УДК 336.71 **DOI**: https://doi.org/10.31521/modecon.V52(2025)-16

Мельник О. В., здобувач третього (освітньо-наукового) рівня вищої освіти, Таврійський державний агротехнологічний університет імені Дмитра Моторного, м. Запоріжжя, Україна

ORCID ID: 0009-0005-3990-6920
e-mail: alexreetwell@gmail.com

Оцінка ризиків шахрайства в платіжному сегменті банківської системи

Анотація. *У статті узагальнено інструменти оцінки ризиків шахрайства, що найбільшою мірою загрожують платіжним трансакціям в кредитному сегменті банківської системи. Важливість оцінки стабільного стану безпеки банківської системи визначається підсистемою фінансових важелів і методів функціонування скорингових технологій ФінТех та Блокчейн, з метою усунення кризових явищ в фінансових установах, що викликані неправовими діями або бездіяльністю клієнтів при здійсненні платіжних трансакцій. Скорингові технології ФінТех та Блокчейн, як інструменти метапростору, попереджують ризики шахрайства, із врахуванням соціальної інженерії, швидко ідентифікують та блокують сервери економічних агентів, що за власної вигоди шкодять іншим суб'єктам економіки. Проаналізовано ризики шахрайства за платіжними трансакціями в банківській системі України. Виокремлено змінні фактори (параметри) платіжного шахрайства в банківській системі України. Доведено, що втрата стабільного стану безпеки банківської системи неминуча, якщо вона ототожнюється з катастрофою втрати прибутку за кредитними операціями в платіжних трансакцій, який виникає в наслідок порушення співвідношення між темпами приросту доходів від трансакційних переказів за кредитами та витратами на їх здійснення, спричинених втратою («розривом») зв'язків між інформаційними FinTech-ресурсами в системі неперервності функцій змінних факторів. Визначено, що варіативність розрахунку інтегральної величини ризику шахрайства в банківській теорії враховує декілька моделей, які за бальної оцінкою дозволяють одержати сукупний результат, що дає загальне уявлення про його масштаби загрози для окремого банку та банківської системи в цілому. Представлена описова статистика змінних моделі катастроф збірки ризиків шахрайства в платіжних трансакціях банківської системи. Визначено рейтинг стабільного стану безпеки банківської системи при нівелюванні ризиків шахрайства, який гарантує цілісність конфігурації системи, створює рішення щодо її кіберзахисту через інструменти метапростору – FinTech та Blockchain систем.*

Ключові слова: *ризики шахрайства; платіжні трансакції; кредити; банківська система; безпека; FinTech-ресурси; Blockchain системи.*

Melnyk Oleksii, graduate student of the third (educational and scientific) level of higher education Dmytro Motornyi Tavria State Agrotechnological University, Zaporizhzhia, Ukraine

Fraud Risk Assessment in the Payment Segment of the Banking System

Abstract. Introduction. *The article summarizes the fraud risk assessment tools that most threaten payment transactions in the credit segment of the banking system. The importance of assessing the stable state of security of the banking system is determined by the subsystem of financial levers and methods of functioning of scoring technologies FinTech and Blockchain, in order to eliminate crisis phenomena in financial institutions caused by illegal actions or inaction of clients when making payment transactions.*

Purpose*. The purpose of the study is to generalize fraud risk assessment tools that most threaten payment transactions in the credit segment of the banking system.*

Results*. FinTech and Blockchain scoring technologies, as metaspace tools, prevent fraud risks, taking into account social engineering, quickly identify and block the servers of economic agents that harm other economic entities for their own benefit. The risks of fraud in payment transactions in the banking system of Ukraine are analyzed. Variable factors (parameters) of payment fraud in the banking system of Ukraine are identified. It is proven that the loss of a stable state of security of the banking system is inevitable if it is identified with the catastrophe of loss of profit on credit operations in payment transactions, which arises as a result of a violation of the ratio between the growth rates of income from transaction transfers on loans and the costs of their implementation, caused by the loss ("break") of connections between information FinTech resources in the system of continuity of functions of variable factors.*

Conclusions*. It is determined that the variability of the calculation of the integral value of fraud risk in banking theory takes into account several models, which, by scoring, allow obtaining an aggregate result, which gives a general idea of its scale of threat for an individual bank and the banking system as a whole. Descriptive statistics of the variables of the catastrophe model of the collection of fraud risks in payment transactions of the banking system are presented. The rating of the stable state of security of the banking system when eliminating fraud risks is determined, which guarantees the integrity of the system configuration, creates solutions for its cyber protection through metaspace tools - FinTech and Blockchain systems.*

Keywords*: fraud risks; payment transactions; loans; banking system; security; FinTech resources; Blockchain systems.*

JEL Classification: *G12; G21; G31*

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

Постановка проблеми. Стабільність банківської системи України неодноразово була задекларована кризовими потрясіннями в національній та міжнародній економіці. З 2022 року ця криза набрала великих масштабів в украї¬ській банківській системі, яка стикнулась із викликами спровокованими військо¬вим станом в країні. У цьому контексті, терміновим завданням в банківському секторі економіки стало розбудова фінансової стратегії відновлення життєздатності країни, в якій банківська система має достатньо стійко реагувати на «шоки» шахрайський дій, втримувати відносну ритмічність та систематичність платіжного процесу. Разом з тим, платіжний процес в банківській системі знаходиться під «прицілом» різних небезпек геофінансового та геополітичного характеру.

Сьогодні відбувається піднесення активної позиції банківських установ розвивати та впроваджувати інноваційні технології метапростору (FinTech та Блокчейн), які мають популяризовані хеш-імпульси щодо попередження та нейтралізації шахрайства в кіберпросторі банківської системи. Це дозволяє запроваджувати різні форми налагодження стратегічного партнерства із тра-диційними учасниками фінансового сектору [6; 11]. Активне використання таких технологій банківськими, парабанківськими установами змінює основні принципи та умови функціонування всієї сфери фінансових послуг та сприяє трансформаційним процесам на кредитному ринку. Особливу роль зазначені технології відіграють у розвитку фінансових установ, які постійно підвищують власну ефективність функціонування та забезпечують зростання якості послуг. Потенціал інноваційних технологій метапростору в банківській системі розширюється та впливає не лише на діяльність фінансових установ, але й на новий світогляд фінансової глобалізації та відновлення стабілізації після кризи, спричиненою шахрайськими діями [11].

Аналіз останніх досліджень та публікацій. Пошук нетрадиційних форм безпечного розвитку та необхідність упровадження новітніх цифрових технологій метапростору в банківську систему України відповідає Стратегії розвитку фінансового сектору України до 2025 року, у якій зазначено про сприяння розбудові платформ регуляторів та взаємодії кредитного ринку та ринку небанківських фінансових послуг, FinTech, SupTech & RegTech. Детальним дослідженням цифровим процесів в економіці та застосування їх банківській системі для усунення загроз і забезпечення позитивної динаміки розвитку оцифровування платіжних продуктів, розглядались А. Мазаракі [24], В. Баранов [1], Т. Гаврилко [6], П. Нікіфоров [8]. Разом з тим значні дискусії в даній області наукових досліджень потребують додаткових доробок. Особливо дана проблематика актуалізується в сучасних умовах безпеки розвитку банківської системи в умовах інноваційних технологій метапростору.

Формулювання цілей дослідження. Метою дослідження є узагальнення інструментів оцінки ризиків шахрайства, що найбільшою мірою загрожують платіжним трансакціям в кредитному сегменті банківської системи.

Виклад основного матеріалу дослідження. Важливою складовою оцінки стабільного стану безпеки банківської системи є підсистема фінансових важелів і методів функціонування скорингових технологій ФінТех та Блокчейн, з метою усунення кризових явищ в фінансових установах, що викликані неправовими діями або бездіяльністю клієнтів при здійсненні платіжних трансакцій. Скорингові технології ФінТех та Блокчейн, як інструменти метапростору, попереджують ризики шахрайства, із врахуванням соціальної інженерії, швидко ідентифікують та блокують сервери економічних агентів, що за власної вигоди шкодять іншим суб'єктам економіки.

У 2022 р. під час повномасштабного втручання країни-агресора на територію України, від шахрайства постраждало 1.22% користувачів-власників платіжних карт, причому загальна частка сішингу та фішингу склала 63%; загальна сума збитків дорівнювала 8.15 млн дол США, з них від сішингу – 6.62 млн дол США, фішингу – 1.53 млн дол США, що в 4.0 разів більше ніж у 2021 р. (рис. 1).

За 2023 р. в Україні було 58.8 мільйонів активних платіжних карток. Їх кількість зросла на 13% по відношенню до 2022 р. Кількість операцій з використанням платіжних карткових трансакцій, емітованих українськими банками та фінансовими установами, за 2024 р. становила 8654.4 млн грн, а їхня загальна сума – 6577,4 млрд грн. Із них в Україні здійснено 91.8% від кількості та 90.1% від суми всіх операцій з картками.

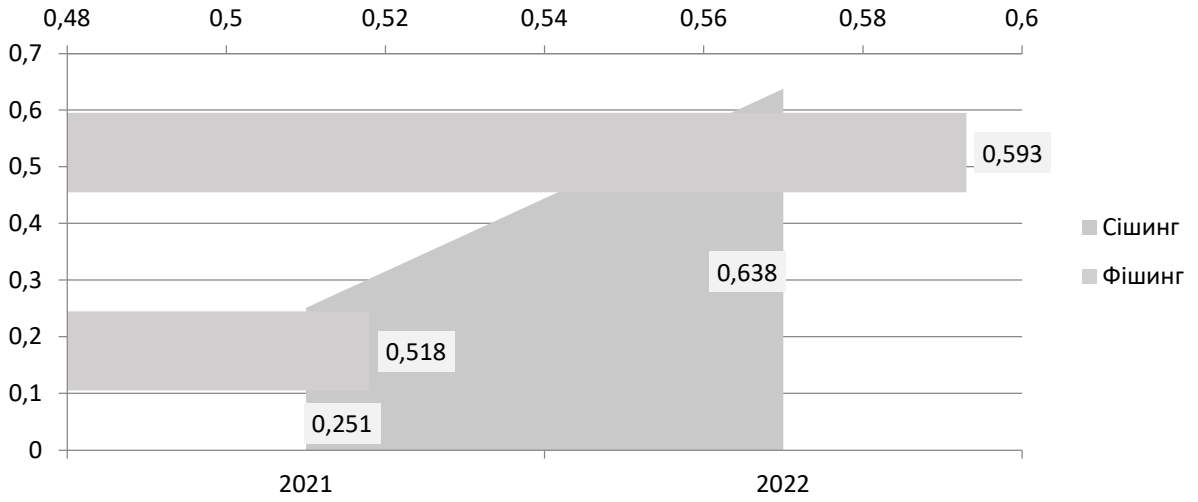

Рисунок 1 – **Ризики шахрайства за платіжними трансакціями в банківській системі України в 2021-2022 рр.**

Джерело: побудовано авторами на основі даних [4]

У 2024 р. спостерігалося зменшення кількості незаконних дій та шахрайських операцій з використанням платіжних карткових трансакцій, за якими були понесені збитки. Цей показник порівняно з 2023 р. знизився на 2 тисяч операцій (або на 1%) – до 270 тис. операцій. За цей період, на один мільйон видаткових операцій із платіжними картками припадала 31 шахрайська операція; кількість шахрайських операцій зменшилася на 8%, якщо порівнювати з 2023 р., завдяки зростанню загальної кількості видаткових операцій. Проте, в 2024 р. збитки від незаконних дій та шахрайських операцій з використанням платіжних карток зросла на 37%. Це пов'язано із зростанням на 39% середньої суми незаконної операції за платіжних картковими трансакціями. У 2024 р., крім зростання суми збитків, на 8% зросла загальна сума видаткових операцій з використання платіжних карток (рис. 2).

У наслідок шахрайських дій виникає асиметрія платіжного потоку фінансових ресурсів, дані яких не захищені. Це шкодить інтересам банків та банківській системі в цілому, які змушені змінювати масштаби багаторівневої системи електронних платежів. Тобто, через таку ситуацію, будь-яка невизначеність, випадковість у вхідних факторах (параметрах) в нижніх потокових рівнях призводить до невизначеностей і випадковостей в вихідних факторах (параметрах) підсистем вищого порядку системи електронних платежів.

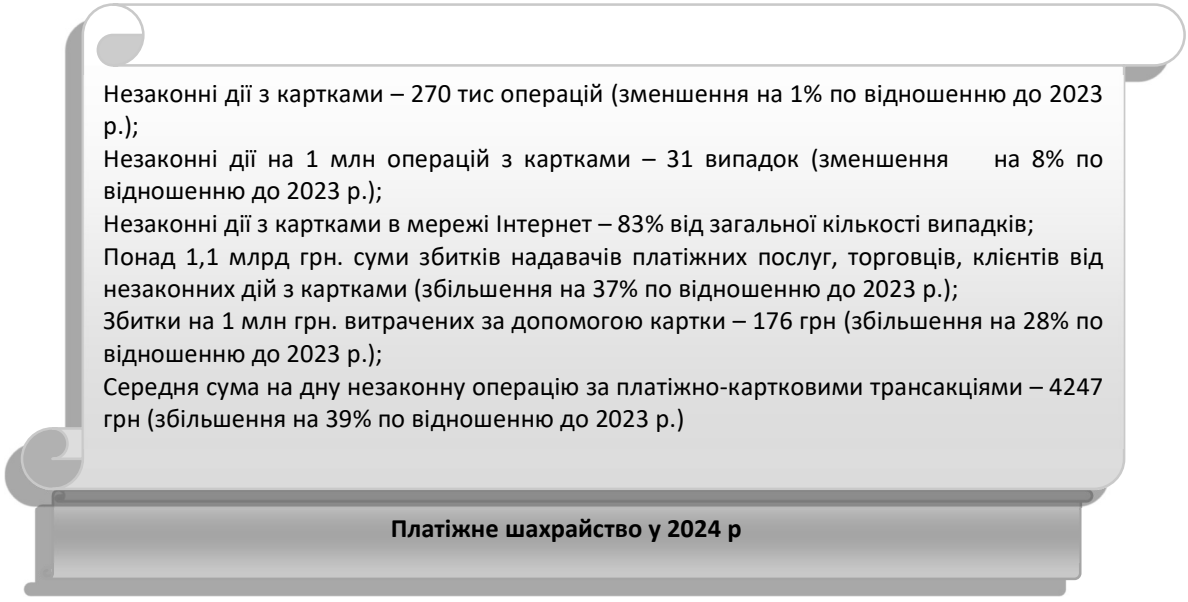

Рисунок 2– **Змінні фактори (параметри) платіжного шахрайства в банківській системі України за 2023-2024 р.**

Джерело: побудовано авторами на основі даних [9]

Відповідно відносний рівень збитків від шахрайства з використанням платіжних трансакцій до загальної суми видаткових операцій у 2024 р. зріс на 28%. Крім того, на один мільйон витрачених коштів через платіжні трансакції, припадало 4.2 тис грн. збитків від шахрайства.

Нестабільний стан безпеки банківської системи через ризики шахрайства відбувається за наступних умов: система гальмує процес зміни з одного стану в інший (при зростанні кількості нових ознак небезпеки, трансформація системи не здійснюється, межа невизначеності (ентропія) підвищується, система функціонує в хаосі і розладі); система вишукує відхиляння від стабільного, передбачуваного стану розвитку (наприклад, фінансові трансакції між клієнтами стають прихованими); збільшується чисельність негативних активів; зростає інформаційна асиметрія потокового процесу банківський операцій, яка швидко скорочує змінні конфігурації системи для посиленого захисту [3].

При зміні факторів (конфігурації) платіжних трансакцій можуть спостерігатись такі типи поведінки в банківській системі: після втрати рівноваги новий проміжок часу платіжних трансакцій визначається між двома послідовними максимальними відхиленнями системи (м'яке відхилення стабільності); незмінний режим платіжних трансакцій в банківській системі втрачає стабільність, коли граничні межі конфігурації її елементів зменшуються і будь-які поточні інциденти збурення виштовхують та блокують будь-які операції, сфера трансакції геть зникає (жорстке відхилення стабільності); банківська система виходить із незмінного стану миттєво і переключається на нову конфігурацію платіжних трансакцій [3]. При цьому, м'яке відхилення стабільності банківської системи розглядається теорією біфуркацій, жорстке – теорією катастроф.

Необхідно зазначити, що втрата стабільного стану безпеки банківської системи неминуча, якщо вона ототожнюється з катастрофою втрати прибутку (рентабельності) за кредитними операціями в платіжних трансакцій, тобто, цей період можна вважати періоди збитку від ризиків шахрайства, що виникають в наслідок порушення співвідношень між темпами приросту доходів від трансакційних переказів за кредитами та витратами на їх здійснення, спричинених втратою («розривом») зв'язків між інформаційними FinTech-ресурсами в системі неперервності функцій змінних факторів.

Згідно з підходом E. Zeeman, який запропонував активні фактори (параметри) платіжних трансакцій, визначено, що із п'ять або меншої кількості активних змінних в платіжних переказах існує всього сім типів узагальнених структур опису траєкторії біфуркацій (катастрофи) шахрайства в банківській системі [2]: складка, збірка, «Хвіст ластівки», «Метелик», Еліптична омбіліка Параболічна омбіліка, Гіперболічна омбіліка.

Підтвердженнями необхідності використання теорії катастроф до моделюванні складних елементів банківської системи за наявності ризиків шахрайства є те, що: система є динамічною; система намагається зберігати стабільний стан якнайдовше; система в стабільній операційній конфігурації затримується до того часу, доти не з'являться асиметричні збурення; траєкторії системи незворотні [13]. Тому до можливих наслідків втрати платіжних трансакцій в банківській системі через ризики шахрайства можна віднести: збільшуються проблемні ознаки в кредитному портфеля; збільшення величина прострочених кредитів; падіння рівня стабільності банків через підвищену ризикованість кредитних трансакцій та їх неповернення.

Варіативність розрахунку інтегральної величини ризику шахрайства в банківській теорії враховує декілька моделей, які за бальної оцінкою дозволяють одержати сукупний результат, що дає загальне уявлення про його масштаби загрози для окремого банку та банківської системи в цілому. Математична модель оцінки ризику шахрайства, пов'язана із кредитуванням клієнтів. Умови кредитного договору мають бути вигідними для клієнта з метою скорішого покриття клієнтських зобов'язань перед банком та уникати зміни угоди під час її дії, або пасивності клієнта щодо неповернення боргу. У математичному вигляді модель представлена таким чином: цільова функція клієнта у випадку погашення кредиту ($F(x_1)$), де x_1 – набір змінних цільової функції, значення якої збільшується за умови покриття зобов'язань, ніж у випадку непогашення кредиту ($F(x_2)$), де x_2 – набір змінних, що трансформують цільову функцію ($F(x_2)$),[13]:

$$F(x_1) \geq F(x_2), \quad (1)$$

Представлена нерівність уособлює в собі коефіцієнт ризику шахрайства (K_{rf}), який розраховується як співвідношення цільової функції клієнта у випадку непогашення позики ($F(x_2)$), до цільової функції клієнта у випадку погашення позики ($F(x_1)$), [13]:

$$K_{rf} = \frac{F(x_2)}{F(x_1)}, \quad (2)$$

Тобто, якщо $K_{rf} \leq 1$ – ризик шахрайства мінімальний та не потребує втручання; $K_{rf} = 1$ – ризик шахрайства наявний, потребує нейтралізації через зміну поведінки клієнта; $1 \leq K_{rf} \leq 1.2$ – початкова межа збільшення ризику шахрайства по кредитних платежам. Банку необхідно вводити обмеження щодо платіжним операціям; $1.2 \leq K_{rf} \leq 1.5$ – критична межа ризику шахрайства. Присутня явна вигода для клієнта щодо цільової функції непогашення позики; $K_{rf} \geq 1.5$ – висока вигода від ризику шахрайства для клієнта,

значення якої межує із загрозою неповернення позики банку.

Загальна кількісна оцінка стабільного стану безпеки банківської системи розраховується за формулою (1) [2]:

$$\begin{cases} S = \sum_{i}^{n} MAX_i \times P_i + D_i \\ P_i = 1,\ K_i \geq C_h \\ P_i = 0.75,\ K_i \geq t_i\ \alpha\ K_i \geq C_i \\ P_i = 0,\ \ K_i \leq C_i \end{cases}, \quad (3)$$

де, S – загальна кількість балів; MAX_i – кількість балів по *i*-му індикатору; t_i – нормативне значення *i*-го індикатора; C_h – верхнє граничне значення індикатора; C_i – нижня граничне значення індикатора; K_i – фактичне значення *i*-го індикатора; P_i – коригуючий коефіцієнт; D_i – «премія» або «штраф» за динаміку зміни *i*-го індикатора.

Визначається один з трьох типів рівня стабільного стану безпеки банківської системи при існування ризиків шахрайства: критичний (менше 5,4 балів), недостатній (5,4-8,5 балів), достатній (8,5-10 балів). Критичний рівень має ознаки суттєвого порушення стабільного стану безпеки банківської системи та ряд збурень, пов'язаних із значним впливом ризиків шахрайства (тобто, системний, кредитний ризик, ризик системи електронних платежів, ризик втрати інформаційних FinTech-ресурсів), що провокують катастрофу в операційній конфігурації платіжних операцій.

З метою визначення змінних моделі катастроф збірки шахрайства в платіжних трансакціях банківської системи, у ролі результуючого фактору обрано проблемні кредити, у якості факторів біфуркації та унормованих (стандартних) факторів нами було використано індикатори стабільного стану безпеки банківської системи України, як: NPL (Частка непрацюючих кредитів); H2 (Норматив достатності (адекватності) регулятивного капіталу); ROA (Норма прибутку на активи); ROE (Норма прибутку на капітал); Spr1 (Спред між ставками за кредитами та депозитами (базисні пункти)); Spr2(Спред між найвищою та найнижчою міжбанківськими ставками (базисні пункти)); Dep (депозити клієнтів до сукупних валових кредитів (крім міжбанківських)); Kred (кредити в іноземній валюті до сукупних валових кредитів); Zob (зобов'язання в іноземній валюті до сукупних зобов'язань).

Акцентуємо увагу, що протягом 2023-2024 рр. ключовими проблемами для української банківської системи стали саме шахрайські дії з кредитами. У 2024 р. частка непрацюючих кредитів (NPLs) в Україні становила 30%. Обсяг NPL за 2024 р. скоротився на 700 млн дол США до 9460 млн дол США. Тенденція його поступового зменшення триває з початку 2023 р. [5].
Можливості побудови моделей катастроф типу збірка даних щодо ризиків шахрайства за платіжними трансакціями, на основі фактичних показників банківської системи України, викликають особливий інтерес, оскільки рівень значущості індикаторів перевищує рівень регресійних рівнянь (рис. 3), які визначають стійкий характер зв'язку між інформаційними FinTech-ресурсами.

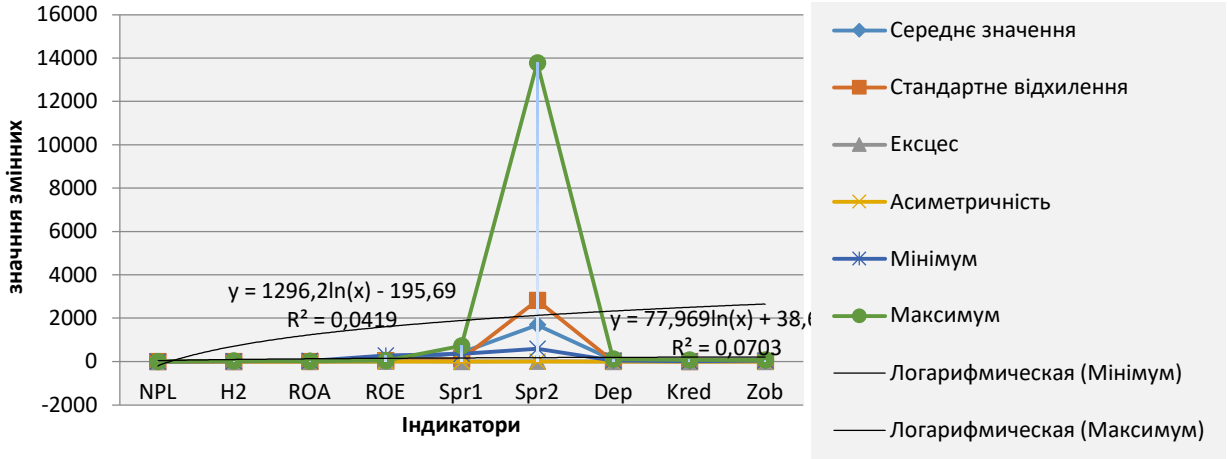

Рисунок 3– **Опис змінних в моделі катастроф (ризиків шахрайства) в платіжних трансакціях банківської системи України за 2024 р.**

Джерело: розраховано автором

Пропонується проблемні кредити розглядати як один із найважливіших індикаторів нестабільного стану безпеки банківської системи, враховуючи значний їх обсяг, що провокує ризик зниження дієздатності банківського сектору в національній фінансовій системі. Інших індикатори стабільного стану безпеки банківської системи також показують високий рівень статистичної значущості логістичної моделі катастрофи збірки, як ви окремного типу

шахрайства із сукупності існуючих в платіжних трансакціях за кредитними операціями.

Ключові чинники скорочення NPL пов'язані, по-перш, із подальшим нарощенням банками гривневих кредитів, зважаючи на підвищений попит до кредитних ресурсів та послаблення вимог до кредитування, зокрема зниження кредитних ставок до рівня 2019 р. Обсяг валових кредитів у банківський системі в 2024 р. зріс на 14,8%; по-друге, списання непрацюючих споживчих кредитів. Частка NPL у споживчому кредитному портфелі знизилася до 15.5%. Врегулювання взаємодії біж банківським сектором та корпоративним бізнесом дозволило зменшити частка NPL до 39% [5].

Зменшення частки недієздатних кредитів зафіксовано в усіх групах банків: у приватних українських банках – до 12,6%; у банках з іноземним капіталом – до 10,9%; у державних – до 43%. Без урахування боргів АТ КБ «ПриватБанк» частка непрацюючих кредитів на початок 2025 р. становить 24,8% в державних банках та 18,6% – загалом у банківській системі (рівень нижче 20% уперше з жовтня 2022 р.), [5].

Прогнозовані точки катастроф зміни обсягу платіжних трансакціях через шахрайські дії клієнтів в періоді з 01.01.2025 по 01.06.2025 р. дозволили визначити вид функціональної залежності між часткою непрацюючих кредитів та стабільним станом безпеки розвитку банківської системи. Визначено, що частка непрацюючих кредитів (NPLs) в ТОП-25 українських банків із найбільшим обсягом кредитного портфелю в Україні, в періоді з 01.01.2025 по 01.06.2025 р., скоротиться до 30.3% або на 7.1 відсоткових пункти порівняно з 2024 р. (рис. 4).

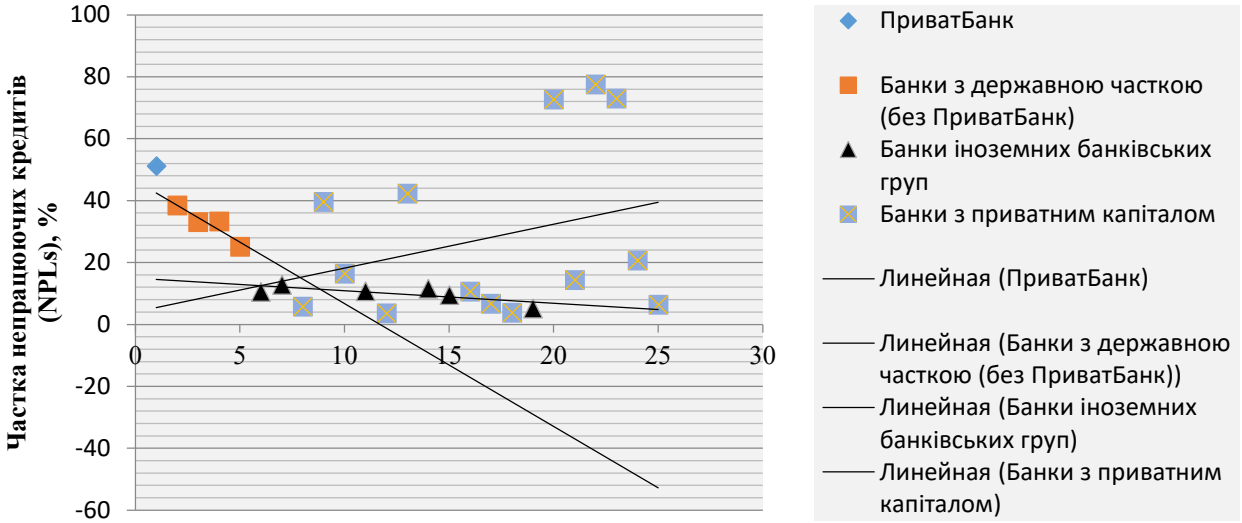

Рисунок 4 – **Частка непрацюючих кредитів (NPLs) в ТОП-25 українських банків із найбільшим обсягом кредитного портфелю в Україні в періоді з 01.01.2025 по 01.06.2025 р., %**

Джерело: побудовано авторами за даними [10]

За допомогою децентралізованих регуляторів банківських установ, що групуються FinTech-аналітиками Big Data, в межах зафіксованих імпульсів (сигналів) Blockchain, відбувається захист інформаційних носіїв за кредитними та депозитними потоками, тобто, нівелюється втручання в їх кіберпростір зловмисників (хакерів, шахрайських дій клієнтів). На їх основі, з високим ступенем надійності розраховано рейтинг стану безпеки банківської системи поза межами поточного досліджуваного періоду. Так, рейтинг стабільного стану безпеки банківської системи України визначено із врахуванням стресостійкості досліджуваних банки з портфелями роздрібних депозитів від 1 млрд дол США, (рис. 5). Банківські установи отримали від 1 до 5 балів залежно від показників, що характеризують їх діяльність (сек'юритизація активів, підвищення рівня достатності власного капіталу, покращення фінансової структури пасивів, підтримки міжнародних фінансових установ, приріст депозитних вкладень, платіжний імідж).

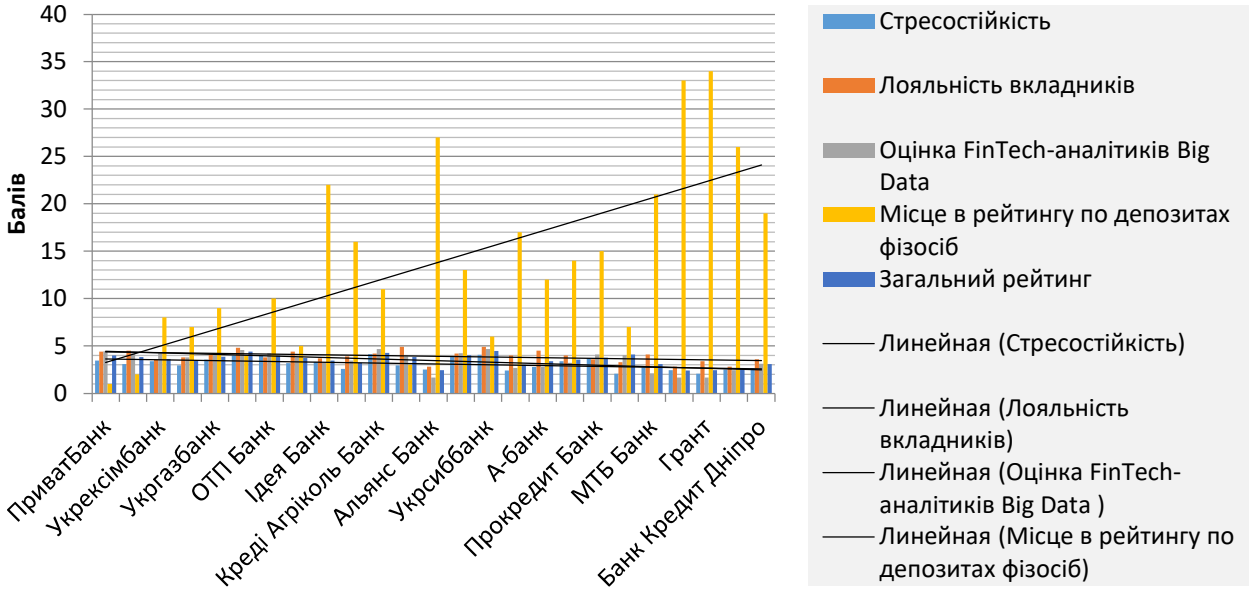

Рисунок 5 – **Рейтинг стабільного стану безпеки банківської системи України за оцінкою експертів в періоді з 01.01.2025 по 01.06.2025 р., балів**

Джерело: побудовано авторами за даними [10]

Рейтинг гарантує цілісність конфігурації стабільного стану безпеки банківської системи та створює рішення щодо її кіберзахисту через інструменти метапростору – FinTech та Blockchain систем.

Технології Blockchain, якщо вони добре впроваджені в банківську систему, можуть запобігти майбутнім кібератакам на платіжні трансакції, особливо, якщо це стосується внутрішньої структурної мережі банків, де виявлено критичний фактор. Зазвичай хакери проникають в центральне адміністрування пристрою і автоматично отримують повний контроль над пристроями та системами. Децентралізуючи системи Blockchain гарантують, що такі атаки важче виконувати, або навіть можливо [12].

Blockchain захищає DNS і DDoS в банківській системі. Атака з розподіленою відмовою в обслуговуванні (DDoS) відбувається, коли користувачам цільового ресурсу, такого як мережевий ресурс, сервер або веб-сайт, відмовляють у доступі або обслуговуванні цільового ресурсу. Ці атаки вимикають або сповільнюють роботу ресурсних систем. З іншого боку, неушкоджена система доменних імен (DNS) дуже централізована, що робить її ідеальною мішенню для хакерів, які проникають у з'єднання між IP-адресою та назвою веб-сайту. Ця атака робить веб-сайт недоступним і навіть створюють перенаправлення на інші шахрайські веб-сайти. Blockchain використовують для зменшення таких атак шляхом децентралізації записів DNS. Застосовуючи децентралізовані рішення, Blockchain видаляє вразливі окремі точки, якими користуються шахраї [12].

Кожна система електронного урядування має гарантувати конфіденційність, цілісність і доступність послуг. Конфіденційність досягається, коли інформація не розкривається неавторизованим користувачам; Цілісність досягається шляхом захисту інформації від будь-якої форми модифікації, тоді як доступність означає, що інформація доступна в разі потреби та вільна від DoS або DDoS чи інших подібних порушень служби. У цьому розділі представлено теоретичний якісний аналіз ефективності безпеки та конфіденційності системи електронного урядування на основі Blockchain [12]. Тому, більшість консенсусних алгоритмів Blockchain (у цьому випадку DPoS) вимагають від зловмисника контролю принаймні 51% одноранговых мереж, щоб змінити запис, чого, як правило, неможливо досягти. Точніше, щоб змінити будь-який блок у ланцюжку блоків, зловмисник повинен змінити кожну копію цього блоку в мережі, а потім переконати більшість вузлів, що новий блок є дійсним.

Крім того, для підвищення конфіденційності даних, що зберігаються в запропонованій мережі, усі блоки користувачів хешуються, а незрозумілі хеші транзакцій зберігаються в Blockchain. Система DPoS, як конфігурація алгоритмів Blockchain є децентралізованою системою p2p, де дані користувача зберігаються в різних вузлах, гарантуючи доступність системи, уникаючи будь-якої єдиної точки збою. Використовуючи DPoS, будь-якому зловмиснику важко запускати DDoS або DoS атаки проти системи, оскільки спочатку потрібна реєстрація. Лише тоді вузол починає обмінюватися інформацією з рештою одноранговых мереж. Будь-які транзакції, отримані від вузла мережі, перевіряються свідками, що ускладнює зловмисним вузлам ініціювання шахайських з'єднань [12]. Отже, технологія Blockchain і консенсусний протокол DPoS, масштабує швидкість, сумісність і прозорість обробки

великої кількості транзакцій, забезпечуючи стабільний стан безпеки банківської системи.

Висновки. Таким чином, кризові явища, які мають просторові хвилеподібні зміни в банківській системі розвіяли міф про її стійкість і невразливість, оскільки вони найбільше пов'язані із платіжними трансакціями за рухом кредитних потоків. Пріоритетним завданням для банківської системи є процес інтеграції з інноваційні технології метапростору, що вимагає досягнення макропроденційного та децентралізованого регулювання її безпеки через функції прогнозування кризи, яка, в комунікативно-структурному аспекті, забезпечує безпеку фінансовим установам та має внутрішню організацію механізму взаємодії складових інструментів метапростору – FinTech-аналітиків Big Data та Blockchain систем. Відповідно до комунікативного аспекту метапростору, в банківській системі відбувається взаємодіє з іншими системами як по горизонталі (з системою парабанківських FinTech-компаній, які впроваджують цифрові технології в банківському секторі), так і по вертикалі (з системою децентралізованих регуляторів). При цьому, Blockchain системи можна використовувати для забезпечення цілісності завантаження програмного забезпечення, щоб запобігти сторонньому вторгненню на сервери банків. Blockchain системи застосовують для перевірки оновлення мікропрограм, інсталяторів і виправлень, з метою нейтралізації шкідливого програмного забезпечення та його проникнення в банківські інформаційні носії, тобто убезпечити ризики шахрайства в кредитному сегменті. Даний інструмент метапростору дозволяє захистити цілісність інформаційних FinTech-ресурсів в міжбанківській інфраструктурі та забезпечити її безпеку.

Можливості Blockchain щодо цілісності та перевірки інформації можуть бути використані для аутентифікації статусу будь-якої кіберфізичної міжбанківської інфраструктури. Тобто, платіжні трансакції через Blockchain в міжбанківській інфраструктурі є надійними для повного ланцюга зберігання інформаційних FinTech-ресурсів. При цьому, масштабування кіберфізичних інфраструктур в банківській системі через Blockchain, за умови виникнення критичних факторів (параметрів) в показниках моделі катастроф збірки ризиків шахрайства запобігають фішингу та скімінгу та підвищують стандарти соціальної інженерії, не дозволяють розвиватись швидкими темпами кіберзлочинності різної модифікації.

Література:

1. Баранова В.Г., Гончаренко О.М., Астахова Н.І. Новітні фінансові технології в контексті цифровізації економіки: досвід розвинених країн та український досвід. Харків: Disa Plus. 2019.
2. Болгар Т. Н. Необхідність врахування моральних ризиків під час оцінки рівня фінансової безпеки банків. Проблеми та перспективи розвитку банківської системи України. 2008. №23. С. 277-281.
3. Бродський Ю. Б., Молодецька К. В. Моделювання економічної динаміки. Житомир: ЖНАЕУ. 2016.
4. Звіт про фінансову стабільність. Національний банк України. 2022. URL: https://bank.gov.ua/ua/news/all/zvit-pro-finansovu-stabilnist-gruden-2022-roku
5. Звіт про фінансову стабільність. Національний банк України. 2024. URL: https://bank.gov.ua/ua/news/all/zvit-pro-finansovu-stabilnist-gruden-2024-roku
6. Гаврилко Т., Антонова Р.. FinTech: зарубіжний досвід та особливості розвитку в Україні. Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світова економіка. №9. 2020. С. 17-22.
7. Мазаракі А., Волосович С. FinTech у системі соціальних трансформацій. Вісник КНТЕУ. 2018. №2. С. 5-18.
8. Нікіфоров П., Бабух І., Кінащук С. FinTech як рушійна сила сучасних трансформацій фінансового ринку: український контекст. Чорноморські економічні дослідження. 2020. №51. С. 189-194.
9. Кількість випадків шахрайства з картками. Національний банк України. 2024. URL: https://bank.gov.ua/ua/news/all/kilkist-vipadkiv-shahraystva-z-kartkami-znizilasya-zbitki-za-nimi--zrosli
10. Частка непрацюючих кредитів (NPL) в Україні. 2025. URL: https://bank.gov.ua/ua/stability/npl
11. Трусова Н.В., Мельник О.В. Методологічний підхід до впровадження цифрових технологій метапростору в інфраструктуру фінансового ринку. Збірник наукових праць Державного технічного економічного університету імені Дмитра Моторного (економічні науки). №1(50), 2024. С. 138-148.
12. Yang, L., Hu, X., Wu, J., & Liu, Y. (2019). A distributed honeypot deployment system based on Blockchain technology. IEEE Access, 7, 35881-35890.
13. Zeeman, E. C. Catastrophe Theory. Reading, MA: Addison-Wesley. 1977. Pp. 1972-1977.

References:

1. Baranova, V.G., Goncharenko, O.M., Astakhova, N.I. (2019). The latest financial technologies in the context of digitalization of the economy: experience of developed countries and Ukrainian experience. Kharkiv: Disa Plus.
2. Bolgar, T. N. (2008). The need to take into account moral hazards when assessing the level of financial security of banks. Problems and prospects of the development of the banking system of Ukraine, 23, 277-281.
3. Brodsky, Yu. B., Molodetska, K. V. (2016). Modeling economic dynamics. Zhytomyr: ZhNAEU.
4. Financial Stability Report. (2022). National Bank of Ukraine. URL: https://bank.gov.ua/ua/news/all/zvit-pro-finansovu-stabilnist-gruden-2022-roku

5. Financial Stability Report. (2024). National Bank of Ukraine. URL: https://bank.gov.ua/ua/news/all/zvit-pro-finansovu-stabilnist-gruden-2024-roku
6. Gavrylko, T., Antonova, R. (2020). FinTech: foreign experience and features of development in Ukraine. Scientific Bulletin of Uzhhorod National University. Series: International Economic Relations and World Economy, 9, 17-22.
7. Mazaraki, A., Volosovych, S. (2018). FinTech in the system of social transformations. Bulletin of the KNTEU, 2, 5-18.
8. Nikiforov, P., Babukh, I., Kinashchuk, S. (2020). FinTech as a driver for today's financial market transformations: the Ukrainian context. Black Sea Economic Studies, 51, 189-194.
9. Number of card fraud cases. (2024). National Bank of Ukraine. URL: https://bank.gov.ua/ua/news/all/kilkist-vipadkiv-shahraystva-z-kartkami-znizilasya-zbitki-za-nimi--zrosli
10. Share of non-performing loans (NPL) in Ukraine. (2025). URL: https://bank.gov.ua/ua/stability/npl
11. Trusova, N.V., Melnyk, O.V. (2024). Methodological approach to the implementation of digital technologies of metaspace in the infrastructure of the financial market. Collection of scientific works of the Dmytro Motorny State Technical University of Economics (economic sciences), 1(50), 138-148.
12. Yang, L., Hu, X., Wu, J., & Liu, Y. (2019). A distributed honeypot deployment system based on Blockchain technology. IEEE Access, 7, 35881-35890.
13. Zeeman, E. C. (1977). Catastrophe Theory. Reading, MA: Addison-Wesley, 1972-1977.