



¹Національний університет водного господарства та природокористування, м. Рівне

²ВСП «Рівненський фаховий технічний коледж НУВГП», м. Рівне

РОЗВИТОК ФІНАНСОВИХ ТЕХНОЛОГІЙ БАНКІВСЬКОЇ СФЕРИ: ЗАГРОЗИ ТА ПЕРСПЕКТИВИ

У статті проведено аналіз сучасного стану та визначено перспективні напрями розвитку фінансових технологій у банківській сфері України. Визначено, що активно в даний час розвиваються технології пов'язані із платіжною інфраструктурою, штучним інтелектом, хмарними технологіями і забезпеченням реалізації концепції відкритого банкінгу. Виокремлено основні загрози розвитку фінансових технологій банківської сфери в Україні. Надано пропозиції щодо протидії потенційним фінансовим ризикам. Значну увагу приділено засобам протидії кіберзагрозам у банківській сфері. Обґрунтовано доцільність створення регуляторної «пісочниці», розкрито її суть та функції.

Ключові слова: фінтех; інноваційні банківські продукти; послуги та сервіси; платіжні технології; хмарні технології; регуляторна «пісочниця»; відкритий банкінг; загрози фінтех.

Постановка проблеми. Із початком повномасштабного вторгнення банківський сектор України зіткнувся із найскладнішими викликами за всю свою історію. При цьому, фінтех-інновації стали невід'ємною складовою підтримки фінансової стабільності сектору насамперед завдяки можливості здійснення безготівкових розрахунків. Нині розвиток сучасних технологій не лише не сповільнився, а й навпаки – пришвидшився.

Запровадження фінансових технологій дозволяє протистояти викликам воєнного часу, сприяє прозорості фінансової системи, фінансовій інклюзії населення, а також залученню інвестицій та акумуляції коштів для відновлення України. Разом з тим, підвищення рівня проникнення фінансових технологій створює додаткові загрози, як банківському сектору, так і фінансовій системі в цілому. Усе це обумовлює актуальність дослідження перспектив впровадження сучасних банківських технологій в Україні.

Аналіз останніх досліджень і публікацій. Вивченням теоретичних питань та практичних аспектів становлення, розвитку та функціонування цифрових фінансових технологій займалися такі українські та зарубіжні науковці як А. Броддаса, С. Волосович, Л. Жердецька, Д. Городинський., Л. Дудинець, М. Диба., Є. Осадчий, В. Коваленко, Р. Мертон, М. Міллер, А. Семенов, І. Троц, М. Тарасюк та інші. Їхні дослідження створили надійний теоретичний фундамент для розуміння та розв'язання проблем, що виникають в процесі розвитку інноваційних фінансових технологій у банківській сфері. Проте недостатньо дослідженим, на нашу думку, є потенційні загрози, обумовлені повномасштабним вторгненням.

Постановка завдання. Метою статті є узагальнення теоретичних положень та формування практичних рекомендацій щодо розвитку фінансових технологій у банківському сегменті та пошуку шляхів протидії загрозам та потенційним фінансовим ризикам.

Виклад основного матеріалу. Серед основних передумов розвитку фінансових технологій в глобальному банківському бізнесі виділяють [1]: втрату довіри до традиційного банківського сектору під час світової фінансової кризи; поширення мобільного інтернету та зростання популярності соціальних мереж; успіх технічних компаній в інших секторах економіки; підвищення рівня очікування від послуг, що надаються та прагнення до інновацій.

Частково віддзеркалюючи світові інноваційні процеси, вітчизняний ринок фінтеху активно впроваджував у банківському секторі технології штучного інтелекту, блокчейн, цифрового банкінгу тощо. Завдяки цьому ще до повномасштабного вторгнення вітчизняний банківський сектор мав досить високий рівень діджиталізації. Поштовхом для його розвитку стали ухвалені у 2020 році Стратегія розвитку фінтеху в Україні до 2025 року, а також зміни до законодавства України та нормативно-правових актів НБУ, які сприяли розвитку віддаленої ідентифікації та верифікації клієнтів фінансових установ, зокрема з використанням Системи BankID НБУ, надання можливості здійснення миттєвих платежів із рахунку на рахунок у СЕП у форматі 24/7; посилення регуляторного периметру у сфері кібербезпеки тощо.

Саме завдяки значним обсягам дистанційних фінансових послуг у попередній період, упродовж 2022 року українці продовжували використовувати платіжні картки для безготівкових розрахунків. Незважаючи на воєнні дії, ракетний терор та обмеження електропостачання, динаміка операцій з платіжними картками, емітованими українськими банками, у травні – грудні 2022 року була



позитивною. Кількість операцій з використанням платіжних карток, емітованих українськими банками, за травень – грудень 2022 року становила 5 599,2 млн, а їхня загальна сума – 5 058,2 млрд грн. Це на 1,4% більше за кількістю та на 40,5% за сумою, ніж за аналогічний період довоєнного 2021 року [2].

Через війну, зниження активності бізнесу та тимчасову окупацію окремих територій платіжна інфраструктура зазнала скорочення порівняно із довоєнним часом. Кількість платіжних терміналів у торговельній та сервісній мережі порівняно з січнем 2022 року була меншою на 6,5% та становила 359,2 тис., з них 348,1 тис. (96,9%) – безконтактні термінали. Протягом травня – грудня 2022 року спостерігалось поступове зростання кількості таких пристроїв, проте рівня довоєнного січня поки не досягнуто [2].

Розвитку платіжної інфраструктури у 2022 році активно сприяло запровадження технології Tap to Phone, які запустили Visa спільно із ПриватБанком, Ощадбанком, Raiffeisen Bank та Kyivstar. Дане рішення дозволяє замінити платіжний термінал на смартфон із NFC-чіпом. Особливо активно використовують цю технологію малий бізнес та підприємці, адже вона дозволяє швидко та безпечно приймати безконтактні платежі в один дотик з фіскалізацією, обліком складу, цифровою вітриною, сервісами чайових та іншими можливостями для торгівлі.

Дану технологію було також інтегровано у Telegram-месенджер у вигляді чат-бота «Онлайн Каса», вона дозволяє створювати фіскальні та нефіскальні чеки, приймати оплату банківськими картами за допомогою телефону, швидко та просто зареєструвати ПРРО в податковій, формувати звіти про реалізацію товарів та послуг.

Ще однією технологією, яка набула особливої актуальності сьогодні, є використання хмарних технологій (Cloud technologies) – це набір інформаційних технологій, які дозволяють доступ до обчислювальних ресурсів (таких як обробка даних, зберігання, мережеві ресурси) через Інтернет з використанням віртуалізованого середовища. Замість того, щоб мати власні фізичні сервери та інфраструктуру, користувачі можуть отримати доступ до цих ресурсів через хмарні платформи. У березні 2022 року НБУ дозволив банкам зберігати та обробляти дані із використанням хмарних технологій [3].

Нині компанії активно використовують хмарні технології для покращення ефективності своєї діяльності та надання кращих послуг клієнтам. Основними перевагами використання хмарних технологій є:

- можливість збереження даних та використання інфраструктури: фінансові компанії переносять свої дані та системи у

хмару, що дозволяє їм знизити витрати на обладнання та підтримку, а також забезпечити більшу надійність інфраструктури, швидкий доступ до фінансових послуг у будь-який час та з будь-якого пристрою;

- аналітичні можливості та обробка даних: провайдери надають компаніям можливість використовувати потужні аналітичні інструменти для обробки великих обсягів даних. Це допомагає здійснювати краще оцінювати ризики та вдосконалювати стратегію прийняття рішень;

- кібербезпека: провайдери часто надають комплексні рішення з кібербезпеки, які допомагають компаніям захистити свої системи та дані від кібератак. Вони забезпечують моніторинг, виявлення вторгнень, шифрування даних та інші заходи безпеки.

Приватбанк першим переніс дата-центри до європейських провайдерів хмарних технологій. В цілому, за 45 днів у хмарі було перенесено 3500 серверів, понад 270 застосунків та понад 4 петабайт клієнтських даних і транзакцій. Це дозволило мінімізувати ризики активних військових дій, відсутності світла та зв'язку, захистити дані від кібератак та забезпечити стабільну роботу фінустанови.

Реалізація концепції відкритого банкінгу, яка має запрацювати за три роки відкриє ще більше можливостей для розвитку фінансових технологій. Сьогодні НБУ працює над розробкою єдиних стандартів відкритих API, які будуть зрозумілими, зручними, прийнятними для всіх, а також захищеними, тобто гарантуватимуть споживачам безпеку, захист даних і транзакцій. Відкритий банкінг (Open Banking) – це концепція, що передбачає доступ до банківських даних і функціоналу шляхом застосування стандартів відкритих програмних інтерфейсів (API). Вона створює можливості для обміну даними між різними банківськими і небанківськими установами та фінтех-компаніями. Це дозволяє реалізувати інноваційні фінансові продукти та послуги, такі як персоналізовані розрахунки, бюджетування, порівняння фінансових умов, розподіл ризиків тощо.

Через відкритий банкінг API-інтерфейси використовуються для передачі команд стороннім постачальникам і вони необхідні для функціонування Banking-as-a-Service (BaaS) – ключового компонента відкритого банкінгу. BaaS – це наскрізний процес, який пов'язує фінтех-компанії та інші компанії з системами банків безпосередньо за допомогою API-інтерфейсів [4]. Загалом BaaS дозволяє компаніям без банківської ліцензії використовувати банківські послуги, такі як відкриття рахунків, обробка платежів, кредитування, зберігання коштів тощо, без необхідності розробляти власну інфраструктуру або отримувати банківську ліцензію. Замість цього вони можуть



підключитися до вже існуючих банківських систем через відкриті API.

Як очікується, перевагу від відкриття API насамперед відчують споживачі фінансових послуг, які зможуть отримати більш якісні та персоналізовані послуги, що відповідають їх потребам, або ж нижчі тарифи на них. Крім того, співпраця банків і фінтех-компаній дозволить не лише, якісно підвищити рівень сервісу, швидкість трансакцій, знизити їх вартість, а й сприяти появі нових стартапів, інноваційних продуктів та послуг. Відкритий банкінг також стимулюватиме конкуренцію та розвиток фінтех-компаній, оскільки дозволяє їм використовувати банківські дані для розробки нових інноваційних рішень. Передбачається, що завдяки відкриттю API прискориться введення на ринок нових фінансових продуктів та послуг, зменшаться витрати на розробку та підтримку власної банківської інфраструктури, розшириться доступ до більш широкого спектру банківських операцій та послуг. Банки при цьому, зберігають лояльність клієнтів та одночасно отримують нові джерела надходжень завдяки розширенню обсягів послуг та надання послуг через зовнішніх партнерів.

У цілому фінансові технології відкривають нові можливості для інновацій, конкуренції та покращення фінансових послуг, прискорюючи цифрову трансформацію галузі банківських послуг та сприяючи зручності та персоналізації для клієнтів, однак важливо враховувати виклики та загрози, пов'язані з запровадженням фінансових технологій (рисунок).



Рисунок. Основні загрози розвитку фінансових технологій банківської сфери в Україні

Під час війни фізичне руйнування інфраструктури, відсутність

світла та зв'язку є однією з ключових загроз функціонуванню банківського сегменту. Частково нівелювати таку загрозу може використання хмарних технологій. Додатково для надання банківських послуг навіть під час блекауту було розпочато ініціативу POWER BANKING. Це об'єднана за ініціативи НБУ мережа із понад 2 300 відділень банків України, забезпечених альтернативними джерелами енергії та резервними каналами зв'язку, посиленою інкасацією готівки та додатковим персоналом.

Створення спільної банківської мережі виявилось унікальним прикладом консолідації та партнерства українських банків, які обрали співпрацю та щоденну координацію замість конкуренції. Це сприяє покращенню комунікації між Національним банком та комерційним банківським сектором, що стало одним із ключових факторів для зміцнення монетарної трансмісії, впровадження нового операційного дизайну монетарної політики та збільшення привабливості гривневих депозитів.

Як бачимо, фінансові технології активно розвиваються в Україні, проте із зростанням кількості віддалених операцій та токенизованих карт, зростає і необхідність захисту даних від витоку, пошкодження інформації та зовнішніх атак.

Використання хмарних технологій для фінансових трансакцій та зберігання персональних даних створює додаткові загрози інформаційній безпеці. Основними ризиками є можливість витоку або крадіжки інформації через навмисне перехоплення даних зловмисниками з мережі постачальника хмарних послуг. Крім того, існує загроза втрати контролю над базами даних та додатками, яка може бути спричинена діями інсайдерів або несанкціонованим доступом до системи. Залежність від якості інтернет-зв'язку також може створювати проблеми користувачам, оскільки відсутність доступу до мережі може призвести до неможливості взаємодії з хмарними сервісами.

Війна суттєво посилила рівень кіберзагроз. За даними НБУ, у 2021 році висока активність хакерських груп була націлена на викрадення даних (Info Stealers), а в 2022 році – на фінансове шахрайство та викрадення коштів. У 2023 році цей тренд зберігається. Варто відзначити, що крім банків, увагу кіберзлочинців привернули також компанії, що займаються розробкою програмного забезпечення для банків. При цьому, лівова частка злочинів – 86% у минулому році відбувалася у мережі Інтернет, тоді як лише 14% – через фізичні пристрої такі як банкомати чи торговельну мережу. Що стосується суми збитків від незаконних дій, то 94% припадає на



мережу Інтернет, 4% – на торговельну мережу і лише 2% – на банкомати [5].

Для поєднання та координації зусиль у сфері забезпечення кібербезпеки та кіберзахисту в банківському та фінансовому секторах України у 2017 році було створено Центр кіберзахисту Національного банку України. З 2018 року у його складі функціонує команда реагування на кіберінциденти в банківській системі (CSIRT-NBU). На початку 2023 року Національний банк України (НБУ) спільно з Національним Координаційним Центром Кібербезпеки при Раді національної безпеки і оборони України розпочали проєкт з протидії фішингу. Вже близько 400 провайдерів в Україні (з них найбільші 10 провайдерів покривають понад 85% користувачів) долучилися до цього проєкту. Основна мета полягає в тому, щоб не дати користувачам переходити на фішингові сайти та перенаправляти їх на сторінку з попередженням про те, що цей сайт використовується зловмисниками. Завдяки цьому проєкту вдалося запобігти понад 2 мільйонам переходів громадян на шахрайські ресурси. В 2022 році НБУ виявив понад 4500 фішингових ресурсів. За період з початку 2023 року і до сьогодні вже виявлено понад 11 000 схожих шахрайських доменів, приблизно по 100 ресурсів на день. Зазначимо, що близько двох третин зі всіх виявлених фішингових сайтів (68%) мають походження з Росії [5].

Для підвищення безпеки під час використання віддалених фінансових технологій і захисту від кіберзагроз, на нашу думку, необхідно вживати наступних заходів.

Насамперед варто поширювати практику багатофакторної автентифікації (MFA) для кожного користувача, що дозволить забезпечити додатковий рівень захисту. Класична комбінація імені користувача та пароля вже не є достатньою для надійного захисту облікового запису. MFA використовує додаткові способи аутентифікації, такі як фізичний пристрій (наприклад, мобільний телефон) або біометричні дані (відбиток пальця, розпізнавання обличчя), для підтвердження ідентифікації користувача. Це означає, що навіть якщо зловмисник отримає доступ до імені користувача та пароля, без додаткового фактора аутентифікації він не зможе проникнути в систему. MFA є відносно недорогим і водночас ефективним засобом захисту, який значно зменшує ризик несанкціонованого доступу до даних та програм.

Для підвищення рівня фінансової безпеки важливим є також управління доступом різних груп користувачів. Встановлення відповідних рівнів авторизації гарантує, що кожен співробітник

матиме можливість переглядати або маніпулювати лише тими програмами та даними, які є необхідними для виконання його робочих обов'язків. Такий підхід дозволяє забезпечити принцип найменшого привілею, де користувачі отримують доступ лише до необхідного мінімуму даних та програм для виконання своїх робочих обов'язків. Це допомагає запобігти несанкціонованому доступу до чутливої інформації та зменшує ризик витоку даних чи зловживання повноваженнями.

Одним з найбільш ефективних способів протидії шахрайству та кіберзлочинам, на нашу думку, є інформування та навчання. Насамперед, інформування та навчання дозволяє запобігти тому, щоб співробітники стали жертвами цих шахраїв і скомпрометували конфіденційні дані компанії чи банку. Фінустанови повинні регулярно проводити навчання персоналу з метою підвищення кваліфікації та практичних навичок працівників банків у сфері кіберзахисту інформаційних систем. Це дозволить підвищити кіберстійкість об'єктів критичної інфраструктури фінансової системи та забезпечити стабільну роботу фінансових технологій банківської системи.

Крім того, підвищення фінансової грамотності та поінформованості населення про фінансові ризики і методи шахрайства сприятиме захисту власних фінансових активів та особистої інформації. Саме завдяки широкому інформуванню можна уникнути соціально-інженерних методів шахрайства, таких як фішинг, підробка вебсайтів і шпигунство в соціальних мережах. Зрештою, це дозволить людям ухвалювати раціональні фінансові рішення, вдало застосовувати фінансові технології, уникати підозрілих фінансових схем та маніпуляцій, забезпечувати стабільність фінансового стану і покращувати якість життя.

Зважаючи на інноваційність фінансових технологій, які впроваджуються у банківському сегменті, загрозою є також відсутність досвіду функціонування нового продукту, а відтак і регуляторних рамок. Саме для продуктів, для яких не існує аналогів на ринку, прийнято створювати регуляторні платформи – так звані «пісочниці». В межах такої спеціалізованої платформи відбуватиметься тестування інноваційних продуктів, послуг, технологій та інструментів та одночасна розробка законодавства, що регулюватиме виведення продукту на ринок.

Національний банк України має наміри запустити регуляторну «пісочницю» у 2023 році [6]. Ця платформа матиме три основні функції. По-перше, вона створить можливість взаємодії з ринком для всіх бажаючих впровадити нові інноваційні продукти та сервіси з



метою поліпшення життя клієнтів. По-друге, вона надасть спеціальний правовий режим для тестування фінансових і платіжних компаній, які бажають запропонувати продукти, що ще не прописані в законодавстві. По-третє, ця регуляторна «пісочниця» допоможе покращити регуляторну функцію Національного банку, дозволяючи швидко вносити зміни у регуляції на основі отриманого досвіду та вимог учасників ринку.

Регуляторна платформа, що створюється, забезпечить авторизованим надавачам фінансових та платіжних послуг можливість тестувати нові фінансові та платіжні продукти у реальних ринкових умовах в обмеженому середовищі з встановленими обмеженнями та квотами, із наглядом регулятора. Основне завдання платформи – сприяти розвитку фінтеху та інноваційних продуктів на фінансових та платіжних ринках. Це також сприятиме підвищенню конкуренції, якості фінансових та платіжних послуг, а також зближенню регулятора та учасників ринку для вдосконалення регулювання фінтех-сфери [6].

Висновки. Загалом зростаюча кількість фінансових технологій в банківській сфері відкриває нові перспективи для клієнтів, забезпечуючи їм зручніші, швидші та доступніші фінансові послуги. Інноваційні технології, такі як мобільні платежі, онлайн-банкінг та електронні гроші, дозволяють клієнтам здійснювати фінансові операції без необхідності відвідувати фізичні банківські відділення, що є особливо актуальним у період активних бойових дій.

Як показав проведений аналіз, у період війни банківські установи продовжують імплементацію новітніх технологій, що дозволяє суттєво покращити доступ до фінансових послуг та забезпечити збереження фінансової стабільності та надійності банківської системи. Нині основні зусилля фінустанов спрямовані на розвиток платіжної інфраструктури, інтеграції можливостей штучного інтелекту, використання хмарних технологій та забезпеченні реалізації концепції відкритого банкінгу.

Водночас варто наголосити, що зростаюча залежність від технологій може створити ризики системних збоїв або вразливостей, які можуть суттєво вплинути на фінансову стабільність та довіру до банківської системи особливо у воєнний період. Крім того, розвиток фінансових технологій також приносить загрози, пов'язані з кібербезпекою. Зростаюча кількість кібератак на банки та платіжні системи є частиною гібридної війни та посилює необхідність в кіберзахисті і застосуванні нових методів аутентифікації, шифрування та моніторингу для запобігання кіберзлочинності.

Регуляторні «пісочниці» створюють сприятливе середовище для інновацій та подальшого розвитку фінтех-послуг у банківській сфері, формуючи тим самим передумови для повоєнного відновлення України. Вони дозволяють фінтех-компаніям перевіряти свої ідеї та продукти в контрольованому середовищі, знижуючи регуляторні обмеження та витрати. Такий підхід сприяє створенню інноваційних рішень, покращує конкуренцію на ринку та сприяє розвитку фінансової технологічної сфери.

Таким чином, розвиток фінансових технологій в банківській сфері є необхідним і невід'ємним процесом у сучасному світі, який набуває ще більшої актуальності у період воєнного конфлікту. Ці технології можуть стати як загрозою, так і перспективою для фінансової стабільності та функціонування банківської системи.

1. Наконечна О., Михайлик О. Fintech в банківському бізнесі: особливості розвитку та потенційні можливості. *Підприємництво та інновації*. 2022. № 23. С. 108–119. URL: <https://doi.org/10.37320/2415-3583/23.19>. (дата звернення: 22.05.2023).
2. Воєнний рік: безготівкові операції – у пріоритеті в українців: Новини НБУ. URL: <https://bank.gov.ua/ua/news/all/voyenniy-rik-bezgotivkovi-operatsiyi--u-prioriteti-v-ukrayintsiv>. (дата звернення: 22.05.2023).
3. Про використання банками хмарних послуг в умовах воєнного стану в Україні : Постанова Правління Національного банку України від 08 березня 2022 року № 42. URL: https://bank.gov.ua/ua/legislation/Resolution_08032022_42. (дата звернення: 22.05.2023).
4. Береславська О. І., Татяніна С. М. Відкритий банкінг як елемент розвитку фінансово-кредитних відносин в Україні. *Фінансова система країни: тенденції та перспективи розвитку* : матеріали ІХ Міжнар. наук.-практ. інт.-конф. (м. Острог, 21 жовт. 2022 р.). Острог : Видавництво Національного університету «Острозька академія», 2022. С. 17–20.
5. Шабан О. Фінансове шахрайство. Як протидіяти кібершахрайству у фінансовому секторі. URL: <https://delo.ua/opinions/finansove-saxraistvo-yak-protidiyati-kibersaxraistvu-u-finansovomu-sektori-418081/>. (дата звернення: 22.05.2023).
6. Про затвердження Положення про регуляторну платформу для тестування послуг, технологій та інструментів на ринках фінансових послуг, платіжному ринку, заснованих на інноваційних технологіях: Правління Національного банку України ухвалило 30 березня 2023 року постановою № 39. URL: https://bank.gov.ua/ua/legislation/Resolution_30032023_39 (дата звернення: 22.05.2023).

REFERENCES:

1. Nakonechna O., Mykhailyk O. Fintech v bankivskomu biznesi: osoblyvosti rozvytku ta potentsiini mozhlyvosti. *Pidpryiemnytstvo ta innovatsii*. 2022. № 23. S. 108–119. URL: <https://doi.org/10.37320/2415-3583/23.19>. (data zvernennia: 22.05.2023).
2. Voiennyi rik: bezgotivkovi operatsii – u prioryteti v ukraintsiv: Novyny NBU. URL: <https://bank.gov.ua/ua/news/all/voyenniy-rik-bezgotivkovi-operatsiyi--u-prioriteti-v-ukrayintsiv>. (data zvernennia: 22.05.2023).
3. Pro vykorystannia bankamy khmarnykh



posluh v umovakh voiennoho stanu v Ukraini : Postanova Pravlinnia Natsionalnoho banku Ukrainy vid 08 bereznia 2022 roku № 42. URL: https://bank.gov.ua/ua/legislation/Resolution_08032022_42. (data zvernennia: 22.05.2023). 4. Bereslavskia O. I., Tatianina S. M. Vidkrytyi bankinh yak element rozvytku finansovo-kredytnykh vidnosyn v Ukraini. *Finansova systema krainy: tendentsii ta perspektyvy rozvytku* : materialy IKh Mizhnar. nauk.-prakt. int.-konf. (m. Ostroh, 21 zhovt. 2022 r.). Ostroh : Vydavnytstvo Natsionalnoho universytetu «Ostrozka akademiia», 2022. S. 17–20. 5. Shaban O. Finansove shakhraistvo. Yak protydiaty kibershakhraistvu u finansovomu sektori. URL: <https://delo.ua/opinions/finansove-saxraistvo-yak-protidiyati-kibersaxraistvu-u-finansovomu-sektori-418081/>. (data zvernennia: 22.05.2023). 6. Pro zatverdzhennia Polozhennia pro rehuliatornu platformu dlia testuvannia posluh, tekhnolohii ta instrumentiv na rynkakh finansovykh posluh, platizhnomu rynku, zasnovanykh na innovatsiinykh tekhnolohiiakh: Pravlinnia Natsionalnoho banku Ukrainy ukhvalylo 30 bereznia 2023 roku postanovoiu № 39. URL: https://bank.gov.ua/ua/legislation/Resolution_30032023_39 (data zvernennia: 22.05.2023).

Kondratska N. M. [1: ORCID ID: 0000-0001-9103-6241],

Candidate of Economics (Ph.D.), Associate Professor,

Duma V. L. [2: ORCID ID: 0000-0002-6568-8884],

Candidate of Economics (Ph.D.), Lecturer

¹National University of Water and Environmental Engineering, Rivne

²VSP «Rivne Professional Technical College NUWEE», Rivne

DEVELOPMENT OF FINANCIAL TECHNOLOGY IN THE BANKING SECTOR: THREATS AND PERSPECTIVES

The article provides a comprehensive overview of the advancements and potential opportunities in financial technologies within the banking sector of Ukraine. It is emphasized that prior to the warfare, the domestic banking sector had already achieved a high level of digitization. After the beginning of military aggression, the main efforts of banks are focused on developing payment infrastructure, integrating artificial intelligence capabilities, leveraging cloud technologies, and ensuring the implementation of the concept of open banking.

The study determines the main threats that pose risks to the development of financial technologies in the banking sector of Ukraine. The main of them are: physical infrastructure destruction; cybersecurity threats and information leaks; absence or insufficient regulation. The article proposes ways to counter threats and potential financial risks. According to the authors, mitigating the threat of physical infrastructure destruction, lack of electricity, and communication can be achieved due to the using of cloud technologies and the consolidation of banks with the **POWER BANKING**

initiative. The increasing number of cyberattacks on banks and payment systems is part of hybrid warfare, highlighting the necessity for cybersecurity measures and the implementation of new methods of authentication, encryption, and monitoring to prevent cybercrime. Regulatory sandboxes create a favorable environment for innovation and further development of fintech services in the banking sector, thereby laying the foundation for post-war recovery in Ukraine.

Therefore, the development of financial technologies in the banking sector is necessary and integral in the modern world, gaining even greater significance during times of armed conflict. These technologies can be both a threat and an opportunity for financial stability and the functioning of the banking system.

Keywords: fintech; innovative banking products; services and solutions; payment technologies; cloud technologies; regulatory sandbox; open banking; fintech threats.

Отримано: 24 травня 2023 року
Прорецензовано: 29 травня 2023 року
Прийнято до друку: 23 червня 2023 року