УДК 330.101
JEL: E42; G20; G21; G29

# КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ПІДВИЩЕННЯ РІВНЯ БЕЗПЕЧНОСТІ БАНКІВСЬКОГО ПЛАТІЖНОГО СЕРЕДОВИЩА УКРАЇНИ

©2020 ДУБИНА М. В., САДЧИКОВА І. В., СЕРЕДЮК І. О.

*УДК 330.101*
*JEL: E42; G20; G21; G29*

**Дубина М. В., Садчикова І. В., Середюк І. О. Концептуальні підходи до підвищення рівня безпечності банківського платіжного середовища України**

*Метою статті визначено дослідження впливу процесів цифрової трансформації на зміну системи фінансової безпеки банківського платіжного середовища. Проаналізовано наукові підходи до трактування сутності категорії «фінансова безпека банку», що дозволило виокремити змістовні ознаки безпеки платіжного середовища банку в сучасних умовах становлення цифрової економіки. Встановлено, що такий вид безпеки залежить від економічної та політичної стабільності країни, а також від рівня доступу користувачів до Інтернету та відповідних електронних пристроїв. Визначено, що найбільша кількість випадків викрадення грошей припадає саме на шахрайство з платіжними картками, тому було описано основні види такого шахрайства: онлайн-платежі на незахищених сайтах (фішингові сайти); телефонний фітинг; перевипуск SIM-картки; незахищені точки доступу Wi-Fi; шахрайство з втраченими та викраденими картками; шахрайство з банкоматами (від англ. skimming). Здійснено опис сутності таких видів шахрайств і способів захисту від них. Ґрунтовно проаналізовано банківське платіжне середовище в Україні в умовах цифровізації, що дало змогу виявити ряд нових і сучасних напрямів інноваційної банківської діяльності (FinTech, InsurTech, WealthTech та ін.). Також наведено аналіз тенденцій щодо втрат від шахрайства з картками в провідних європейських країнах. Розглянуто основні інструменти підвищення належного рівня безпеки банківського платіжного середовища (відкритий банкінг на основі протоколу API, Third Party Provider (TPP), Strong Customer Authentication (SCA), 3D Secure та ін.) та наведено способи захисту конфіденційної інформації для банківської установи та її клієнтів. Значну увагу приділено опису переваг відкритого банкінгу (Open Banking), який поступово змінює процедуру аутентифікації клієнтів на основі сучасних цифрових можливостей і сприяє оперативнішому впровадженню інновацій; персоналізації банківських продуктів під клієнта; захищеності клієнтів і банків; спрощенню процедури отримання ліцензії; переходу від конкуренції між банками і FinTech до співпраці; здешевленню банківських продуктів для клієнта; доступності банківських продуктів.*

***Ключові слова:*** *фінансова безпека, платіжне середовище, банківська система, цифровізація, фінансові технології.*
***DOI:*** *https://doi.org/10.32983/2222-4459-2020-3-349-359*
***Рис.:*** *3.* ***Табл.:*** *4.* ***Бібл.:*** *17.*

***Дубина Максим Вікторович*** *– доктор економічних наук, доцент, завідувач кафедри фінансів, банківської справи та страхування, Національний університет «Чернігівська політехніка» (вул. Шевченка, 95, Чернігів, 14027, Україна)*
***E-mail:*** *maksim-32@ukr.net*
***ORCID:*** *http://orcid.org/0000-0002-5305-7815*
***Researcher ID:*** *http://www.researcherid.com/F-3291-2014*
***SPIN:*** *http://elibrary.ru/1183-5775*

***Садчикова Ірина Володимирівна*** *– кандидат економічних наук, доцент, доцент кафедри фінансово-економічної безпеки, Національний університет «Чернігівська політехніка» (вул. Шевченка, 95, Чернігів, 14027, Україна)*
***E-mail:*** *aspirant_chstu@ukr.net*
***ORCID:*** *https://orcid.org/0000-0001-5144-1306*
***Researcher ID:*** *http://www.researcherid.com/F-4936-2014*
***SPIN:*** *http://elibrary.ru/1873-5962*

***Середюк Ірина Олександрівна*** *– магістр, Національний університет «Чернігівська політехніка» (вул. Шевченка, 95, Чернігів, 14027, Україна)*
***E-mail:*** *i.seredyuk36@gmail.com*
***ORCID:*** *http://orcid.org/0000-0002-6100-7164*

*УДК 330.101*
*JEL: E42; G20; G21; G29*

***Дубина М. В., Садчикова И. В., Середюк И. А. Концептуальные подходы к повышению уровня безопасности банковской платежной среды Украины***

*Целью статьи определено исследование влияния процессов цифровой трансформации на изменение системы финансовой безопасности банковской платежной среды. Проанализированы научные подходы к пониманию сущности категории «финансовая безопасность банка», что позволило определить основные признаки безопасности платежной среды банка в современных условиях становления цифровой экономики. Определено, что такой вид безопасности зависит от экономической и политической стабильности страны, а также от уровня доступа пользователей к Интернету и соответствующим электронным устройствам. Определено, что наибольшее количество случаев потери денег приходится именно на мошенничество с платежными карточками, поэтому были описаны основные виды такого мошенничества: онлайн-платежи на незащищенных сайтах (фишинговые сайты); телефонный фитинг; перевыпуск SIM-карты; незащищенные точки доступа Wi-Fi; мошенничество с потерянными и похищенными карточками; мошенничество с банкоматами (от англ. skimming). Описаны сущность таких видов мошенничеств и способы защиты от них. Подробно проанализирована банковская платежная среда в Украине в условиях цифровизации, что позволило определить ряд новых направлений инновационной банковской деятельности (FinTech, InsurTech, WealthTech и др.). Также представлен анализ тенденций потерь от мошенничества с картами на примере ведущих европейских стран. Рассмотрены основные инструменты повышения надлежащего уровня безопасности банковской платежной среды (открытый банкинг на основе протокола API, Third Party Provider (TPP), Strong Customer Authentication (SCA), 3D Secure и др.) и приведены способы защиты конфиденциальной информации для банковских учреждений и их клиентов. Значительное внимание уделено описанию преимуществ открытого банкинга (Open Banking), который постепенно меняет процедуру*

*аутентификации клиентов на основе современных цифровых возможностей и способствует оперативному внедрению инноваций; персонализации банковских продуктов под клиента; защищенности клиентов и банков; упрощению процедуры получения лицензии; перехода от конкуренции между банками и FinTech к сотрудничеству; удешевлению банковских продуктов для клиента; доступности банковских продуктов.*
***Ключевые слова:*** *финансовая безопасность, платежное средство, банковская система, цифровизация, финансовые технологии.*
***Рис.:*** *3.* ***Табл.:*** *4.* ***Библ.:*** *17.*

***Дубина Максим Викторович*** *– доктор экономических наук, доцент, заведующий кафедрой финансов, банковского дела и страхования, Национальный университет «Черниговская политехника» (ул. Шевченко, 95, Чернигов, 14027, Украина)*
***E-mail:*** *maksim-32@ukr.net*
***ORCID:*** *http://orcid.org/0000-0002-5305-7815*
***Researcher ID:*** *http://www.researcherid.com/F-3291-2014*
***SPIN:*** *http://elibrary.ru/1183-5775*

***Садчикова Ирина Владимировна*** *– кандидат экономических наук, доцент, доцент кафедры финансово-экономической безопасности, Национальный университет «Черниговская политехника» (ул. Шевченко, 95, Чернигов, 14027, Украина)*
***E-mail:*** *aspirant_chstu@ukr.net*
***ORCID:*** *https://orcid.org/0000-0001-5144-1306*
***Researcher ID:*** *http://www.researcherid.com/F-4936-2014*
***SPIN:*** *http://elibrary.ru/1873-5962*

***Середюк Ирина Александровна*** *– магистр, Национальный университет «Черниговская политехника» (ул. Шевченко, 95, Чернигов, 14027, Украина)*
***E-mail:*** *i.seredyuk36@gmail.com*
***ORCID:*** *http://orcid.org/0000-0002-6100-7164*

*UDC 330.101*
*JEL: E42; G20; G21; G29*

***Dubyna M. V., Sadchykova I. V., Seredyuk I. O. The Conceptual Approaches to Improving the Security of the Banking Payment Environment of Ukraine***

*The article is aimed at studying the impact of digital transformation processes on changing the financial security system of the banking payment environment. Scientific approaches to understanding the essence of the category of «financial security of bank» are analyzed, allowing to identify the main signs of the bank's payment environment in the current conditions of establishing the digital economy. It is defined that this type of security depends on the economic and political stability of the country, as well as on the level of the users' access to the Internet and related electronic devices. It is determined that the largest number of cases of loss of money accounted for payment card fraud, so the main types of fraud are described: online payments on unprotected sites (fishing sites); phone fitting; re-issue of SIM cards; unprotected Wi-Fi hotspots; fraud with lost and stolen cards; ATM fraud (skimming). The nature of these types of scams and ways to protect against them are described. The banking payment environment in Ukraine in the conditions of digitization is analyzed in detail, which has allowed to identify a number of new directions of innovative banking activity (FinTech, InsurTech, WealthTech, etc.). Also presented is an analysis of the tendencies of losses from card fraud on the example of leading European countries. The main instruments to improve the proper level of security of the banking payment environment (open banking based on the API protocol, Third Party Provider (TPP), Strong Customer Authentication (SCA), 3D Secure, etc.) are considered and ways to protect confidential information for banking institutions and their customers are presented. Much attention is been paid to describing the benefits of Open Banking, which is gradually changing the authentication of customers based on modern digital capabilities and enabling rapid innovation; personalizing banking products for the customer; customer and bank security; simplifying the licensing procedure; transition from competition between banks and FinTech to a cooperation; cheaper banking products for the customer availability of banking products.*
***Keywords:*** *financial security, payment instrument, banking system, digitalization, financial technology.*
***Fig.:*** *3.* ***Tabl.:*** *4.* ***Bibl.:*** *17.*

***Dubyna Maksym V.*** *– D. Sc. (Economics), Associate Professor, Head of the Department of Finance, Banking and Insurance, National University "Chernihiv Polytechnic" (95 Shevchenka Str., Chernihiv, 14027, Ukraine)*
***E-mail:*** *maksim-32@ukr.net*
***ORCID:*** *http://orcid.org/0000-0002-5305-7815*
***Researcher ID:*** *http://www.researcherid.com/F-3291-2014*
***SPIN:*** *http://elibrary.ru/1183-5775*

***Sadchykova Iryna V.*** *– PhD (Economics), Associate Professor, Associate Professor of the Department of Financial and Economic Security, National University "Chernihiv Polytechnic" (95 Shevchenka Str., Chernihiv, 14027, Ukraine)*
***E-mail:*** *aspirant_chstu@ukr.net*
***ORCID:*** *https://orcid.org/0000-0001-5144-1306*
***Researcher ID:*** *http://www.researcherid.com/F-4936-2014*
***SPIN:*** *http://elibrary.ru/1873-5962*

***Seredyuk Iryna O.*** *– Master, National University "Chernihiv Polytechnic" (95 Shevchenka Str., Chernihiv, 14027, Ukraine)*
***E-mail:*** *i.seredyuk36@gmail.com*
***ORCID:*** *http://orcid.org/0000-0002-6100-7164*



В умовах стрімкого розвитку сучасних банківських технологій запорукою стабільної конкуренції кредитної установи серед приватних користувачів та бізнесу є розвиток системи фінансової безпеки банківського платіжного середовища в умовах трансформаційних змін і цифровізації. Завдяки зростаючій відкритості економік держав і послідовній їх інтеграції у світове господарство актуальними стають питанням формування безпеки банківського платіжного середовища.

Теоретичні та методичні основи питання розвитку системи фінансової безпеки банківського платіж-

ного середовища в умовах цифрової трансформації знайшли відображення в роботах таких науковців: О. І. Барановський, Т. А. Васильєва, В. Я. Вовк, Ю. О. Голобородько, М. І. Зубок, В. П. Ільчук, В. В. Коваленко, Ю. М. Коваленко, Т. В. Савченко, С. В. Саранчук, Р. Е. Сміт (*R. E. Smith*), В. А. Шурпаков, О. А. Ягольницький та інші.

Незважаючи на значний внесок вищезазначених науковців, швидкий розвиток фінансового сектора в результаті впливу цифрової економіки обумовлює постійну актуальність проведення наукових досліджень у даній сфері, вивчення особливостей такого впливу та трансформацій класичних моделей розвитку банківських установ.

*Метою* статті є дослідження впливу процесів цифрової трансформації на зміну системи фінансової безпеки банківського платіжного середовища.

Розвиток і поширення безготівкових розрахунків автоматично зменшує готівкове навантаження на фінансову систему країни, що гарантує зростання ліквідності та підвищення капіталізації банківського сектора та фінансової системи в цілому.

Зростання популярності та різноманіття технологій безготівкових розрахунків у світі створюють сприятливі умови для їх поширення в Україні, де вже існує позитивна динаміка користування ними. Розвиток електронної комерції та онлайн-технологій приводить до появи нових видів фінансових послуг і сервісів, що пропонуються банківськими та небанківськими платіжними системами [15].

Банківські установи вкладають значні кошти в інформаційні технології та ефективні інформаційні системи для вдосконалення бізнес-процесів і стратегій з метою отримання конкурентної переваги. Інтернет-банкінг – це інфраструктура інформаційних технологій, яку банки наразі використовують на додаток до інших відомих каналів, таких як телефонний банкінг і відділення банків.

Швидкий розвиток інформаційно-комунікаційних технологій протягом останніх років привів до появи низки нововведень. Клієнти, які використовують Інтернет-банкінг, мають безперервний доступ до своїх рахунків, можуть здійснювати платежі будь-коли та де вони бажають, показувати виписку банку за транзакцією, виплачувати свої борги та здійснювати багато інших банківських операцій в електронному вигляді.

Впровадження в банківську діяльність сучасних інформаційно-комунікаційних технологій потребує від комерційних банків належної уваги до власної фінансової безпеки для збереження як інформації клієнтів, так і фінансової стабільності самої установи. Саме тому, для систематизації та узагальнення наукових положень у сфері впливу процесів цифровізації на трансформацію системи фінансову безпеки банківських установ, спочатку розглянемо сутність поняття «фінансова безпека банку» (*табл. 1*).

Згідно з Концепцією розвитку цифрової економіки та суспільства України на 2018–2020 рр. цифрова економіка базується на інформаційно-комунікаційних і цифрових технологіях, стрімкий розвиток і поширення яких уже сьогодні впливає на традиційну економіку, трансформуючи її від такої, що споживає ресурси, до економіки, що створює ресурси. Цифровізація – насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично уможливлює інтегральну взаємодію віртуального та фізичного, тобто створює кіберфізичний простір [15].

Отже, безпеку платіжного середовища банку в умовах цифровізації, слід розуміти як одну із найважливіших складових національної безпеки, яка залежить від економічної та політичної стабільності країни та рівня доступності користувачів до мережі Інтернет і відповідних електронних пристроїв.

В Україні найбільша кількість постраждалих від викрадення грошей припадає саме на шахрайство з платіжними карткам. Шахрайство з платіжними картками – це діяння, вчинене будь-якою особою, яка з наміром обману використовує банківську карту, щоб отримати з неї гроші без відома власника рахунку. Використання реквізитів картки, без фактичного володіння нею, також є формою злочину. Шахраї використовують інформацію для придбання товарів на ім'я жертв або отримання несанкціонованих коштів з рахунків жертв. Скомпрометовані дані картки також можуть бути виставлені для продажу на «чорних ринках». У багатьох випадках дані, викрадені в одній країні, використовуються вже в іншій, що ускладнює їх відстеження. Для забезпечення належного рівня безпеки платіжного середовища необхідно впроваджувати дієві заходи та механізми, а також дотримуватися правил безпечних розрахунків. Детальний аналіз видів шахрайства з поясненням та способами захисту від нього наведено в *табл. 2.*

На сучасному етапі розвитку, завдяки використанню цифрових технологій, вітчизняним банкам вдається все більше залучати клієнтів до використання можливостей Інтернет-банкінгу, тим самим збільшуючи безготівковий обіг грошей в економіці. За даними НБУ, рівень готівки в економіці у 2019 р. порівняно з 2014 р. зменшився із 17,8% до 9,2% від ВВП. Частка безготівкових операцій у загальному обсязі операцій із використанням платіжних карток збільшилася з 25,0% у 2014 р. до 49,7% на кінець вересня 2019 р.

Загальна кількість платіжних карток в Україні за три квартали 2019 р. зросла на 9% – до 64,7 млн шт. Для оцінки рівня забезпеченості користувачів банківськими платіжними інструментами проаналізуємо частку активних банківських карток у платіжному середовищі України (*рис. 1*) [6]. У зв'язку з тим, що Національним банком України надано інформацію лише

**Таблиця 1**

**Сутність поняття «фінансова безпека банку»**

| Автор, джерело | Визначення |
|---|---|
| Коваленко В. В. [7] | Фінансова безпека банків залежить від: політичної та економічної стабільності як на національному, так і на міжнародному рівнях; рівня залежності банків від внутрішніх і зовнішніх джерел залучення фінансових ресурсів; рівня концентрації активів банків в інших транснаціональних корпораціях; рівня концентрації активів банків за галузями економіки або фінансово-промисловими групами; структури власності банків |
| Зубок М. І. [5] | Безпека банківської діяльності трактується як: стан стійкої життєдіяльності, за якого забезпечується реалізація мети банку та основних його інтересів, захист від внутрішніх і зовнішніх дестабілізуючих факторів незалежно від умов функціонування; властивість своєчасно й адекватно реагувати на всі негативні прояви внутрішнього та зовнішнього середовища банку; здатність протистояти різним посяганням на власність, діяльність й імідж банку, створювати ефективний захист від внутрішніх і зовнішніх загроз |
| Наказ Про затвердження Методичних рекомендацій щодо розрахунку рівня економічної безпеки України № 1277 від 29.10.2013 р. [14] | Фінансова безпека – це стан фінансової системи країни, за якого створюються необхідні фінансові умови для стабільного соціально-економічного розвитку країни, забезпечується її стійкість до фінансових шоків та дисбалансів, створюються умови для збереження цілісності та єдності фінансової системи країни. Згідно з даними рекомендаціями банківська безпека – це рівень фінансової стійкості банківських установ країни, що дає змогу забезпечити ефективність функціонування банківської системи країни та захист від зовнішніх і внутрішніх дестабілізуючих чинників незалежно від умов її функціонування |
| Барановський О. І. [1] | Фінансова безпека комерційного банку: сукупність умов, при яких потенційно небезпечні для фінансового стану комерційного банку дії або обставини, попереджені або зведені до такого рівня, при якому вони не здатні наносити шкоди встановленому порядку функціонування банку, збереження та відтворення його майна та інфраструктури і перешкоджати досягненню банком поставлених цілей; стан захищеності фінансових інтересів комерційного банку, його фінансової стійкості, а також середовища, в якій він функціонує |
| Голобородько Ю. О. [2] | Фінансова безпека банку – це такий стан, який характеризується оптимальним рівнем залучення та розміщення ресурсів при мінімальних загрозах і здатністю банку до саморозвитку, підвищення ефективності його діяльності та конкурентоспроможності |

**Таблиця 2**

**Види шахрайства з платіжними картками та способи захисту**

| Вид | Суть | Захист |
|---|---|---|
| 1 | 2 | 3 |
| Онлайн-платежі на незахищених сайтах (фішингові сайти) | Шахрайство без картки (Card-not-present (CNP)): це випадки шахрайства, коли фізична картка не потрібна. Зазвичай це онлайн-платежі з «віддаленою покупкою» («remote purchase»). При вводі даних з карти шахраї можуть їх скопіювати | Уважно перевіряти адресу сайту, вона повинна починатися з https. Якщо адреса починається з http – це означає, що система використовує застарілу технологію передачі даних і робити оплату на такому сервісі небезпечно |
| Телефонний фітинг | Шахрайства з CNP, пов'язані з викраденими даних платіжної картки, що здійснюється по телефону | Нікому не повідомляти такі особисті дані, як CVV-код, чи код з SMS, термін дії картки та логін і пароль для входу в Інтернет-банкінг |
| Перевипуск SIM-карти | Після звернення до оператора мобільного зв'язку з проблемою втрати SIM-карти її можна прив'язати на інший номер. Таким чином, шахраї отримають доступ до онлайн-банкінгу | Безпечніше оформити SIM-карту на умовах контракту, яку неможливо замінити без паспорта, а також нікому не повідомляти останні набрані номери або номери, на які найчастіше робиться дзвінок, і суми поповнень |
| Незахищені точки доступу Wi-Fi | При використанні Wi-Fi у публічних місцях серед вже підключених користувачів може бути хакер, який моніторить відвідувані сайти | При підключенні до таких мереж не проводити Інтернет-покупки та не заходити до онлайн-банкінгу |

*Закінчення табл. 2*

| 1 | 2 | 3 |
|---|---|---|
| Шахрайство з втраченими та викраденими картками | Фізична картка або втрачається, або викрадається та використовується іншими людьми для здійснення покупок | Блокування карти в Інтернет-банкінгу або на гарячій лінії. Попередньо можливе встановлення денних лімітів |
| Шахрайство з банкоматами (від англ. skimming) | Крадіжка даних картки за допомогою спеціального пристрою, що зчитує карту. Зловмисники копіюють всю інформацію з магнітної смуги карти (ім'я власника, номер картки, термін закінчення терміну її дії, CVV-код) | Установлення денних лімітів в особистому кабінеті. Перевірка банкомату на наявність сторонніх пристроїв. За наявності в банкоматі безконтактного модуля NFC – проводити зняття за допомогою PayPass або PayWave |

**Джерело:** авторська розробка.

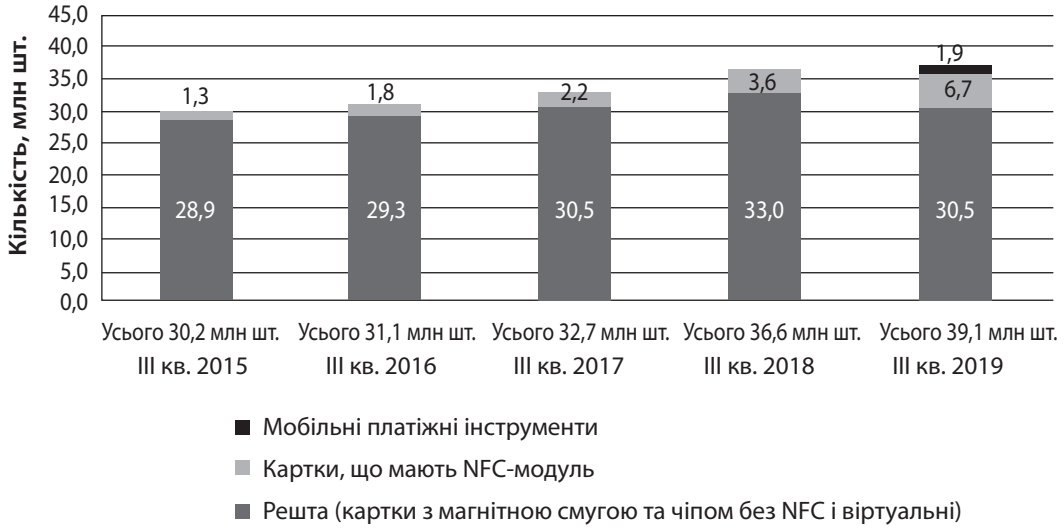


**Рис. 1. Активні електронні платіжні засоби за видами носіїв**

**Джерело:** складено за [13].

за три квартали 2019 р., то дослідження попередніх років буде за аналогічний період.

Згідно з даними рис. 1 активні платіжні картки складають 60% від загальної кількості карток, причому 22% активних платіжних карток є безконтактними та токенізованими (їх кількість за 9 місяців зросла майже на 70% – до 6,7 млн шт. і 1,9 млн шт. відповідно). Аналіз показав значне зростання кількості активних платіжних карток з наявністю NFC-модуля, майже у 2 рази порівняно з попереднім періодом.

Токенізація платіжних карток – це заміна реальних карткових даних, які є на пластиковій картці, на унікальні цифрові ідентифікатори, які можуть зберігатися на персональних пристроях і використовуються для здійснення операцій з використанням гаджетів з функцією NFC. Безготівкові операції з використанням безконтактних і токенізованих карток разом становили третину від загальної кількості та обсягу безготівкових операцій у торговельній мережі (33% та 32,8% відповідно).

Загальна кількість операцій (безготівкових та отримання готівки) з використанням платіжних карток, емітованих українськими банками, за 9 місяців 2019 р. становила 3651,7 млн шт., а їхній обсяг – 2582,7 млрд грн. Якщо порівняти з аналогічним періодом 2018 р., то кількість операцій зросла на 29%, а сума – на 27%. Розглянемо динаміку зростання частки безготівкових операцій за кількістю (*рис. 2*).

Дані рис. 2 демонструють стабільне зростання кількості безготівкових операцій за останні 5 років на 4–8% у середньому. Така позитивна динаміка означає забезпеченість вітчизняного ринку платіжними терміналами та популярність розрахунків у мережі Інтернет. Розглянемо розподіл безготівкових операцій з використанням платіжних карток (*табл. 3*).

Отже, популярність безконтактних операцій позитивно впливає на розширення безконтактної платіжної інфраструктури. Від початку 2019 р. мережа торговельних POS-терміналів в Україні зросла на 14,1% – до 318,4 тис. од., із них 89% торговельних POS-терміналів забезпечують можливість здійснення безконтактної оплати (станом на 1 січня 2019 р. – 79,4%).

За даними публікації Концепції розвитку цифрової економіки та суспільства України до 2020 року [15] та Стратегії розвитку фінансового сектора Украї-


**Рис. 2. Динаміка зростання частки кількості безготівкових операцій за I–III квартали 2015–2019 рр., %**

**Джерело:** складено за [13].

**Таблиця 3**

**Розподіл безготівкових операцій з використанням платіжних карток за III квартал 2019 р.**

| Тип операції | Обсяги операцій | | Кількість операцій | |
|---|---|---|---|---|
| | (млрд грн) | % | (млн шт.) | % |
| Переказ з картки на картку | 529,9 | 41,3 | 327 | 10,9 |
| Операції з оплати товарів/послуг у мережі Інтернет | 230,8 | 18,0 | 496,6 | 16,6 |
| Переказ коштів з карти на банківський рахунок у мережі Інтернет | 129 | 10,1 | 582,7 | 19,5 |
| Розрахунки з використанням платіжних терміналів | 367,7 | 28,7 | 1538,2 | 51,4 |
| Операції у пристроях самообслуговування | 25,1 | 2,0 | 47,2 | 1,6 |
| Усього | 1282,6 | 100,0 | 2991,7 | 100,0 |

**Джерело:** складено за [13].

ни до 2025 року [16], які створені за підтримки Національного банку України, Міністерства фінансів України, Національної комісії, що здійснює державне регулювання у сфері ринків фінансових послуг та Фонду гарантування вкладів фізичних осіб, запроваджено регулювання нових і сучасних напрямів у банківській діяльності, а саме:

- FinTech, InsurTech, WealthTech і платформ кредитування (Машинне навчання та Штучний інтелект будуть використовуватися в напрямах FinTech);
- упроваджено стандарти ЄС щодо директиви PSD2, що дає змогу підвищити конкурентоспроможність на фінансовому ринку;
- розроблено концепцію використання е-гривні на національному рівні;
- у частині SupTech та RegTech запроваджено більш легке, швидке й ефективне виконання регуляторних вимог учасниками фінансових ринків;
- систему BankID НБУ впроваджено в промислову експлуатацію та затверджено як один із інструментів ідентифікації для дистанційного відкриття рахунків фізичних осіб. Упровадження такої системи дало можливість дистанційного відкриття рахунків фізичним особам, а також збільшення кількість послуг, що може бути отримано за допомогою системи (державних, адміністративних і комерційних);
- з метою модернізації та вдосконалення системи електронних платежів вітчизняна банківська система перейшла до впровадження міжнародних стандартів обміну фінансовими повідомленнями на базі європейського стандарту IBAN (International Bank Account Number) – міжнародний номер банківського рахунку, який складається із 29 літерно-цифрових символів: коду країни, контрольного розряду, коду банку та номера рахунка [13];

- створено відкриті консолідовані реєстри, що поєднують інформацію з різних джерел. Такі реєстри широко використовуються гравцями фінансового ринку для ідентифікації клієнтів, автоматизації бізнес-процесів.

У 2019 р. за підтримки Національного банку України та міжнародної платіжної системи Visa Українська асоціація Fintech та інноваційних компаній провела дослідження серед Fintech-компаній та банків України щодо залучення їх до співпраці. У дослідженні взяли участь 110 респондентів. За даними дослідження, під час аналізу було зроблено розподіл Fintech-компаній, серед яких найбільшу частину займають організації, що спеціалізуються на проведенні платежів та переказів (19,4% від загальної кількості). До систем платіжного середовища також мають відношення мобільні гаманці – 11,2%, кібербезпека – 5,6%, персональні позики – 5,1% і цифрові та необанки – 4,1%.

З другої половини 2019 р., з метою захисту користувачів банківських платіжних карток, Альфа-банк Україна та Monobank почали випуск перших платіжних карт без реквізитів (відсутні номер карти, термін дії та CVV), пластик матиме лише ім'я та прізвище власника карти. Ідентифікаційна інформація для проведення платежів буде перенесена в мобільний додаток Інтернет-банкінгу відповідного банку.

Шахраям для здійснення протиправних операцій необхідні завжди конфіденційні дані клієнтів банку. Саме тому більшість зусиль здійснюється для того, щоб дізнатися номер карти, термін її дії та CVV-код. Знаючи ці реквізити, шахраї можуть використовувати карту для оплати товарів онлайн, де не потрібно підтвердження 3D Secure-коду. Тому так важливо зробити перенесення реквізитів картки з пластика в мобільний додаток. Найчастіше щоб отримати реквізити карти, клієнт повинен увійти в мобільний додаток свого банку. Більшість смартфонів самі по собі захищені паролями, сканерами відбитків пальця або системами розпізнавання осіб, що є додатковим захистом [17]. Безконтактне шахрайство становить найбільшу частку серед загальної кількості викрадення грошей з рахунків. Злочинці намагаються отримати конфіденційну інформацію, таку як імена користувачів, паролі та облікові дані платіжної картки. Потім викрадені дані про оплату використовуються для шахрайських транскордонних платежів.

Фішинг-атака стала одним із найпоширеніших фінансових злочинів за останні роки. З метою отримання фінансової інформації та даних користувача шахраї порушують безпеку банку та проводять широкий спектр незаконних дій. Розглянемо офіційну статистику втрат від шахрайства з картами в деяких країнах Європи, а також в Україні та Росії, у 2018 р. (*рис. 3*).

Інформація рис. 3 показує загальну вартість втрат від шахрайства з картами у 2017 і 2018 рр. по країнах. Згідно з даними статистики, Велика Британія і Франція понесли значно більші збитки від шахрайства з картками порівняно з будь-якими іншими країнами Європи.

У період між 2017 і 2018 рр. у Великій Британії збільшився збиток від шахрайства з картками на 18%, що склало приблизно 759 млн євро у 2018 р. Для порівняння: в Україні збитки за 2017–2018 рр. склали в середньому 2,2 млн євро. Шахрайство з картками включає в себе підробку карт із використанням скимінгу, через крадіжку або втрату картки, відсутність картки (CNP), втрату або крадіжку картки поштою, шахрайство з посвідченням особи та інші.

Посилене використання технологій і цифрових каналів зробило банківську індустрію більш сприйнятливою до кібератак. Нові правила щодо відкри-

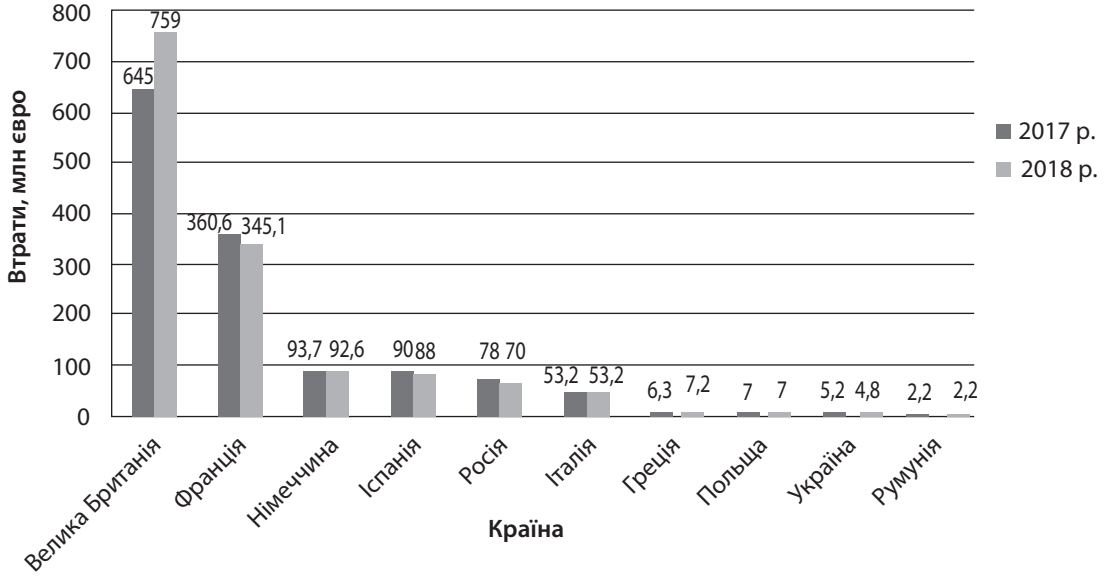


**Рис. 3. Загальна вартість втрат від шахрайства з картками по деяких країнах у 2018 р., млн євро**

**Джерело:** складено за даними [3; 12].

тих банківських операцій, які вимагають від банків обміну інформацією про клієнтів із сторонніми постачальниками, роблять галузь ще більш вразливою. Бажання споживачів отримати прості сервіси для користування та максимальний захист даних вимагатиме від банківських установ впровадження багатофакторної аутентифікації, захищених програм, цифрових підписів, біометрії та інших форм безпеки.

Втрати від шахрайства з картками в Інтернеті значно зросли. Після впровадження EMV (міжнародний стандарт для операцій по банківських картах з чіпом, який розроблений компаніями Europay, MasterCard і Visa) шахрайство з картками все більше переміщується до країн, де POS-термінали чи Інтернет-магазини ще не перейшли на EMV і SCA, та до транскордонного шахрайства з використанням компрометованих карт.

Найбільшими глобальними проблемами шахрайства з картками є:

- шахрайство з карткою без присутності (шахрайство з CNP);
- транскордонне шахрайство;
- підробка на картках, що не належать до EMV.

Європейський банківський орган (ЄБО) опублікував регуляторні технічні стандарти (РТС) [8], де визначено, що потрібно враховувати провайдерам платежів за допомогою аналізу ризиків у реальному часі, а саме:

- попередні схеми витрат замовника;
- історія платежів усіх клієнтів; місцезнаходження платника та одержувача платежу;
- інформацію про пристрій/програмне забезпечення замовника;
- сценарії шахрайства.

Всесвітньовідомі фінансові організації протидіють шахрайству картками таким чином:

- вкладають кошти у передові системи безпеки для захисту клієнтів, включаючи аналіз транзакцій у режимі реального часу та біометрику поведінки на пристроях;
- проводять сильну аутентифікацію клієнтів для підозрілих операцій з метою зменшення випадків шахрайства;
- займаються розробкою інструментів виявлення шахрайства, доступних для роздрібної торгівлі, таких як технологія 3D Secure, яка захищає покупки карт в Інтернеті;
- мають доступ до визначення скомпрометованих даних картки через розвідувальні центри;
- працюють з урядом і правоохоронними органами в спільній групі боротьби з шахрайством.

На даний момент Європейський банківський орган дозволяє постачальникам платіжних послуг не застосовувати строгу аутентифікацію клієнтів, коли платник ініціює транзакцію віддаленого електронного платежу, яка, як встановлено постачальником платіжних послуг, представляє низький рівень ризику відповідно до механізмами моніторингу транзакцій.

Розглянемо більш детально основні інструменти щодо забезпечення належного рівня фінансової безпеки банківського платіжного середовища.

*Відкритий банкінг* – це система, за допомогою якої банки відкривають інтерфейси програмування прикладних програм (API), дозволяючи третім сторонам отримувати доступ до фінансової інформації, необхідної для розробки нових додатків та послуг, та надаючи власникам рахунків більші можливості фінансової прозорості. Відкриті банківські послуги розвивають конкуренцію в банківській галузі, змушуючи суб'єктів господарювання або розширювати свої фінансові послуги, або співпрацювати з фінансовими технологіями.

*API* – це набір кодів і протоколів, які вирішують, як різні компоненти програмного забезпечення повинні взаємодіяти – вони по суті дозволяють різним програмам спілкуватися один з одним. Відповідно до звіту «Про монетизацію відкритого банкінгу» від Business Insider Intelligence [11], API використовувались для підключення розробників до платіжних мереж, а також для відображення платіжних даних на веб-сайті банку. API також необхідні для функціонування Baking-as-a-Service (BaaS) – ключового компонента відкритого банкінгу. BaaS – це комплексний процес, який з'єднує fintechs та інші треті сторони до банківських систем безпосередньо за допомогою API.

Завдяки *Third Party Provider* (*TPP*) – авторизованому постачальнику послуг, який використовує інтерфейси ASPSP, розроблені відповідно до вимог PSD2 для доступу до рахунків клієнта, відбувається надання інформації щодо наявності доступних коштів на рахунку.

*Strong Customer Authentication* (*SCA*) – це нова європейська нормативна вимога щодо зменшення шахрайства та підвищення онлайн-платежів. Щоб прийняти платежі та відповідати вимогам SCA, потрібно вбудувати додаткову аутентифікацію в потоці оформлення замовлення.

У даний час найпоширеніший спосіб аутентифікації оплати за допомогою онлайн-картки покладається на *3D Secure* – стандарт аутентифікації, який підтримує переважна більшість європейських карток. Застосування 3D Secure додає додатковий крок після оформлення замовлення: необхідно надати додаткову інформацію для здійснення платежу (наприклад, одноразовий код, надісланий на телефон, або аутентифікацію відбитків пальців через додаток для мобільного банкінгу).

*3D Secure 2* – нова версія протоколу аутентифікації, яка була впроваджена у 2019 р., – повинна стати основним методом аутентифікації платежів через Інтернет-картку та виконання нових вимог SCA. Ця нова версія представляє кращий досвід користувача,

який допоможе мінімізувати тертя, які аутентифікація додає до потоку оформлення замовлення. 3DS 2 дозволяє постачальникам платежів надсилати набагато більше даних аналізу ризику до банку клієнта, щоб вони могли використовувати це для розпізнавання клієнта та уникнення сильної аутентифікації клієнта.

Інші способи оплати на основі картки, такі як *Apple Pay* чи *Google Pay*, уже підтримують платіжні потоки із вбудованим шаром аутентифікації (біометричним чи паролем). Це може бути гарним способом для підприємств запропонувати безперешкодне оформлення каси, дотримуючись нових вимог.

Оскільки більшість Інтернет-продавців використовують 3DS лише для найризикованіших транзакцій, клієнти іноді бувають не готові отримати інформацію для проведення оплати та не можуть підтвердити платіж. Надсилання паролю часто стомлює та може займати деякий час – 26% клієнтів відмовляються від транзакцій через складний процес оформлення замовлення.

Згідно з даними від компанії з управління ризиками Ravelin [9], яка співпрацює з Booking.com, Glovo, EasyTaxi, Boohoo та багатьма іншими відомими компаніями, у 1 кварталі 2019 р. 22% платежів, відправлених у 3DS, втрачено – подальший аналіз виявив, що 91% платежів потребують для аутентифікації близько 5 секунд, але іноді вони можуть займати до 37 секунд.

3DS 2 пропонує більш гнучкі способи аутентифікації, що відповідають клієнту, такі як сканування обличчя та одноразові паролі. Знову ж таки, це все ще залежить від того, що пропонує банк власника картки. Продавець може налаштувати сторінку виклику, і 3D Secure 2 буде оптимізований для мобільних пристроїв за допомогою наборів розробки програмного забезпечення для iOS та Android.

Хоча 3D Secure 2 виглядає так, що це буде великим поліпшенням попередніх версій, є деякі ознаки того, що він все ж таки може викликати проблеми. 3DS 2 сильно залежатиме від способів аутентифікації мобільних телефонів для багатьох платежів, що все ще спричинить проблеми у клієнта, який не приносить свій телефон, або в районах із низьким рівнем сигналу. Аналіз платежів 3DS від компанії з управління ризиками Ravelin показав, що навіть банки з аутентифікацією на рівні 3DS 2, такі як аутентифікація на основі додатків та одноразові паролі, все ж втратили 19% платежів.

Отже, при виборі елементів системи безпеки необхідно враховувати вимоги законодавчих актів, а також порівнювати ризики з витратами. Безумовну гарантію того, що користувач дійсно є тим, за кого себе видає, забезпечує тільки біометрія, оскільки вона використовує невід'ємні атрибути на зразок частин тіла людини. Методи аутентифікації, засновані на вимірі біометричних параметрів людини, забезпечують майже 100% ідентифікацію, вирішуючи проблеми втрати паролів і особистих ідентифікаторів. Однак двофакторна (і багатофакторна) аутентифікація навряд чи зникне, адже два фактори завжди краще одного, і навіть біометрію краще підкріпити додатковим рівнем захисту.

Оскільки шахраїв можна поділити на тих, які націлені на приватних клієнтів банківських установ і на саму фінансову структуру, то, щоб уникнути ризику втрати грошей внаслідок кібератаки, необхідно дотримуватися простих правил користування програмним забезпеченням та електронними платіжними системами, які застосовуються в усьому світі (*табл. 4*).

Через те, що фінансова політика України орієнтована на міжнародні платіжні стандарти, то завдяки впровадженню ще у 2015 р. Payment Services Directive 2015/2366 – директиви Європейського Союзу про платіжні послуги на внутрішньому ринку – вітчизняна банківська система зазнала значних змін. Остаточний перехід до другої платіжної директиви ЄС PSD2 відбувся у вересні 2019 р. Директива вводить принципи відкритого банкінгу (Open Banking) та змінює процедуру аутентифікації клієнтів на основі сучасних цифрових можливостей

На сьогодні обов'язковими стають і нові технічні стандарти аутентифікації для прийому онлайн-платежів – Strong Customer Authentication (SCA, сувора аутентифікація) – вимоги, розроблені європейськими регуляторами, щоб знизити ймовірність шахрайства та зробити оплату в Інтернеті більш надійною. Проведення ідентифікації клієнта вітчизняними банками передбачено ст. 9 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [4].

За вимогами SCA аутентифікація повинна включати хоча б два з трьох компонентів (рекомендовано – три):

1) те, що користувач знає: наприклад, пароль або пін-код;

2) те, чим він володіє: телефон, карта, апаратний токен;

3) те, що є унікальною відмінністю клієнта: розпізнавання відбитка пальця або обличчя (фей сайди).

Позитивний вплив Open Banking на український ринок відчуватиметься в такому:

1. *Більш оперативне впровадження інновацій.* Створення єдиної системи стимулюватиме FinTech створювати все нові продукти під різні потреби користувача, не прив'язуючи їх при цьому до конкретного банку.

2. *Персоналізація банківських продуктів під клієнта.* Відкритий доступ третім компаніям до інформації дає можливість фінансовим установам краще розуміти своїх клієнтів, у т. ч. і потенційних, створюючи для них «ідеальний» продукт.

**Таблиця 4**

**Способи захисту конфіденційної інформації для банківської установи та її клієнтів**

| Для приватних клієнтів банку: | Для банківської установи: |
|---|---|
| 1) не переходити за підозрілими посиланнями, вони здебільшого розроблені для завантаження зловмисного програмного забезпечення на пристрій;<br>2) не відкривати та не зберігати незнайомі файли на своєму пристрої;<br>3) бути обережними під час використання загальнодоступних мереж Wi-Fi, оскільки вони можуть бути небезпечними та ненадійними;<br>4) якщо сайт здається підозрілим або незнайомим, не потрібно вводити дані своєї платіжної картки та не робити покупки;<br>5) завантажувати додатки Інтернет-банкінгу з Google Play Market або iOS App Store;<br>6) використовувати для платежів лише веб-сайти, які починаються з HTTPS: //, вони мають систему захисту 3D Secure;<br>7) ніколи нікому не розголошувати свої паролі, CVV чи PIN-коди – навіть родичам і друзям | 1) інвестувати в регулярні навчання з інформованості про кібербезпеку для працівників, щоб навчити їх не натискати на посилання або відкривати вкладення, отримані з підозрілих джерел;<br>2) регулярно проводити тестові фішинг-атаки, щоб переконатися, що працівники знають, як розрізняти фішинг-листи;<br>3) при використанні хмарних сервісів електронної пошти необхідно переконатися, що є встановлено спеціальний захист від спам-атак електронної пошти;<br>4) переконатися, що всі рівні корпоративного програмного забезпечення надійно захищені – від основних центрів обробки даних до спеціалізованих систем (наприклад, банкоматів);<br>5) для ATM і POS використовувати рішення, розроблені спеціально для цих систем, які захищають пристрої навіть зі слабким або застарілим обладнанням |

**Джерело:** складено на основі [10].

3. *Захищеність клієнтів і банків*. При отриманні єдиного каналу доступу до всіх рахунків знизиться ризик шахрайства, однак потрібно враховувати, що такий «відкритий банківський простір» має поліпшити й інструменти безпеки: аутентифікацію, авторизацію тощо.

4. *Спрощення процедури отримання ліцензії.* Відкритий API дозволить фінансовим платформам у режимі онлайн проводити платежі, випускати картки, управляти цифровими гаманцями без відповідної ліцензії або партнерства з офлайн-банками.

5. *Перехід від конкуренції між банками і FinTech до співпраці.* Випуск додатків і платформ для банків необхідно буде робити розробникам FinTech, які будуть конкурувати між собою та створювати продукт на більш вигідних умовах, що, своєю чергою, дозволить банкам заощадити на особистому IT-підрозділі.

6. *Здешевлення банківських продуктів для клієнта*. Відкрита конкуренція стимулюватиме установи знижувати комісії, оптимізувати швидкість обробки транзакцій та інше.

7. *Доступність банківських продуктів.* Сьогодні лише 48% українців повноцінно використовують всі можливості банківських продуктів. Створення відкритого банкінгу дозволить навіть у найвіддаленіших регіонах користуватися банківськими продуктами на рівні з жителями столиць.

## ВИСНОВКИ

Отже, застосування в банківському платіжному середовищі сучасних цифрових технологій потребує від комерційних банків особливу увагу звертати на фінансову безпеку задля збереження як клієнтів, так і фінансової стабільності самої установи.

З'ясовано, що основним видом шахрайства в банківській сфері є шахрайство з платіжними картками. При цьому безконтактне шахрайство становить найбільшу частку серед загальної кількості викрадення грошей з рахунків. Також було визначено способи щодо протидії шахрайству з картками. Отже, для забезпечення фінансової безпеки банківського платіжного середовища банківським установам необхідно запроваджувати сучасний інструментарій для аутентифікації клієнтів та своєчасно проводити роз'яснювальну роботу щодо протидії шахрайству серед споживачів фінансових послуг і своїх працівників.

Таким чином, підтримка належного рівня фінансової безпеки банківського платіжного середовища України вимагає застосування комплексу заходів як на національному рівні (удосконалення законодавства, банківського нагляду), так і на рівні окремих фінансових установ (використання сучасних технологій, побудова ефективно діючих систем інформаційної безпеки, роз'яснювальна робота тощо). ■

## ЛІТЕРАТУРА

1. Барановський О. І. Банківська безпека: проблема виміру. *Економіка і прогнозування*. 2006. № 1. С. 7–25. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/19797/01-Baranovskyi.pdf?sequence=1
2. Голобородько Ю. О. Теоретичні підходи до розкриття суті та складових фінансової безпеки банківських установ. *Науковий вісник НЛТУ України*. 2012. Вип. 22.12. С. 194–198. URL: https://nv.nltu.edu.ua/Archive/2012/22_12/194_Gol.pdf
3. Total value of card fraud losses in Europe in 2018, by country. URL: https://www.statista.com/statis-

tics/911873/value-of-losses-to-card-fraud-in-europe-by-country/
4. Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» від 14.10.2014 р. № 1702-VII. URL: https://zakon.rada.gov.ua/laws/show/1702-18
5. Зубок М. І. Безпека банківської діяльності : навч. посіб. Київ : КНЕУ, 2002. 190 с.
6. Ільчук В. П., Садчикова І. В., Савченко Т. В. Основні тенденції розвитку ринку платіжних карток в Україні. *Збірник наукових праць Державного економіко-технологічного університету транспорту. Серія «Економіка і управління»*. 2016. Вип. 36. С. 187–198.
7. Коваленко В. В. Філософія безпеки банків в умовах структурних дисбалансів економіки України. *Економічний форум*. 2016. № 1. С. 256–262.
8. Regulatory Technical Standards on Business Reore ganisation Plans / European Banking Authority. URL: https://eba.europa.eu/regulation-and-policy/recovery-and-resolution/regulatory-technical-standards-on-business-reorganisation-plans
9. Ravelin data reveals one in five payments are lost through 3D Secure. URL: https://www.ravelin.com/blog/one-fifth-of-payments-sent-to-3d-secure-are-lost
10. Financial Cyberthreats in 2018 / kaspersky. March, 7. 2019. URL: https://securelist.com/financial-cyberthreats-in-2018/89788/
11. Business Insider Intelligence. URL: https://www.businessinsider.com/intelligence
12. UK Finance. URL: https://www.ukfinance.org.uk/
13. Національний банк України : офіційний сайт. URL: https://bank.gov.ua
14. Методичні рекомендації щодо розрахунку рівня економічної безпеки України : затв. Наказом Міністерства економічного розвитку і торгівлі України від 29.10.2013 р. № 1277. URL: https://ips.ligazakon.net/document/ME131588
15. Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації» від 17 січня 2018 р. № 67-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-р
16. Стратегія розвитку фінансового сектору України до 2025 року. URL: https://bank.gov.ua/admin_uploads/article/Strategy_FS_2025.pdf?v=4
17. Чому карта без номера найбезпечніша / Мінфін. 22.11.2019 р. URL: https://minfin.com.ua/ua/2019/11/22/39799330/

**REFERENCES**

Baranovskyi, O. I. "Bankivska bezpeka: problema vymiru" [Banking Security: a Problem of Measurement]. Ekonomika i prohnozuvannia. 2006. http://dspace.nbuv.gov.ua/bitstream/handle/123456789/19797/01-Baranovskyi.pdf?sequence=1

Business Insider Intelligence. https://www.businessinsider.com/intelligence

"Chomu karta bez nomera naibezpechnisha" [Why a Card without a Number is the Safest]. Minfin. November, 22. 2019. https://minfin.com.ua/ua/2019/11/22/39799330/

"Financial Cyberthreats in 2018". kaspersky. March, 7. 2019. https://securelist.com/financial-cyberthreats-in-2018/89788/

Holoborodko, Yu. O. "Teoretychni pidkhody do rozkryttia suti ta skladovykh finansovoi bezpeky bankivskykh ustanov" [Theoretical Approaches to the Disclosure of the Essence and Components of Financial Security of Banking Institutions]. Naukovyi visnyk NLTU Ukrainy. 2012. https://nv.nltu.edu.ua/Archive/2012/22_12/194_Gol.pdf

Ilchuk, V. P., Sadchykova, I. V., and Savchenko, T. V. "Osnovni tendentsii rozvytku rynku platizhnykh kartok v Ukraini" [The Key Trends in the Payment Card Market in Ukraine]. *Zbirnyk naukovykh prats Derzhavnoho ekonomiko-tekhnolohichnoho universytetu transportu. Seriia «Ekonomika i upravlinnia»*, no. 36 (2016): 187-198.

Kovalenko, V. V. "Filosofiia bezpeky bankiv v umovakh strukturnykh dysbalansiv ekonomiky Ukrainy" [Philosophy of Safety Bank in a Structural Imbalance Ukraine Economy]. *Ekonomichnyi forum*, no. 1 (2016): 256-262.

[Legal Act of Ukraine] (2013). https://ips.ligazakon.net/document/ME131588

[Legal Act of Ukraine] (2014). https://zakon.rada.gov.ua/laws/show/1702-18

[Legal Act of Ukraine] (2018). https://zakon.rada.gov.ua/laws/show/67-2018-p

Natsionalnyi bank Ukrainy : ofitsiinyi sait. https://bank.gov.ua

"Ravelin data reveals one in five payments are lost through 3D Secure". https://www.ravelin.com/blog/one-fifth-of-payments-sent-to-3d-secure-are-lost

"Regulatory Technical Standards on Business Reorganisation Plans". European Banking Authority. https://eba.europa.eu/regulation-and-policy/recovery-and-resolution/regulatory-technical-standards-on-business-reorganisation-plans

"Stratehiia rozvytku finansovoho sektoru Ukrainy do 2025 roku" [Strategy for the Development of the Financial Sector of Ukraine until 2025]. https://bank.gov.ua/admin_uploads/article/Strategy_FS_2025.pdf?v=4

"Total value of card fraud losses in Europe in 2018, by country". https://www.statista.com/statistics/911873/value-of-losses-to-card-fraud-in-europe-by-country/

UK Finance. https://www.ukfinance.org.uk/

Zubok, M. I. *Bezpeka bankivskoi diialnosti* [Banking Security]. Kyiv: KNEU, 2002.