МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАДИМА ГЕТЬМАНА

Факультет фінансів

Кафедра банківської справи та страхування

галузь знань	07 «Управління та адміністрування»
Спеціальність	072 «Фінанси, банківська справа, страхування»
освітня програма	«Управління фінансовим бізнесом»

Форма навчання: *Денна*

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему **«Розвиток цифрового банкінгу в Україні»**

здобувача **АНДРУЩЕНКО Анни Олександрівни** _____
(підпис здобувача)

Науковий керівник:
професор кафедри банківської справи та страхування,
доцент, канд.екон.наук.
(вчене звання, наукова ступінь)

_____ Білошапка В.С.
(підпис) *(Прізвище, ініціали)*

Робота допущена до захисту перед Екзаменаційною комісією з атестації здобувачів вищої освіти (ЕК)

Завідувач кафедри банківської справи та страхування:
доктор економічних наук, професор _____ Примостка Л.О.
(підпис)

Київ 2025

РЕФЕРАТ

Кваліфікаційна бакалаврська робота містить 68 сторінок, 8 таблиць, 16 рисунків, список використаних джерел з 58 найменувань, 4 додатки на 4 сторінках.

«Розвиток цифрового банкінгу в Україні»

Об'єктом дослідження є діяльність банків в умовах цифрової трансформації

Предметом дослідження є економічні відносини і процеси, що викають у зв'язку з розвитком цифрового банкінгу

Мета кваліфікаційної бакалаврської роботи – вивчення і розширення теоретико-методичних положень сутності та організації цифрового банкінгу, визначення його проблем в Україні, шляхів їх вирішення та напрямів оптимізації.

Для досягнення поставленої мети визначено такі *завдання:*

– дослідити виникнення, сутність та концептуальні основи цифрового банкінгу;

– вивчити та систематизувати знання щодо організації та правового забезпечення цифрового банкінгу в Україні;

– визначити тенденції розвитку цифрового банкінгу в Україні та світі;

– проаналізувати ризики цифрового банкінгу, виділити основні тренди щодо злочинної діяльності в цій сфері та вказати шляхи протидії їм;

– виявити проблеми цифрового банкінгу в Україні та рекомендувати шляхи їх вирішення;

– визначити завдання центрального банку в умовах інтенсивної цифровізації банків;

– проаналізувати напрямки регуляторного контролю в контексті підтримки безпеки банків та протидії кіберризикам;

– оцінити поточні заходи інформаційної безпеки банків та розробити пропозиції щодо їх оптимізації з урахуванням світового досвіду.

Теоретична, методична та практична значущість отриманих результатів полягає в дослідженні сутності та організації цифрового банкінгу, визначенні його проблем в Україні та шляхів їх вирішення.

Практичне значення отриманих результатів полягає в здійсненні аналізу показників цифрового банкінгу в Україні, визначенні його проблемних аспектів і розробці рекомендацій щодо їх вирішення.

Рік виконання кваліфікаційної бакалаврської роботи – 2025.

Рік захисту роботи – 2025.

Ключові слова: банк, цифровізація, цифровий банкінг, трансформація, банківська конкуренція, кіберризик, інформаційна безпека

ЗМІСТ

ВСТУП

Людство переживає епоху глобальних технологічних змін. Швидкий розвиток інформаційного суспільства, глобалізація інформаційних процесів призвели до становлення інноваційних форм ведення господарської діяльності, таких як Інтернет-магазини, Інтернет-банки, поява нових видів грошових знаків (віртуальних валют), створення цілої галузі економіки — «цифрової економіки». Термін «цифрова економіка» вперше з'явився наприкінці XX століття. 1995 року американський вчений Ніколас Негропонте сформулював концепцію цифрової економіки, представивши її у формі переходу від руху атомів до рухів бітів [1]. У широкому значенні слова цифрова економіка – це економічна діяльність, заснована на цифрових технологіях, пов'язана з електронним бізнесом та електронною комерцією, і вироблених і цифрових товарів і послуг, що збуваються ними. В «академічних дослідженнях термін «цифрова економіка» також часто використовується для опису стану та стадії розвитку економічних відносин країни. По-перше, цифрова економіка пов'язана з четвертим етапом технологічної революції, що характеризується такими тенденціями, як розвиток автоматизації, симбіоз інтелектуальних технологій та активне використання ШІ. Строго кажучи, цифрова економіка відноситься в основному до процесу використання складного апаратного та програмного забезпечення, включаючи різні інформаційні та цифрові елементи, для управління ресурсами економічного суб'єкта.

Вкажемо, що у основі поняття «цифрова трансформація» (англ. digital transformation, DT) лежать кардинальні зміни у технологічних процесах, що спостерігаються у всіх сферах життя. У бізнесі цифрова трансформація призводить до перегляду бізнес-стратегії, моделей, операцій, продуктів, маркетингового підходу, цілей. Вона прискорює продажі та зростання бізнесу.

Цифрова трансформація є ключовим компонентом загальної стратегії трансформації банківського бізнесу. Проте не слід фетишизувати її роль, вона не є єдиним чинником успіху, але багато в чому визначає результат будь-якого проекту

трансформації. Правильно обрані технології в поєднанні з компетенціями співробітників, процесами та операціями дозволяють банкам швидко адаптуватися до складних ситуацій, використовувати перспективні можливості, задовольняти нові потреби клієнтів, що змінюються, стимулювати зростання і впроваджувати інновації – найчастіше несподіваними способами. Якісне перетворення інформації та інших даних дозволяє оптимізувати багато процесів, такі як розробка і запуск нових продуктів і маркетинг нових товарів і послуг (ці процеси більш ефективні і можуть бути краще адаптовані до зовнішніх змін). Крім того, децентралізація адміністративної діяльності підвищує якість інформаційної підтримки, що веде до створення більш гнучких адміністративних структур і, отже, значного підвищення ефективності банку. Цифрова трансформація банківського сектора має такі цілі: підвищення швидкості прийняття рішень, збільшення варіативності процесів залежно від потреб та особливостей клієнта, зниження кількості залучених до процесу співробітників.

У всьому світі відбувається адаптація банківських систем та банківського обслуговування до цифрової трансформації. Практичні аспекти цифровізації широко обговорюються у літературі та інших відкритих джерелах інформації. Багато зарубіжних та вітчизняних дослідників та розробників пропонують свої параметри та критерії оцінки ефективності цифрової моделі банківського бізнесу і пропонують споживачам принципово нові технології з великою кількістю функціональних можливостей, що відрізняються від стандартного банківського обслуговування [2].

Проте слід зазначити недостатній рівень теоретичного осмислення процесів цифрової трансформації банківського бізнесу. Експерти єдині в тому, що у найближчій перспективі цифрові технології кардинально змінять світову економіку, бізнес та особисте життя людини. У найближчій перспективі цифрові технології кардинально змінять світову економіку, бізнес та особисте життя людини. Саме тому вивчення перспектив цифрового банкінгу є цілком виправданим, а обрана тема дослідження є *актуальною.*

Об'єктом дослідження є діяльність банків в умовах цифрової трансформації

Предметом дослідження є економічні відносини і процеси, що викають у зв'язку з розвитком цифрового банкінгу

Мета кваліфікаційної бакалаврської роботи – вивчення і розширення теоретико-методичних положень сутності та організації цифрового банкінгу, визначення його проблем в Україні, шляхів їх вирішення та напрямів оптимізації

Для досягнення поставленої мети визначено такі *завдання:*

– дослідити виникнення, сутність та концептуальні основи цифрового банкінгу;

– вивчити та систематизувати знання щодо організації та правового забезпечення цифрового банкінгу в Україні;

– оцінити вплив цифрової трансформації на банківську конкуренцію;

– визначити тенденції розвитку цифрового банкінгу в Україні та світі;

– проаналізувати ризики цифрового банкінгу, виділити основні тренди щодо злочинної діяльності в цій сфері та вказати шляхи протидії їм;

– виявити проблеми цифрового банкінгу в Україні та рекомендувати шляхи їх вирішення;

– визначити завдання центрального банку в умовах інтенсивної цифровізації банків;

– проаналізувати напрямки регуляторного контролю в контексті підтримки безпеки банків та протидії кіберризикам;

– оцінити поточні заходи інформаційної безпеки банків та розробити пропозиції щодо їх оптимізації з урахуванням світового досвіду.

У процесі здійснення дослідження й підготовці роботи задля досягнення визначеної мети й розв'язання поставлених завдань, застосовувалися загальнонаукові та спеціальні *методи наукового дослідження*: групування, системного аналізу та синтезу – для дослідження та систематизації підходів до визначення сутності цифрового банкінгу; логіко-діалектичного пізнання та

теоретичного узагальнення – для виявлення чинників розвитку цифрового банкінгу та розробці заходів щодо його розвитку; системного аналізу і синтезу – для дослідження інструментарію цифрового банкінгу.

Теоретична, методична та практична значущість отриманих результатів полягає в дослідженні сутності та організації цифрового банкінгу, визначенні його проблем в Україні та шляхів їх вирішення.

Практичне значення отриманих результатів полягає в здійсненні аналізу показників цифрового банкінгу в Україні, визначенні його проблемних аспектів і розробці рекомендацій щодо їх вирішення.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ СУТНОСТІ, ОРГАНІЗАЦІЇ ТА ЗНАЧЕННЯ ЦИФРОВОГО БАНКІНГУ

1.1 Генезис цифрового банкінгу та його організаційне підгрунтя

Розвиток дистанційного банківського обслуговування в Україні є важливим етапом цифрової трансформації фінансового сектору. За останні десятиліття, особливо з середини 2010-х років, відбувся стрімкий ріст цієї галузі, що стало можливим завдяки впровадженню інноваційних технологій та підвищенню доступності інтернету та мобільних пристроїв.

Ключові етапи розвитку, зокрема створення перших інтернет-банкінг платформ і впровадження повністю цифрових банків, значно поліпшили банківське обслуговування. Вплив пандемії та війни також прискорив перехід клієнтів на дистанційні сервіси, що дозволило банківському сектору функціонувати навіть у надзвичайно складних умовах.

Таким чином, дистанційне банківське обслуговування в Україні стає невід'ємною частиною сучасної фінансової системи. Воно надає можливість ефективного, зручного і безпечного доступу до банківських послуг, що відповідає світовим тенденціям цифровізації та модернізації фінансового сектору.

За допомогою дистанційних та віддалених банкінгів банк стає все ближче до клієнта, тобто банківські послуги доступні 24/7 для клієнта та завжди під рукою. Досягнення з використанням технологій завжди є результатом взаємовідносин банку з клієнтом. А розробка кожного нового продукту – це створення повноцінного бізнесу та його подальша інтеграція. Тут доведеться пройти всі стадії: дослідження ринку, організація бізнес-процесів, управління, розробка цифрового сервісу та його інтеграція з екосистемою, підтримка та залучення користувачів.

Різницю між традиційним та дистанційним банківським обслуговуванням ілюструє таблиця 1.1.

Таблиця 1.1 – Різниця між традиційним та дистанційним банківським обслуговуванням

Ознаки	Традиційна	Дистанційна
Час обслуговування клієнтів	Обмежений. Здійснюється в певний час роботи відділення	Необмежений. 24/7 можливість доступу
Швидкість обслуговування	Залежить від працівника	Миттєве опрацювання
Вартість обслуговування	Достатньо висока (% від послуг)	Послуги безкоштовні
Обсяг обслуговування	Виконуються обслуговування в межах відділень по країні	Виконуються обслуговування в межі країни та за її межами
Ознайомлення з новими послугами та продуктами	Витрати на рекламу та час	Здійснюється миттєво через сайт, sms та інші види повідомлень
Витрати на систему обслуговування	Витрати на утримання персоналу та відділень	Витрати на сервер та програми

Джерело: розроблено автором на основі [7]

Етапи розвитку дистанційного банківського обслуговування представлено на рисунку 1.1.

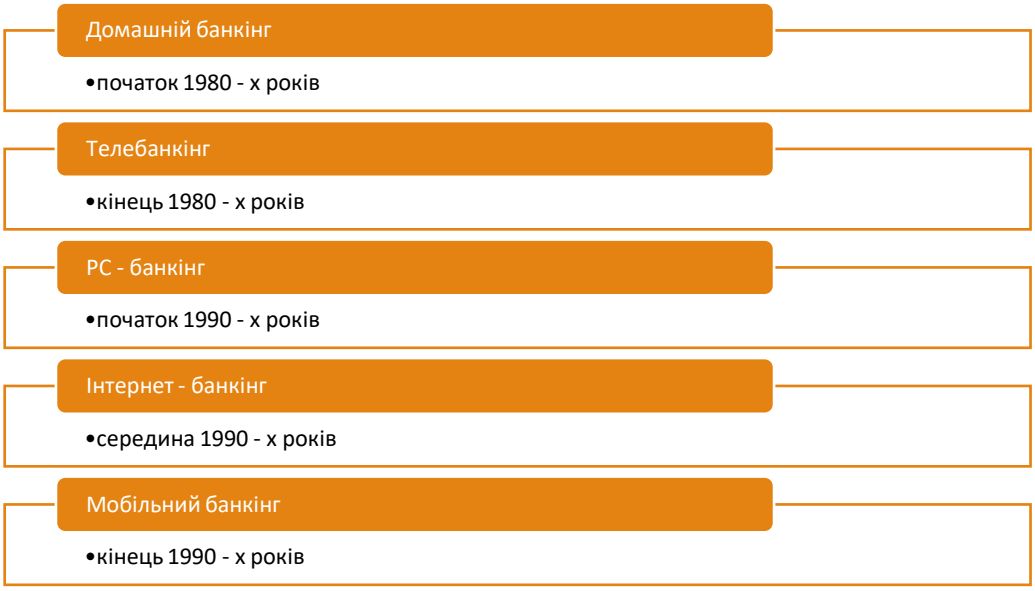

Рисунок 1.1 – Етапи розвитку дистанційного банківського обслуговування

Джерело: розроблено автором на основі [5]

Перші форми цифрового банкінгу з'явилися ще 1960-х роках – тоді таким вважалося просте використання банкоматів і карток. Тепер перенесемося в 2020-і і побачимо, що доступ в Інтернет вже є на постійній основі, значно покращено широкосмуговий зв'язок, смартфони набули широкого поширення, а онлайн-

банкінг стає новою нормою, оскільки клієнти хочуть отримувати всі типи фінансових та нефінансових послуг у цифровому форматі дистанційно та швидко.

Що являє собою цифровий банкінг сьогодні? Чи перетворився він на обов'язкове рішення чи залишається лише бажаним?

Говорячи простою мовою, це автоматизація традиційних банківських послуг, завдяки якій роздрібні та корпоративні клієнти отримали можливість користуватися банківськими продуктами та послугами через онлайн-канали (мережа Інтернет та мобільні мережі).

Перехід до цифрового банкінгу носить глобальний характер, банки реалізують масштабні ініціативи щодо перенесення взаємодії з клієнтами з фізичного світу до цифрового. Для цього вони використовують різні шляхи, зокрема, перетворюють свої послуги на цифровий формат, змінюють години роботи відділень, надають цифрові способи оплати.

Якщо подивитися на те, що змінилося у традиційних банках за останній рік, ми побачимо наступне: 60% банків скоротили кількість своїх відділень або їх години роботи, 34% впровадили повністю цифрові процеси та 18% запустили безконтактні способи оплати.

Перехід до цифрового банкінгу неминучий, оскільки обумовлений змінами вимог ринку і очікуваннями клієнтів. Більше того, банки, окрім прагнення зберегти конкурентні переваги та частку ринку, також хочуть скористатися і новими перевагами, які дає цифровий банкінг. Перерахуємо їх нижче.

Розширення географії діяльності: з економічного погляду цифровий банкінг вважається найвигіднішою можливістю розширення географії діяльності банку – ви можете збільшити охоплення аудиторії банківськими послугами без необхідності відкривати нові відділення.

Нові потоки доходів: платформи цифрового банкінгу допомагають банкам створювати нові потоки доходів, уможливлюючи використання даних клієнтів для вибудовування змістовної взаємодії з клієнтами та розробки нових послуг.

Безпаперові транзакції: одним із найбільших недоліків традиційного банківського обслуговування була надмірна кількість паперових документів, використання яких стає необов'язковим із розвитком цифрового банкінгу.

Зниження витрат: усунення необхідності обробляти паперові документи та вручну виконувати низку інших процесів, витрачаючи на цей час банківських службовців, призводить до значного скорочення витрат банків.

Зручність: надання клієнтам виключно зручного досвіду є пріоритетом для банків, а цифровий банкінг є тим рішенням, яке забезпечує клієнтам можливість користуватися всіма видами банківських послуг у режимі 24x7.

Також важливо відзначити, що у фінансовому секторі різко зросла конкуренція, що змушує банки прискорити темпи переходу на цифрові технології.

Для того, щоб банк вважався постачальником цифрового банкінгу, він повинен пропонувати:

Повний спектр всіх послуг: необхідно реалізувати повний спектр послуг, включаючи всі процеси від реєстрації нових роздрібних та корпоративних клієнтів до віддаленого надання всіх послуг фронт-офісу, як фінансових, так і нефінансових у віддаленому режимі.

Доступність послуг 24x7: доступність послуг 24 години на добу 7 днів на тиждень. Клієнти не повинні бути обмежені годинами роботи банку, вони повинні мати можливість отримувати послуги у будь-який час.

Послуги поза рамками традиційного банківського обслуговування: щоб відповідати новому цифровому стилю життя, необхідно впроваджувати нові послуги, такі як геоконтекстна реклама, гейміфікація, управління особистими фінансами, а також прогнозний аналіз на основі поведінки клієнтів.

Уніфіковані шляхи клієнта: правильна платформа цифрового банкінгу повинна забезпечувати клієнтам одноманітний клієнтський досвід у всіх каналах обслуговування, незалежно від того, який клієнт використовує в різних випадках. Це означає, що треба постійно тримати клієнта в центрі вашої уваги, надаючи йому персональні повідомлення та єдине джерело для оперативного доступу до інформації.

Інтуїтивно зрозумілий досвід користувача (UX): мета UX – створити цифровий фінансовий сервіс, що відповідає потребам користувачів, який пропонує прості та зручні у використанні можливості банківського обслуговування.

Привабливий інтерфейс (UI): інноваційний і привабливий дизайн інтерфейсу в цифрових продуктах дійсно необхідна, але недостатня умова. Інтерфейс користувача повинен бути орієнтований на користувача. Це означає, що його технологія повинна здійснюватися з розумінням того, чого клієнт хоче як користувач і чого він очікує від вашого продукту.

Ефективні сервіси: час має велике значення, адже що менше часу чи дій потрібно користувачеві виконання будь-якої операції, краще. Відповідно, необхідно скоротити кількість дій користувача, у цьому випадку «менше означає більше». Розробляйте максимально зрозумілі рішення, що вимагають мінімуму дій від користувача.

Вся справа у створенні правильного цифрового досвіду. Якщо клієнтам буде складно отримати той результат, якого вони очікують від послуг, що надаються, то вони можуть просто повністю відмовитися від них і звернутися до іншого постачальника цих послуг.

Банкам, які планують перехід на цифрові банківські послуги треба діяти швидко і почати прямо зараз! Як показує розвиток ситуації у сучасному банкінгу, кілька років успішної роботи можуть ще нічого не означати. Щоб залишатися на лідируючих позиціях, треба діяти швидко. Цифровий банкінг більше не є лише бажаним рішенням, а став обов'язковим. Цифрові банки можуть бути гнучкішими у виборі того, кому вони надають послуги та як вони залучають клієнтів. Крім того, дослідження показали, що клієнти надають перевагу банкам з цифровими банківськими порталами їхнім традиційним аналогам. Останнім часом багато великих банківських установ перенаправили кошти від створення нових філій на модернізацію платформ електронного банкінгу. Очікується, що ця тенденція збережеться в міру розширення оцифрування ринку. На даний момент цифровий банк є ідеальним рішенням для всіх банківських потреб клієнтів під час пандемій та війни.

Якщо класифікувати дистанційне банківське обслуговування, отримаємо наступне (рис. 1.2).

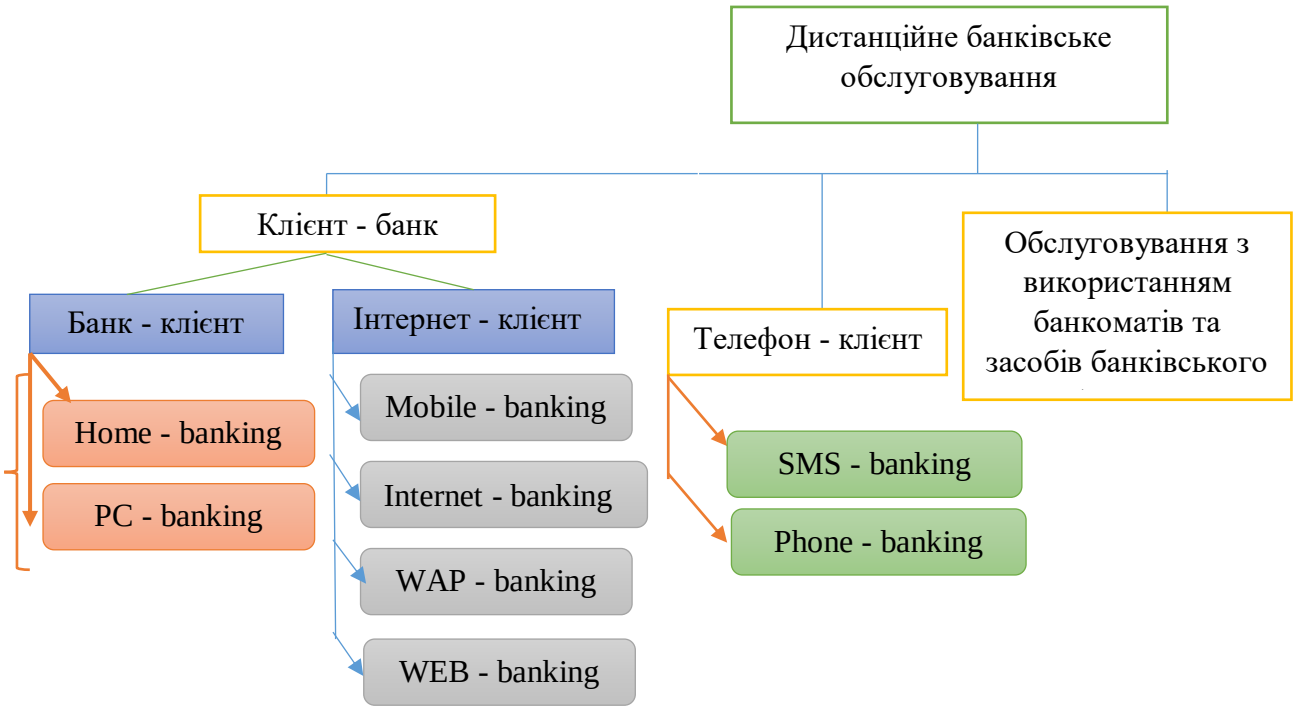

Рисунок 1.2 – Види дистанційного банківського обслуговування

Джерело: розроблено автором на основі [6,7]

На сьогодні сучасні технології дають можливість проводити банківські операції за лічені хвилини, так в Україні в середньому проведення банківського переказу з рахунка на рахунок займає 6-9 секунд (див. табл.1.2)

Таблиця 1.2 – Швидкість проведення банківського переказу з рахунка на рахунок

Банк	Час проведення платежу
Приватбанк	6.84с
Монобанк	07.41с
Ощадбанк	5.40с
Укрексімбанк	3.50с
Таскомбанк	9.12.с

Джерело: розроблено автором на основі [12]

Використання віддалених методів банківського обслуговування дозволяє банкам скорочувати витрати, покращувати ефективність роботи співробітників та розширювати доступ до послуг для клієнтів, включаючи людей з обмеженими

можливостями та тих, що мешкають у віддалених районах. Це відповідає принципам сталого розвитку. Крім того, віддалене банківське обслуговування сприяє підвищенню прозорості фінансових операцій, контролю за особистими коштами та оперативному інформуванню про пропозиції, що сприятливо впливає на фінансову грамотність населення.

1.2 Open Banking як одна з найважливіших технологічних ініціатив у сучасному банківництві

Open Banking, або відкрите банківське обслуговування, є однією з найважливіших технологічних ініціатив у сучасному фінансовому секторі. Це підхід, що передбачає використання відкритих API (інтерфейсів програмування додатків) для надання третім сторонам доступу до фінансових даних користувачів з їхнього дозволу. Ініціатива Open Banking спрямована на підвищення конкуренції на фінансових ринках та надання клієнтам можливості отримувати більш інноваційні та персоналізовані фінансові послуги.

Цей підхід набирає популярності в багатьох країнах завдяки законам, що стимулюють прозорість та конкуренцію, зокрема PSD2 (Revised Payment Services Directive) у Європейському Союзі. В Україні Open Banking також має перспективи впровадження, що може суттєво змінити фінансовий ландшафт країни.

Open Banking полягає в тому, що банки дозволяють фінтех-компаніям та іншим сервісам доступ до своїх баз даних за допомогою спеціальних API. Це дозволяє зовнішнім постачальникам фінансових послуг розробляти додатки та послуги, які покращують користування банківськими послугами.

Основна ідея полягає в тому, щоб надати споживачам більше контролю над своїми фінансами інформаційної безпеки дозволити їм користуватись новими сервісами, що можуть бути зручнішими чи дешевшими, ніж традиційні банківські послуги.

Основні принципи Open Banking включають:

Прозорість і безпека: Користувачі мають повний контроль над тим, кому і як надаються їхні дані.

Конкуренція: Сприяє появі нових гравців на ринку, що розширює вибір для споживачів.

Інновації: Open Banking стимулює появу нових технологій та бізнес-моделей, таких як інтеграція різних банківських рахунків в одному додатку, автоматичне управління витратами, тощо.

Одним із ключових напрямів розвитку Open Banking є поява нових фінансових продуктів та сервісів, що використовують банківські дані користувачів для створення додаткової цінності. Наприклад, це можуть бути:

Інструменти для управління бюджетом: Додатки, що допомагають користувачам планувати витрати на основі аналізу їх банківських транзакцій.

Сервіси швидкого кредитування: Завдяки доступу до історії рахунків клієнтів, фінансові компанії можуть швидше оцінювати кредитоспроможність і пропонувати вигідніші умови.

Агрегатори рахунків: Користувачі можуть керувати кількома банківськими рахунками через один додаток, що значно спрощує управління фінансами.

Відкрите банківське обслуговування відкриває нові можливості для малих фінансових компаній та фінтех-стартапів, що можуть конкурувати з традиційними банками. Вони можуть пропонувати користувачам інноваційні рішення, зокрема у сфері мобільних платежів, інвестиційних сервісів або страхування. Це сприяє зниженню цін на фінансові послуги та підвищенню їх якості через зростання конкуренції.

Завдяки Open Banking фінансовий ринок стає привабливішим для технологічних компаній, які можуть розробляти нові послуги на основі банківських даних. В Україні вже існують фінтех-компанії, які активно розвиваються в цьому напрямку, і Open Banking створює для них ще більші можливості для зростання. Особливо це актуально для мобільних платіжних систем, сервісів автоматичного інвестування.

Покращення клієнтського досвіду Open Banking дозволяє банкам та фінансовим організаціям створювати більш персоналізовані продукти для своїх клієнтів. Наприклад, автоматизовані фінансові консультації, засновані на аналізі даних користувача, можуть допомагати оптимізувати витрати або заощаджувати кошти. Окрім того, за допомогою Open Banking користувачі отримують можливість контролювати всі свої рахунки в різних банках.

Одним з головних ризиків є питання безпеки даних. Відкриття доступу до фінансових даних потребує високих стандартів захисту інформації. У разі неправомірного використання цих даних виникають ризики шахрайства та кібератак. Ось чому безпека користувачів і дотримання регуляторних норм є ключовими умовами для успішного впровадження Open Banking. Для ефективного впровадження Open Banking необхідні чіткі законодавчі рамки. У багатьох країнах вже прийняті відповідні закони (наприклад, PSD2 у ЄС), але в інших регіонах, включаючи Україну, процес впровадження регуляцій ще триває. Непослідовна регуляція або її відсутність може уповільнити розвиток Open Banking.

Один з викликів Open Banking полягає в тому, що споживачі можуть відчувати занепокоєння щодо передачі своїх фінансових даних третім сторонам. Необхідно підвищувати рівень фінансової грамотності та пояснювати переваги цього підходу.

Open Banking в Україні тільки починає свій розвиток, але вже існують передумови для його швидкого впровадження. НБУ активно працює над впровадженням законодавчої бази, яка відповідає європейським стандартам (що підтверджує табл.1.3). Очікується, що з ухваленням нових нормативних актів ринок повинен розширитися, а споживачі – отримати доступ до інноваційних фінансових рішень.

Впровадження Open Banking створює передумови для покращення якості обслуговування клієнтів і сприяє розвитку нових фінансових технологій. А зручний клієнтський шлях дозволяє забезпечити залучення населення до використання сервісів на базі відкритих API.

Таблиця 1.3 – Порівняння законів «Про платіжні системи та переказ коштів в Україні» і «Про платіжні послуги»

Параметр	Закон України «Про платіжні системи та переказ коштів в Україні» (№2346-III від 05.04.2001 р.)	Закон України «Про платіжні послуги» (№1591-IX від 30.06.2021 р.)
Основна мета	Регулювання відносин у сфері платіжних систем та переказу коштів в Україні встановлення загальних норм для роботи платіжних систем	Гармонізація українського законодавства з європейськими нормами (PSD2) та впровадження сучасних стандартів на ринку платіжних послуг
Сфера регулювання	Платіжні системи (вітчизняні та міжнародні) - Переказ коштів - Правила взаємодії учасників платіжних систем	Ширший спектр платіжних послуг, включаючи інноваційні фінансові технології - Захист прав споживачів платіжних послуг
Захист прав споживачів	В основному спрямовано на забезпечення безпечних переказів коштів	Розширені права споживачів, включаючи їх право на отримання чіткої інформації про платіжні послуги та механізми вирішення спорів

Джерело: розроблено автором самостійно

Отже, головні відміності наступні:

1. Сфера регулювання: Закон 2001 року більше орієнтований на традиційні банківські системи та їх взаємодію у сфері переказів коштів. Закон 2021 року має ширший спектр регулювання, включаючи інноваційні фінансові технології, fintech-компанії та платіжні сервіси.

2. Права споживачів: Закон 2021 року передбачає більш захищені права споживачів інформаційної безпеки впроваджує нові механізми для вирішення спорів і компенсацій, що відповідає європейським стандартам.

3. Відкритий банкінг: Новий закон враховує сучасну концепцію Open Banking, що дозволяє третім сторонам (наприклад, fintech-компаніям) отримувати доступ до банківських даних з дозволу користувача, що не було передбачено у попередньому законі.

4. Європейські стандарти: Закон 2021 року адаптований до європейської директиви PSD2, що дозволяє інтегрувати українську банківську систему до європейського фінансового ринку.

Отже, Закон України «Про платіжні послуги» 2021 року є сучаснішим та більш гнучким нормативним актом, що враховує технологічні інновації та

європейські регуляторні норми, тоді як закон 2001 року більш обмежений в рамках класичних платіжних систем. Закон 2021 року відкриває нові можливості для розвитку фінансових технологій, покращує захист прав споживачів і підвищує рівень lконкуренції на ринку платіжних послуг.

Процес засвоєння Open banking як надавачами банківських послуг, так і споживачами, буде тривалим. На це є декілька причин:

1) Open banking в силах посилити конкуренцію між банками (що на даний момент є важливим питанням), яким не вигідно ділитися даними про своїх клієнтів задля запобігання переманювання. Однак тут є і протилежний аспект – в погоні за збереженням своєї клієнтської бази створюватимуть унікальні та якісні продукти, що позитивно плине на ринок банківських послуг. Крім того, значущості на ринку набудуть небанківські установи, оскільки вони матимуть доступ до клієнтури банків, їх дій та вподобань, та, відповідно, розроблятимуть конкурентоспроможні продукти.

2) Споживачі імовірно будуть вразливі до втрати коштів через невгамовану (навіть процвітаючу) кіберзлочинність та низьку фінансову грамотність. Процес входу нових технологій в повсякденне життя зазвичай тривалий, тому переважна більшість населення довго не зможуть довіритися роздачі своїх даних через Open banking.

3) Процес створення необхідної та дієвої нормативної бази, правового регулювання діяльності через Open banking безперечно буде довгим. Навіть якщо він і запрацює із середини 2025, у регулюванні все ж іще будуть прогалини, якими зможуть скористатися злочинці.

Загалом, зважаючи на рівень розвитку дистанційного банківського обслуговування, Open banking точно увіллється у життя українців, однак не настільки швидко, як планує НБУ (2025 рік). Наразі в Україні існує малесенька частинка Open banking (гугл, епл гаманці та можливість додавання карток інших установ в додатку певного банку), однак ці послуги не дуже поширені. Розквіту нова технологія набуде лише за умови хорошої обізнаності клієнтів про переваги та можливості, а також за умови якісного захисту конфіденційної інформації.

1.3 Вплив цифрової трансформації на банківську конкуренцію

Цифрова трансформація дозволяє банкам перейти на новий рівень конкуренції:

- між цифровими та традиційними банками;
- між фінтех компаніями та традиційними банками;
- у сфері окремих сервісів чи процесів (рис.1.3).

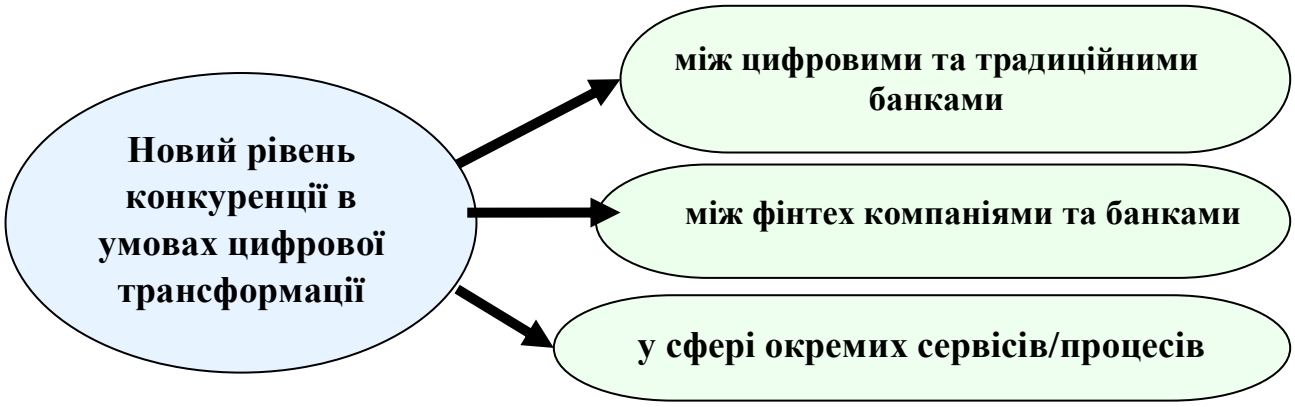

Рисунок 1.3 – Конкуренція в умовах цифрової трансформації

Джерело: складено автором самостійно

Розвиток технологій у фінансовому секторі спричинив формування нової фінансово-технологічної екосистеми (FinTech).

Фінансові технології, або ФінТех (FinTech) – це галузь, що складається з компаній, які використовують технології та інновації, що дозволяють їм конкурувати з банками та іншими фінансовими посередниками. В даний час до ФінТех себе відносять як численні технологічні стартапи, так і великі організації, що відбулися, намагаються поліпшити та оптимізувати фінансові послуги, що надаються. ФінТех-компанії працюють у наступних напрямках: криптовалюти та цифрові валюти; технології блокчейну з децентралізованою системою; так звані «розумні контракти», які дозволяють безпечно обмінюватися грошима та даними

без допомоги третіх осіб; RegTec (регулятори technology) - технології, що забезпечують швидке та надійне дотримання норм законодавства; робопомічники - програмні алгоритми, які включають різні типи інвестиційних порад за набагато менші гроші, ніж реальні консалтингові фірми; небанківські послуги, що пропонують послуги населенню з низьким доходом, яке не може отримати з тих чи інших причин підтримки традиційних банків чи інших фінансових посередників; кібербезпека та інші напрямки.

Ряд операцій фінансового посередництва (грошові перекази, залучення коштів за рахунок краудфандингу тощо) вже зараз здійснюється поза банківською сферою та класичними фінансовими посередниками.

Низькі відсоткові ставки на світових ринках ведуть до зниження процентної маржі банків та уповільнення темпів зростання їхнього прибутку. До того ж конкуренція з боку небанківських посередників веде до зниження комісійних прибутків від класичних банківських операцій.

Найчастіше в банках при розробці інформаційних систем використовують каскадну модель (Waterfall). Каскадна методологія Waterfall – така модель процесу розробки програмного забезпечення, в якій процес розробки виглядає як потік, що послідовно проходить фази аналізу вимог, проектування, реалізації, тестування, інтеграції та підтримки. Для даної методології характерна зрозуміла та проста структура процесу розробки. Взаємодія з замовником відбувається тільки на початковій та фінальній стадіях, що передбачає неможливість внесення змін замовником до закінчення розробки продукту. Методологія передбачає жорстку послідовність етапів розробки. Тестування відбувається під кінець проекту, відповідність вимогам – головний показник прогресу.

Наразі класична Waterfall-методологія відходить, змінюючись гнучкішими моделями. Гнучка методологія розробки (Agile) – серія підходів до розробки програмного забезпечення, орієнтованих на використання ітеративної розробки, динамічне формування вимог забезпечення їх реалізації внаслідок постійного взаємодії всередині робочих груп, що складаються зі спеціалістів різного профілю. Ця технологія розкривається в послідовній реалізації різних методів у створенні

програмного забезпечення, орієнтованих на використання ітеративних розробок. Методологія Agile передбачає гнучкість та динамічне формування вимог на всіх етапах розробки програмних технологій. Робота поділяється на етапи. На кожному з них продукт тестується, і далі його адаптують відповідно до вимог клієнта на мікрорівні та поточної ситуації на макрорівні. Впровадження Agile-технологій у банку дозволяє підвищити його конкурентоспроможність за рахунок створення чіткої структури бізнес-процесів та надання актуальних банківських продуктів. Позитивним результатом розвитку Agile у банківському секторі є прискорення цифрової трансформації як одного із стратегічних завдань сучасної банківської системи. Втім, вибір методології залежить від заданих параметрів. Якщо потрібно розробити програмне забезпечення з чіткими вимогами та результатами, але з варіативною вартістю та терміном розробки, краще використовувати каскадну модель. Якщо потрібно розробити програмне забезпечення жорстко задані терміни та встановлений бюджет, краще застосовувати гнучку модель [9]. Порівняння Agile та Waterfall методологій розробки програмного забезпечення представлене у табл. 1.4.

Таблиця 1.4 – Порівняльний аналіз Agile та Waterfall

Waterfall	**Agile**
1	2
Зрозуміла та проста структура процесу розробки	Підвищені вимоги до кваліфікації та досвіду команди
Взаємодія із замовником відбувається лише на початковій та фінальній стадіях	Постійна взаємодія із замовником
Неможливість внесення змін замовником до закінчення розробки продукту	Готовність до змін важливіше за початковий план
Орієнтований на процес	Люди та взаємодія важливіші за процеси та інструменти
Жорстка послідовність етапів розробки	Незначні процеси відсуваються на задній план
Тестування відбувається під кінець проекту	Тестування безперервно протягом усього проекту
Фіксована вартість проекту	Плаваюче значення вартості проекту
Відповідність вимогам – головний показник прогресу	Працюючий продукт – головний показник прогресу

Джерело: [9]

Слід зазначити, що підхід agile, що передбачає роботу у невеликих крос-функціональних командах, отримав широке поширення у контексті цифровізації. Головна відмінність цих команд полягає у тому, що в них немає чіткої ієрархії, і вони працюють разом тільки протягом короткого періоду часу. Цей тип організації бізнесу дозволяє досягти високих результатів за короткий період часу, що є значною перевагою перед традиційними методами організації банківського бізнесу.

Сторонніми постачальниками послуг можуть бути провайдери фінансової інформації, які інформують клієнта про різні фінансові продукти, дозволяють отримувати доступ до рахунків клієнта у різних банках, допомагають керувати фінансами. Це може бути один додаток до всіх рахунків клієнта у різних банках. Створювані платформи дозволять об'єднати в одному місці рахунки та картки клієнта. З'являться простіші та зручніші інтерфейси. Отримавши інформацію від банків, соціальних мереж, з інших джерел, проаналізувавши її, ФінТех-компанії зможуть запропонувати такий фінансовий продукт для клієнта, від якого йому буде важко відмовитися. Банківські послуги будуть дуже індивідуалізовані, враховувати фінансовий стан клієнтів, їх вікові особливості, поведінкові патерни (рис.1.4).

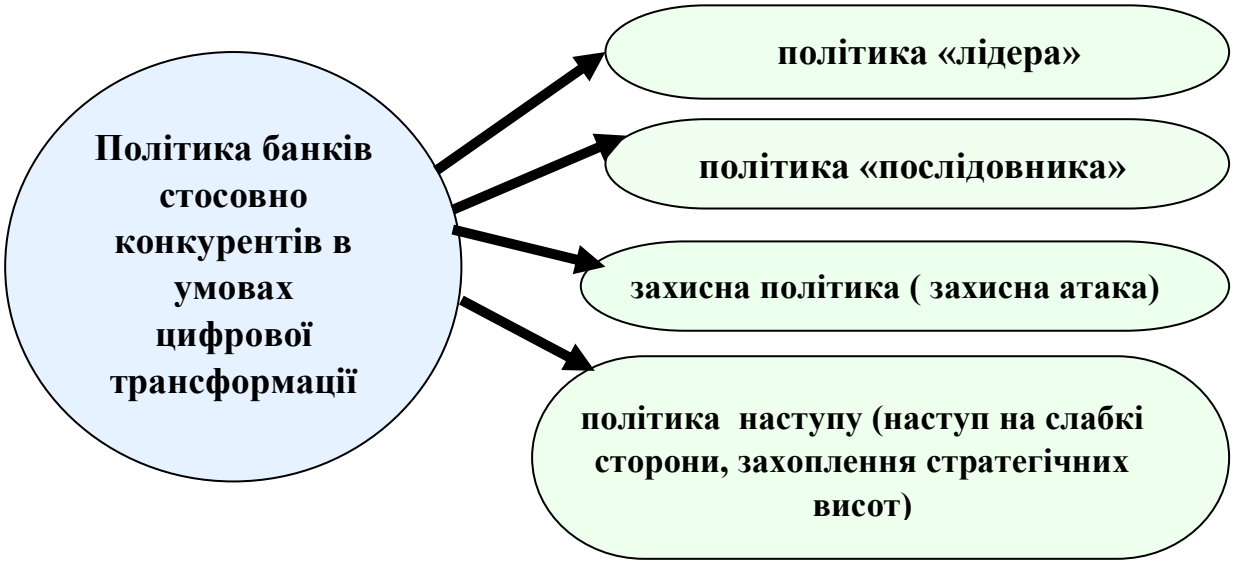

Рисунок 1.4 – Політика банків стосовно конкурентів в умовах цифрової трансформації

Джерело: складено автором самостійно

В таких умовах нові банківські продукти виходитимуть на ринок швидше і стануть більш різноманітними, індивідуалізованими. Стороннім організаціям, які спеціалізуються на фінансових технологіях та надають свої послуги банкам та клієнтам, надається рівний з банками доступ до даних клієнтів для їх аналізу та надання фінансових рекомендацій.

Відповідно до цифрових змін сучасним трендом маркетингових комунікацій банку є персоналізація. Персоналізація – система надання релевантного інтересам клієнта контенту. Така система заснована на зборі інформації про клієнта: його поведінку на сайті, купівлю продуктів банку, інформації із соціальних мереж. Сукупність такої інформації називається профайлом клієнта, а контент, підібраний під цей профайл, – персональним контентом. Існує стійке переконання, яке поділяємо і ми, що використання методик персоналізації дає банку значні переваги.

Вже зараз менеджери провідних банків прагнуть перетворити банки на IT-компанії з особливою екосистемою, в якій торгівля, виробництво, послуги, фінанси та грошові розрахунки дуже тісно пов'язані. Взаємодія пристроїв та програмних технологій удосконалюється з кожним роком, а концепція Open Banking спрямована на забезпечення такого зв'язку із фінансовими сервісами.

Сучасні цифрові технології скорочують дистанцію між виробником та споживачем банківських послуг, істотно загострюється міжбанківська конкуренція, і навіть конкуренція з глобальними технологічними компаніями.

Автори найрадикальніших прогнозів обіцяють, що через 5-10 років роздрібні банки зникнуть зовсім. І не лише тому, що програють у технологічній конкуренції, а ще й тому, що їхні відділення клієнти сприйматимуть як спадок минулого. Дослідження показують, що банки у всьому світі активно закривають свої відділення та інвестують кошти у мобільні додатки.

Так, за словами представника Royal Bank of Scotland, з 2014 року кількість клієнтів, які використовують філії банку по всій Великій Британії, скоротилося на 40%, а мобільні трансакції зросли на 73% за цей же період. Дослідження у Голландії показало, що відділення банків на околицях міст відвідує дві особи на добу. У США

1984 року налічувалося 14 400 комерційних банків, нині їх близько 4 тисяч. Починаючи з 2000-х років, у Німеччині закрився майже кожний четвертий офіс. У Великій Британії з 2015 по 2018 роки закрилося 2 868 філій. [17].

Менш радикальний прогноз — відділення збережуться, а ось їх функції, вигляд та устрій стануть зовсім іншими.

То яким буде банк? На думку автора, є кілька шляхів розвитку в умовах диджиталізації, які розкриємо нижче і які ілюструє рис.1.5.

– Банк перетвориться на розумний, він має навчитися розуміти своїх користувачів. Нова ера персоналізації призводить до необхідності об'єднання великих обсягів даних із розрізнених систем у дієву та корисну інформацію. У результаті, кожен клієнт повинен отримувати продукт або послугу, адаптовані для його індивідуальних потреб, за найбільш відповідними йому каналами.

– Банк буде модульним. Штучний інтелект все частіше сприймається як конкурентна перевага, оскільки банки прагнуть перетворити дані на інструмент підвищення доходів, скорочення втрат і витрат або досягнення одразу всіх цілей.

– Відбудеться створення банківських екосистем, де користувачам доступно безліч послуг.

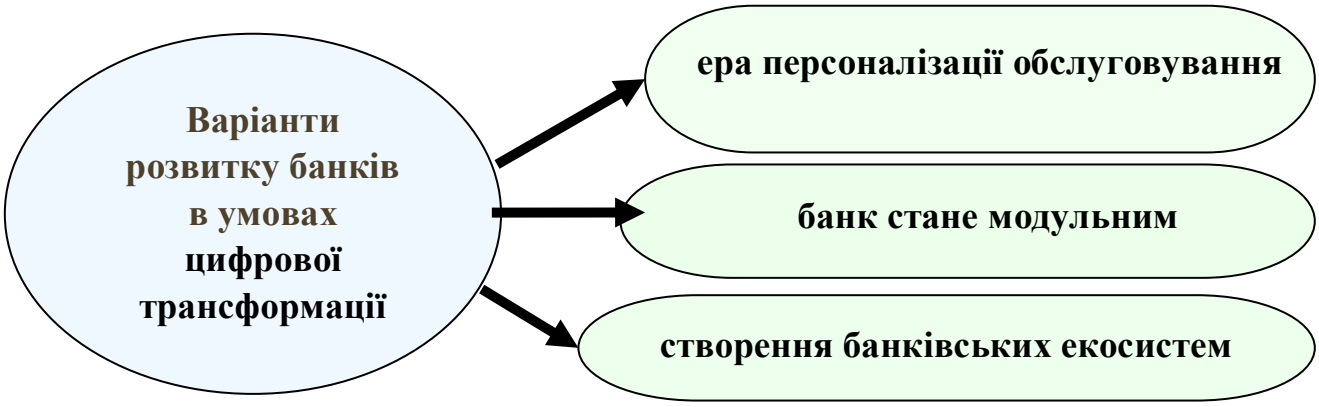

Рисунок 1.5 – Варіанти розвитку банків в умовах диджиталізації

Джерело: складено автором самостійно

На нашу думку, екосистемний підхід найперспективніший і саме він змінить модель бізнесу, коли банківська діяльність стане одним із численних бізнесів у загальній екосистемі. При виборі екосистемної бізнес-моделі банк перестає бути у

класичному розумінні банком, а стає платформним рішенням, що об'єднує у собі різні напрямки. При цьому підході змінюється стратегія ведення бізнесу, де дохід приносить не лише банківська діяльність, а й інші компанії, що входять до екосистеми. Деколи навіть банківська діяльність може не бути основним джерелом прибутку для екосистеми. Тому при екосистемній бізнес-моделі банк перестає бути банком у класичному розумінні, а стає платформним рішенням.

На рис. 1.6 представлено схему взаємозв’язку банк-середовище-клієнт.

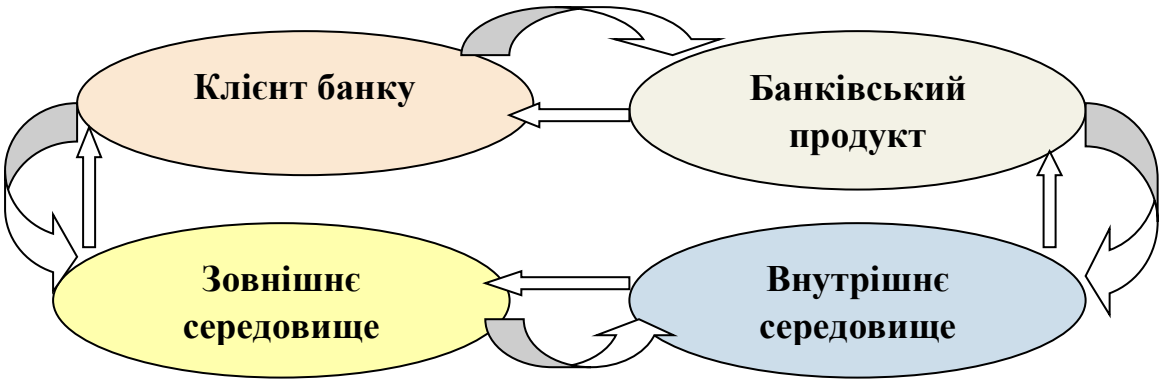

Рисунок 1.6 – Схема взаємозв’язку банк-середовище-клієнт

Джерело: складено автором самостійно

Дійсно, у сучасному світі, де конкуренція на ринку досягає свого піку, «клієнт завжди має рацію» – це не просто фраза, а ключовий принцип побудови з клієнтом міцного фундаменту довгострокових відносин.

Клієнтоцентричність – це фокус у стратегії розвитку банку загалом. Клієнтоорієнтованість – дії, спрямовані на розуміння потреби клієнта, виконання вимог та прагнення перевершити очікування кожного клієнта. Клієнтоцентричність – це концепція та філософія розвитку організації для задоволення інтересів та потреб клієнта, вона автоматично прагне вдосконалення якості послуг. За останні роки уявлення про це поняття зазнало значних змін. Якщо раніше воно могло зводитися до надання відмінного сервісу, то сьогодні це глибоке розуміння потреб клієнтів, його психологічного портрета та поведінкових звичок, коли відбувається збирання зворотного зв'язку на всіх етапах взаємодії: від розробки продукту до післяпродажного обслуговування та зв'язку з клієнтом.

Таким чином, слід визнати, що цифрова трансформація банківської сфери полягає не лише у застосуванні інноваційних цифрових технологій, але також змінює бізнес-модель банку від традиційної до екосистемної. Розвиток цифрових екосистем банків на сучасному етапі можна розглядати як сильну конкурентну перевагу, яка дозволить надавати індивідуальний підхід клієнтам банку.

Слід зазначити, що опір інноваціям, невдачі проектів та пов'язані з ними ризики є неминучим наслідком розвитку та прогресу. У той же час здорова відданість змінам та усвідомлення природності та вірності цього процесу є факторами успіху банку. Послідовність та обсяг дій надають суттєвий вплив на досягнення значних результатів та контроль потенційних ризиків.

Вплив фінтеху на традиційний ринок фінансових послуг реалізується як наслідок успішності на полі аутсорсингу окремих складових процесу надання фінансових послуг (рис. 1.7).

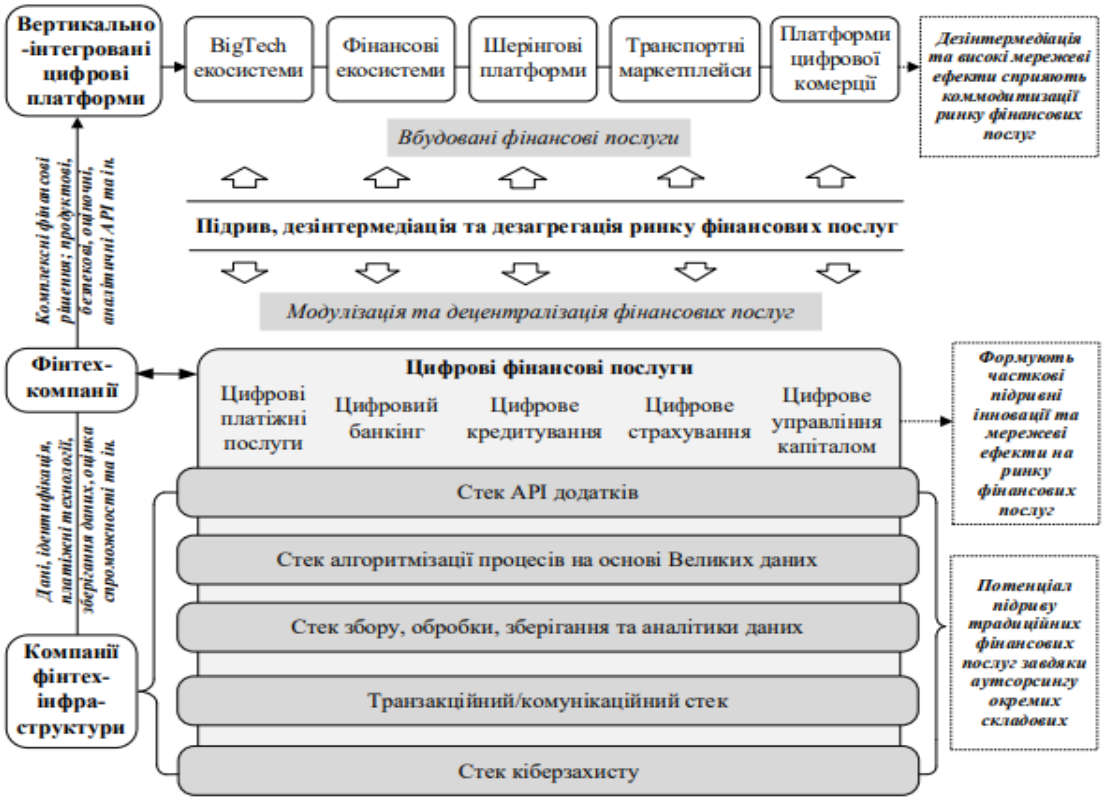

Рисунок 1.7 – Методологічні засади процесів підриву, дезінтермедіації та дезагрегації на ринку фінансових послуг

Джерело: [30]

За допомогою передової аналітики даних та алгоритмів машинного навчання компанії фінтех можуть аналізувати величезні обсяги даних клієнтів для розуміння їх переваг, поведінки та фінансових потреб. Це дозволяє створювати налаштовані фінансові продукти та послуги, що відповідають специфічним вимогам індивідуальних клієнтів.

Очевидними перевагами від розвитку цифрових екосистем є:

– підвищена безпека та прозорість фінансових транзакцій,

– операційна ефективність компаній та покращена зручність для користувачів,

– зростання персоналізації цифрових послуг та якості обслуговування клієнтів,

– автоматизація бізнес-процесів та аналітика для прийняття управлінських рішень.

Розвиток цифрових екосистем, а в деяких випадках – їх інтеграція, веде до зміни суті конкуренції на ринках. Це важливо враховувати іншим гравцям, які не мають подібних цифрових екосистем, і своєчасно реагувати на їх появу та розвиток.

Для клієнтів переваги екосистем зводяться в основному до двох ключових речей – вони зручні та вигідні. Якщо екосистема побудована на основі гаджетів, то зручність полягає у безшовному зв'язку між ними, повною сумісністю та додатковою функціональністю. Якщо це пов'язано з софтом, то найчастіше для доступу до всіх можливостей численних сервісів потрібен лише один обліковий запис, підтримка теж стає єдиною.

Для надання передових інноваційних фінансових послуг у здоровій екосистемі значну роль відіграють центральні банки, які мають:

– підтримувати постійний діалог з постачальниками технологій та фінтех-компаніями, які можуть допомогти в оцінці наслідків та покращенні балансу між використанням інновацій та управлінням ризиками;

– сприяти співпраці між банками для оптимізації регулювання, а також для задоволення нових запитів ринку;

– заохочувати ініціативи відкритого банкінгу для полегшення безперешкодного обміну даними та просування інновацій у фінансових продуктах та послугах;

– співпрацювати з міжнародними партнерами для гармонізації нормативних стандартів та стимулювання транскордонних фінансових операцій.

РОЗДІЛ 2. СУЧАСНИЙ СТАН ЦИФРОВОГО БАНКІНГУ ТА ОПТИМІЗАЦІЯ ЙОГО РОЗВИТКУ В РЕАЛІЯХ УКРАЇНИ

2.1 Аналіз ринку цифрових банківських платформ та конкурентного ландшафту

Традиційний банк може бути повністю цифровим банком з допомогою цифрової банківської платформи. Ці платформи допомагають розширити можливості цифровізації банку з погляду орієнтації на клієнтів, внутрішньої оптимізації та готовності екосистеми і, таким чином, підтримують довгострокову цифрову трансформацію банку через готові можливості та гнучка архітектура. Ринок цифрових банківських платформ сегментований за розгортанням (хмара, локально), типом (корпоративний банкінг, роздрібний банкінг) та географічним розташуванням (Північна Америка, Європа, Азіатсько-Тихоокеанський регіон, Латинська Америка, Близький Схід та Африка). Розміри ринку та прогнози представлені у вартісному вираженні (млн доларів США) для всіх вищезгаданих сегментів.

Таблиця 2.1 – Сегментація ринку цифрових банківських платформ

По розгортанню	Хмара Локально
За типом	Корпоративний банкінг Роздрібні банківські послуги
Географія	Північна Америка Азіатсько-Тихоокеанський регіон Європа

Джерело:[23]

Обсяг світового ринку цифрових банківських платформ оцінюється в 10,14 млрд. доларів США в 2024 році і, як очікується, досягне 19,56 млрд. доларів США до 2029 року, при цьому середньорічний темп зростання складе 14,04% протягом прогнозованого періоду (2024-2029 рр.).

Банківська галузь швидко переживає цифрову трансформацію, і споживачам потрібні розумні мобільні пристрої та цифрові банківські послуги. Це деякі з основних факторів, що сприяють зростанню ринку.

Так, більшість банків надають перевагу платформам цифрового банкінгу через різні запропоновані переваги, такі як зниження витрат на IT, швидкий час виходу на ринок, відкритий банкінг, готові, але налаштовані можливості, омніканальне обслуговування клієнтів і мікросервісна архітектура, тощо. буд. небагато. Наприклад, у грудні 2022 року Deloitte оголосила про співпрацю з AWS для вирішення хронічної проблеми у банківській сфері переходу до цифрових систем, які охоплюють клієнтський інтерфейс та операції бек-офісу.

Хоча необанки, як і раніше, є нішевим ринком, вони демонструють вищі темпи зростання частки ринку та обслуговують клієнтів приблизно за одну третину вартості традиційних банків. Фінтех-компанії націлені на прибуткові ніші у ланцюжку створення вартості. Великі технологічні гравці з їх великими клієнтськими базами становлять реальну загрозу, а деякі традиційні гравці вкладають значні кошти в інновації, відтісняючи решту в тінь.

Однак такі проблеми, як інтеграція цифрових банківських платформ зі застарілими системами, збої в мережі та проблеми безпеки можуть призвести до серйозних втрат банків і, отже, такі фактори можуть перешкоджати зростанню ринку.

Після Covid-19 відбулося зростання активності онлайн-банкінгу, зокрема збільшення кількості цифрових транзакцій та зниження кількості поїздок до звичайних відділень. Пандемія змусила окремих споживачів, а також корпорації, які колись чинили опір онлайн-банкінгу, прийняти додатки цифрового банкінгу як нові послуги за умовчанням. Пандемія призвела до підвищення зручності для споживачів, що може призвести до зростання попиту у довгостроковій перспективі. Що стосується вендорів, більшість постачальників концентруються на залученні клієнтів, надаючи послуги, затребувані у важкі часи.

Тенденції ринку цифрових банківських платформ наступні. Збільшення використання хмарних платформ веде до прискорення зростання ринку. У січні

2023 року цифровий банк на Філіппінах GoTyme Bank у співпраці зі всесвітньою платформою хмарного банкінгу Mambu створив інноваційне рішення для цифрового банкінгу, спрямоване на розширення доступу філіппінців до високоякісних фінансових послуг.

Багато банків воліють скорочувати витрати на IT-інфраструктуру, необхідну для локальної установки, за рахунок використання хмарних сервісів, які дозволяють їм швидко розгортати нові продукти та масштабувати інфраструктуру, швидше обслуговувати ширшу клієнтську базу з різними потребами та швидко керувати збільшенням платежів у реальному часі при забезпеченні відповідності стандарту.

Оскільки абонентська плата сплачується постачальнику SaaS, витрати на обслуговування системи та проблеми зі застарілими технологіями скорочуються. Замість того, щоб витрачати невеликий стан на IT, SaaS надає банкам можливість перерозподіляти бюджети, щоб вони могли зосередитися на інноваціях, задоволенні клієнтів та зростанні бізнесу.

Використання хмари також допомогло платформам мобільного банкінгу запропонувати гнучкий інтерфейс користувача (UI) і підтримати весь банківський шлях клієнтів банку, починаючи з реєстрації та закінчуючи транзакційними банківськими запитами, на їх мобільних пристроях. Банки швидко впроваджують платформи мобільного банкінгу через зміну їх переваг на користь мобільного банкінгу.

Більше того, ширше впровадження сторонніх додатків для платежів у реальному часі, таких як Whatsapp Pay та PhonePay, призвело до збільшення попиту банків на надійну інфраструктуру для безперебійного виконання транзакцій UPI. Наприклад, Visa нещодавно завершила операцію з придбання Plaid, фінтех-стартапу, який дозволяє програмам легко та миттєво підключатися до банківських рахунків клієнтів за 5,3 мільярда доларів США. Подібні технологічні зрушення призвели до збільшення попиту на хмарну інфраструктуру в промисловості цифрового банкінгу.

Значне число найбільших банків знаходяться в Північній Америці (рис.2.1) , і це основна причина зростання ринку цифрових банківських платформ. Цифрові банківські компанії у регіоні пропонують програмне забезпечення як послугу, що дозволяє перетворити застарілі системи на цифрові. Наприклад, Temenos допомагає новим цифровим банкам США розпочати роботу за 90 днів, пропонуючи найбільш функціонально багату та технологічно просунуту комплексну пропозицію цифрового банку SaaS.

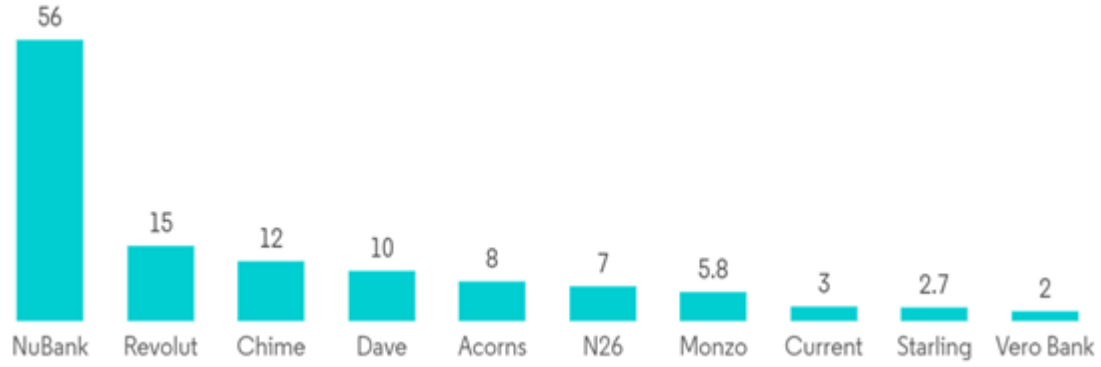

Рисунок 2.1 – Число користувачів цифрового банкінгу найкрупніших цифрових платформ світу

Джерело:[23]

Платформи цифрового банкінгу стають все популярнішими, оскільки технологія блокчейна, що підвищує безпеку, використовується все більше і більше, особливо в секторі BSFI. Цей чинник сприяє зростанню ринку країни. Багато компаній розробляють цифрові хмарні банківські платформи на основі блокчейну.

Північна Америка також є одним з найінноваційних та перших місць використання хмари. Постачальники хмарної інфраструктури мають міцні позиції у регіоні, що допомагає ринку зростати ще більше.

Стійке зростання використання цифрових банківських платформ (рис.2.2) слідує за аналогічним зростанням використання фінтех-додатків, які примітні тим, що є одним із найшвидше зростаючих типів додатків у США і у всьому регіоні.

Рисунок 2.2 – Зростання цифрових банківських платформ за регіонами світу
Джерело:[23]

Ринок цифрових банківських платформ рухається до фрагментації. Це відбувається через вихід на ринок компаній та рішень, що створює фрагментоване середовище в екосистемі цифрового банкінгу. Однак завдяки технологічним досягненням та інноваціям у продукції компанії середнього та малого бізнесу збільшують свою присутність на ринку за рахунок укладання нових контрактів та партнерських відносин.

У січні 2023 року Axis Bank у співпраці з OPEN надав своїм клієнтам, у тому числі підприємствам малого та середнього бізнесу, фрілансерам, домашнім підприємцям, впливовим особам та іншим повністю власний цифровий поточний рахунок. Ця співпраця надає ширшій бізнес-спільноті доступ до комплексного банківського досвіду Axis Bank та комплексних можливостей фінансової автоматизації OPEN для бізнес-адміністрування, таких як платежі, бухгалтерський облік, розрахунок заробітної плати, дотримання вимог, управління витратами та інші послуги.

У листопаді 2022 року Capco та Savana оголосили, що працюватимуть разом стратегічно, щоб прискорити трансформацію банків та стимулювати постійні інновації у цифрових продуктах. Це партнерство допоможе банкам подолати технічні проблеми, з якими вони стикаються при задоволенні очікувань, що

зростають, і потреб клієнтів у забезпеченні безперебійного сучасного омніканального обслуговування.

Лідери ринку цифрових банківських платформ:

- Oracle Corporation;
- SAP SE;
- Tata Consultancy Services Limited;
- Temenos Headquarters SA;
- Worldline SA.

У квітні 2025 пройшли експертні ради “Цифровий банкінг: Україна” та “Цифровий банкінг: країни Центральної Азії”, присвячені питанням розвитку цифрового онбордингу, інтернет- та мобільного банкінгу для клієнтів МСБ та небанківських сервісів. За результатами оцінок експертами SME Banking Agency виявлені рейтинги на рівні країн:

Категория “Digital Onboarding” для клиентов МСБ:

1. ПУМБ
2. ПриватБанк
3. А-банк
4. Ощадбанк
5. Raiffeisen Bank

Категория “Mobile banking” для клиентов МСБ:

1. ПриватБанк
2. А-банк
3. ПУМБ
4. Sense Bank
5. monobank

Категория “Online banking” для клиентов МСБ:

1. ПриватБанк
2. ПУМБ
3. Raiffeisen Bank
4. Ощадбанк

5. Sense Bank

Категория “Beyond Banking” для клиентов МСБ:

1. ПриватБанк
2. monobank
3. Sense Bank
4. NovaPay
5. Raiffeisen Bank

Український цифровий банкінг повинен враховувати той факт, що Україна йде в напрямку членства в ЄС. Так що всі гравці вже зараз повинні орієнтуватися на європейське законодавство, оскільки в майбутньому кордони з Європою будуть знищені, а послуги цифрового банкінгу стануть більш відновленими. До цих євроінтеграційних змін сектор цифрового банкінгу повинен бути готовий заздалегідь.

У нашій країні сектор цифрового банкінгу створюватиме нові додатки, які стануть простими, зручними та зрозумілими, зараз ця філософія мігрує у філософію супер-апа, оскільки діджитал банкінг трансформується в супер-ап.

В таких умовах в Україні будуть з'являтися цікаві фінансові сервіси. Наприклад, страхові компанії інтегруються в цю діджитал історію, цей тренд переросте в індустрію, і такі перспективи цілком реальні.

2.2 Аналіз особливостей та наповненості цифрового банкінгу на прикладі вітчизняних банків

Для власного дослідження ми обрали два державні банки: *ПриватБанк* та *Sense bank*. За рейтингом Forbes вони є лідерами за діджиталізацією та впровадженням інноваційних послуг. Метою є виявлення та порівняння специфіки дистанційного банківського обслуговування двох банків, аналіз переваг та недоліків.

Порявняємо спектр і наповненість послуг.

ПриватБанк:

Спектр послуг:

- Онлайн відкриття рахунків і депозитів.
- Оформлення кредитних заявок через сайт і мобільний додаток.
- Валютний обмін онлайн.
- SWIFT-перекази через систему.
- Платежі та перекази між картками, комунальні послуги.
- Мобільний додаток: Приват24, доступний для iOS і Android.
- Адаптивна версія сайту – доступна.

Особливі функції: Підтримка міжнародних переказів через Western Union та інші сервіси. Унікальна система кешбеку для платежів. Підтримка NFC-платежів через смартфони.

Для отримання кредиту необхідно відкрити картку *«Універсальна».*

Способи відкриття картки: 1) Миттєво відкрити віртуальну Digital картку в *Приват24* (вебверсія/додаток). 2)Замовити доставку пластикової картки через *Приват24*, а на наступний день після замовлення отримати її у відділенні «Нової Пошти» чи поштоматі.

Можливість відкриття депозитного рахунку онлайн у мобільному додатку *Приват24*/на веб-сайті. У мобільному додатку та на сайті доступні всі операції за вкладами. Є можливість навіть закривати вклад, що відкритий дистанційно в додатку Приват24 або на сайті. Для відкриття та керування вкладами у ПриватБанку є окремий застосунок – *Мої вклади.*

У *Sense bank* для отримання кредиту теж необхідно відкрити картку. Миттєве відкриття карткового рахунку та/або випуск цифрової картки без відвідування банку у мобільному додатку.

Можливість відкриття депозитного рахунку онлайн у мобільному додатку Sense SuperApp. У мобільному додатку доступні всі операції за вкладами. Мін. сума вкладу у разі відкриття вкладу в Sense SuperApp або в інтернет-банкінгу My Sense

Bank – 100 UAH, 20 USD, 20 EUR є нижчою ніж у разі відкриття вкладу у відділеннях – 1000 UAH, 200 USD, 200 EUR.

Депозити online для корпоративних клієнтів в обох банках дають змогу:

• миттєво розміщувати кошти на депозитному рахунку онлайн;

• дистанційно поповнювати чи знімати гроші з депозитного рахунку;

• контролювати в режимі реального часу залишки на рахунках.

Спектр депозитних послуг та їх наповненість в *ПриватБанку* та *Sense Bank* є майже однаковою, проте на сайті *Sense bank* не вказано чи можна відкрити строковий депозит онлайн.

Таблиця 2.2 – Наявність особливих послуг в ПриватБанку та Sense Bank

Послуга	***ПриватБанк***	***Sense bank***
Платежі за QR-кодом	+ *Умови: відкрити додаток, відсканувати код на квитанції, вибрати послуги та оплатити їх*	+ *Умови: через мобільний додаток просканувати код і оплатити*
Підтвердження документів без візиту в банк	+	+
Сервіс «Зібрати гроші»	-	+ *Умови: щоб зібрати кошти на подарунок тощо потрібно просто поділитись посиланням на збір або дати відсканувати QR-код.*
Персональний фінансовий помічник	-	+ *Умови: віртуальний помічник контролюватиме виконання будь-яких операцій*

Джерело:[23]

Зручність користування

ПриватБанк:

Інтерфейс: Приват24 – один із найбільш розвинених додатків в Україні. Він пропонує широкий функціонал, але інтерфейс може бути перевантаженим для нових користувачів.

Мобільний додаток: Високоякісний додаток із стабільною роботою.

Інтуїтивний дизайн, але іноді занадто багато кроків для виконання базових операцій.

Sense Bank :

Інтерфейс: Інтерфейс додатка менш розвинений порівняно з конкурентами. Можуть виникати труднощі з навігацією або пошуком потрібних функцій.

• Мобільний додаток: Працює стабільно, але інтерфейс виглядає застарілим. Функціональність достатня для базових операцій, але не вистачає деяких новітніх функцій, таких як кешбек чи інтеграція з сервісами NFC.

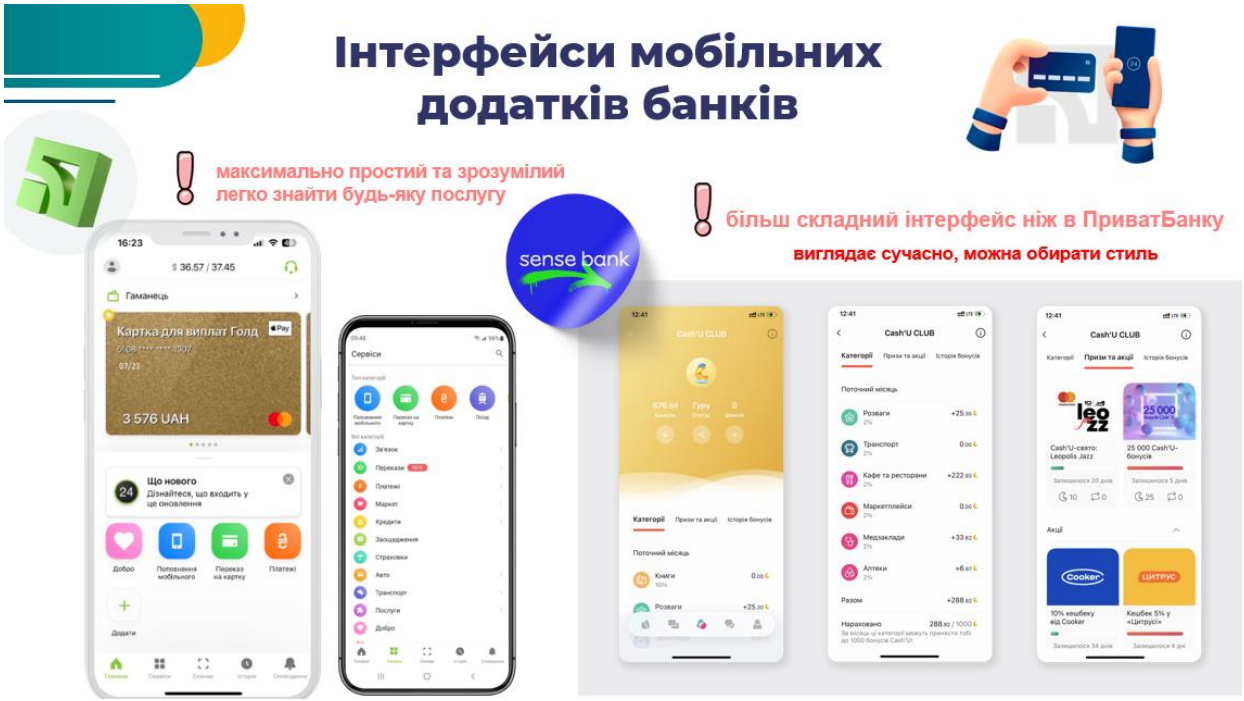

Рисунок 2.3 – Інтерфейси мобільних додатків ПриватБанку та Sense Bank

Джерело:[23]

Отже, ПриватБанк має такі переваги: більший набір послуг, добре розвинений мобільний додаток і сайт. Дистанційне банківське обслуговування ПриватБанку є достатньо зручним та комплексно наповненим. Існує можливість користування як веб-сайтом так і мобільним додатком.

Всі базові операції можна здійснити онлайн:

– будь-які перекази, в тому числі міжнародні;

– платежі;

– оформлення кредиту;

– відкриття депозиту;

– інформаційні послуги тощо.

ДБО наявне і для корпоративних клієнтів, що є вагомим фактором збільшення обсягу коштів.

Інтерфейс додатку є максимально простим та зрозумілим у користуванні.

Недоліки: Можливе перевантаження інтерфейсу та наявність зайвих функцій, які ускладнюють використання.

Рекомендації: Підходить для користувачів, яким потрібен широкий спектр послуг і високий рівень безпеки, але може бути складним для початківців.

Дистанційне банківське обслуговання ***Sense bank*** також відповідає всім вимогам сучасного цифровізованого суспільства.

В ДБО впроваджено багато інноваційних продуктів, які дають змогу насолоджуватись проведенням будь-яких операцій миттєво.

Наявний повний перелік операцій для здійснення онлайн: перекази, платежі, оформлення кредитів, відкриття депозитів, допомога віртуального помічника.

ДБО для корпоративних клієнтів існує на базі окремого додатку Sense Business Online, що робить послуги максимально орієнтованими.

Інтерфейс також є зручним та комфортним для користування.

Рекомендацією буде подальше вдосконалення та застосування інноваційних продуктів.

Оскільки боротьба за фінансове панування між фінтех та банками триває, важливо бути в курсі останніх подій та оцінити, які рішення найкраще задовольняють фінансові потреби клієнтів. Слід пам'ятати, що кожен сектор має свої сильні та слабкі сторони, і ключ до успіху полягає у знаходженні гармонійної синергії між ними для досягнення фінансового успіху.

Подорожуючи динамічним полем битви між фінтех і традиційним банкінгом, стає ясно, що інновації відіграють ключову роль у досягненні фінансового панування.

2.3 Аналіз ризиків цифрового банкінгу та визначення шляхів протидії їм

В даний час глобальна економіка загалом і банківська сфера зокрема переживає два найсильніші виклики: з одного боку, жорсткий вихід із постпандемійної кризи, з іншого боку, трансформація внаслідок п'ятої промислової революції, яка прискорилася після пандемії і характеризується ще більшою цифровізацією та широким впровадженням штучного інтелекту. Пандемія виклала важливий урок про те, що майбутнє – це не незначна зміна минулого. Тож треба чітко розуміти, що майбутні зміни не завжди можуть позитивно позначатися на діяльності банків.

Для ухвалення рішення про трансформацію банки повинні прорахувати всі ризики та зважити вигоди. Цифровізація здатна як збільшити традиційні банківські ризики, так і зменшити їх. У багатьох випадках для подолання ризиків відкриваються нові можливості, які стали можливими лише в епоху цифровізації.

Процентний ризик виникає через дві сновні причини: інтернет дозволяє залучати ширшу аудиторію, яка зацікавлена у більш вигідних для себе умовах (особливо процентні ставки), також йде розвиток онлайн-трейдингу. Даного ризику можна уникнути при повсюдному впровадженні відкритого інтернет-банкінгу. Цей ризик може так само супроводжуватись і фондовим ризиком. Він пов'язаний із розширенням інтернет-трейдингу і можливістю здійснювати операції в режимі реального часу одночасно на кількох майданчиках. Однак, інтернет-трейдинг залучає капітал фізичних та юридичних осіб.

Ризик ліквідності пов'язаний з тим, що клієнтам тепер доступно цілодобово здійснювати операції з переказу коштів, а це негативно позначається на волатильності депозитних рахунків, а також на контролі банком змін у депозитах та кредитах. Правовий ризик в основному залежить від країни, де знаходиться сам банк, та рівня правової бази, яка впроваджена у ній. Репутаційний ризик може виникнути при виникненні одного з перерахованих вище ризиків. Тобто, на будь-

якому етапі банк може з ним зіткнутися - чим більший рівень будь-якого ризику та нездатність банку з ним впоратися, тим більше буде виникатиме репутаційний ризик. Якщо представити всі ризиків банків за 100%, то частка кожного з найбільш поширених видів ризику зображена рисунком 2.4.

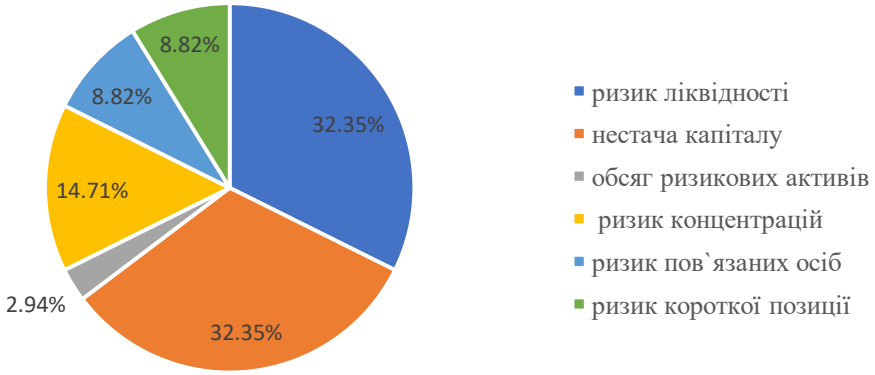

Рисунок 2.4 – Структура ключових ризиків банків станом на 1.01.2025р.

Джерело:[24]

Враховуючи, що чисельність банків доволі велика (рис.2.5), зрозуміло, що проблему управління ризиками ігнорувати неможливо.

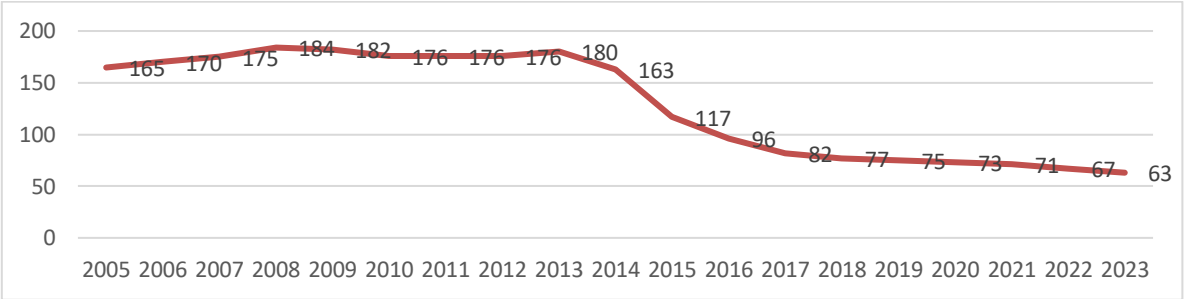

Рисунок 2.5 – Динаміка кількості діючих банків в Україні

Джерело:[24]

Відтак, в даний час банківська спільнота зазнає постійно зростаючої потреби протидіяти ризикам. І в цьому зв’язку очевидним стає тиск, пов'язаний з необхідністю відповідати вимогам регулятора, підтримувати високий рівень операційної ефективності та стабільності. Тож у банківському середовищі, що швидко розвивається, з'являються нові виклики, пов'язані з динамікою зовнішніх загроз, з'являються нові цифрові технології, блокчейн, а також нові види атак.

В умовах зростання кількості різноманітних комп'ютерних атак та кіберзлочинів, підвищеного інтересу злочинців до рахунків клієнтів та іншої конфіденційної інформації банки більше не можуть дозволити собі займатися інформаційною безпекою епізодично. Щоб забезпечити безпеку та захист інтелектуальної власності, коштів клієнтів й банків, конфіденційної клієнтської інформації та іншої інформації, що має важливе значення для ефективного ведення бізнесу, необхідно мати комплексну стратегію у сфері безпеки.

Аналіз статистики з кіберінцидентів показує, що найпоширенішим джерелом загроз є зовнішні суб'єкти (таблиця 2.3). До джерел загроз можна віднести нинішніх та колишніх співробітників компаній. Більшість навмисних кіберінцидентів викликані загрозою, що виходить із зовнішніх джерел.

Таблиця 2.3 – Структура кіберінцидентів по секторах у країнах Організації економічного співробітництва та розвитку (дані на кінець 2023 р.), %

Сектор / Інцидент	Фінанси й страхування	Інформаційні послуги	Освіта	Торгівля	Виробництво	інші
Інцидент з використанням шкідливих програм	19,4	12,0	6,5	6,4	5,3	50,4
Інцидент у сфері втрати особистих конфіденційних даних	28,3	5,0	3,1	4,9	2,0	56,7
IT-помилки впровадження та обробки	17,9	24,0	5,8	4,8	6,3	41,2

Джерело:[30]

Дійсно, фінансові установи, і в першу чергу – банки, у всьому світі є найбільш частими об'єктами кібератак. Банки працюють з грошовими коштами, і для кіберзлочинців, що атакують банки, є безліч способів отримання прибутку за рахунок вимагання, крадіжок та шахрайства. Регулятори впроваджують нові засоби контролю за кіберризиками. Боротьба з кіберзлочинністю передбачає великі фінансові витрати із боку фінансових установ. За оцінками експертів, банки витрачають утричі більше на кібербезпеку, ніж нефінансові інституції.

Оскільки для усунення кіберзагроз одних лише стимулів з боку приватного сектора може бути недостатньо (наприклад, компанії можуть не повною мірою

враховувати загальносистемні наслідки інцидентів), може знадобитися втручання держави і центрального банку, про що буде сказано в наступному параграфі даної роботи.

До кіберризиків відносяться (рисунок 2.6):

1. розкрадання коштів клієнтів банків,
2. фінансові втрати самого банку,
3. порушення надійності та безперервності надання фінансових послуг,
4. розвиток системної кризи всього банківського сектора через кібератаку, що вразила найбільші банки в системі.

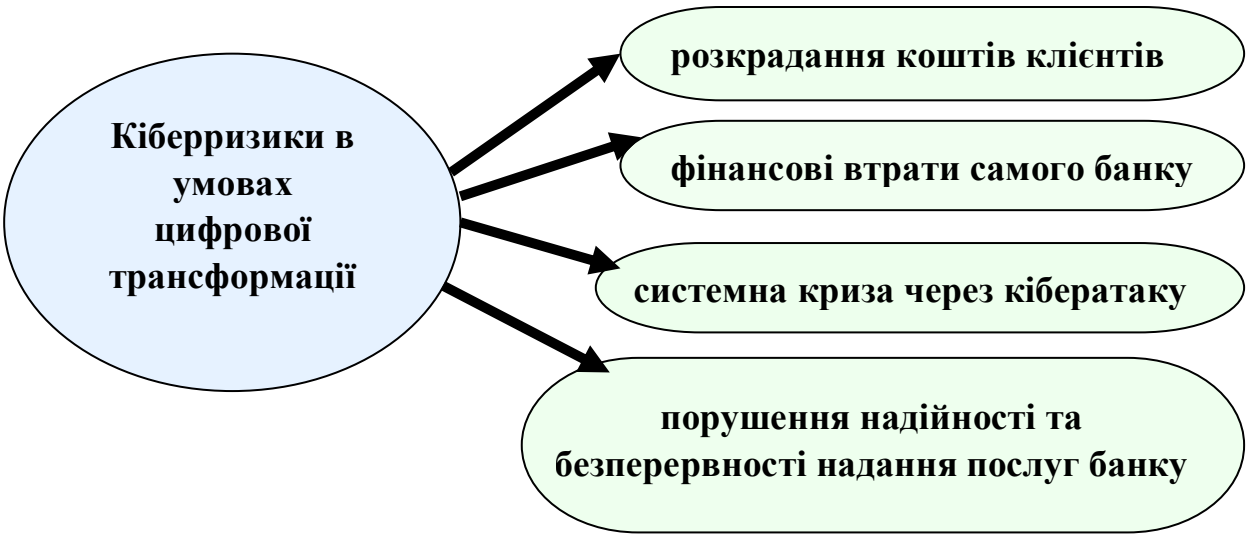

Рисунок 2.6 – Кіберризики в умовах цифрової трансформації

Джерело:складено автором самостійно на основі [17,31,36]

Щоб кіберризики не призводили до таких серйозних наслідків, центральний банк стежить за кіберстійкістю усіх фінансових організацій, попереджає їх про можливі нові типи атак і способи реагування на них.

Поширеність кіберінцидентів із внутрішнім джерелом у фінансовому секторі (13 %) близька до середньої (11 %) по всіх секторах і менше, ніж у секторах економіки, функціонування яких також передбачає обробку великих обсягів конфіденційних даних (комунальні послуги – 27%, охорона здоров'я – 25%, державне управління – 18%, транспорт – 16%). Найменша питома вага

кіберінцидентів від внутрішніх джерел фіксується у сферах будівництва – 12 % й роздрібної торгівлі – 11%.

Особливості цифровізації у банківському секторі та характерних ризиків ілюструє таблиця 2.4.

Таблиця 2.4 – Особливості цифровізації у банківському секторі та характерних ризиків

Особливості процесу цифровізації у банківському секторі	Особливості ризиків цифровізації банківських послуг
процес цифровізації зачіпає не окремі галузі чи напрями діяльності банків, а всю систему банківських відносин	ризики виявляються більш масштабно
готовність до швидкої зміни технологій та активне впровадження інновацій	можливість постійного вдосконалення та доопрацювання систем інформаційної безпеки, з урахуванням нових даних
безготівковий та бездокументарний характер більшості операцій, що не потребує фізичного переміщення, швидкий перехід на надання більшої частини продуктів (послуг) через цифрові канали	банки – основні об'єкти кібератак та загроз; високий рівень фінансових втрат під час реалізації загрози
зростаюча фінансова та цифрова грамотність споживачів банківських продуктів (послуг)	зростання особистого ризику клієнта-фізичної особи за відсутності у нього необхідних фінансових та цифрових компетенцій
активне використання інноваційних технологій як інструмент забезпечення конкурентоспроможності	суттєвість стратегічних ризиків у разі усунення пріоритету діяльності банку на швидкий результат від діджиталізації
відсутність консервативного підходу до інновацій у значної частини персоналу банку	зростання ризиків, що походять від внутрішніх джерел
традиційно велика кількість даних, які вимагають зберігання, обробки, аналізу для покращення клієнтського досвіду	вищий рівень витрат на інформаційну безпеку

Джерело:складено автором на основі [36,39,40]

Виділимо основні тренди щодо злочинної діяльності в сфері цифрового банкінгу.

Перший тренд – нефінансова мотивація злочинців. Раніше основною мотивацією для більшості організованих злочинних угруповань було фінансове. Однак зараз слід зазначити, що наразі з'явилися нефінансово мотивовані угруповання, основне завдання яких — кібершпигунство банківської галузі (отримання інформації про фінансову еліту країни, VIP-клієнти, платежі держкомпаній).

Другий тренд – зростання диверсійних атак. Якщо раніше зловмисники обмежувалися лише крадіжкою коштів, нині після шпигунства чи розкрадання виробляється диверсія з метою знищення інфраструктури та доказової бази. У результаті банки змушені займатися відновленням роботи інфраструктури, а не розслідуванням інцидентів.

Третій тренд – нові способи фішингу. Банки повинні використовувати віддалену ідентифікацію клієнта, що ідентифікує шкідливе програмне забезпечення.

Четвертий тренд — слабка налагодженість міжнародної співпраці. Це велика проблема, тому що угруповання цим користуються, обираючи країни, що конфліктують.

В цілому очевидно, що банки сильно недофінансували свою інформаційну безпеку, і сьогодні робота ведеться на початковій стадії розвитку інформаційної безпеки в цій галузі. У зв'язку з цим у фінансовому секторі необхідний інформаційний обмін, необхідно підтягувати один одного в освітньому значенні системою вірусів, ділитися інформацією.

Практично всі перевірки, які зараз проводить НБУ, включають і перевірку з точки зору виконання вимог і нормативних документів Банку в галузі інформаційної безпеки. І на сьогоднішній день немає жодного банку, що повністю відповідає всім вимогам.

Єдиний спосіб боротьби з новими видами кібератак – це інформаційний обмін. Інформаційний обмін важливий не лише всередині країни, а й за межами

Отже, щоб запобігти значним фінансовим втратам і репутаційним збиткам, банківським установам необхідно запровадити низку дій. Нижче наведено кроки, які необхідно зробити, щоб протидіяти ризикам, які супутні цифровому банкінгу, та уникнути загроз для банку:

• Оцінити поточні заходи безпеки. Ознайомитися з основними загрозами кібербезпеки та з'ясувати, чи є у тактиці банку слабкі місця.

• Делегувати послуги із забезпечення кібербезпеки стороннім партнерам. Це допоможе усунути розрив у рівні кваліфікації та забезпечити необхідний захист.

• Використовувати багатофакторну аутентифікацію. Така форма аутентифікації означає, що користувач отримає доступ до своїх даних лише у тому випадку, якщо він зможе назвати два або більше облікових даних. Таким чином, навіть якщо зловмисники викрадуть реєстраційні дані клієнтів банку, буде забезпечено додатковий рівень безпеки, який не дозволить їм отримати доступ до даних клієнтів.

• Навчити персонал. Розказати співробітникам про наявні загрози та ризики та пояснити, як їх розпізнати. Таке навчання має бути регулярним, щоб не пропустити важливих змін.

• Інформувати клієнтів про способи розкрадання їхньої особистої інформації та грошей, що використовуються кіберзловмисниками. Таким чином, їм буде легше не потрапити на хитрощі.

• Подумати про кіберстрахування. Кіберстрахування є обов'язковим елементом всього плану забезпечення кібербезпеки. Воно дозволить банку бути впевненим у фінансовій безпеці у разі кібератаки. Воно дозволить стримати судові витрати, поінформувати клієнтів про порушення, а також допоможе компанії покрити витрати на ремонт пошкоджених систем та відновлення даних. Наразі кіберстрахування потрапляє під визначення пункту 23 статті 6 №85/96-ВР «інші види добровільного страхування».

Зупинимось на пункті кіберстрахування детальніше, бо бачимо в цьому напрямку суттєві перспективи. Почнемо з того, що поліси кіберстрахування як страхові продукти для захисту бізнесу не мають уніфікованих характеристик. Створення єдиних стандартів для такого продукту ще не відбулось. Але застрахувати можна збитки, що настануть в результаті таких інцидентів:

– Технічні збої, помилки програмування та відмови роботи IT-систем;

– Нецільові атаки – фішинг, картинг, хактивізм:

– Цільові (таргетовані) атаки – DdoS атаки, промислове шпигунство, кріптолокерство (кіберздирництво);

– Внутрішні атаки – викрадення конфіденційної інформації та відомостей, що являють собою комерційну таємницю, сприяння зовнішнім атакам зсередини.

Розглянемо, у чому полягають особливості укладення договору кіберстрахування.

У зв'язку з відсутністю законодавчого регулювання сфери кіберстрахування в Україні, основою для встановлення регламентів, прав та зобов'язань між страхувальником та страховиком, а також для можливого вирішення спорів є договір кіберстрахування. Як у світі, так і в Україні, зокрема, поступово зростає обсяг виплат за такими договорами. А це своєю чергою підвищує рівень довіри страхувальників до послуги кіберстрахування як такої. Так, лише за 2021-22рр. лише за ризиками, пов'язаними з вірусами-вимагачами, обсяг страхових виплат у світі збільшився у 4 рази [40].

Щоб отримати за настанням страхового випадку страхову виплату в адекватному обсязі, потрібно достатньо ретельно проаналізувати договір зі страховою компанією. Зокрема, іноді страховики задовольняють попит компаній на дане покриття через пропозицію додаткових розширень у договорах страхування майна та відповідальності. Але покриття за кіберризиками у таких договорах, з огляду на специфіку даних видів страхування, досить обмежене. Отже, бажано закріплювати правовідносини зі страхування кіберризиків окремим договором.

У сучасних умовах страхові компанії швидко змінюються. Наразі швидко розвивається InsurTech, що передбачає технології машинного навчання та передові розробки у сфері кібербезпеки, технологію блокчейн та аналіз великих даних. Це дозволяє формувати для споживачів справді актуальні продукти зі страхування кіберризиків.

Проте страхувальникам зі свого боку теж потрібно чітко усвідомлювати, якого саме покриття вони очікують за договором. Як правило, розробляється договір кіберстрахування з індивідуальними умовами на основі побажань клієнта та специфіки його бізнесу.

Аналізуючи актуальні пропозиції від українських страховиків, можна говорити про можливість включення до договору основного та додаткового покриття.

Основне покриття може охоплювати:

– реагування на кіберінцидент: компенсацію витрат на послуги експертів безпосередньо для припинення кібератаки;

– відшкодування втраченого прибутку внаслідок порушення IT-інфраструктури банку, знищення та/або крадіжки даних, тимчасової зупинки в роботі банку після кібератаки;

– викупну суму, сплачену вимагачам за дешифрування заблокованої інформації;

– судові витрати, зокрема – задоволення позовних вимог від третіх осіб, які зазнали збитків внаслідок інциденту.

Додаткове покриття може передбачати:

– компенсацію витрат на розслідування інциденту та проведення експертиз – технічної та юридичної для виявлення причин атаки та оцінки масштабів завданої шкоди;

– антикризовий PR та відновлення репутації після кібератаки;

– відновлення втрачених чи пошкоджених внаслідок інциденту електронних даних;

– покриття штрафних санкцій, які ймовірно накладено державою за недотримання банком вимог закону щодо здачі звітності.

У майбутньому типи загроз залишаться незмінними. Компанії стикатимуться з шифрувальниками, троянами, програмами-вимагачами та DDoS-атаками. Однак хакери використовуватимуть ці інструменти інтенсивніше. Поширення AI дозволить їм створювати нові віруси, шукати вразливості у ПЗ, генерувати фішингові сайти та підроблені сторінки.

Важливо сказати, що до глобальних завдань центрального банку і регулюючих органів має увійти створення національної стратегії кібербезпеки для

всього банківського сектора. Це дозволить банкам легше протистояти кіберзагрозам.

2.4 Розвиток завдань центрального банку і напрямків регуляторного контролю в умовах інтенсивної цифровізації банків

Зростання ступеня цифровізації та посилення геополітичної напруженості мають на увазі, що ризик кібератаки з системними наслідками зріс. Як вже зазначено нами у попередньому розділі, ризик екстремальних втрат від інцидентів у кіберсфері зростає. Такі втрати потенційно можуть спричинити проблеми з фінансуванням для банків і навіть поставити під загрозу їхню платоспроможність. Інциденти у банківському секторі можуть становити загрозу для фінансової та економічної стабільності, якщо вони підривають довіру до фінансової системи, порушують процеси надання критично важливих послуг або викликають вторинні ефекти в інших організаціях.

Наприклад, серйозний інцидент у банківській установі може підірвати довіру до неї, а в крайніх випадках призвести до обвалу на ринку і масового вилучення вкладів із банків. Незважаючи на те, що досі не відбулося жодного значного масового вилучення вкладів у результаті кіберінцидентів, невеликі банки США, як показує аналіз, відзначали помірний та досить стійкий відтік вкладів після кібератак.

Кіберінциденти, які порушують надання критично важливих послуг, таких як платіжні мережі, можуть серйозно вплинути на економічну активність. Наприклад, атака на Центральний банк Лесото, що відбулася в грудні 2023р., дестабілізувала роботу національної платіжної системи країни, порушивши проведення операцій місцевими банками.

Згідно з проведеним МВФ опитуванням центральних банків і наглядових органів, основи політики кібербезпеки – особливо в країнах з ринком, що

формується, і країнах, що розвиваються, – як і раніше, нерідко недосконалі. Так лише близько половини опитаних країн мали національну стратегію кібербезпеки, орієнтовану на банківський сектор, або спеціальні нормативні акти, що регламентують питання кібербезпеки.

При цьому, досить великий відсоток атак, що відбуваються у світі, фінансується на державному рівні [40]. Це серйозний аспект, бо вкладаються великі інвестиції. Прихід державних грошей у сферу інформаційних нападів викликає побоювання у фінансового сектора, оскільки у державних структур зовсім інші цілі, вони зовсім по-іншому працюють, вони мають зовсім інші метрики роботи.

Для підвищення стійкості банківського сектора органам влади слід розробити адекватну національну стратегію кібербезпеки, поряд з ефективним регулюванням та наглядовим потенціалом, який має охоплювати такі елементи:

– періодичну оцінку сфери кібербезпеки та виявлення потенційних системних ризиків, зумовлених взаємопов'язаністю та концентрацією, у тому числі з боку сторонніх постачальників послуг;

– заохочення «кіберзрілості» серед банків, включаючи доступ до експертних знань у галузі кібербезпеки на рівні керівництва компаній;

– поліпшення кібергігієни банків, їх онлайн-безпеки та працездатності системи (захист від шкідливих програм та багатофакторна автентифікація), а також навчання та обізнаність.

Оскільки джерела атак нерідко розташовуються за межами країни походження банку, а доходи можуть спрямовуватись через кордони, для успішного усунення кіберзагроз необхідне міжнародне співробітництво.

Незважаючи на те, що кіберінциденти відбуватимуться і надалі, фінансовому сектору необхідні можливості для надання критично важливих бізнес-послуг під час таких збоїв. Для цього фінансовим компаніям слід розробляти та тестувати процедури реагування та відновлення, а національним органам слід мати ефективні протоколи реагування та механізми антикризового управління.МВФ активно допомагає державам-членам зміцнювати свої системи кібербезпеки через надання консультацій з питань економічної політики, наприклад, у рамках

Програми оцінки фінансового сектора, а також за допомогою заходів щодо розвитку потенціалу.

Як виявлено, 9 представників центробанків з розвинутих країн та 12 – з тих, що розвиваються, відповіли, що найпоширенішим типом атаки вважають фішинг та інші форми соціальної інженерії (рис. 2.7).

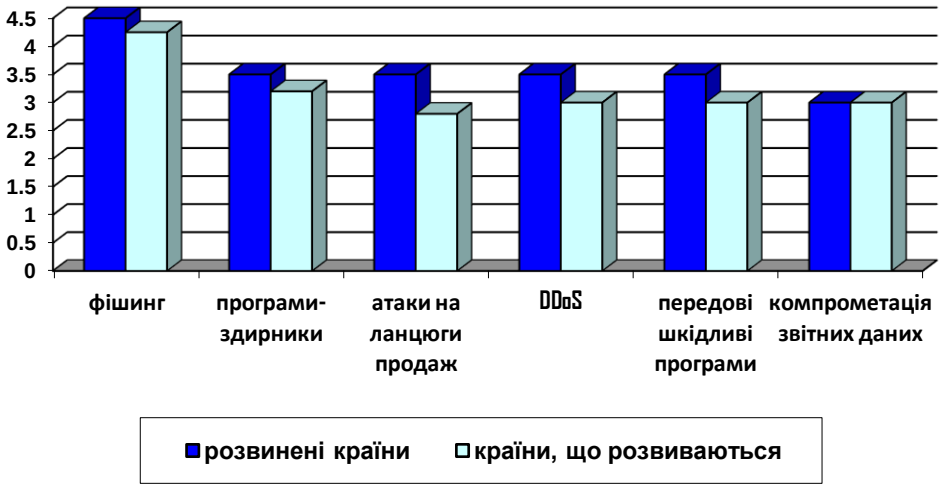

Рисунок 2.7 – Вірогідність інцидентів в сфері інформаційної безпеки й кіберзахисту банків (від 1 – вкрай низька до 5 – максимальна), станом на кінець 2022р.

Джерело: [1]

При цьому, у розвинутих країнах центробанки доволі сильно стурбовані атаками на банки – і, відповідно, вище оцінюють пов'язані з ними витрати. При цьому з найбільшими витратами, на думку центральних банків, пов'язані атаки з використанням шкідливого програмного забезпечення (як навмисні атаки на IT-інфраструктуру, так і ненавмисні інциденти). Більшість опитаних центробанків у відповідь на загрози кібербезпеці нарощують IT-бюджети: понад 60% центробанків розвинених країн і близько 50% у країнах, що розвиваються, з 2020 року збільшили бюджет на IT-інфраструктуру на 5–20%, ще близько чверті центробанків країн, що розвиваються, збільшили бюджети більш як на 20%, що ілюструє рис. 2.8.

Для протидії згаданим загрозам фінансові установи мають вибудовувати багаторівневу систему захисту, що охоплює всі технології, процеси та персонал. Ключові принципи кіберзахисту фінансового сектора сформулюємо таким чином:

— багаторівневий захист (defense-in-depth);

— постійний моніторинг і виявлення інцидентів;

— надійна аутентифікація та управління доступом;

— управління вразливостями та оновлення;

— управління інцидентами та забезпечення безперервності бізнесу;

— відповідність міжнародним та вітчизняним стандартам і регуляціям;

— навчання персоналу та підвищення культури безпеки.

Рисунок 2.8 – Зростання витрат центральних банків на інформаційну безпеку та сферу кіберзахисту (%), станом на кінець 2022р.

Джерело: [1]

Враховуючи актуальні виклики у сфері інформаційної безпеки в умовах інтенсивної цифровізації НБУ передбачає:

– захист прав споживачів фінансових послуг та підвищення рівня довіри до цифрових технологій,

– створення умов для безпечного впровадження цифрових та платіжних технологій та забезпечення технологічного суверенітету,

– забезпечення контролю за ризиками інформаційної безпеки, операційної надійності для безперервності надання банківських та фінансових послуг.

Ефективна система кібербезпеки повинна не лише запобігати вторгненням, а й вчасно їх виявляти і для цього фінансові установи мають розгортати центри моніторингу безпеки (SOC), оснащені SIEM-системами, які збирають логи з усіх критичних систем та в режимі реального часу аналізують їх на предмет підозрілих інцидентів. Водночас, важливо вести журнали реєстрації подій (лог-файли) на всіх вузлах і зберігати їх достатньо довго, утім, за даними опитувань, лише близько 15% українських підприємств загалом займаються повноцінним веденням логів безпеки [32], що вказує на прогалини у можливостях виявлення кіберінцидентів (рис. 2.9).

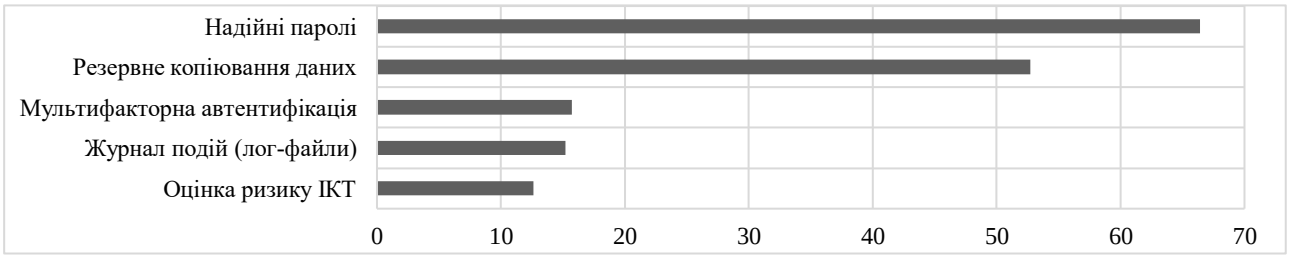

Рисунок 2.9 – Частка українських банків, що впроваджують окремі заходи кібербезпеки (2023 р.), %

Джерело: [54]

Завдання забезпечення інформаційної безпеки та кіберстійкості з метою фінансової стабільності кожного банку може виконуватися завдяки:

– сформованим пропорційним регуляторним вимогам щодо захисту інформації при наданні банківських послуг, здійсненні діяльності у сфері фінансових ринків, здійсненні переказів коштів у платіжній системі НБУ;

– організованому наглядовому процесу з питань захисту інформації, здійсненням на системній основі дистанційного та контактного нагляду;

– методології, згідно якої на регулярній основі проводяться кібернавчання.

Завдання забезпечення операційної надійності та безперервності діяльності банків виконуються за допомогою:

– сформованих пропорційних регуляторних вимог для всіх піднаглядових організацій кредитно-фінансової сфери;

– інтегрованості питань операційної надійності у питання управління операційним ризиком.

Завдання протидії комп'ютерним атакам при використанні інноваційних фінансових технологій будуються навколо потреби протидіяти кіберзлочинам.

Вибір цілей кіберзлочинців обумовлений технічною підготовкою, наявними інструментарієм і знаннями про внутрішні процеси банку [36]. При цьому, як правило, основним фактором таргетованої атаки на банк є слабкий захист інформаційних систем.

Типова схема таргетованої кібератаки на банківську установу складається з наступних етапів:

- здійснюється масове розсилання листів на e-mail адреси працівників банку, в яких міститься шкідливе програмне забезпечення;

- при відкритті листа працівником банку відбувається процес впровадження шкідливого програмного забезпечення, після чого зловмисник отримує доступ до зараженого комп'ютера;

- атакуючий проводить дослідження доступних із зараженого комп'ютера сегментів локальної мережі банку та встановлює доступ до контролера домену з метою отримання паролів адміністраторів;

- після отримання доступу до контролера домену і паролів адміністратора мережі кіберзлочинець заходить у мережу банку;

- на банкоматах встановлюється шкідливе програмне забезпечення, що забезпечує видачу фінансової готівки за допомогою віддаленої команди.

Далі після встановлення контролю над банкоматом до процесу підключаються співучасники, які займаються отриманням коштів. Їхнє завдання – безпосередня присутність у підконтрольного банкомату в певний час для

отримання грошей. Після успішного вилучення готівки шкідливе програмне забезпечення, як правило, з банкоматів деінсталюється [36].

Також необхідно згадати і таку діяльність зловмисників, як соціальна інженерія – одну з головних загроз кібербезпеці. Соціальна інженерія – це методи психологічної маніпуляції людиною, створені задля змусити жертву виконати певні дії на користь атакуючого. Необхідно пам'ятати, що працівник банку, як користувач, є однією з ланок інформаційної системи, оскільки має певні привілеї, здійснює різні операції у процесі виконання трудових операцій. Також необхідно чітко уявляти, що ступінь захищеності інформаційної системи в банку вимірюється захищеністю її найслабшої ланки. Потенційно цією ланкою якраз і може бути користувач (наприклад, розчарований заробітною платою системний адміністратор або працівник відділу кадрів, що посварився з керівником). Масу корисної інформації для здійснення таргетованої кібератаки зловмисник може отримати зі спілкування зі співробітниками банківської організації та з відкритих джерел, при цьому не вдаючись до допомоги шкідливого програмного забезпечення та інших технічних засобів.

Для успішного запобігання кібератакам на банківські установи необхідно виконання фінансовими установами наступних заходів:

– використання відповідних апаратних, програмних та програмно-апаратних комплексів засобів захисту інформації;

– постійний моніторинг подій безпеки;

– підвищення кваліфікації працівників, які відповідають за інформаційну безпеку;

– навчання працівників банків основ інформаційної безпеки;

– підтримка здорового клімату в колективі (задоволений працівник з меншою часткою ймовірності усвідомлено нашкодить банку, де працює);

– інформування та навчання клієнтів банків фінансової та цифрової грамотності;

– розробка пакету нормативної документації, що регламентує сферу інформаційної безпеки у банку;

– скрупульозний підбір персоналу до банків з урахуванням їх професійних, моральних та моральних якостей;

– взаємодія та обмін інформацією про кібератаки між банками та правоохоронними органами.

Успіх у боротьбі з кіберзагрозами можна досягти у випадку комплексного підходу.

Щоб бути на крок попереду хакерів, потрібна актуальна зведена інформація про їх методики та сценарії.

Кібербезпека має безліч різних аспектів:

– Архітектурні уразливості.

– Захищеність мережі та сайту.

– Належне зберігання конфіденційних та персональних даних

– Безпека паролів та розмежування рівнів доступу всередині інфраструктури.

– Правила інформаційної безпеки співробітникам.

– Готовність до DDoS-атак.

У 2025 році Національний банк України запланував провести перевірки з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг у шести банках. Як повідомляє прес-служба НБУ, в першому кварталі перевірку проведуть у "Креді Агріколь Банку", у другому – в "Райффайзен Банку", у третьому перевірять банк "Південний" та "Банк Кредит Дніпро", а в четвертому – "Комінбанк" та "Альтбанк".

План перевірок сформували на основі ризик-орієнтованого підходу, враховуючи наявну в НБУ інформацію про факти, події та обставини роботи банків, особливості їх функціонування, характер та обсяги надання банківських та фінансових послуг. Це сприятиме вдосконаленню банками власних можливостей

щодо реагування на сучасні кіберзагрози, а також зміцненню кіберстійкості як банків, зокрема, так і банківської системи в цілому.

Також в 2025р. Національний банк пропонує оновити деякі норми, що стосуються функціонування системи кіберзахисту та контролю за станом інформаційної безпеки і кіберзахисту в банківській системі України. Зокрема, передбачається удосконалити процес щорічного звітування банками за результатами проведеної самооцінки процесів організації й забезпечення інформаційної безпеки та кіберзахисту.

Також пропонується врегулювати порядок інформування банками Національного банку про значні кіберінциденти та істотні зміни в організації інформаційної безпеки та кіберзахисту. Відповідні норми містить проєкт постанови Правління Національного банку "Про затвердження змін до деяких нормативно-правових актів Національного банку України з питань інформаційної безпеки та кіберзахисту".

Відповідно, буде внесено наступні зміни до:

1) Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг, що затверджено постановою Правління Національного банку України від 16 січня 2021 року № 4, зокрема у частині: вдосконалення процедури проведення банками регулярної самооцінки процесів організації та забезпечення інформаційної безпеки / кіберзахисту і подання Національному банку України результатів такої самооцінки у вигляді звітів; впровадження обов'язкового інформування банками Національного банку України про істотні зміни в організації заходів з інформаційної безпеки та кіберзахисту в банках;

2) Положення про організацію кіберзахисту в банківській системі України, що затверджено постановою Правління Національного банку України від 12 серпня 2022 року № 178, зокрема у частині впровадження обов'язкового інформування банками Національного банку про значні кіберінциденти.

Отже, прийняття постанови Правління сприятиме виконанню Національним банком України його функцій, встановлених пунктом 6 статті 8 Закону України

“Про основні засади забезпечення кібербезпеки України”, пунктом 32 статті 7 Закону України “Про Національний банк України”.

Підкреслимо необхідність централізованого підходу при вирішенні зростаючих проблем кібербезпеки. Такий підхід повинен включати координацію реагування на загрози на галузевому рівні, а також аналіз можливих ланцюжків подій, які можуть призвести до фатальних наслідків.

ВИСНОВКИ

На основі проведеного дослідження можемо зробити наступні висновки.

Вітчизняний сегмент дистанційних банківських технологій перебуває в активній стадії розвитку, удосконалюються технології взаємодії учасників, спрямовані на зниження ризиків, підвищення ефективності операцій, що здійснюються, а також на захист персональних даних клієнтів у цифровій інфраструктурі.

Цифрова трансформація є ключовим компонентом загальної стратегії трансформації банківського бізнесу. Проте не слід фетишизувати її роль, вона не є єдиним чинником успіху, але багато в чому визначає результат будь-якого проекту трансформації. Правильно обрані технології в поєднанні з компетенціями співробітників, процесами та операціями дозволяють банкам швидко адаптуватися до складних ситуацій, використовувати перспективні можливості, задовольняти нові потреби клієнтів, що змінюються, стимулювати зростання і впроваджувати інновації – найчастіше несподіваними способами.

Для того, щоб банк вважався постачальником цифрового банкінгу, він повинен пропонувати:

Повний спектр всіх послуг: необхідно реалізувати повний спектр послуг, включаючи всі процеси від реєстрації нових роздрібних та корпоративних клієнтів до віддаленого надання всіх послуг фронт-офісу, як фінансових, так і нефінансових у віддаленому режимі.

Доступність послуг 24x7: доступність послуг 24 години на добу 7 днів на тиждень. Клієнти не повинні бути обмежені годинами роботи банку, вони повинні мати можливість отримувати послуги у будь-який час.

Послуги поза рамками традиційного банківського обслуговування: щоб відповідати новому цифровому стилю життя, необхідно впроваджувати нові послуги, такі як геоконтекстна реклама, гейміфікація, управління особистими фінансами, а також прогнозний аналіз на основі поведінки клієнтів.

Уніфіковані шляхи клієнта: правильна платформа цифрового банкінгу повинна забезпечувати клієнтам одноманітний клієнтський досвід у всіх каналах обслуговування, незалежно від того, який клієнт використовує в різних випадках. Це означає, що банк повинний постійно тримати клієнта в центрі уваги, надаючи йому персональні повідомлення та єдине джерело для оперативного доступу до інформації.

Інтуїтивно зрозумілий досвід користувача (UX): мета UX – створити цифровий фінансовий сервіс, що відповідає потребам користувачів, який пропонує прості та зручні у використанні можливості банківського обслуговування.

Привабливий інтерфейс (UI): інноваційний і привабливий дизайн інтерфейсу в цифрових продуктах дійсно необхідна, але недостатня умова. Інтерфейс користувача повинен бути орієнтований на користувача. Це означає, що його технологія повинна здійснюватися з розумінням того, чого клієнт хоче як користувач і чого він очікує від продукту.

Ефективні сервіси: час має велике значення, адже що менше часу чи дій потрібно користувачеві виконання будь-якої операції, краще. Відповідно, необхідно скоротити кількість дій користувача, у цьому випадку «менше означає більше». Розробляйте максимально зрозумілі рішення, що вимагають мінімуму дій від користувача.

Автором відзначені актуальні тренди вдосконалення дистанційного банківського обслуговування в Україні:

– Технологічний прогрес та розвиток інформаційних технологій, у тому числі безпечних та зручних способів оплати онлайн.

– Зростання кількості користувачів Інтернету та мобільних пристроїв, що дозволяє банкам розширяти свою клієнтську базу та забезпечити ширший спектр дистанційних послуг.

– Прагнення банків до скорочення витрат обслуговування клієнтів і підвищення ефективності роботи.

– Конкуренція між банками, обумовлена наявністю великої кількості гравців на ринку, які намагаються запропонувати клієнтам найпривабливіші умови та послуги.

В Україні дистанційне банківське обслуговування активно розвивається останні роки, банки пропонують своїм клієнтам нові послуги починаючи з оплати комунальних послуг, купівлі квитків на транспорт і закінчуючи інвестуванням в акції та облігації. Як результат – дедалі більше громадян обирають саме дистанційне обслуговування замість відвідин відділень банків у реальному часі.

Загалом, на фінансовому ринку відбуваються суттєві зміни, пов'язані із застосуванням нових інноваційних технологій та цифровими екосистемами у діяльності фінансових суб'єктів. При цьому цифрові екосистеми, які раніше не мали відношення до фінансового сектору, тепер беруть активну участь у ньому як самостійно, так і через партнерства.

Підкреслимо необхідність централізованого підходу при вирішенні зростаючих проблем кібербезпеки. Такий підхід повинен включати координацію реагування на загрози на галузевому рівні, а також аналіз можливих ланцюжків подій, які можуть призвести до фатальних наслідків.

В цілому ми прийшли до висновку, що змінюються способи, час та місце надання фінансових послуг та продуктів, формуються нові умови взаємодії банків та фінтех-компаній та їх клієнтів. В результаті з'являється велика кількість бізнес-моделей, що потребує знаходження правильного балансу між збереженням фінансової стабільності та захистом споживачів, залишаючи місце для інновацій.

Важливо, щоб керівники банків постійно переоцінювали нинішні моделі навчання персоналу, щоб знання, навички та інструменти залишалися актуальними та ефективними в галузі нагляду за новими технологіями та інноваційними бізнес-моделями.

Оскільки боротьба за фінансове панування між фінтех та банками триває, важливо бути в курсі останніх подій та оцінити, які рішення найкраще задовольняють фінансові потреби клієнтів. Слід пам'ятати, що кожен сектор має

свої сильні та слабкі сторони, і ключ до успіху полягає у знаходженні гармонійної синергії між ними для досягнення фінансового успіху.

Подорожуючи динамічним полем битви між фінтех і традиційним банкінгом, стає ясно, що інновації відіграють ключову роль у досягненні фінансового панування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Білошапка В., Охрименко І., Чуб П. Регуляторний контроль за інформаційною та кібербезпекою банків в умовах інтенсивної цифровізації. *Наука і техніка сьогодні (серія Економіка).* 2022. №14(14). С.96-110. URL: https://doi.org/10.52058/2786-6025-2022-14(14)-96-109.(Дата звернення: 26.01.2025).

2. Чуб П., Охрименко І., Білошапка В. Стан та перспективи розвитку необанків України. *Наукові перспективи*. 2023. №1(31). С.405-420. URL: https://doi.org/10.52058/2708-7530-2023-1(31)-405-421.(Дата звернення: 26.01.2025).

3. Стратегія розвитку фінансового сектору України до 2025 року. Національний банк України. URL: https://bank.gov.ua/admin_uploads/article/Strategy_FS_2025.pdf?v=4. (Дата звернення: 27.01.2025).

4. Стратегія розвитку фінтеху в Україні до 2025 року. Національний банк України. URL: https://bank.gov.ua/ua/files/DDWIAwXTdqjdClp. (Дата звернення: 27.01.2025).

5. Лобозинська С.М., Скоморович І.Г., Владичин У.В. Діяльність необанків на ринку фінансових послуг в Україні та світі. *Фінансовий простір*, №3 (43), 2021.

6. Іршак О.С., Творидло О.І. Розвиток необанків в Україні. Фінансовий простір, 2021, № 3 (43). URL:https://economyandsociety.in.ua/index.php/journal/article/view/1135. (Дата звернення: 27.01.2025).

7. Маркевич К. Необанки vs традиційні банки: як необанки змінюють фінансову систему. URL: https://razumkov.org.ua/statti/neobanky-vs-tradytsiini-banky-iak-neobankyzminiuiut-finansovu-systemy#a4. (Дата звернення: 27.01.2025).

8. Кіберризики: оцінка центральних банків. URL: https://www.bis.org/ijcb.htm?m=1012. (Дата звернення: 28.01.2025).

9. What is Agile Software Development? [Electronic resource] / Agile Alliance. — Available at : https://www. Agilealliance.org/agile101. (Дата звернення: 28.01.2025).

10. Лавренюк В.В. Ключові драйвери кібер-ризиків фінансових установ. Сучасні гроші, банківські послуги та фінансові інновації в цифровій економіці: матеріали наук.-практ. інтерн. конф. студ. аспір. і молод. вчених. Дніпро: Середняк Т. К., 2021, с. 297-299.

11. Охрименко І.Б., Шуляк Д.А. Актуальність цифровізації страхового бізнесу на тлі сучасних соціально-економічних і геополітичних викликів. Наукові перспективи: журнал. 2022. № 8(26) 2022. С. 186-199. URL: http://perspectives.pp.ua/index.php/np/article/view/2374 .(Дата звернення: 29.01.2025).

12. Соснін О. Цифровізація як нова реальність України. Lex. Inform. URL: https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny/. (Дата звернення: 29.01.2025).

13. Безпека банківських систем : навч. посіб. / П. С. Усік, К. О. Буравченко; М-во освіти і науки України, Центральноукр. нац. техн. ун-т. Кропивницький: ЦНТУ, 2022. 194 с.

14. Financial Sector's Cybersecurity: A Regulatory Digest. The World Bank Group. 2017. URL: https://pubdocs.worldbank.org. (Дата звернення: 29.01.2025).

15. Cyber resilience oversight expectations for financial market infrastructures. European Central Bank. 2018. URL: https://www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr181203_1.en.html. (Дата звернення: 28.01.2025).

16. ESG Research Report: Technology Perspectives from Cybersecurity Professionals. URL: https://www.esg-global.com/research/topic/issa. (Дата звернення: 28.01.2025).

17. Лобозинська С.М., Скоморович І.Г., Владичин У.В. Діяльність необанків на ринку фінансових послуг в Україні та світі. *Фінансовий простір*, № 3 (43), 2021.

18. Іршак О.С., Творидло О.І. Розвиток необанків в Україні. *Фінансовий простір,* 2021, № 3 (43). URL:

https://economyandsociety.in.ua/index.php/journal/article/view/1135.(Дата звернення: 30.01.2025).

19. Маркевич К. Необанки vs традиційні банки: як необанки змінюють фінансову систему. URL: https://razumkov.org.ua/statti/neobanky-vs-tradytsiini-banky-iak-neobanky-zminiuiut-finansovu-systemy#a4.(Дата звернення: 30.01.2025).

20. Гриньков Д. Скільки необанків потрібно Україні. URL: https://minfin.com.ua/ua/credits/articles/skolko-neobankov-nuzhno-ukraine/. (Дата звернення: 30.01.2025).

21. Стратегія розвитку фінансового сектору України до 2025 року. Національний банк України. URL: https://bank.gov.ua/admin_uploads/article/Strategy_FS_2025.pdf?v=4. (Дата звернення: 31.01.2025).

22. Чуб П.М. Необанки України: стан та перспективи розвитку. Сучасні інструменти управління корпоративними фінансами. Зб. матеріалів VI Всеукр. наук.-практ. інтернет-конф. студентів, аспірантів та молодих вчених, КНЕУ, Київ 16 листопада 2022 р.

23. Аналіз розміру та частки ринку цифрових банківських платформ – тенденції зростання та прогнози (2024–2029 рр.) URL: https://www.mordorintelligence.com/ru/industry-reports/digital-banking-platform-market.(Дата звернення: 31.01.2025).

24. Наглядова статистика. Офіційне Інтернет-представництво Національного банку України. URL: https://bank.gov.ua/ua/statistic/supervision-statist.(Дата звернення: 31.01.2025).

25. Мірошник, Роман, Кухта, Ігор. 2023. Діджиталізація банківської системи України в сучасних умовах. *Економіка та суспільство*, вип. 49 (Березень). URL:https://doi.org/10.32782/2524-0072/2023-49-39. (Дата звернення: 31.01.2025).

26. Болдова А.А., Болдов А.О. Діджиталізація банківських сервісів як передумова подальшого розвитку фінансового простору України. *Економіка та суспільство.* 2022. № 42. URL: https://doi.org/10.32782/2524-0072/2022-42-8.(Дата звернення: 1.02.2025).

27. Малишко Є.О. Діджиталізація на фінансовому ринку: переваги та недоліки. *Економіка та суспільство*. 2022. № 39. URL: https://doi.org/10.32782/2524-0072/2022-39-34.(Дата звернення: 1.02.2025).

28. Романовська Ю.А., Складанюк М.С. Діджиталізація банківського сектору в умовах пандемії. *Економіка та суспільство*. 2022. № 36. С. 16–20. URL: https://doi.org/10.32782/2524-0072/2022-36-44.(Дата звернення: 8.02.2025).

29. Сорока Б.Р. Діджиталізація фінансового ринку України: ключові ризики для індивідуальних інвесторів. *Економіка та суспільство*. 2022. № 43. URL: https://doi.org/10.32782/2524-0072/2022-43-76.(Дата звернення: 12.02.2025).

30. Холявко Н.І., Козлянченко О.М. Світові тенденції діджиталізації банківського сектору. *Проблеми економіки*. 2021. № 2 (48). URL: https://doi.org/10.32983/2222-0712-2021-2-217-224. (Дата звернення: 15.02.2025).

31. Корицька, О., & Кухта, І. (2024). Диджиталізація банків України: сучасні тренди та перспективи. *Економіка та суспільство,* (67). URL:https://doi.org/10.32782/2524-0072/2024-67-89.(Дата звернення: 2.02.2025).

32. Науменкова С., Міщенко С. Цифрова фінансова інклюзія: можливості та обмеження для України. *Науковий вісник Одеського національного економічного університету*. 2020. № 1–2. С. 133–149.

33. Краус К., Краус Н., Поченчук Г. Інституціональні аспекти та цифровізація фінансової інклюзії в національній економіці. *Innovation and Sustainability*. 2022. № 2. С. 18–28.

34. Винник Р. Розвиток фінансової інклюзії в Україні. *Економіка та суспільство.* 2021. №31. URL: https://economyandsociety.in.ua/index.php/journal/article/view/714. (Дата звернення:1.02.2025).

35. Статистика. Національний банк України. URL: https://bank.gov.ua/ua/statistic . (Дата звернення: 1.02.2025).

36. Андрушків І.П., Надієвець Л.М. Діджиталізація в банківському секторі: світовий та вітчизняний досвід. *Проблеми економіки*. 2018. № 4. С. 195–200. URL: http://nbuv.gov.ua/UJRN/Pekon_2018_4_24 .(Дата звернення: 12.02.2025).

37. Блащук Ю. Віртуальні банки та електронний банкінг: загрози чи нові можливості? Досвід України. *Економічний Часопис-XXI.* 2001. № 9. URL: http://soskin.info/ea/2001/9/20010985.html. (Дата звернення: 13.02.2025)

38. Вареник Н. Інтернет-банкінг: для людини чи проти неї? Зеркало недели. № 49. 2016. URL: https://zn.ua/ukr/business/internet-banking-dlya-lyudinichi-proti-neyi-_.html. (Дата звернення: 13.02.2025).

39. Диба М.І., Гарнего Ю.О. Діджиталізація економіки: світовий досвід та можливості розвитку в Україні. *Фінанси України*. 2018. № 7. С. 50–61.

40. Дубина М., Шеремет О. Розвиток e-banking: світовий та вітчизняний досвід. *Проблеми і перспективи економіки та управління*. 2019. № 2(18). С. 154–162.

41. Дульська І.В. Пріоритети діджиталізації національної економіки. *Сучасні проблеми економіки і підприємництво.* 2015. № 16. С. 34–40.

42. Дульська І.В. Цифрові технології як каталізатор економічного зростання. *Економіка і прогнозування*. 2015. № 2. С. 119–133.

43. Житар М.О., Зелінська В.С. Необанкінг: зарубіжний досвід та українська перспектива. *Збірник наукових праць Університету державної фіскальної служби України.* 2019. Вип. 2. С. 81–95.

44. Максимова Ю.О., Фудім Т.О., Шевченко А.Ю. Сучасні інформаційні технології як перспективні засоби розвитку банків України. *Економіка та управління підприємствами.* 2019. Вип. 29. С. 237–242.

45. Романюк О. Банкінг у месенджері: що це таке і як ним користуватися. Сьогодні. 2018. URL: https://economics.segodnya.ua/ua/economics/finance/ banking-v-messenjere-pumb-1179513.html. (Дата звернення: 16.02.2025).

46. Філатова О. Чат-боти в Україні: 11 сервісів для вирішення фінансових питань. *PaySpace Magazine Global*. 2020. URL: https://psm7.com/uk/articles/chatboty-

v-ukraine-denezhnye-perevody-i-kredity-v-mes sendzherax.html. (Дата звернення: 20.02.2025).

47. Чайковський Я., Ковальчук Я. Банківські інновації: перспективи та загрози електронних банківських послуг. *Світ фінансів*. 2018. № 4(57). С. 121–136.

48. Семеног А. Ю., Цирулик С. В. Зарубіжний досвід регулювання Fintech послуг. Проблеми системного підходу в економіці (Index Copernicus та ін.). 2018. Вип. 5 (67). С. 186–193. DOI: https://doi.org/10.32782/2520-2200/2018-5-31. (Дата звернення: 20.02.2025).

49. Семеног А. Ю., Цирулик С. В. Тенденції розвитку Fintech послуг на світовому та вітчизняному ринках фінансових послуг. *Бізнес Інформ* (RePEC та ін.). 2018. №10. С. 327–334.

50. Банк даних Державної служби статистики України. *Державна служба статистики України*. URL: https://stat.gov.ua/uk/explorer?urn=SSSU:DF_INFORM_COMMUN_TECH_ENTRP(8.0.0). (Дата звернення: 29.02.2025)

51. Guidance on cyber resilience for financial market infrastructures. *Bank for International Settlements*. URL: https://www.bis.org/cpmi/publ/d146.htm. (Дата звернення: 2.04.2025)

52. Національний банк України. Контроль за кіберзахистом та інформаційною безпекою банків посилюється. *Національний банк України*. URL: https://bank.gov.ua/ua/news/all/kontrol-za-kiberzahistom-ta-informatsiynoyu-bezpekoyu-bankiv-posilyuyetsya. (Дата звернення: 12.03.2025)

53. Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах : Постанова Нац. банку України від 11.06.2018 № 64 : станом на 1 січ. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/v0064500-18#Text. (Дата звернення: 9.04.2025)

54. Банк даних Державної служби статистики України. *Державна служба статистики України*. URL: https://stat.gov.ua/uk/explorer?urn=SSSU:DF_INFORM_COMMUN_TECH_ENTRP(8.0.0). (Дата звернення: 12.04.2025)

55. Трусова Н. В., Чкан І. О. Кіберзахист банківської системи України в умовах цифрових трансформацій. *Науковий вісник Таврійського державного агротехнологічного університету*. 2023. Т. 1, № 47. С. 151–163. URL: https://doi.org/10.31388/2519-884x-2023-47-151-163 . (Дата звернення: 29.03.2025)

56. Ситник Н. С., Половчак І. Р. Цифровізація та кібербезпека у забезпеченні фінансової безпеки банків в умовах війни. *Галицький економічний вісник.* Тернопіль: ТНТУ. 2024. Том 89. № 4. С. 70–81. URL: https://elartu.tntu.edu.ua/handle/lib/46455 . (Дата звернення: 6.04.2025)

57. Стражник Б. О., Смирнов С. А. Найпопулярніші атаки на веб-додатки та методи протидії їм. *Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених. Системи та технології кібернетичної безпеки.* 2023. с. 307-309. URL: https://ela.kpi.ua/server/api/core/bitstreams/68a81487-152c-4eac-9988-2a9dd32553ea/content (Дата звернення: 16.04.2025)

58. Лавренюк В. В. Ключові драйвери кібер-ризиків фінансових установ. *Сучасні гроші, банківські послуги та фінансові інновації в цифровій економіці : матеріали IV Всеукр. наук.-практ. інтернет-конф. студентів, аспірантів і молодих вчених, Київ, 12 квіт. 2021 р*. М-во освіти і науки України, ДВНЗ «Київ. нац. екон. ун-т ім. В. Гетьмана», Фін.-екон. ф-т, Каф. банк. справи, Банк. клуб КНЕУ. Дніпро: Середняк Т. К., 2021. С. 297–300. URL: https://ir.kneu.edu.ua/bitstream/handle/2010/36143/sgbp_21_4_8.pdf?sequence=1.
(Дата звернення: 29.04.2025)

ДОДАТКИ

Додаток А

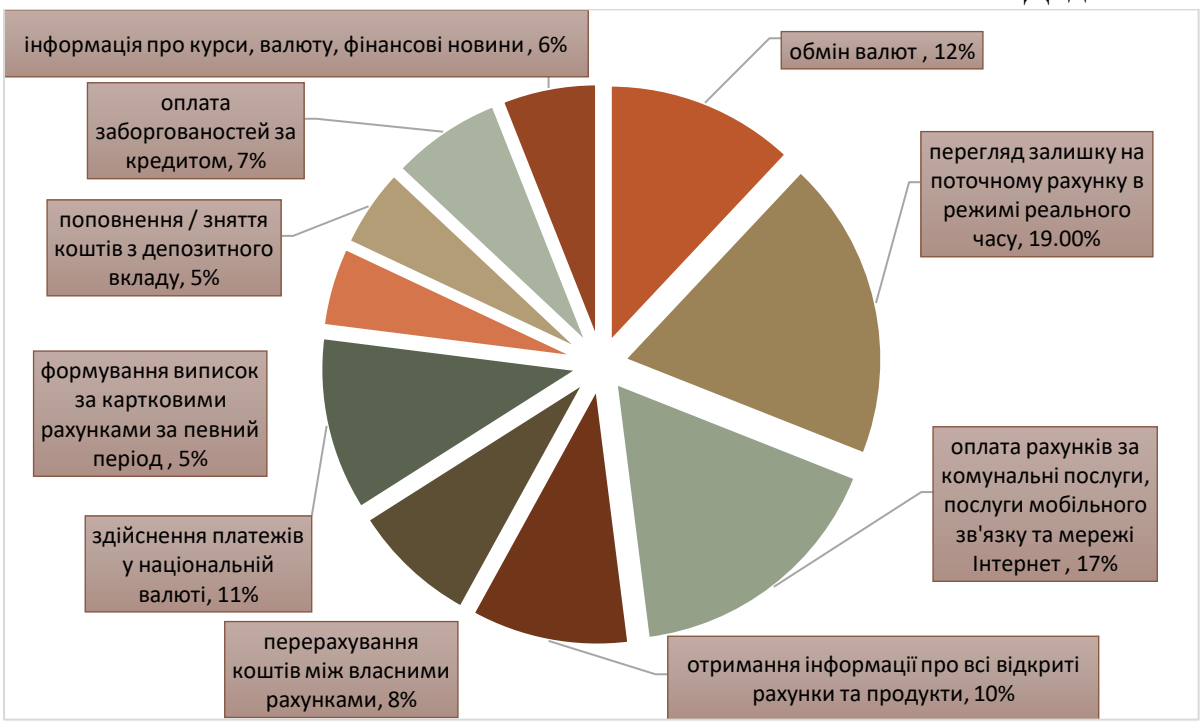

Рисунок А – Найпоширеніші послуги, що використовуються клієнтами банків в Інтернет – банкінг

Джерело: розроблено автором

Додаток Б

Таблиця Б – Роль інтернет-технологій у сучасній банківській діяльності

Технологія	Опис
Інтернет-банкінг	Дозволяє клієнтам здійснювати фінансові операції через Інтернет, включаючи перевірку балансу, перекази коштів, оплату рахунків та інші операції.
Мобільний банкінг	Забезпечує доступ до банківських рахунків через мобільні додатки, що дозволяє клієнтам керувати своїми фінансами зі смартфонів і планшетів.
Онлайн-кредитування	Надає можливість отримання позик та кредитів через онлайн-платформи, зменшуючи бюрократичні процедури і роблячи фінансування більш доступним.
Електронні платежі	Дозволяють здійснювати різноманітні електронні платежі, включаючи перекази коштів, платежі за товари та послуги через Інтернет і мобільні додатки.
Захист і безпека	Використовуються для забезпечення безпеки клієнтських даних шляхом методів аутентифікації, шифрування та захисту від шахрайства і несанкціонованого доступу.
Автоматизація і оптимізація	Дозволяють банкам автоматизувати багато рутинних процесів і вдосконалювати роботу шляхом зменшення витрат та підвищення ефективності.
Аналітика та Big Data	Використовуються для аналізу даних клієнтів і прогнозування ризиків, допомагають банкам розуміти потреби клієнтів і надавати персоналізовані послуги.
Віддалена робота	Дозволяє банкам та їх працівникам працювати віддалено, що стає важливим у сучасних умовах, зокрема під час пандемій.

Джерело: [56]

Додаток В

Таблиця В – Класифікація інтернет-технологій у сучасному банкінгу

Класифікація	Ознака	Приклади
Залежно від сфери застосування	Технології, що забезпечують доступ до банківських послуг	Інтернет-банкінг, мобільний банкінг, банкомати, термінали самообслуговування
Технології, що підвищують ефективність роботи банку	CRM-системи, системи управління ризиками, системи управління ланцюгами поставок	
Технології, що створюють нові можливості для банків	Штучний інтелект, блокчейн, Big Data	
Залежно від рівня складності	Основні технології	Інтернет, мобільні мережі, електронна пошта, системи захисту інформації
Залежно від сфери впливу	Технології, що впливають на взаємодію банку з клієнтами	Інтернет-банкінг, мобільний банкінг, чат-боти
Технології, що впливають на внутрішні процеси банку	CRM-системи, системи управління ризиками, системи управління ланцюгами поставок	
Технології, що впливають на зовнішнє середовище банку	Штучний інтелект, блокчейн, Big Data	

Джерело: [56]

Додаток Д

Таблиця Д – Порівняння інтернет-банкінгу в банках України

банк	Назва інтернет банкінгу	Підключення до системи	Витрати та тарифи на послуги				Нетрадиційні функції
			підключення	перекази між рахунками	перекази в середині банку	перекази по Україні	
Приват банк	Приват24	В інтернеті	0	0-0,5 від суми	0-1% від суми	Від 1% від суми	Обмін валют, перекази за кордон, авіа та залізничних квитків, оплата послуг
Райфф айзен банк	Raiffeisen Online	В інтернеті	0	0	0	0	Обмін валют, перекази за кордон, оплата послуг, смс – інформування
Пумб	ПУМБ Online	У відділенні	0	0	0	0	«Депозитний конструктор» - підбір депозиту по терміну, валюті та іншим умовам
Ощад банк	Ощад24	У відділенні		0	3 грн	1%+5 грн	Управління картками(замовлення, блокування і заповнення заявки на отримання кредиту
Креді Агріколь банк	i-bank	В інтернеті	0	0	3 грн	6 грн	Купувати та продавати валюту, розміщувати вклади, формувати виписки

Джерело: розроблено автором на основі даних офіційних банківських сайтів