гібридного підходу, який поєднує національний пруденційний нагляд Finantsinspektsioon, стандарти ЄЦБ та вимоги Регламенту (ЄС) 2022/2554 [4; 18]. Україна може використати цей досвід через гармонізацію вітчизняного законодавства із DORA і GDPR, а також впровадження системи цифрової ідентифікації клієнтів за аналогією з естонською e-Residency, що сприятиме інтеграції українських банків у європейський фінансово-кібернетичний простір і зміцненню довіри іноземних партнерів.

На практичному рівні ПриватБанк здатен стати національним хабом кіберстійкості, що акумулює досвід США, Британії та Естонії. Його масштабна IT-інфраструктура, інституційна підтримка держави та впроваджені стандарти NIST і ISO/IEC 27001 створюють основу для трансформації банку у модельний центр банківської безпеки України. На основі такого досвіду доцільно розробити державну Стратегію кіберрезильєнтності фінансового сектору, яка об'єднає зусилля НБУ, Служби безпеки України, Мінцифри та провідних банків. Уособлення міжнародних практик у діяльності ПриватБанку спроможне прискорити інституціональну модернізацію української фінансової екосистеми, сформувати синергію між регуляторними механізмами, технологічним захистом та людським капіталом, і в перспективі – забезпечити інтеграцію України до європейської системи фінансової безпеки.

Висновки та перспективи подальших досліджень. Проведене дослідження довело, що фінансова політика банківських установ у сучасних умовах формується на перетині фінансової, операційної та кібернетичної резильєнтності, утворюючи триєдину архітектуру стійкості, притаманну сучасним фінансовим системам розвинених країн. На матеріалах АТ КБ «ПриватБанк» засвідчено, що у вітчизняних умовах ця модель має потенціал перетворитися на інституційний каркас національної фінансової безпеки. Банк виконує роль системного індикатора ефективності ризик-менеджменту, демонструючи високий рівень адаптивності до воєнно-економічних шоків, збалансованість між ліквідністю, капітальною адекватністю та технологічною операційною стійкістю. Його державна форма власності та пряма інтеграція в регуляторний контур НБУ забезпечують прозорість управлінських процесів і стабільність фінансової архітектоніки країни. Паралельно впровадження міжнародних фреймворків NIST Cybersecurity Framework та ISO/IEC 27001 створює платформу для розвитку цифрового суверенітету банківського сектору. Запропонована модель поєднує фінансову дисципліну, технологічну кіберрезильєнтність та регуляторну відповідність, що відповідає європейським практикам DORA і NIS2. Інтегральна оцінка ризикованості діяльності ПриватБанку вказує на середньо-високий рівень загроз, спричинених макрофінансовою волатильністю, частотою кібератак і регуляторно-репутаційними чинниками. Буфери фінансової безпеки, понад 85 % резервування NPL, капітальна підтримка держави та диверсифікація активів гарантують контрольованість ризикового профілю. Відповідно, це дозволяє класифікувати банк як фінансово стабільний інститут із підвищеним потенціалом до довгострокової кіберстійкості.

З позиції міжнародної конвергенції, досвід США, Великої Британії та Естонії (може бути інтегрований у національну нормативну екосистему для формування єдиного стандарту операційної та кібернетичної безпеки фінансового сектору). Він має об'єднати регуляторні вимоги НБУ, державні політики кіберзахисту та інституційні протоколи банківської спільноти, забезпечивши конвергенцію з європейською фінансово-технологічною системою.

У цьому контексті ПриватБанк може стати пілотним центром кіберстійкості України, що практично демонструє інтеграцію міжнародних стандартів інформаційної безпеки, внутрішнього комплаєнсу та ризик-менеджменту в умовах воєнно-економічної турбулентності. Його досвід доцільно масштабувати для розроблення Національної стратегії кіберстійкості фінансового сектору, у межах якої мають взаємодіяти НБУ, СБУ, Мінцифри, Міністерство фінансів та провідні комерційні банки.

Перспективи подальших досліджень полягають у створенні інтегрованих моделей оцінювання кіберрезильєнтності на основі багатокритеріальних індикаторів; емпіричному аналізі ефективності імплементації директив DORA і NIS2 у вітчизняну практику; моделюванні впливу кіберінцидентів на ліквідність і кредитоспроможність банків; розробці національної методики resilience-scoring для системно важливих установ; дослідженні поведінкових аспектів фінансової безпеки – human factor security, комплаєнс-етики, навчання персоналу.

Отже, майбутня система банківської безпеки України має ґрунтуватися на синергії між регуляторним комплаєнсом, фінансовою стабільністю та цифровою кіберрезильєнтністю. Вона забезпечить не лише захист банківської інфраструктури, а й поступову інтеграцію України в європейський фінансово-технологічний простір, підвищуючи її глобальну економічну суб'єктність і стійкість у посткризовій архітектурі світової фінансової системи.

Список використаної літератури:

1. Про банки і банківську діяльність : Закон України від 07.12.2000 р. № 2121-III ; станом на 30 лип. 2025 р. [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2121-14.
2. Про Національний банк України : Закон України від 20.05.1999 р. № 679-XIV ; станом на 28 серп. 2025 р. [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/679-14.
3. Оновлено вимоги щодо організації системи внутрішнього контролю в банках та банківських групах / Національний банк України [Електронний ресурс]. – Режим доступу : https://bank.gov.ua/ua/news/all/onovleno-vimogi-schodo-organizatsiyi-sistemi-vnutrishnogo-kontrolyu-v-bankah-ta-bankivskih-grupah.
4. 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. – 2022. – L 333/80 [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text.

5. Огляд банківського сектору, травень 2025 року / Національний банк України [Електронний ресурс]. – Режим доступу : https://bank.gov.ua/ua/news/all/oglyad-bankivskogo-sektoru-traven-2025-roku.
6. Сервіси CSIRT-NBU. Команда реагування на кіберінциденти в банківській системі України / CSIRT-NBU [Електронний ресурс]. – Режим доступу : https://cyber.bank.gov.ua/bankam.
7. Про банк / ПриватБанк [Електронний ресурс]. – Режим доступу : https://privatbank.ua/about.
8. Рейтинги і нагороди / ПриватБанк [Електронний ресурс]. – Режим доступу : https://privatbank.ua/about/credentials.
9. Організаційна структура управління АТ КБ «ПриватБанк» [Електронний ресурс]. – Режим доступу : https://static.privatbank.ua/files/0000003455633596.pdf.
10. Кіберзахист під час війни: виклики та рішення / PROIT. – 2024 р. [Електронний ресурс]. – Режим доступу : https://proit.ua/kiberzakhist-pid-chas-viini-vikliki-ta-rishiennia/.
11. *Кльоба Л.* Кіберзагрози банківського сектора в умовах воєнного стану в Україні / *Л.Кльоба, Т.Кльоба* // Financial and Credit Activity: Problems of Theory and Practice. – 2022. – Т. 5, № 46. – С. 19–28. DOI: 10.55643/fcaptp.5.46.2022.3883.
12. *Грудзевич У.Я.* Комплаєнс-політика банків України на сучасному етапі / *У.Я. Грудзевич, С.М. Пилипенко, С.В. Огінок* // Економіка та суспільство. – 2024. – Вип. 60. DOI: 10.32782/2524-0072/2024-60-128.
13. A Framework for Cybersecurity. – Washington, D.C. : FDIC [Electronic resource]. – Access mode : https://www.fdic.gov/bank-examinations/framework-cybersecurity.
14. Cybersecurity and Financial System Resilience Report : Report to Congress / Federal Reserve System. – 2025 [Electronic resource]. – Access mode : https://www.federalreserve.gov/publications/files/cybersecurity-report-202507.pdf.
15. Operational resilience of the financial sector / Bank of England. – 2025 [Electronic resource]. – Access mode : https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector.
16. Operational resilience / Financial Conduct Authority (FCA). – 2017 [Electronic resource]. – Access mode : https://www.fca.org.uk/firms/operational-resilience.
17. АТ КБ «ПриватБанк» / Opendatabot [Електронний ресурс]. – Режим доступу : https://opendatabot.ua/c/14360570.
18. Cybersecurity Strategy 2024–2030 «Cyber-Conscious Estonia» / Ministry of Economic Affairs and Communications for Estonia. – Tallinn, 2024 [Electronic resource]. – Access mode : https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_2024_en.pdf.

References:

1. Verkhovna Rada Ukrainy (2000), *Pro banky i bankivsku diialnist*, Zakon Ukrainy vid 07.12.2000 r. No. 2121-III, stanom na 30 lyp. 2025 r., [Online], avaible at: https://zakon.rada.gov.ua/laws/show/2121-14
2. Verkhovna Rada Ukrainy (1999), *Pro Natsionalnyi bank Ukrainy*, Zakon Ukrainy vid 20.05.1999 r. No. 679-XIV, stanom na 28 serp. 2025 r., [Online], avaible at: https://zakon.rada.gov.ua/laws/show/679-14
3. Natsionalnyi bank Ukrainy, *Onovleno vymohy shchodo orhanizatsii systemy vnutrishnoho kontroliu v bankakh ta bankivskykh hrupakh*, [Online], avaible at: https://bank.gov.ua/ua/news/all/onovleno-vimogi-schodo-organizatsiyi-sistemi-vnutrishnogo-kontrolyu-v-bankah-ta-bankivskih-grupah
4. *Dyrektyva Yevropeiskoho Parlamentu i Rady (YeS) 2022/2555 vid 14 hrudnia 2022 r. pro zakhody dlia vysokoho spilnoho rivnia kiberbezpeky na vsii terytorii Soiuzu, vnesennia zmin do Rehlamentu (YeS) No. 910/2014 ta Dyrektyvy (YeS) 2018/1972 ta skasuvannia Dyrektyvy (YeS) 2016/1148 (Dyrektyva NIS 2)* (2022), Ofitsiinyi visnyk Yevropeiskoho Soiuzu, L 333/80, [Online], avaible at: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text
5. Natsionalnyi bank Ukrainy (2025), *Ohliad bankivskoho sektoru, traven 2025 roku*, [Online], avaible at: https://bank.gov.ua/ua/news/all/oglyad-bankivskogo-sektoru-traven-2025-roku
6. CSIRT-NBU, *Servisy CSIRT-NBU. Komanda reahuvannia na kiberintsydenty v bankivskii systemi Ukrainy*, [Online], avaible at: https://cyber.bank.gov.ua/bankam
7. PryvatBank, *Pro bank*, [Online], avaible at: https://privatbank.ua/about
8. PryvatBank, *Reitynhy i nahorody*, [Online], avaible at: https://privatbank.ua/about/credentials
9. *Orhanizatsiina struktura upravlinnia AT KB «PryvatBank»*, [Online], avaible at: https://static.privatbank.ua/files/0000003455633596.pdf
10. PROIT (2024), *Kiberzakhyst pid chas viiny: vyklyky ta rishennia*, [Online], avaible at: https://proit.ua/kiberzakhist-pid-chas-viini-vikliki-ta-rishiennia/
11. Kloba, L. and Kloba, T. (2022), «Kiberzahrozy bankivskoho sektora v umovakh voiennoho stanu v Ukraini», *Financial and Credit Activity: Problems of Theory and Practice*, Vol. 5, No. 46, pp. 19–28, doi: 10.55643/fcaptp.5.46.2022.3883.
12. Hrudzevych, U.Ya., Pylypenko, S.M. and Ohinok, S.V. (2024), «Komplaiens-polityka bankiv Ukrainy na suchasnomu etapi», *Ekonomika ta suspilstvo*, Issue 60, doi: 10.32782/2524-0072/2024-60-128.
13. *A Framework for Cybersecurity*, FDIC, D.C., Washington, [Online], avaible at: https://www.fdic.gov/bank-examinations/framework-cybersecurity
14. Federal Reserve System (2025), *Cybersecurity and Financial System Resilience Report, Report to Congress*, [Online], avaible at: https://www.federalreserve.gov/publications/files/cybersecurity-report-202507.pdf
15. Bank of England (2025), *Operational resilience of the financial sector*, [Online], avaible at: https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector
16. Financial Conduct Authority (2017), *Operational resilience*, [Online], avaible at: https://www.fca.org.uk/firms/operational-resilience
17. Opendatabot, *AT KB «PryvatBank»*, [Online], avaible at: https://opendatabot.ua/c/14360570
18. Ministry of Economic Affairs and Communications for Estonia (2024), *Cybersecurity Strategy 2024–2030 «Cyber-Conscious Estonia»*, [Online], avaible at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_2024_en.pdf

Виговська Наталія Георгіївна – доктор економічних наук, професор, завідувач кафедри фінансів та цифрової економіки Державного університету «Житомирська політехніка».
https://orcid.org/0000-0001-7129-6169.
Наукові інтереси:
- публічні фінанси;
- фінанси підприємств;
- державний фінансовий контроль.

Остапчук Тетяна Петрівна – доктор економічних наук, професор, завідувач кафедри менеджменту, бізнесу та маркетингових технологій Державного університету «Житомирська політехніка».
https://orcid.org/0000-0001-9623-0481.
Наукові інтереси:
- облік інвестиційної діяльності;
- облікове забезпечення управління земельними ресурсами суб'єктів господарювання;
- облік в системі управління підприємством;
- HR-менеджмент;
- маркетинг-менеджмент.

Литвинчук Ірина Вікторівна – кандидат економічних наук, доцент кафедри фінансів та цифрової економіки Державного університету «Житомирська політехніка».
https://orcid.org/0000-0003-3316-4952.
Наукові інтереси:
- бюджетний менеджмент;
- банківський менеджмент;
- податковий менеджмент.

Новак Оксана Сергіївна – кандидат економічних наук, доцент кафедри фінансів та цифрової економіки Державного університету «Житомирська політехніка».
https://orcid.org/0000-0002-5671-0306.
Наукові інтереси:
- похідні фінансові інструменти;
- фінансові ринки та фінансова стабільність;
- валютна політика.

Шатонська Крістіна Геннадіївна – магістр фінансів, банківської справи, страхування та фондового ринку Державного університету «Житомирська політехніка».
https://orcid.org/0009-0005-3840-9797.
Наукові інтереси:
- банківський менеджмент.

Vyhovska N.H., Ostapchuk T.P., Lytvynchuk I.V., Novak O.S., Shatonska K.G.

Financial policy features of systemically important banks: a case study of JSC CB «PrivatBank»

This article provides a comprehensive analysis of the financial policy features of systemically important banks (SIBs) through the prism of financial, operational, and cyber resilience, based on the case study of JSC CB «PrivatBank» and the broader Ukrainian banking system. The relevance of the study is driven by military-economic turbulence, the increasing frequency and complexity of cyberattacks, and tightening regulatory requirements for risk management. Methodologically, the research relies on the analysis of official bank documents (charter, governance structure, capital), public financial statements for 2022–2024, NBU reviews (May 2025), and a comparative analysis of international regulatory frameworks.

The study reveals that the strategy of Ukrainian banks, particularly PrivatBank, leans toward conservative risk management: a dominance of investments in government securities, high liquidity buffers, and substantial provisioning for non-performing loans (NPL coverage of 83–96 %) are combined with limited lending activity amid high uncertainty. An integrated risk map confirms a medium-high threat profile – a cumulative index of 2483.33 – driven by the dominance of macro and force majeure factors, amplified by credit, operational, and cyber risks, as well as reputational and regulatory impacts.

On this basis, a model for targeted security enhancement is justified: (1) implementation of NIST CSF functions within IT and business continuity processes; (2) regular operational resilience testing using British SS1/21/CBEST approaches; (3) harmonization with DORA/NIS2 by 2025, emphasizing ICT risk management and oversight of critical third-party providers; (4) development of a national cyber threat intelligence sharing platform similar to FS-ISAC and expanded cooperation with CSIRT-NBU. The scientific novelty lies in the integration of financial stability metrics with operational-cyber indicators within a single risk matrix. The practical significance consists in the formation of a roadmap for the NBU and SIBs regarding the scalable implementation of resilience frameworks and compliance procedures under wartime conditions.

Keywords: financial policy; systemically important bank; banking security; operational resilience; cybersecurity; DORA; NIS2; CSIRT-NBU; FS-ISAC; NPL; risk management; compliance; stress testing; PrivatBank; National Bank of Ukraine.

Стаття надійшла до редакції 05.01.2026.