УДК 336.7-049.5 DOI:10.32680/2409-9260-2023-9-310-90-97

ФІНАНСОВА БЕЗПЕКА БАНКІВ НА РИНКУ ПЛАТІЖНИХ КАРТОК УКРАЇНИ

Сергєєва О.С., кандидат економічних наук, доцент кафедри банківської справи, Одеський національний економічний університет, м. Одеса, Україна
e-mail:lenasergeeva2007@ukr.net
ORCID: 0000-0002-5523-3894

Анотація. *У статті висвітлені особливості організації фінансової безпеки банків на ринку платіжних карток. Зі збільшенням використання банківських платіжних карток зростає ризик зловживання та шахрайства в цій сфері. Тому, захист карткових даних та безпека фінансових транзакцій стали пріоритетними завданнями для банків та фінансових установ в сучасних умовах. Зменшення ризиків злочинної діяльності в цій сфері повинно розглядатися комплексно, зі застосуванням банками сучасних технологій, методів кібербезпеки та підвищенням знань користувачів щодо правил безпеки використання банківських платіжних карток. В статті запропоновано алгоритм прийняття рішень щодо уникнення загроз при організації фінансової безпеки з платіжними картками.*
За результатами проведеного дослідження зазначено, що організація безпеки стосовно платіжних карток має вплив на фінансову безпеку банків та повинна розглядатися як ключовий елемент управління банківським сектором.
Ключові слова: *банк, фінансова безпека, ризик, ринок платіжних карток, кібератаки, шахрайство.*

FINANCIAL SECURITY OF BANKS AT THE PAYMENT CARD MARKET IN UKRAINE

Serhieieva Olena, PhD (Economics), Associate Professor, Department of Banking Odessa National University of Economics, Odessa, Ukraine
e-mail:lenasergeeva2007@ukr.net
ORCID: 0000-0002-5523-3894

Abstract. *Introduction. The modern development of the banking business is associated with a significant number of risks that, in light of globalization processes, political and economic issues in Ukraine and the world, and the advancement of technological and information systems, tend to transform, making them very challenging to identify. Adhering to the financial security of banks is an essential element of bank management, as it enables a focus on long-term results, successfully develop measures to achieve set objectives, and enhance the ability to more effectively control the activities of banks.*
Purpose. An analysis of research in the direction of financial security of banks has revealed that the pressing issue is the enhancement of financial security for operations involving payment cards. This necessitates the adoption of decision-making policies that allow for timely and consistent utilization of all the bank's capabilities while simultaneously maintaining risks at an acceptable and manageable level.
Results. The development of payment infrastructure and the implementation of innovative payment methods for goods and services create a continuous demand for banking payment cards. However, the risk of abuse and fraud in this sphere is on the rise, making it a contemporary challenge for banks to anticipate and mitigate these risks. Banks and financial institutions are becoming increasingly vulnerable to cybercriminals who employ various methods and techniques to obtain card data and gain unauthorized access to user accounts. Mitigating criminal activities in this area should be considered holistically, involving the use of modern technologies and cybersecurity methods by banks, as well as increasing user awareness regarding the security rules for using banking payment cards.
Conclusions. The issue of financial security for banks in the Ukrainian payment card market is quite serious and requires continuous improvement in the age of digitalization. It is the prevention of losses in their operations that enhances financial security and the robust financial stability of banks..
Keywords: *bank, financial security, risk, payment card market, fraud, cyber attacks.*

JEL Classification: G210; G340.

Постановка проблеми. Банківська система має важливе значення для економіки країни, оскільки виконує низку важливих функцій, ефективна реалізація яких особливо важлива в поточних умовах функціонування.

Актуальність забезпечення фінансової безпеки банків України в умовах війни набуває великого значення з погляду забезпечення їх життєдіяльності, здатності виконувати фінансові зобов'язання та відновлення економічного стану країни в післякризовий період. «Сучасний

розвиток банківського бізнесу пов'язаний зі значною кількістю ризиків, які з урахуванням глобалізаційних процесів, політичних, економічних проблем в Україні та світі, розвитку технологічних та інформаційних систем, мають тенденцію до трансформації, внаслідок чого їх дуже складно ідентифікувати» [1]. Тому дотримання фінансової безпеки банків є неодмінним елементом управління банками, адже дає змогу орієнтуватись на довгострокові результати, успішно розробляти заходи, що забезпечать досягненню поставлених цілей та можливість ефективніше контролювати діяльність банків.

В умовах цифрової економіки банківські платіжні карти є одним з найсучасніших та найпоширеніших засобів безготівкових розрахунків, що забезпечують доступ клієнтів до різноманітних фінансових послуг та товарів. Однак, зростання використання банківських платіжних карток призвело до збільшення кількості кіберзлочинності, яка пов'язана з операціями з цими картками, що негативно впливає на фінансову безпеку банків та як слід, на їх прибутковість. Отже, організація фінансової безпеки банку є надзвичайно важливою для забезпечення захисту фінансових активів клієнтів й збереження репутації банку.

Відокремлення невирішених раніше частин загальної проблеми. Проведений аналіз досліджень в напряму фінансової безпеки банків засвідчив, що актуальним питанням є удосконалення безпеки банків за операціями з платіжними картками, що вимагає в першу чергу організації політики прийняття рішень таким чином, щоб вчасно і послідовно використовувати усі можливості діяльності банку й одночасно утримувати ризики на прийнятному і керованому рівні.

Мета дослідження. Мета дослідження з огляду на зазначене, доцільним є розробка рекомендацій для підвищення рівня фінансової безпеки банків на ринку платіжних карток в Україні в сучасних умовах.

Основний матеріал. Провідна роль фінансової безпеки банків зумовлена тим, що за допомогою забезпечення стабільності їх фінансової складової, вони здатні вирішувати питання забезпечення ресурсної, кадрової, інформаційної та фізичної безпеки.

З нашої точки зору, найбільш повним є визначення фінансової безпеки, надане О. Барановським, який розглядає її як «стан захищеності фінансових інтересів банків, його фінансової стійкості, а також середовища, в якому він функціонує» [2].

Ми погоджуємось з авторкою Коваленко В.В., яка визначає, що «фінансова безпека банків залежить від наступних чинників: політична та економічна нестабільність як на національному, так і на міжнародному рівнях, рівень залежності банків від внутрішніх та зовнішніх джерел залучення, рівня діджиталізації» [3].

За останні десять років ринок платіжних карток в Україні зазнав значного розвитку та став необхідністю для задоволення потреб споживачів. Для підвищення конкурентоспроможності банки виводять на ринок нові картки з різними умовами видачі та користування.

Розвиток платіжної інфраструктури та впровадження інноваційних методів оплати товарів та послуг дає можливість стверджувати про постійний попит на банківські платіжні картки. Так, у 2018 році українськими банками було емітовано 59,4 млн шт. платіжних карток, серед яких 36,9 млн шт. є активними. З кожним роком прослідковується позитивна тенденція, адже кількість емітованих та активних карток зростає. Аналізуючи динаміку безконтактних платіжних карток, можна зазначити стрімкий розвиток та збільшення карток такого виду. Якщо у 2018 році, кожна 9 активна платіжна картка була безконтактною, то у 2020 році кожна 5 (п’ята), що вказує на їх збільшення майже у два рази, дивлячись на дані станом на кінець 2022 року, можна стверджувати, що майже кожна картка є безконтактною, а загальна кількість платіжних карток склала 109,8 млн шт. (рис. 1).

Слід зазначити, що з відкриттям нових можливостей використання платіжних карток, зростає також ризик зловживання та шахрайства в цій сфері, тому сучасними викликами для банків є передбачення виникнення ризику та його зниження. Банки та фінансові установи стають все більш уразливими перед кіберзлочинцями, які використовують різні методи та техніки для здобуття карткових даних та незаконного доступу до рахунків користувачів. Злочини у сфері виготовлення та обігу платіжних карток можуть мати різні форми та способи здійснення, а також різну мотивацію та цілі.

Тому, захист карткових даних та безпека фінансових транзакцій стали пріоритетними завданнями для банків та фінансових установ в сучасних умовах. Зменшення ризиків злочинної діяльності в цій сфері повинно розглядатися комплексно, зі застосуванням банками сучасних технологій, методів кібербезпеки та підвищенням знань користувачів щодо правил безпеки використання банківських платіжних карток.

Рис.1. Розподіл безготівкових операцій з використанням платіжних карток, за 2018 – 2022 (на кінець року)

Джерело: складено автором за матеріалами [4]

Тому, захист карткових даних та безпека фінансових транзакцій стали пріоритетними завданнями для банків та фінансових установ в сучасних умовах. Зменшення ризиків злочинної діяльності в цій сфері повинно розглядатися комплексно, зі застосуванням банками сучасних технологій, методів кібербезпеки та підвищенням знань користувачів щодо правил безпеки використання банківських платіжних карток.

За останні роки НБУ зробив прорив в підвищенні безпеки з платіжними картками, запровадивши Системи BankID. Завдяки взаємодії Системі BankID НБУ та Єдиного порталу державних послуг «Дія» було створена послуга цифрового підпису, як способу підтвердження автентичності та цілісності електронних документів, який використовує криптографічні алгоритми, тільки за 4 роки кількість ідентифікацій збільшилось майже в 100 разів [5].

Варто звернути увагу, що багато зарубіжних країн вже використовують систему міжнародного співробітництва та обміну досвідом у сфері кібербезпеки. Ці країни розробили відповідні стратегії, у яких проблема боротьби з кіберзлочинністю займає ключове місце. Ця тенденція є позитивною для України, яка наразі розробляє власну стратегію щодо захисту кіберпростору.

Сьогодення регулювання безпеки українських банків регламентується міжнародними положеннями, так Базельський комітет з банківського нагляду встановив 7 категорій подій, які стосуються ризиків управління операціями та пов’язані з: «внутрішнім чи зовнішнім шахрайством; управлінням персоналом та охороною праці, клієнтами, продуктами та нормами ділової практики; пошкодженням або знищенням активів; унеможливленням діяльності та функціонування систем; виконанням переказів; наданням платіжних доручень, у здійснених переказах та управлінням процесами» [6].

Міжнародний стандарт ISO 27001:2013 встановлює «вимоги до управління інформаційною безпекою для організації захисту інформаційних ресурсів як модель впровадження, моніторингу та покращення менеджменту інформаційної безпеки» [7].

На жаль, в сучасному інформаційному світі кібератаки мають за мету маніпуляцію суспільством, дестабілізацію всередині суспільства, дискредитацію органів державної влади України, а також дискредитацію України на міжнародній арені.

У банківській системі України спостерігається стійка тенденція до зростання кількості кіберзлочинів у сфері високих технологій. З огляду на високий рівень інформатизації суспільства, Україна повинна постійно удосконалювати належний та ефективний механізм боротьби з кіберзлочинами. «Це є однією з серйозних загроз національній безпеці держави, тому для розв'язання цієї проблеми слід врахувати міжнародний досвід у розробці стратегій

кібербезпеки» [8].

Одним з найбільш вагомих загроз для фінансової безпеки банків є кіберризики та кібершахрайства, що можуть спричинити масштабні втрати та порушити роботу платіжних та банківських систем. За період з початку 2021 року кібератаки зафіксував 51 банк (рис. 2).

З рис. 2 наочно бачимо, що після початку повномасштабної війни кількості кібератак на банки суттєво зросла.

Рис. 2. Розподіл банків залежно від зміни кількості кібератак порівняно з попереднім місяцем

Джерело: складено автором за матеріалами [4]

При таких умовах, для зменшення кіберризиків пропонуємо розглянути основні ключові принципи стратегій кібербезпеки банку з платіжними картками (рис. 3).

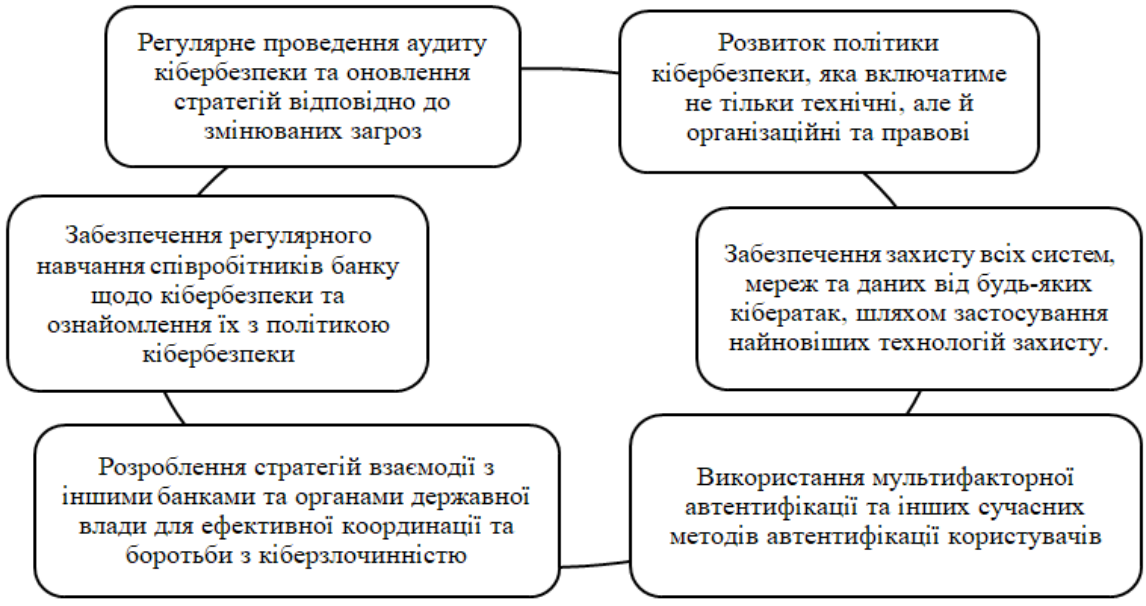

Рис. 2 Основні ключові принципи стратегій кібербезпеки банку з платіжними картками

Джерело: розроблене автором за матеріалами [8]

На нашу думку, дотриманням цих принципів можуть допомогти банкам розробити ефективні та комплексні стратегії кібербезпеки з платіжними картками, які захистять їх від можливих загроз.

Для підвищення фінансової безпеки з платіжними картками рекомендуємо

використовувати певний алгоритм прийняття рішень щодо рівнів захисту, а тощо: емісія, видача, обслуговування та закриття платіжних карток. Кожен рівень безпеки має свій ступінь відповідальності та веде до мінімізації ризиків в цьому напряму (табл. 1).

Таблиця 1

Алгоритм прийняття рішень щодо уникнення загроз
при організації фінансової безпеки з платіжними картками

Рівень захисту	Загроза	Рішення щодо уникнення загрози
Рівень 1 – Емісія платіжних карток	Можливість крадіжки чи фальсифікації карток. Це може статися на різних етапах емісії, включаючи період збору та обробки даних, виготовлення фізичних карток, та їх відправлення клієнтам	1. Контроль якості фізичних карток: захист від копіювання, використання унікальних фізичних характеристик та технології обробки зображень. 2. Використання захищених методів відправлення карток. 3. Контроль доступу до платіжних карток. 4. Аудит безпеки емісії платіжних карток.
Рівень 2 – Оформлення та видача платіжних карток	1. Крадіжка особистих даних клієнтів та використання їх для шахрайських цілей. 2. Недостатня аутентифікація клієнта. 3.Вразливість програмного забезпечення банку, яке використовується для обробки платіжних транзакцій та зберігання даних клієнтів	1. Банк повинен забезпечувати захист особистої інформації клієнтів, застосовуючи різноманітні технології шифрування та сучасні методи аутентифікації. 2. При оформленні та видачі платіжних карток банку необхідно вживати комплексних заходів технічного, організаційного та юридичного характеру. 3. Банк повинен забезпечити безпеку програмного забезпечення, застосовуючи заходи безпеки програмування та перевіряти на вразливості програмне забезпечення з регулярністю від відомих загроз безпеки, таких як віруси та хакерські атаки.

Рівень 3 – Обслуговування платіжних карток	1.Використання слабких паролів. 2.Втрата чи крадіжка карток. 3.Атаки на сервери банку з метою отримання доступу до даних карток. 3.Соціальний інжиніринг.	1. Банк може надавати клієнтам поради з приводу безпеки паролів та нагадувати їм про необхідність регулярно змінювати свої паролі. 2. Банк повинен вчасно реагувати на підозрілі операції, шляхом моніторингу транзакцій, зателефонувати клієнту в разі підозри на шахрайські операції. 3. Банк повинен постійно підвищувати рівень захисту своїх серверів, використовуючи сучасні заходи безпеки, такі як шифрування даних, захист від DDoS атак та захист від вторгнень.
Рівень 4 – Закриття карткового рахунку	В процесі закриття карткового рахунку, банк може не закрити остаточно картковий рахунок і картка є активною, хоча клієнт впевнений, що рахунок закритий	При закритті рахунків співробітникам банків необхідно ретельно вносити інформацію в систему та надавати клієнтам достатню інформацію про закриття їх карток.

Джерело: розроблено автором

Дані табл. 1, відображають, що більша частина причин небезпеки з банківськими платіжними картками є спроби проникнення в програмне забезпечення злочинників; помилка персоналу випадкова або в корисливих цілях; вихід техніки із ладу; вихід конфіденційної інформації за межі банку та ін. Тому інформаційна безпека при використанні платіжних карток є важливою складовою для банків, але це тільки один аспект захисту фінансових даних клієнтів. Організація безпеки банку з платіжними картками повинна також включати співпрацю зі спеціалізованими організаціями, такими як платіжні системи та антишахрайні асоціації, для забезпечення міжнародної безпеки фінансових транзакцій.

Для забезпечення максимальної безпеки фінансових транзакцій, банкам необхідно удосконалити захист своєї інформаційної системи та персональних даних клієнтів через використання сучасних технологій шифрування даних, захист від хакерських атак та зламу системи. Впровадження постійного моніторингу транзакцій дасть змогу виявляти будь-які підозрілі активності, що можуть свідчити про шахрайство або крадіжку даних. Необхідною умовою для банків також є підтримка клієнтів у разі шахрайства та допомога їм у відновленні втрачених коштів. Це допоможе забезпечити безпеку не тільки фінансової системи, але й довіру клієнтів до банків та платіжних систем в цілому.

Однак, організація фінансової безпеки банку з платіжними картками не закінчується на рівні банку, основною проблемою є не достатньо висока фінансова грамотність населення щодо використання платіжних карток, що приводить до крадіжок особистих даних шахраями,

використання фальшивих карток або навіть до втрати грошей. Тому Урядом, НБУ та банками постійно проводяться заходи «Підвищення фінансової грамотності населення» [9].

Відомі міжнародні платіжні система не зупиняються на впровадженні класичних карт та постійно їх вдосконалюють, в тому числі матеріал з яких вони виготовляються. Так, прес-служба платіжної системи Mastercard оприлюднила інформацію щодо заміни своїх карток. «Масштабні оновлення карт Mastercard будуть здійснені з метою переходу на нові стандарти виготовлення, які базуються на використанні екологічних матеріалів замість ПВХ-пластику» [10]. До 2028 року компанія планує повністю відмовитися від використання ПВХ-пластику та перейти на використання біопластику та пластику вторинної переробки, що дозволить зменшити відходи та шкідливі викиди під час виробництва. Наразі ініціатива підтримується понад 330 емітентами карток у 80 країнах, які обговорюють процес оновлення карток з постачальниками.

Зазначимо, що в Україні оновлення карток планується здійснювати поступово з перехідним періодом до 2028 року. Оновлені картки будуть сертифіковані відповідно до екологічних вимог та отримають позначку Card Eco Certification перед видачею користувачам. Організація Mastercard має на меті перейти на низьковуглецеву регенеративну економіку та боротися зі світовими проблемами, пов'язаними зі змінами клімату.

Висновки. Зважаючи на викладене вище можемо зазначити, щодо умов в яких сьогодні працюють банки, зазначимо, що проблема фінансової безпеки банків на ринку платіжних карток України є досить серйозною та вимагає в умовах цифровізації постійного удосконалення. До основних напрямів підвищення рівня фінансової безпеки банків в реаліях сьогодення пропонується; удосконалення системи контролю банків, через підвищення ролі фінансового контролінгу, постійного моніторингу та аналізу транзакцій клієнтів банків, оновленню програмного забезпечення для захисту від нових загроз, через формування в працівниках банків професійної досконалості щодо прийняття правильних рішень та удосконалення підвищення фінансової грамотності, фінансової інклюзії населення України. Саме запобіганням збитків у діяльності підвищує фінансову безпеку та як слід фінансову стійкість банків.

Список літератури

1. Сучасні детермінанти управління банківськими ризиками: колективна монографія / За ред. В.В. Коваленко. Одеса, ОНЕУ, 2022. 331 с. URL: http://dspace.oneu.edu.ua/jspui/handle/123456789/14769. (дата звернення 10.10.2023).

2. Барановський О. І. Фінансова безпека в Україні (методологія оцінки та механізми забезпечення): монографія. К.: Київ. нац. торг. - екон. ун-т, 2004. 759 с.

3. Коваленко В.В. Філософія безпеки банків в умовах структурних дисбалансів економіки України. Економічний форум. 2016. № 1. С. 256-262. URL: http://dspace.oneu.edu.ua/jspui/handle/123456789/4958.(дата звернення 10.10.2023).

4. Грошово-кредитної статистики України. URL: https://bank.gov.ua/ua/statistic/sector-financial#1ms. (дата звернення 10.10.2023).

5. Ризик-менеджмент в умовах високої невизначеності. URL: https://zplawoffice.com/tpost/bxhptg7ohn-rizik-menedzhment-v-umovah-visoko-nevizn.(дата звернення 12.10.2023).

6. Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework. URL: https://www.bis.org/publ/bcbs107.htm (дата звернення 12.10.2023).

7. BS ISO/IEC 27002:2013. ISO 27002 - The Information Security Standard.
Standards Direct. URL: https://standardsdirect.org/ (дата звернення 13.10.2023).

8. Йона О.О., Казакова Н.Ф. Світові тенденції боротьби з кіберзлочинністю. Вісник Східноукраїнського Національного університету ім. В. Даля. Луганськ, 2013. №15 (204). С. 59-61.

9. Фінансова грамотність, фінансова інклюзія та фінансовий добробут в Україні у 2021. Звіт за результатами дослідження. URL: https://bank.gov.ua/admin_uploads/article/Research_Financial_Literacy_Inclusion_Welfare_2021.pdf?v=4 (дата звертання 15.10.2023 р.)

10. Офіційний сайт платіжної системи Mastercard. URL: https://www.mastercard.ua/uk-ua.html. (дата звернення 14.10.2023).

References

1. Kovalenko V.V. (2022). Suchasni determinanty upravlinnia bankivskymy ryzykamy [Modern determinants of banking risk management]. Odesa, ONEU [In Ukrainian].
2. Baranovskyi O. I. (2004). Finansova bezpeka v Ukraini (metodolohiia otsinky ta mekhanizmy zabezpechennia) [Financial security in Ukraine (assessment methodology and security mechanisms] . K.: Kyiv. nats. torh. - ekon. un-t [In Ukrainian].
3. Kovalenko V.V. (2016). The philosophy of bank security in conditions of structural imbalances of thS Ukrainian economy. Ekonomichnyi forum. 1. 256-262. http://dspace.oneu.edu.ua/jspui/handle/123456789/4958 [In Ukrainian].
4. Pokaznyky bankivsjkoji systemy. Statystyka. Oficijnyj sajt Nacionaljnogho banku Ukrajiny [Indicators of the banking system. Statistics. Official site of the National Bank of Ukraine]. Retrieved from: https://bank.gov.ua/control/uk/publish/article?art_id=34661442&cat_id=34798593 (accessed Zhovten10, 2023) [In Ukrainian].
5. Ryzyk-menedzhment v umovakh vysokoi nevyznachenosti [Risk management in conditions of high uncertainty]. https://zplawoffice.com. Retrieved from https://zplawoffice.com/tpost/bxhptg7ohn-rizik-menedzhment-v-umovah-visoko-nevizn [in Ukrainian].
6. Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework. Retrieved from https://www.bis.org/publ/bcbs107.htm
7. BS ISO/IEC 27002:2013. ISO 27002 - The Information Security Standard.
Standards Direct. URL: https://standardsdirect.org/
8. Yona O.O., Kazakova N.F. (2013). Global trends in the fight against cybercrime. Visnyk Skhidnoukrainskoho Natsionalnoho universytetu imeni V. Dalia. Luhansk, 15 (204), 59-61. Retrieved from http://dspace.oneu.edu.ua/xmlui/handle/123456789/1176?show=full [In Ukraine].
9. Finansova hramotnist, finansova inkliuziia ta finansovyi dobrobut v Ukraini u 2021. Zvit za rezultatamy doslidzhennia. Retrieved from https://bank.gov.ua/admin_uploads/article/Research_Financial_Literacy_Inclusion_Welfare_2021.pdf?v=4 (accessed Zhovten10, 2023) [In Ukrainian].
10. Ofitsiinyi sait platizhnoi systemy Mastercard. Retrieved fromhttps://www.mastercard.ua/uk-ua.html [In Ukraine].

Стаття надійшла до редакції 19.10.2023
Прийнята до публікації 23.10.2023