УДК 336.71 **DOI**: https://doi.org/10.31521/modecon.V52(2025)-33

Чкан І. О., кандидат економічних наук, доцент, доцент кафедри фінансів, обліку та оподаткування, Таврійський державний агротехнологічний університет імені Дмитра Моторного, м. Запоріжжя, Україна

ORCID ID: 0000-0003-3764-8380
e-mail: ir4ikrok@gmail.com

Трусова Н. В., доктор економічних наук, професор, професор кафедри фінансів, обліку та оподаткування, Таврійський державний агротехнологічний університет імені Дмитра Моторного, м. Запоріжжя, Україна

ORCID ID: 0000-0001-9773-4534
e-mail: trusova_natalya5@ukr.net

Імплементація захисних параметрів електронних платежів центробанку та фінансових установ: безпеки та стабільність банківської системи

Анотація. *У статті розглядаються поглиблена методика ризик-менеджменту, для імплементації захисних параметрів в електронних платежах центробанку та фінансових установ, що використовують інформаційні FinTech-ресурси та продукти, для мінімізації загроз, управління операційною діяльністю та стабілізації платіжного депозитно-кредитного портфеля банків із державним капіталом. Обґрунтовано, що ймовірність (загроза) втрати банками частини своїх ресурсів, викликає збитки, недоотримання доходів або здійснення додаткових витрат у результаті неефективного здійснення платіжних операцій в депозитно-кредитному сегменті та у порівнянні з очікуваним варіантом, призводить до появи неочікуваних ризиків. Розширено методику ризик-менеджменту та його функціоналу щодо мінімізації загроз в трансакції депозитно-кредитних потоків фінансових установ державної та приватної форми власності. Унормування захисних параметрів електронних платежів в ризик-менеджменті банків дозволяє стримувати загрозу втрати їх ліквідної стійкості та втілює в собі складну технологічну взаємодію сервісної банківської інфраструктури та FinTech-компаній для здійснення FinTech-послуг. Визначено ТОП-20 прибуткових банків України та проведено оцінку загроз та їх впливу на рівень безпеки СЕП НБУ та банків із державним та приватним капіталом. Виокремлено еталонний державний банк, у якого найкращим є поєднання процесу сек'юритизації платіжного депозитно-кредитного портфеля та захисту активних інформаційних FinTech-ресурсів, враховуючи виконання вимог за напрямами: «поточний рівень SPDLP», «менеджмент SPDLP», «рівень усвідомлення SPDLP». Запропоновано монетарний регулятор обов'язкових вимог, як інструмент СЕП НБУ та чинник формування помірного структурного дефіциту ліквідної стійкості фінансових установ перенести до категорії інструментів довгострокового та структурного впливу для контролю за вчасного блокуванням тегрованих та фітингових атак в системі електронних платежів. Це дозволить нараховувати відсотки на величину обов'язкових резервів в платіжному депозитно-кредитному портфелі фінансових установ з метою підвищення ефективності переказів учасників СЕП.*

Ключові слова: *банківська система; безпека; електронні платежі; FinTech-ресурси; ризики; загрози; інноваційні технології.*

Chkan Iryna, PhD of Economic, Associate Professor Dmytro Motornyi Tavria State Agrotechnological University, Zaporizhzhia, Ukraine

Trusova Natalia, Doctor of Economic Sciences, Professor, Professor of the Department of Finance, Accounting and Taxation Dmytro Motornyi Tavria State Agrotechnological University, Zaporizhzhia, Ukraine

Implementation of Protective Parameters for Electronic Payments by the Central Bank and Financial Institutions: Security and Stability of the Banking System

Abstract. Introduction. *The article considers an in-depth risk management methodology for implementing protective parameters in electronic payments of the central bank and financial institutions using FinTech information resources and products to minimize threats, manage operational activities and stabilize the payment deposit and credit portfolio of banks with state capital. It is substantiated that the probability (threat) of banks losing part of their resources causes losses, lack of income or additional costs as a result of inefficient payment transactions in the deposit and credit segment and, compared to the expected option, leads to the emergence of unexpected risks.*

Purpose*. of the study and implementation of risk management methods, reserve parameters, electronic payments to the central bank and financial institutions that use information resources for FinTech products risk reduction, operational diligence management and stabilization of the payment deposit and loan portfolio from government capital.*

Results*. The risk management methodology and its functionality have been expanded to minimize threats in the transaction of deposit and credit flows of financial institutions of state and private ownership. Standardization of protective*

[1]**Стаття надійшла до редакції**: 25.07.2025
Received: 25 July 2025

parameters of electronic payments in the risk management of banks allows to contain the threat of loss of their liquidity stability and embodies the complex technological interaction of service banking infrastructure and FinTech companies for the implementation of FinTech services. The TOP-20 profitable banks of Ukraine have been determined and an assessment of threats and their impact on the level of security of the NBU's SEP and banks with state and private capital has been carried out.

***Conclusions**. A reference state bank is identified that has the best combination of the process of securitization of the payment deposit and loan portfolio and protection of active information FinTech resources, taking into account the fulfillment of requirements in the areas: "current level of SPDLP", "SPDLP management", "level of awareness of SPDLP". It is proposed to transfer the monetary regulator of mandatory requirements, as a tool of the NBU SEP and a factor in the formation of a moderate structural deficit of the liquidity stability of financial institutions, to the category of instruments of long-term and structural influence to control the timely blocking of tagged and fitting attacks in the electronic payment system. This will allow interest to be accrued on the amount of mandatory reserves in the payment deposit and loan portfolio of financial institutions in order to increase the efficiency of transfers of SEP participants.*

***Keywords**: banking system; security; electronic payments; FinTech resources; risks; threats; innovative technologies.*

***JEL Classification:** G12; G21; G31*

Постановка проблеми. В Україні банківська система як індикатор безпеки платіжних операцій, забезпечує безперебійне та якісне обслуговування споживачів банківських послуг за допомогою альтернативних засобів, які під впливом глобального поглинання паперових грошей, змінюються та набувають досконалої цифрової форми – найбільш придатної для використання на платіжному ринку технологічних новацій, що інтегруються в банківські продукти та в співробітництві із компаніями індустрії FinTech чинять вплив на національну економіку країни.

З позиції безпеки банківської системи, FinTech-ресурси забезпечують зростання децентралізованої інклюзії банківських установ на платіжному ринку, гнучкість, швидкість, доступність, якість якого стимулює розвиток платіжно-розрахункових потоків за електронними та криптовалютними операціями, з іншого – традиційний потенціал масштабування клієнтських розрахунків через банківські установи схильний до загроз навіть із гарантованою централізованою та децентралізованою регуляцією й наглядом НБУ. Зазначене потребує розробки надійного механізму забезпечення безпеки банківської системи, який спроможний модифікувати та інтегрувати захисні параметри в інформаційних FinTech-ресурсах банківських установ з метою максимізації прибутку, зростання ліквідної стійкості, з урахуванням вже оцифрованих платіжних процесів.

Аналіз останніх досліджень та публікацій. Дослідженням питань функціонування платіжних розрахунків в трансформаційному процесі банківської системи та проблематикою розвитку систем електронних платежів в Україні в контексті цифровізації економіки та глобалізаційних процесів досліджували І. Ситник, О. Богдан [4], О. Бакалинський [5], Я. Гладищук [1], О. Гривківська, О. Герасимова [2], Е. Надері, С. Пазукі, А. Асрарі [13], Н. Дієєва, В. Делейчук [6], Є. Рошан, Є. Абді [14], Б. Вишивана, О. Терешко [15]. Однак, досягти нормалізації макросередовища функціонування банківської системи лише при зміні зовнішнього і внутрішнього середовища неможливо. Цьому може сприяти алгоритми прогнозування ризикованості та ліквідності діяльності банків, здійснення заходів із регулювання високотехнологічних інструментів мінімізації платіжно-розрахункових ризиків в функціонуючому механізмі забезпечення безпеки банківської системи, за допомогою яких можливе здійснення корекції депозитно-кредитної політики у середньо- та довгостроковій перспективі.

Формулювання цілей дослідження. Метою дослідження є імплементація на засадах поглибленої методики ризик-менеджменту, захисних параметрів електронних платежів центробанку та фінансових установ, що використовують інформаційні FinTech-ресурси та продукти, для мінімізації загроз, управління операційною діяльністю та стабілізації платіжного депозитно-кредитного портфеля із державним капіталом.

Виклад основного матеріалу дослідження. Розширення методики ризик-менеджменту та його функціоналу щодо мінімізації загроз в трансакції депозитно-кредитних потоків фінансових установ державної та приватної форми власності, дозволяє забезпечувати безперебійність процесу обслуговування клієнтів системи електронних платжів на міжбанківському рівні. Унормування захисних параметрів в ризик-менеджменті банків дозволяє стримувати загрозу втрати ліквідної стійкості та втілює в собі складну технологічну взаємодію сервісної інфраструктури банків та FinTech-компаній для здійснення FinTech-послуг, за сукупністю взаємопов'язаних елементів і зв'язків між ними, впливаючи один на одного й утворюючи цілісну систему електронних платежів.

Стабільність функціонування системи електронних платежів НБУ (СЕП НБУ) під час кібернападу країни-агресора в 2022 р. дозволила упередити загрозу харекських атак злочинців та шахраїв, обмежити їх доступ до регулятора системи та нівелювати ризики розрахункових операцій учасників та користувачів платіжних систем, як в країні, так і за її межами. Війна сформувала нову парадигму розвитку СЕП НБУ, відсікаючи простір деградації в нових реаліях та зберігаючи ліквідність українських банків, оскільки останні формують основний фінансовий сектор економіки України та забезпечують країну валютним капіталом, надаючи послуги у сегменті B2B. Незважаючи на воєнні дії в Україні в 2022 р. повністю відновлено інноваційні банківські послуги щодо

обслуговування фізичних та юридичних осіб в СЕП НБУ. У середньому в день СЕП НБУ обробляє 1,4 млн платежів на суму 9,62 млрд дол. США [3]. Проте, потенціал СЕП має більший запас пропускної спроможності та щоденно може обробляти у 10 разів більше документів, ніж в теперішній воєнний час.

Забезпечення безпеки СЕП НБУ, в умовах воєнного часу, спонукає до трансформації інформаційних FinTech-ресурсів, які сконцентровані на протидії загрозам, які впливають на банківські регулятори у кіберпросторі системи електронних платежів. Для цього використовуються хмарні технологій, які не дозволяють злочинцям отримати доступ та здійснити руйнацію системи захисту в міжбанківській інфраструктурі. Регулятори безпеки СЕП НБУ захищають учасників та користувачів від загроз віртуалізації, компрометації контролерів домену, веб-сайтів банківських установ, а також знищення даних шифрування інформації. Зазначимо, що в Україні потужні кібератаки країни-агресора почались ще до початку відкритої воєнної агресії. Це були традиційні і нетрадиційні засоби-атаки, а саме: DDOS-атаки, BGP Hijacking-атаки, атаки вірусами-шифрувальниками, панічні атаки (атаки, спрямовані на спотворення контенту держсайтів), (рис. 1).

Згідно даних НБУ, майже усі кібератаки на банківську систему країни здійснювались хакерськими угрупованнями Armageddon, Fancy Bears [3]. Проти банківської системи України використовувались складні, добре підготовлені кібернапади, зокрема, атаки на ланцюжок грошових потоків. Наприклад, атака на M.E.doc призвела до зупинки частини банківської системи України. Подібні кібервтручання були спрямовані на компрометацію розробника програмного забезпечення і готувались дуже довго – навіть роками. Однак уже за 4 місяці повномасштабної війни в 2022 р. агресор перейшов до більш простих атак: DDoS, дискредитації контенту, панічних атак, злому маршрутизаторів [3].

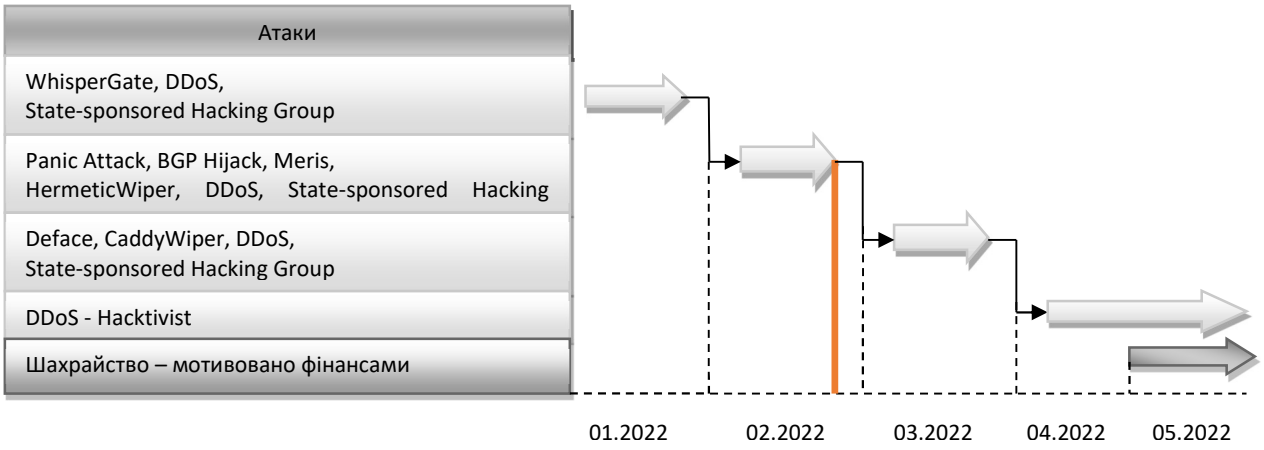

Рисунок 1 – **Хронологія атак на НБУ та банківську систему України в 2022 р.**

Джерело: побудовано за даними [3]

Кібернапади країни-агремора на СЕП НБУ складались з двох напрямів: тегретовані DDoS-атаки різного характеру, врятовані на знищення банківська система країни; фішингові атаки різних типів – різні види шахрайств проти учасників та користувачів системи електронних платежів.

Хронологічність кібератак свідчить, що з грудня 2021 р. по березень 2022 р. НБУ було складно протистояти кіберзагрозам. Починаючи з квітня 2022 р. всі атаки стали грубішими та масованішими у кіберпросторі СЕП НБУ. Тегретовані DDoS-атаки різного характеру, позбавляли власників платіжних карток (фізичних та юридичних осіб) можливості своєчасно отримувати грошові перекази та проводити розрахункові операції через СЕР, як в межах країни, так і за кордоном [3].

В контексті протидії загрозам інформаційним FinTech-ресурсам в кіберпросторі СЕП банківської системи були введені деякі заходи. По-перше, НБУ прискорив адаптації банків до регуляторно-нормативної бази в умовах воєнного часу (наприклад, оперативно ухвалено постанову №42 «Про використання банками хмарних послуг в умовах воєнного стану в Україні») [8]. Згідно цієї постанови, у рекордно стислі терміни, технічний банківській сервіс щодо послуг на обслуговування учасників та користувачів СЕП перемістились у хмари, які знаходяться на безпечній території. Тобто, НБУ надав дозвіл банкам впровадити безпечні інформаційні FinTech-ресурси за кордоном. По-друге, встановлення нового виду взаємодії та взаємодопомоги, як із правоохоронними органами та службами безпеки банківських установ, а також із міжнародними партнерами [3].

Центр захисту СЕП НБУ працює в режимі реального часу, надає інформацією про загрози в FinTech-ресурсах та засоби боротьби із ними, які масово

використовуються для кібератак, шляхом взаємодії із національними телеком-провайдерами та надсилання Abuse-reports користувачам платіжних систем, розробникам IT-систем, міжнародним організаціям та провайдерам хмарних послуг із кіберзахисту даних для блокування фішингових ресурсів та зловмисних мобільних дій. Наприклад, керування ключами – тобто збільшення тривалості життєвого циклу ключів або паролів, а також віддалений доступ і використання хмарних систем. В 2022 р. жодна система НБУ не була взламана у платіжних системах банківського сектору. При наявності загроз внаслідок DDoS-атак та атак пов'язаних із вірусами-шифрувальниками, не відбулось витоку інформації, зокрема чутливих даних [3].

Проте, використання хмарних технологій вимагає певного рівня зрілості від їх провайдерів. Це стосується не тільки інформаційної безпеки СЕП НБУ, але й забезпечення вимог законодавства щодо імплікації фінансового моніторингу у встановленому законом порядку для ведення операційної діяльності групою банків державної та приватної форми власності, із законами країн, чиї провайдери надають хмарні послуги. Зазначимо, що хмарні послуги можуть використовуватись у будь якому географічному просторі і дуже складно встановити бенефіціара. На сьогодні НБУ рекомендує банкам використовувати хмарні технології, але усвідомлювати свою відповідальність, запроваджуючи цифровізацію FinTech-ресурсів з країнами світу, пришвидшуючи процеси кредитування та депозитування через платіжні системи, розвиваючи банківські послуги, розширюючи мережу сервісу розстрочки та QR-платежів [16, с. 584].

Блокчейн, як пріоритетний інструмент «блакитних океанів» фінансових інновацій дозволяє зберігати та використовувати інформаційні FinTec-ресурси у сфері P2P-депозитування. В Україні послуги P2P-депозитування надає АТ «Приватбанк», пропонуючи високу дохідність (у середньому +5% річних від базових ставок за вкладами) [16, с. 585]. Серед платіжних цифрових сервісів необанкінгу, які впроваджені в українську СЕП є електронні платіжні системи Skrill та Transfer Wise, а також Venmo та Braintree, які ввійшли до складу міжнародної платіжної системи PayPal та WePay. Партнером системи Transfer Wise є АТ «Приватбанк» [11, с. 76], водночас Monobank активно використовує власну клієнтську базу [12].

В умовах воєнного часу СЕП підтримується за допомогою НБУ та банків з державним та приватним капіталом, в яких загроза ліквідної стійкості нівелюється за допомогою цифрових IT-платформ країн ЄС із використання інноваційної моделі «4Р». За допомогою банківського регулятора, ефективність функціонування системи електронних платежів в Україні щоквартально відновлюється після диспропорцій у відхиленні від безпечних захисних параметрів, спричинених дезінформацією та шахрайством злочинців. Зазначимо, що загрози банківським інноваціям (системі електронних платежів) за походженням та можливістю впливу на ліквідну стабільність фінансових установ є більш керованими. Оцінка загроз в електронних платіжних системах України в 2024 рр. та їх вплив на рівень безпеки НБУ, а також групи банків із державним та приватним капіталом представлено на рис. 2.

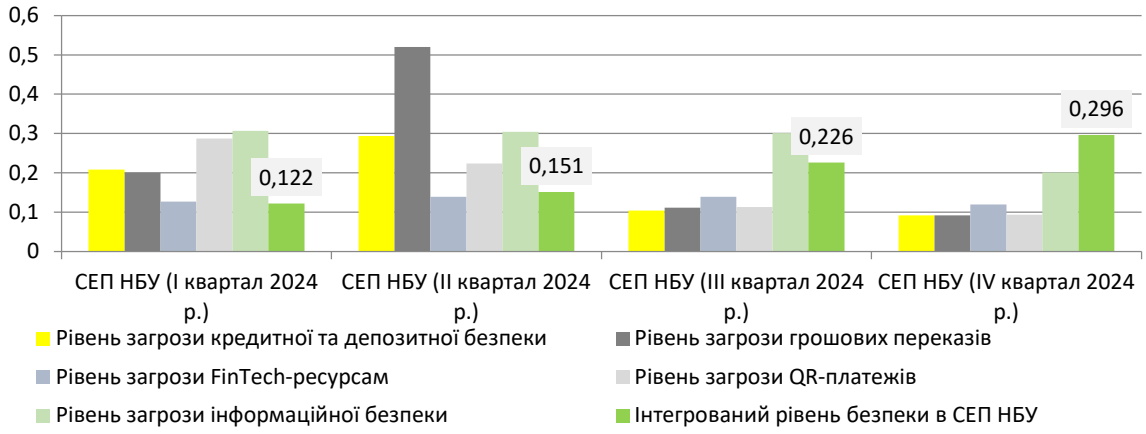

Рисунок 2 **Оцінка загроз та їх вплив на рівень безпеки СЕП НБУ за I-VI квартал 2024 р.**

Джерело: побудовано за даними [7; 8; 10; 11]

Високий рівень загроз кібератак спостерігався на СЕП НБУ, зокрема, у I-II кварталі 2024 р. – від 0,208 до 0,294 (рівень загрози кредитної та депозитної безпеки), від 0,200 до 0,520 (рівень загроз грошових переказів), від 0,287 до 0,224 (рівень загроз QR-платежів), а також у I-IV кварталі 2024 р. – від 0,307 до 0,201 (рівень загроз інформаційної безпеки). Проте, за рахунок зниження загроз в FinTech-ресурсах НБУ в проміжку між III-IV кварталами із 0,139 до 0,119 або до рівня 85,6%. Це дозволило стабілізувати рівень безпеки банківської системи до 29,6%, який має

динаміку до підвищення в 2025 р., що характеризує позитивну тенденцію для економіки країни.

Оцінка загроз в електронних платіжних системах в групі банків із державним та приватним капіталом представлено на рис. 3.

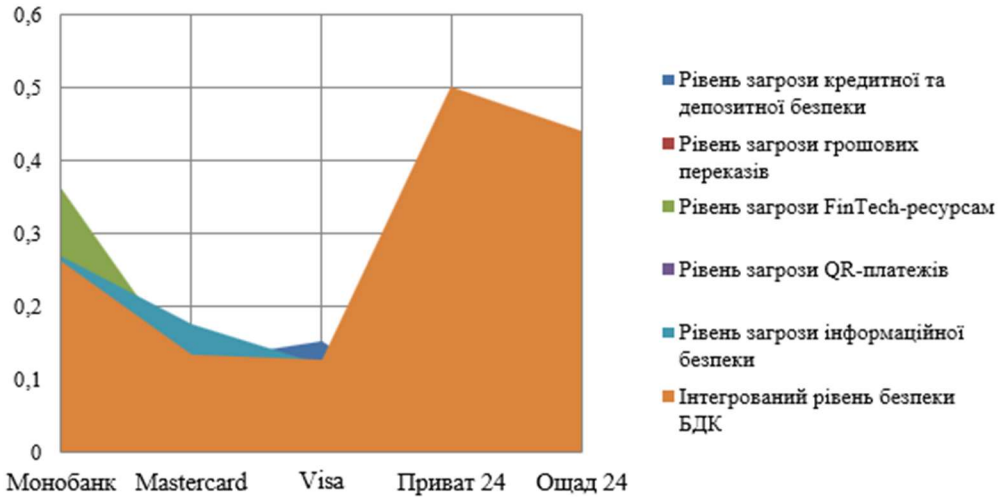

Рисунок 3 – **Оцінка загроз в електронних платіжних системах та їх вплив на рівень безпеки банків із державним та приватним капіталом (БДК) за 2024 р.**

Джерело: побудовано за даними [7; 8; 10; 11]

Зокрема, протягом I-IV кварталу 2024р. рівень впливу загроз в системі електронних платежів «Монобанк» коливався в межах від 0,243 до 0,361, що обумовлено високим рівнем кібератак на FinTech-ресурси (0,361), кредитної та депозитної безпеки (0,243), високим рівнем шахрайства в грошових переказах (0,265), а також загроз інформаційної безпеки платіжної системи в цілому (0,268). Тобто, рівень безпеки електронної платіжної системи «Монобанк» складає лише 26,2%.

Нестабільний період функціонування платіжної системи «Приват 24» спостерігався в I-II кварталі 2024 р. (рівень загроз QR-платежів в цей період дорівнював від 0.086 до 0.083, рівень загроз інформаційної безпеки – від 0.116 до 0,113). В цілому, рівень безпеки електронної платіжної системи «Приват 24» з-поміж сукупності платіжних систем склав 50,2%. Найбезпечнішими платіжними системами, які функціонують наразі в воєнний період в Україні – системи електронних платежів «Mastercard», «Visa». В цілому, за 2024 р., інтегрований рівень безпеки електронної платіжної системи «Mastercard» в нестабільних умовах функціонування інформаційних FinTech-ресурсів склав 13,4%, «Visa» – 12,8%. Рівень безпеки електронної платіжної системи «Ощад 24» за 2024 р. коливається в межах 44,1%.

Об'єктивні фактори зовнішнього середовища функціонування групи фінансових установ на вимоги регуляторів до ризиковості обсягу операційної діяльності дозволили нам констатувати, що зростання прибутку банків України призупинилось через неврегульованість повномасштабного воєнного конфлікту та нестабільність фінансово-політичної ситуації в країні. Проте вони продовжують демонструвати прибуткову діяльність. Так, платоспроможні банки України за І квартал 2025 р. отримали 39,97 млрд грн прибутку, що на 0,2% більше, ніж в аналогічному періоді 2024 р. За рейтингом прибутковості серед групи державних банків перше місце займає ПриватБанк, який отримав 16,89 млрд грн. На другому місці Ощадбанк (4,775 млрд грн), на третьому – Укрексімбанк (2,47 млрд грн). На четвертому місці установа іноземної банківської групи – Райффайзен Банк із 2,215 млрд грн і приватний Універсал Банк – 1,74 млрд грн [8]. ТОП-20 прибуткових банків України представлено на рис. 4.

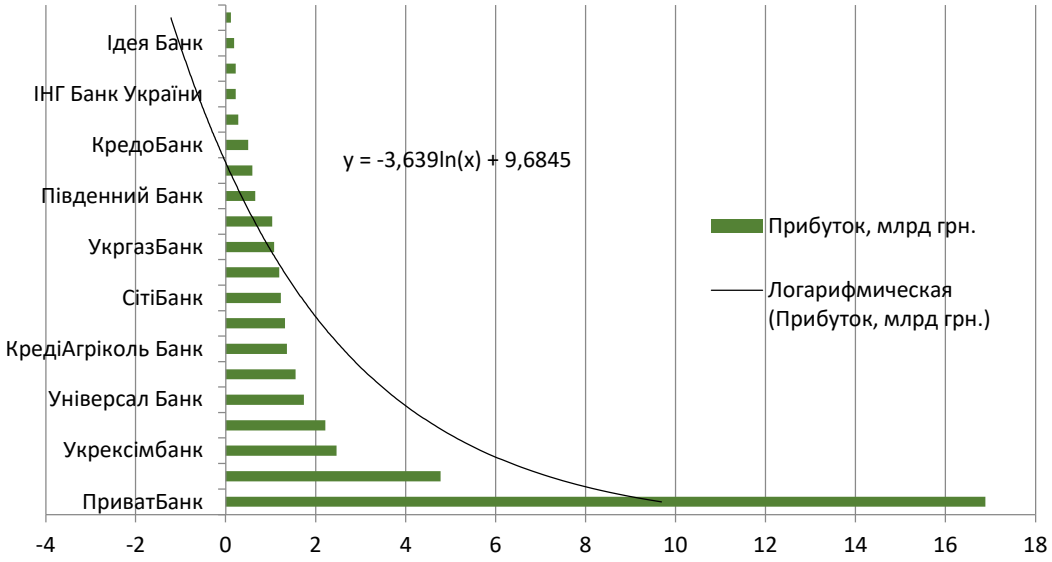

Рисунок 4 – **ТОП-20 прибуткових банків України за І квартал 2025 р., млрд грн**

Джерело: побудовано авторами за даними [8]

Необхідно зазначити, що за І квартал 2025 р. 10 із 60 банків отримали збиток в обсязі 263 млн грн. За цей період із загальної їх чисельності лише сім державних баків України (ПриватБанк, Ощадбанк, Укрексімбанк, Укргазбанк, СенсБанк, Мотор-Банк, Перший інвестиційний банк) сформували 65,7% прибутку. За підсумками І-ІІ кварталів 2025 р. банки отримали 65,52 млрд грн чистого прибутку, що на 3,61% менше за аналогічний період 2024 р. (67,97 млрд грн). Основну частку прибутку (64,4% від загального обсягу), забезпечили державні банки, банківська група з іноземних капіталом – 21,5%, привабні банки 14,1%. В групі банків із державною часткою капіталу прибутковість становила 85,7%. Серед 39 приватних банків лише 79,5% були дохідними [8].

На 01.06.2025 р. основу доходів банків формували процентні надходження – 70,9%, комісійні доходи – 21,3% загального обсягу, яка в порівняно з довоєнним періодом зменшилась, а доходи від торговельних операцій та переоцінки цінних паперів – 5,6%. Частка процентних доходів складала 64,1%, комісійних – 33,5%. Співвідношення операційних витрат до операційних доходів в банківській системі в цілому становила 42,9%. Для державних банків цей показник дорівнював 35,4%, для банків іноземних груп – 43,2%, для приватних банків – 59,1% Найнижчі значення спостерігаються у ПриватБанку – 24,6% та деяких іноземних банків, зокрема, у Сітібанку – 15,3%, у банку ING – 25,2%. Найбільший обсяг прибутку на 5 місяців отримав ПриватБанк – 28,5 млрд грн., друге місце займає Ощадбанк – 7 млрд грн., третє – Райффайзен Банк із 4,4 млрд грн [8].

У І кварталі 2025 р. частка чистих активів держбанків залишалася на рівні 53,3% (-0,3 п.п. від аналогічного періоду 2024 р.), який тримається з ІІІ кварталу 2024 р. Своєю чергою частка держбанків у коштах населення поступово знижується: на 0,4 в.п. за І квартал і на 1,0 в.п. від І кварталу 2024 р., до 62,9%. Станом на 01.06.2025 р. рентабельність активів банків склала лише 4,6% проти 5,5% в аналогічному періоді 2024 р., рентабельність капіталу – 39,6%, проти 20,6%. Порівняно з 2024 р. даний показник мав динаміку зменшення. На це вплинуло такі чинники, як фондування, збільшення витати на оплату праці (через дефіцит кадрів), а також потреба в оновленні основних засобів та вдосконаленні платіжної інфраструктури [8].

Зазначимо, що з 2023 по 2024 р. рівень прибутковості банків зменшував податок за підвищеною ставкою (ставка податку на прибуток збільшили з 18% до 50%). За 2024 р. фінансовий результат після оподаткування в прибуткових банках склав лише 103,7 млрд грн. Крім того, основним чинником суттєвого зниження прибутку банків є відсутність оновленої методики мінімізації ризиків в системі електронних платежів, які не адаптовані до інноваційних фінансових інструментів метапростору, що запроваджуються в структуру механізму забезпечення безпеки банківської системи, але не регламентовані регулятором депозитно-кредитного обігу [8].

Складність оцінки безпеки банківської системи пов’язана з нечіткими цілями регулятора електронних платежів під час кібератак та злочинних шахрайських нападів на депозитно-кредитний портфель фінансових установ [12]. На нашу думку, оцінювання безпеки банківської системи необхідно проводити з використанням процесу сек’юритизації платіжного депозитно-кредитного портфеля банків та захисту їх активних FinTech-ресурсів на фінансовому ринку за допомогою методу використання аналогів [17].

В процесі сек'юритизації його платіжного депозитно-кредитного портфелю та за умови впровадження захисних параметрів активних інформаційних FinTech-ресурсів визначається еталонний банк, який має відповідати вимогам регулятора за такими напрямами: «поточний рівень сек'юритизації», «менеджмент сек'юритизації», «рівень усвідомлення сек'юритизації», що дозволить описати компоненти і функції захисного процесу за активними об'єктами FinTech при кібератаках та розрахувати результативну величину – рівень безпеки СЕП банку.

Висновки. Таким чином, забезпечення безпеки банківської системи в країні повинно здійснюватися на основі ефективного використання захисних параметрів інформаційних FinTech-ресурсів в системі електронних платежів як центробанку так і окремої фінансової установи, шляхом посилення в депозитно-кредитної політиці вартісної послуг на FinTech-продукти, які спрощують QR-платежі для учасників та користувачів платіжного процесу.

Одним із інструментів СЕП НБУ, як чинник формування помірного структурного дефіциту ліквідної стійкості фінансових установ та контролю за вчасним блокуванням тегрованих та фітингових атак в системі електронних платежів має бути монетарний регулятором обов'язкових вимог. Він дозволяє удосконалити критерії СЕП НБУ шляхом диференціювання величини резервної грошової маси, внесеної на банківські депозити, за цільовою спрямованістю; зменшення обсягів обов'язкових резервів на величину довгострокових інвестиційних кредитів, які надані за рахунок самостійно сформованих ресурсів, величину придбаних ОВДП та депозитних сертифікатів НБУ; запровадження нарахування відсотків на величину обов'язкових резервів в платіжному депозитно-кредитному портфелі фінансових установ з метою підвищення ефективності переказів учасників СЕП.

Водночас, даний інструмент в депозитно-кредитному регулюванні фінансових установ не відноситься до числа операційних, а використовується лише в умовах виникнення загроз кібернападу на функціонуючі інформаційні FinTech-ресурси, в проміжку активної дії платіжних систем. Тому, на нашу думку, цей інструмент монетарного впливу доцільно виокремити зі списку інструментів оперативного функціонування СЕП НБУ, та перенести до категорії інструментів довгострокового та структурного впливу для посилення захисту від загроз макрофінансової дестабілізації в системі електронних платежів державних та приватних фінансових установ.

Література:

1. Гладищук Я.А. Аналіз динаміки активів банків України в умовах трансформаційних змін. Економіка та суспільство. 2025. № 75. URL: https://economyandsociety.in.ua/index.php/journal/article/view/6135.
2. Гривківська О. В., Герасимова О. В. Інструментарій функціонування механізму мінімізації ризиків платіжних систем. Економіка і управління. 2020. № 3. С. 98-105.
3. Національний Банк України. (2022). URL: https://bank.gov.ua/ua/statistic/supervision-statist#1.
4. Ситник І. П., Богдан О. С. Особливості функціонування та перспективи подальшого використання світових криптовалют в платіжних системах. Вісник Одеського національного університету. Серія: «Економіка». 2016. №21(4). С. 149-152.
5. Bakalynskyi O. Model and methods for determining the design characteristics of information security management systems. IRL: https://www.researchgate.net/publication/348788054_Model_ta_metodi_viznacenna_proektnih_harakteristik_sistem_upravlinna_informacijnou_bezpekou_Monografia
6. Dieieva N.E., Deleichuk V.V. Mechanisms for attracting investments by issuers in the conditions of digital economy development. Young Scientist. 2018. Vol. 3(55). Pp. 653-659.
7. European Systemic Risk Board. URL: https://euagenda.eu/publications/esrb-annual-report-2024
8. Financial Stability Report for 2024. National Bank of Ukraine. https://bank.gov.ua/admin_uploads/article/FSR_2024-H2_eng.pdf?v=9.
9. ISA/IEC 62443. URL: https://www.isa.org/standards-and-publications/isa-standards/search.
10. ISO/IEC 27001. URL: https://www.iso.org/isoiec-27001-information-security.html.
11. Mishchenko V.I., Mishchenko S.V. (2018). Marketing of digital innovations in the market of banking services. Financial space. 2018. Vol. 1(29). Pp. 75-79.
12. Mellow C. World's Best Private Banks. Global Finance: Global news and insight for corporate financial professionals. 2019. URL: https://www.gfmag.com/magazine/december-2019/worlds-best-private-banks-2020-tough-get-going.
13. Naderi E., Pazouki S., Asrari A. (2022). A remedial action scheme against false data injection cyber attack sin smart transmission systems: Application of thy ristor-controlled series capacitor (TCSC). IEEE Transaction son Industrial Informatics. 2022. Vol. 18(4). Pp. 2297-2309.
14. Roshan Y.E., Abdi Y. ICT and Information Asymmetry; New Evidence of the Financial System in Selected MENA Countries. Iranian Economic Review. 2022. Vol. 26(2). Pp. 445-458.
15. Vyshyvana B.M., Tereshko O.M. Oversight of payment and settlement systems: theoretical aspects and implementation mechanism in Ukraine. Scientific Bulletin of the International Humanities University. Economics and management, 2015. Vol. 11. Pp. 216–222.
16. Zherdetska L.V., Horodynskyi D.I. Development of banking technologies: threats and opportunities for banks. Economy and society. 2017. Vol. 10. Pp. 583-588.
17. Yehorycheva S.B. Methodological principles of organization of innovation process in commercial banks. Bulletin of the National Bank of Ukraine. 2011. Vol. 1. Pp. 53-57.

References:

1. Gladyshchuk, Ya.A. (2025). Analysis of the dynamics of the assets of Ukrainian banks in the context of transformational changes. Economy and society, 75. URL: https://economyandsociety.in.ua/index.php/journal/article/view/6135.
2. Hryvkivska, O.V., Gerasimova, O.V. (2020). Toolkit for the functioning of the mechanism for minimizing the risks of payment systems. Economics and Management, 3, 98-105.
3. National Bank of Ukraine. (2022). URL: https://bank.gov.ua/ua/statistic/supervision-statist#1.
4. Sytnyk, I.P., Bohdan, O.S. (2016). Peculiarities of functioning and prospects for further use of world cryptocurrencies in payment systems. Bulletin of Odessa National University. Series: "Economics", 21(4), 149-152.
5. Bakalynskyi, O. (2020). Model and methods for determining the design characteristics of information security management systems. https://www.researchgate.net/publication/348788054_Model_ta_metodi_viznacenna_proektnih_harakteristik_sistem_upravlinna_informacijnou_bezpekou_Monografia.
6. Dieieva, N.E., Deleichuk, V.V. (2018). Mechanisms for attracting investments by issuers in the conditions of digital economy development. Young Scientist, 3(55), 653-659.
7. European Systemic Risk Board. (2024). https://euagenda.eu/publications/esrb-annual-report-2024.
8. Financial Stability Report (2024). National Bank of Ukraine. https://bank.gov.ua/admin_uploads/article/FSR_2024-H2_eng.pdf?v=9.
9. ISA/IEC 62443. URL: https://www.isa.org/standards-and-publications/isa-standards/search.
10. ISO/IEC 27001. URL: https://www.iso.org/isoiec-27001-information-security.html.
11. Mishchenko, V.I., Mishchenko, S.V. (2018). Marketing of digital innovations in the market of banking services. Financial space, 1(29), 75-79.
12. Mellow, C. (2019). World's Best Private Banks. Global Finance: Global news and insight for corporate financial professionals. URL: https://www.gfmag.com/magazine/december-2019/worlds-best-private-banks-2020-tough-get-going.
13. Naderi, E., Pazouki, S., Asrari, A. (2022). A remedial action scheme against false data injection cyber attack sin smart transmission systems: Application of thy ristor-controlled series capacitor (TCSC). IEEE Transaction son Industrial Informatics, 18, 4, 2297-2309.
14. Roshan, Y.E., Abdi, Y. (2022). ICT and Information Asymmetry; New Evidence of the Financial System in Selected MENA Countries. Iranian Economic Review, 26 (2), 445-458.
15. Vyshyvana. B.M., Tereshko. O.M. (2015). Oversight of payment and settlement systems: theoretical aspects and implementation mechanism in Ukraine. Scientific Bulletin of the International Humanities University. Economics and management, 11, 216–222.
16. Zherdetska, L.V., Horodynskyi, D.I. (2017). Development of banking technologies: threats and opportunities for banks. Economy and society, 10, 583-588.
17. Yehorycheva, S.B. (2011). Methodological principles of organization of innovation process in commercial banks. Bulletin of the National Bank of Ukraine, 1, 53-57.