Міністерство освіти і науки України

Західноукраїнський національний університет

Чортківський навчально-науковий інститут підприємництва та бізнесу

Кафедра фундаментальних та спеціальних дисциплін

Підгородецький Олександр Вікторович

Вплив цифрової трансформації на банківський сектор

Спеціальність 072 «Фінанси, банківська справа і страхування»

Магістерська робота

Студент групи ФМСчм – 11

Підгородецький О.В.

_____ **(підпис)**

Науковий керівник

к.е.н., доцент Кульчицька Н.Є.

_____ **(підпис)**

Кваліфікаційну роботу допущено

до захисту

«____»_____2025р.

Зав. кафедри

Дерманська Л.В._____

(підпис)

Чортків – 2025

ЗМІСТ

ВСТУП

Сучасний світ зазнає значних змін під впливом цифрових технологій. Інтенсивна цифровізація зумовлює трансформацію соціально-економічних процесів, створюючи нові механізми взаємодії між споживачами та підприємствами. Люди активно використовують комп'ютерні технології та Інтернет для здійснення онлайн-покупок, проведення банківських операцій та обігу цифрових активів, таких як криптовалюти (наприклад, біткойн).

Ці процеси отримали назву цифрова економіка. Вона почала формуватися наприкінці 1990-х років, коли вчений Ніколас Негропонте висловив ідею переходу від фізичних носіїв вартості (наприклад, паперових грошей) до цифрових ресурсів, представлених у вигляді інформаційних фрагментів, що зберігаються та обробляються за допомогою комп'ютерних систем.

Цифрова трансформація визначається як комплексне використання інформаційних технологій з метою зміни традиційних моделей організаційної діяльності та підвищення ефективності бізнес-процесів. Зокрема, банківські установи застосовують програмні рішення та системи кібербезпеки для оптимізації надання фінансових послуг, підвищення їх швидкості, якості та доступності для клієнтів. Водночас цифрова трансформація передбачає не лише технологічні зміни, а й розвиток компетенцій персоналу, впровадження нових робочих процесів і удосконалення методів виконання завдань.

Цифрова економіка включає використання технологій для ведення бізнесу та електронної комерції. Крім того, вона передбачає інтеграцію інтелектуальних систем, таких як роботи та штучний інтелект, для автоматизації рутинних процесів та підвищення ефективності діяльності. Дані процеси є складовою так званої четвертої технологічної революції, яка характеризується широким впровадженням комп'ютерних технологій, автоматизації та інтелектуальних систем у різні сфери суспільного життя.

Таким чином, цифрова економіка та цифрова трансформація є механізмами використання інформаційних технологій для підвищення

ефективності бізнесу та поліпшення якості життя. Вони сприяють оптимізації організаційних процесів, забезпечують інтеграцію інтелектуальних систем у повсякденну практику та визначають сучасні тенденції розвитку глобальної економіки. Цифрова трансформація банківського сектора спрямована на досягнення кількох ключових цілей: підвищення оперативності та ефективності прийняття управлінських рішень, розширення варіативності процесів відповідно до індивідуальних потреб та специфіки клієнтів, а також зменшення чисельності співробітників, які безпосередньо залучені до виконання операційних процесів.

На глобальному рівні спостерігається системна адаптація банківських установ та сервісів обслуговування клієнтів до умов цифрової трансформації. Практичні аспекти впровадження цифровізації активно досліджуються та широко обговорюються у науковій літературі, а також у публічних інформаційних джерелах. Значна кількість як зарубіжних, так і вітчизняних дослідників та розробників пропонує власні параметри та критерії оцінки ефективності цифрових моделей банківського бізнесу, одночасно впроваджуючи для споживачів принципово нові технологічні рішення з розширеним функціоналом, які суттєво відрізняються від традиційних форм банківського обслуговування [2].

Проте слід зазначити, що на сьогодні спостерігається недостатній рівень теоретичного осмислення процесів цифрової трансформації банківського бізнесу. Експерти одностайні в тому, що в найближчій перспективі цифрові технології радикально змінять глобальну економіку, бізнес-моделі та особисте життя людини. Саме тому дослідження перспектив цифрового банкінгу є обґрунтованим, а обрана тема роботи — актуальною.

Об’єкт дослідження - діяльність банківських установ в умовах цифрової трансформації.

Предмет дослідження - економічні відносини та процеси, що формуються у зв’язку з розвитком цифрового банкінгу.

Мета дослідження полягає у вивченні та поглибленні теоретико-методичних положень щодо сутності та організації цифрового банкінгу, визначенні його проблем в Україні, розробці шляхів їх вирішення та визначенні напрямів оптимізації.

Завдання дослідження

1. Проаналізувати сутність і зміст цифрової трансформації банківської системи.
2. Вивчити нормативно-правове забезпечення цифровізації банківської діяльності в Україні.
3. Дослідити роль банків як ключових суб'єктів формування цифрової інфраструктури фінансового ринку.
4. Оцінити сучасні виклики та ризики функціонування банківської системи в умовах цифровізації.
5. Вивчити поточний рівень цифрової трансформації банків України.
6. Проаналізувати вплив цифрових сервісів на фінансову стабільність та конкурентоспроможність банків.
7. Дослідити міжнародний досвід цифровізації банківської справи та можливості його застосування в Україні.
8. Визначити ключові напрями вдосконалення цифрових рішень у банківському секторі України.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ У БАНКІВСЬКОМУ СЕКТОРІ

1.1. Сутність і зміст цифрової трансформації банківської системи

Сучасний розвиток дистанційного банківського обслуговування в Україні є невід'ємною складовою процесу цифрової трансформації фінансового сектору. Протягом останніх років, зокрема з середини 2010-х, спостерігається інтенсивне зростання цього напряму, що зумовлено впровадженням передових інформаційних технологій, поширенням доступу до мобільного Інтернету та збільшенням використання цифрових пристроїв серед населення [26; 30].

Важливу роль у розвитку дистанційного банкінгу відіграли етапи створення перших платформ інтернет-банкінгу та запуск повністю цифрових банківських структур. Ці інновації забезпечили підвищення ефективності обслуговування клієнтів, скорочення часу виконання операцій та розширення спектру доступних послуг. Крім того, зовнішні чинники, такі як глобальна пандемія COVID-19 та військові події, стимулювали масовий перехід клієнтів на віддалені банківські сервіси, що дозволило забезпечити безперервність фінансових операцій навіть у кризових умовах [5; 17; 36].

У сучасних умовах дистанційне банківське обслуговування стає ключовим інструментом підвищення конкурентоспроможності фінансових установ та відповідає світовим стандартам цифровізації. Такий підхід надає користувачам безпечний та зручний доступ до послуг банку у режимі 24/7, дозволяючи значно підвищити рівень задоволеності клієнтів. [30; 40].

Реалізація дистанційних банківських сервісів передбачає комплексну взаємодію банку з клієнтами, де кожен новий продукт створюється як цілісний бізнес-процес з подальшою інтеграцією у загальну екосистему банку. Цей процес включає етапи: проведення маркетингового та конкурентного аналізу, організацію та оптимізацію внутрішніх бізнес-процесів, управлінські рішення щодо запуску сервісу, безпосередню розробку цифрового продукту, його

інтеграцію в корпоративну екосистему, а також забезпечення супроводу та залучення користувачів [7; 19].

Різницю між традиційним та дистанційним банківським обслуговуванням ілюструє таблиця 1.1.

Таблиця 1.1 – Різниця між традиційним та дистанційним банківським обслуговуванням

Ознаки	Класичне обслуговування	Дистанційне обслуговування
Час надання послуг клієнтам	Обмежений; надається у межах робочого графіка відділення	Необмежений; цілодобовий доступ до сервісів (24/7)
Оперативність обслуговування	Залежить від кваліфікації та завантаженості працівника	Миттєва обробка запитів завдяки цифровій автоматизації
Вартісні показники послуг	Високі витрати для клієнта (% від обслуговування)	Значно знижені витрати; у більшості випадків послуги безкоштовні
Масштаб обслуговування	Обмежується фізичною присутністю у відділеннях країни	Широкий доступ; обслуговування доступне як у межах країни, так і за її межами
Інформування про нові продукти та послуги	Вимагає додаткових витрат на рекламу та часу клієнтів	Оперативне інформування через веб-портали, SMS-повідомлення та інші цифрові канали
Витрати на функціонування системи	Витрати на персонал та утримання відділень	Витрати на серверні ресурси, програмне забезпечення та підтримку

обслуговування		цифрової інфраструктури

Створено автором на основі джерела: [7]

Процес еволюції дистанційного банківського обслуговування ілюстрований на рисунку 1.1.

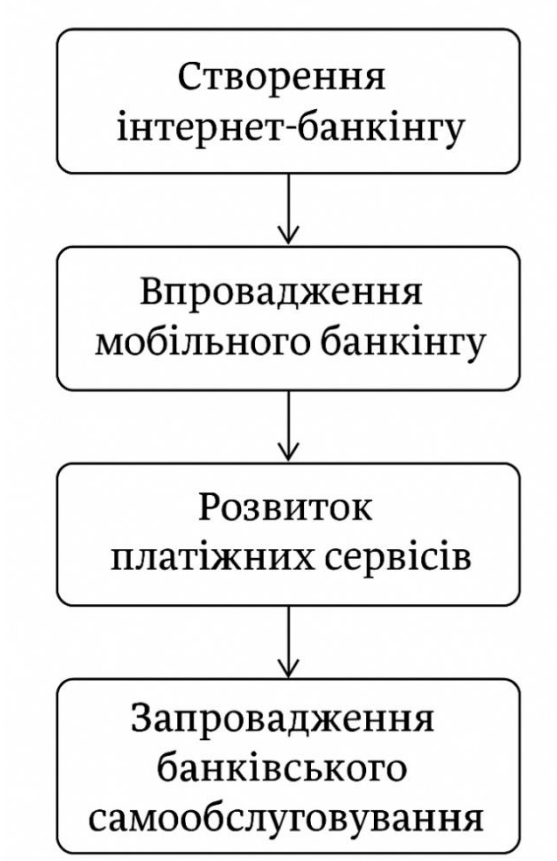

Рисунок 1.1 – Етапи розвитку дистанційного банківського обслуговування
Створено автором на основі джерела: [5]

Цифрові форми банківського обслуговування почали з’являтися ще в 1960-х роках, коли основними інноваціями були банкомати та пластикові картки. Перенісшись у 2020-і, ми спостерігаємо зовсім інший ландшафт: постійний доступ до Інтернету, значно вдосконалений широкосмуговий зв’язок, поширення смартфонів і зростання популярності онлайн-банкінгу, який стає звичною практикою. Клієнти очікують швидкого та дистанційного доступу до всіх фінансових і нефінансових послуг [30; 36].

Сучасний цифровий банкінг – це, по суті, автоматизація класичних банківських сервісів. Завдяки цьому як роздрібні, так і корпоративні користувачі можуть здійснювати операції через онлайн-канали, включно з Інтернетом та мобільними мережами. Перехід до цифрового формату є глобальною тенденцією: банки активно переводять взаємодію з клієнтами з фізичного світу в цифровий, впроваджуючи різні стратегії, зокрема трансформуючи послуги в онлайн, змінюючи графік роботи відділень та пропонуючи цифрові способи оплати [5; 18].

За останній рік у традиційних банках відбулися такі зміни: 60% установ скоротили кількість відділень або змінили години їх роботи, 34% впровадили повністю цифрові процеси, а 18% запровадили безконтактні способи оплати [7; 19]. Цей перехід не є випадковим: він викликаний новими потребами ринку та очікуваннями клієнтів. Крім того, банки прагнуть не лише зберегти конкурентоспроможність, а й скористатися перевагами, які відкриває цифровий банкінг [26; 30].

Основні переваги цифрового банкінгу включають:

- Розширення географії: цифрові платформи дозволяють охоплювати ширшу аудиторію без відкриття нових відділень.
- Нові джерела доходу: аналітика даних клієнтів допомагає створювати нові продукти та послуги та покращувати взаємодію з користувачами.
- Безпаперові транзакції: розвиток цифрового банкінгу значно зменшує потребу у паперових документах.
- Зниження витрат: автоматизація процесів та відмова від ручної обробки паперу дозволяє економити ресурси банку.
- Зручність для клієнта: 24/7 доступ до всіх банківських сервісів створює комфортний та ефективний користувацький досвід [26; 36; 43].

Крім того, зростання конкуренції у фінансовому секторі змушує банки прискорювати впровадження цифрових технологій [30; 36]. Ключовим моментом є створення правильного цифрового досвіду: якщо користувачам

важко отримати очікуваний результат, вони можуть повністю відмовитися від послуг і перейти до іншого постачальника [40].

Банки, які планують впровадження цифрових послуг, мають діяти оперативно й розпочати цей процес вже сьогодні. Досвід показує, що навіть кілька років успішної традиційної роботи не гарантують стабільності на сучасному ринку. Щоб утримувати лідерські позиції, потрібно швидко адаптуватися до нових умов.

Цифровий банкінг перестав бути просто бажаним варіантом і став необхідністю. Банки, що працюють у цифровому форматі, можуть гнучкіше обирати цільові сегменти клієнтів та способи їх залучення [5; 7; 19]. Дослідження демонструють, що клієнти віддають перевагу банкам із цифровими платформами порівняно з класичними відділеннями. У багатьох великих установах кошти, які раніше витрачали на відкриття нових філій, зараз спрямовуються на модернізацію електронних банківських сервісів. Очікується, що така практика збережеться у міру подальшої цифровізації ринку.

Сьогодні цифровий банк є оптимальним рішенням для задоволення всіх банківських потреб клієнтів, особливо в умовах пандемій та війни [6; 7].

Якщо класифікувати дистанційне банківське обслуговування, можна представити його наступним чином (рис. 1.2).

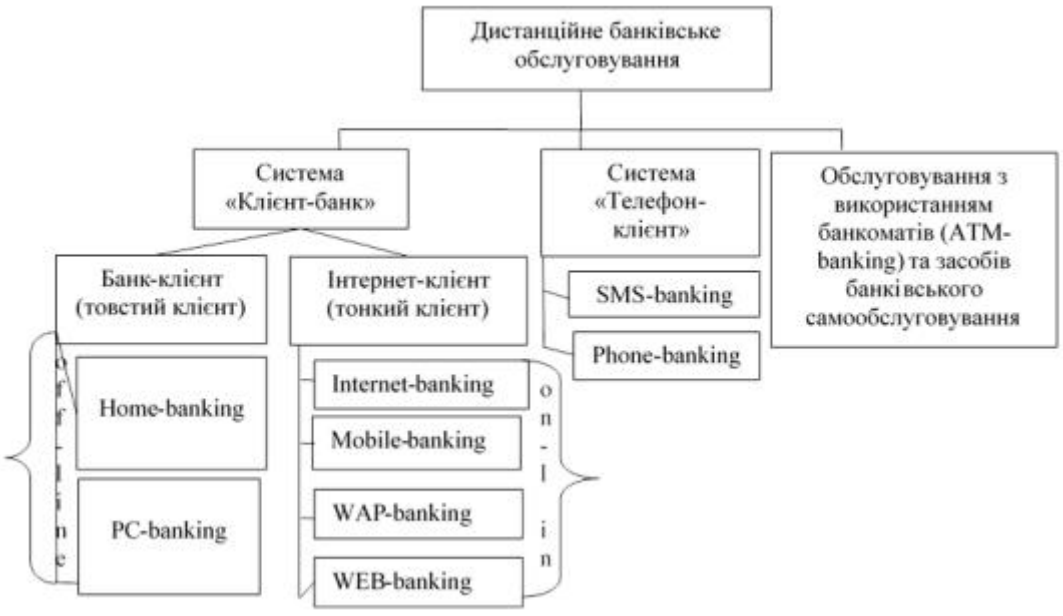

Рисунок 1.2 – Види дистанційного банківського обслуговування

Створено автором на основі джерела: [6, 7]

Сучасний рівень технологій дозволяє виконувати банківські операції миттєво: наприклад, в Україні середній час переказу коштів між рахунками становить 1–10 секунд (табл.1.2).

Таблиця 1.2. Час, за який здійснюється переказ коштів між рахунками, у банківських системах

Банк	**Миттєві перекази / SEП-4.1**	**Орієнтовний час переказу**
ПриватБанк	Так, підтримує миттєві карткові та рахункові перекази	6–9 секунд (P2P, рахунок→рахунок)
Монобанк	Так, через внутрішні P2P та підтримку SEП	Миттєво (декілька секунд)
Ощадбанк	Так, учасник SEП-4.1	До 10 секунд за рахунок SEП
Укрексімбанк	Так, учасник SEП-4.1	До 10 секунд за рахунок SEП
ТАСКОМБАНК	Немає публічної інформації про гарантію секундних переказів	Може займати хвилини, залежно від системи
ПУМБ	Так, підтримує миттєві перекази через SEП	До 10 секунд (за наявності SEП)
А-Банк (àbank)	Публічно підтвердження немає	Може займати стандартний час банківського переказу (хвилини–години)

Створено автором на основі джерела: [12]

Застосування дистанційних форм банківського обслуговування дає можливість установам зменшувати витрати, підвищувати продуктивність

співробітників і забезпечувати ширший доступ до послуг для всіх клієнтів, зокрема людей з обмеженими можливостями та мешканців віддалених територій. Такий підхід відповідає принципам сталого розвитку. Крім того, дистанційні сервіси сприяють більшій прозорості фінансових операцій, контролю за власними коштами та своєчасному отриманню інформації про пропозиції банку, що позитивно позначається на рівні фінансової грамотності населення.

1.2. Нормативно-правове забезпечення цифровізації банківської діяльності

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 [54].

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. 1.3).

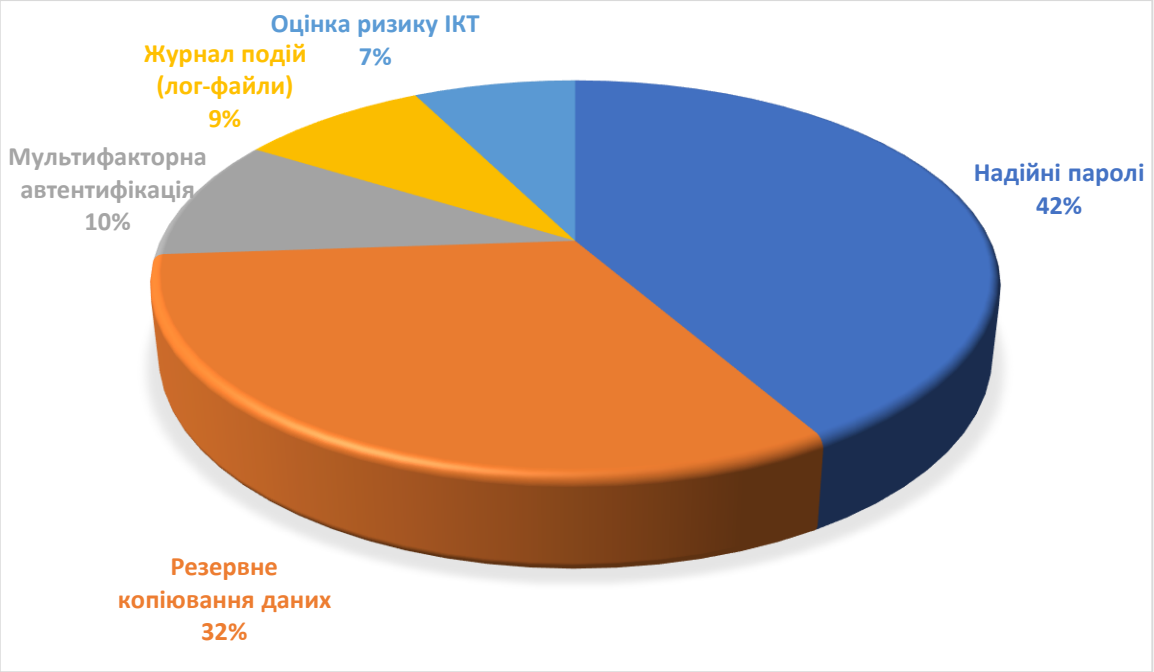

Рисунок 1.3 – Частка українських банків, що впроваджують окремі заходи кібербезпеки (2023 р.), %

Створено автором на основі джерела: [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].

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 [1; 14; 15; 51; 52].

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 [3; 4; 48; 49].

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 [26; 30].

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) [3; 21; 52; 53]. 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 [26; 48; 49].

Таблиця 1.3. Порівняльний аналіз законодавчих актів «Щодо функціонування платіжних систем і переказів коштів в Україні» та «Щодо надання платіжних сервісів»

Параметр	**Закон України «Щодо платіжних систем і переказу коштів на території України» (№2346-III від**	**Закон України «Щодо надання платіжних послуг» (№1591-IX від 30.06.2021 р.)**

	05.04.2001 р.)	
Основна мета	Встановлення правил взаємовідносин у сфері діяльності платіжних систем і здійснення переказів, визначення базових норм функціонування	Уніфікація законодавчих положень України з європейськими стандартами (PSD2) та впровадження сучасних методик у секторі платіжних послуг
Сфера регулювання	Платіжні системи (вітчизняні та міжнародні); здійснення переказів; правила взаємодії учасників	Різноманітні платіжні послуги, включно з інноваційними фінансовими технологіями; захист прав користувачів платіжних послуг
Захист прав клієнтів	Спрямовано на гарантування безпечного проведення переказів	Розширений спектр прав клієнтів: право на повну та зрозумілу інформацію про послуги та доступ до механізмів вирішення спорів

Створено автором на основі джерела: [3,4,21]

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.

1.3. Банки як ключові суб'єкти формування цифрової інфраструктури фінансового ринку

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 [36; 39]. 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 [40; 31].

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.

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.

Переваги, які дає цифровий банкінг перерахую 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 [9].

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.

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, обслуговування клієнтів.

У грудні 2022 року Deloitte оголосила про співпрацю з AWS для вирішення хронічної проблеми у банківській сфері переходу до цифрових систем. А Temenos допомагає новим цифровим банкам США розпочати роботу за 90 днів, пропонуючи найбільш функціонально багату та технологічно просунуту комплексну пропозицію цифрового банку SaaS [23] .

Особливості цифровізації у банківському секторі та характерних ризиків ілюструє таблиця 1.4.

Таблиця 1.4. Специфіка діджиталізації в банківській сфері та властиві їй загрози

Особливості процесу діджиталізації в банківській сфері	**Характерні риси ризиків цифровізації банківських послуг**

Процес цифровізації охоплює не окремі галузі чи напрями діяльності банків, а всю систему взаємозв'язків у банківському секторі	Ризики проявляються у більш масштабному форматі
Готовність до оперативного впровадження нових технологій та активне використання інновацій	Можливість постійного вдосконалення та адаптації систем інформаційної безпеки з урахуванням оновлених даних
Безготівковий та бездокументарний характер більшості операцій, що не потребує фізичного переміщення, швидкий перехід на надання більшої частини послуг через цифрові канали	Банки стають основними об'єктами кібератак; високий рівень фінансових втрат у разі реалізації загроз
Зростання фінансової та цифрової грамотності користувачів банківських продуктів	Підвищення індивідуального ризику клієнта-фізичної особи за відсутності необхідних фінансових і цифрових компетенцій
Активне застосування інноваційних технологій як інструмент підвищення конкурентоспроможності	Значущість стратегічних ризиків у разі, якщо пріоритети банку зміщуються від швидкого результату діджиталізації
Відсутність консервативного ставлення до інновацій у значної частини персоналу	Зростання ризиків, що походять із внутрішніх джерел
Традиційно велика кількість даних, що потребують зберігання, обробки та аналізу для покращення клієнтського досвіду	Підвищені витрати на забезпечення інформаційної безпеки

Створено автором на основі джерела: [36,39,40]

Висновки до розділу 1

У першому розділі проведено аналіз сутності цифрової трансформації банківського сектору та визначено основні передумови формування цифрового фінансового середовища в Україні. З дослідження випливають такі висновки.

Цифрова трансформація банківської системи є логічним етапом її розвитку, обумовленим зміною поведінки споживачів, технологічним прогресом та посиленням конкуренції з боку фінтех-компаній і необанків. Перехід до цифровізації означає рух від традиційних операційних моделей до автоматизованих, клієнтоорієнтованих рішень, які забезпечують швидкість, мобільність і доступність фінансових послуг. Це впливає як на обслуговування клієнтів, так і на внутрішні бізнес-моделі, структуру рішень і стратегії банків.

Нормативно-правове забезпечення створює основу для безпечного та організованого розвитку цифрової банківської сфери. Національний банк України визначає вимоги щодо кіберзахисту, технологічних стандартів, дистанційної ідентифікації, регулювання платіжних систем, відкритого банкінгу та електронних каналів обслуговування. Регуляторна політика орієнтована на відповідність міжнародним стандартам, що сприяє формуванню прозорого, конкурентного та технологічно стійкого середовища. Нормативна база постійно оновлюється для реагування на нові ризики — кіберзагрози, шахрайство, збої інфраструктури та зростаючу взаємозалежність учасників фінансового ринку.

Банки залишаються центральними інституціями цифрової інфраструктури фінансового ринку. Вони забезпечують технологічні рішення — цифрові платформи, мобільні застосунки, дистанційні сервіси, комплексні екосистеми, сервіси миттєвих платежів та інструменти відкритих API. Завдяки масштабам діяльності, доступу до великих обсягів даних і досвіду управління ризиками банки задають темп розвитку цифрового фінансового середовища, визначають рівень його безпеки та впровадження інноваційних стандартів. Їхня роль

посилюється через партнерство з технологічними компаніями, інтеграцію хмарних рішень та розвиток платформної моделі функціонування.

Цифрова трансформація банківського сектору охоплює технологічні, регуляторні та інституційні зміни. Вона змінює архітектуру фінансового ринку, створює нові умови конкуренції та формує основу для інтеграції інновацій у банківську сферу. Розуміння цих процесів необхідне для подальшого аналізу впливу цифровізації на ефективність, стабільність і безпеку банківської системи.

РОЗДІЛ 2. АНАЛІЗ ВПЛИВУ ЦИФРОВИХ ТЕХНОЛОГІЙ НА ДІЯЛЬНІСТЬ БАНКІВ

2.1. Сучасні виклики та ризики функціонування банківської системи в умовах цифровізації

У сучасних умовах світова економіка, а разом із нею й банківська індустрія, стикаються з двома надзвичайно потужними викликами. Перший пов'язаний із різким та складним виходом із постпандемійних наслідків, другий — із глибокими зрушеннями, спричиненими п'ятою індустріальною революцією, що після пандемії отримала додатковий імпульс розвитку. Цей етап характеризується інтенсивним поширенням цифрових технологій та активним застосуванням штучного інтелекту [31]. Події періоду COVID-19 продемонстрували, що майбутній розвиток не можна розглядати як просте продовження попередніх тенденцій [25]. Важливо усвідомлювати, що майбутні зміни можуть не лише стимулювати розвиток, але й створювати суттєві загрози для функціонування банківських установ [1].

Плануючи перехід до нових моделей діяльності, банкам необхідно ретельно оцінити можливі ризики й співставити їх із ймовірними вигодами. Процеси цифровізації здатні як посилювати традиційні ризики у фінансовій сфері, так і знижувати їхню силу впливу [55]. У низці ситуацій саме завдяки цифровим рішенням з'являються інструменти, які дозволяють нівелювати окремі загрози або трансформувати їх у нові можливості [26].

Процентний ризик формується з кількох ключових причин: інтернет-середовище розширює доступ банків до більшої кількості потенційних клієнтів, які прагнуть найвигідніших умов, зокрема щодо процентних ставок; паралельно відбувається активний розвиток онлайн-торгівлі фінансовими інструментами [56]. Зменшити ймовірність прояву цього ризику допомагає широке впровадження відкритих інтернет-банкінгових сервісів [1]. Варто підкреслити, що процентний ризик може поєднуватися з ризиком фондового

ринку. Він зумовлений можливістю проводити торговельні операції у режимі реального часу на кількох біржових платформах, що підсилює коливання фінансових інструментів [10]. Водночас розвиток інтернет-трейдингу сприяє залученню фінансових ресурсів як приватних осіб, так і бізнесу [56].

Ризик ліквідності виникає у зв'язку з тим, що клієнти отримали можливість здійснювати фінансові операції будь-якої миті, що підвищує мінливість залишків на депозитних рахунках і ускладнює контроль за динамікою коштів на рахунках банку [1]. Правові ризики напряму залежать від юрисдикції, у якій функціонує банк, та від якості нормативно-правових положень, що регулюють його діяльність [55]. Репутаційні втрати можуть бути наслідком реалізації будь-якого з уже згаданих ризиків [58]. Фактично на будь-якому етапі функціонування банку цей ризик може проявитися, і що сильніше банк піддається іншим видам ризиків і не здатний ефективно на них реагувати, то вищою стає ймовірність репутаційних втрат [1].

Якщо умовно прийняти загальний обсяг банківських ризиків за 100%, то співвідношення основних їх видів представлено на рисунку 2.1.

Рисунок 2.1 – Структура ключових ризиків банків станом на 1.01.2025р. Створено автором на основі джерела: [24]

Беручи до уваги значну кількість банківських установ у системі (рис. 2.2), стає очевидним, що питання контролю та мінімізації ризиків не може залишатися поза увагою.

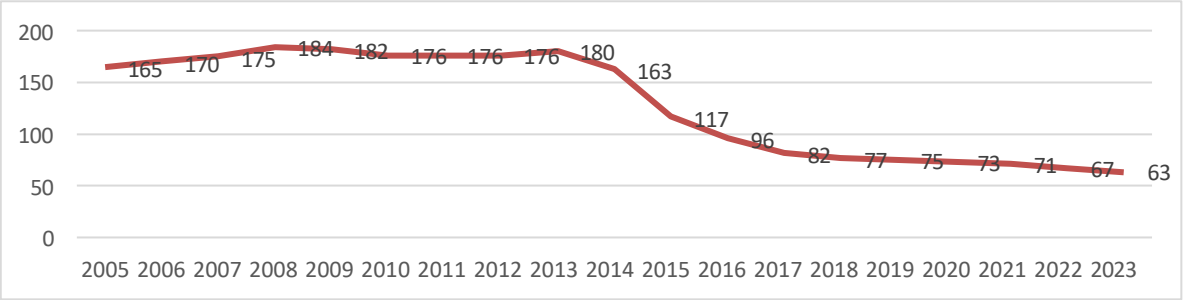

Рисунок 2.2 – Динаміка кількості діючих банків в Україні [24]

У сучасних умовах банківські установи стикаються з постійно зростаючою необхідністю посилювати заходи протидії різним видам ризиків. На цьому тлі посилюється тиск, пов'язаний із обов'язком дотримуватися регуляторних вимог, забезпечувати належну операційну стійкість та підтримувати стабільність функціонування [30]. Динамічний розвиток фінансового ринку зумовлює появу нових викликів, що виникають унаслідок швидких змін у середовищі загроз, активного поширення цифрових технологій, застосування блокчейн-рішень та появи нових форм кібератак [52].

За умов систематичного зростання кількості кіберзлочинів, цифрових атак та підвищеної зацікавленості злочинних груп до рахунків клієнтів і конфіденційних даних, банки вже не можуть обмежуватися несистемним управлінням інформаційною безпекою [55]. Для гарантування захисту інтелектуальних активів, фінансових ресурсів клієнтів і банків, а також конфіденційних відомостей, що мають важливе значення для стабільної діяльності установи, потрібне впровадження комплексної й узгодженої стратегії безпеки [57].

Статистичні дані щодо кіберінцидентів засвідчують, що основну частку

загроз формують зовнішні суб'єкти [8]. Джерелами небезпеки можуть бути як чинні, так і колишні співробітники організацій [56]. Переважна більшість навмисних інцидентів у сфері кібербезпеки пов'язана саме з активністю зовнішніх зловмисників [51].

Таблиця 2.1. Розподіл випадків кіберпорушень між окремими галузями у державах – членах Організації економічного співробітництва та розвитку (статистичні показники станом на кінець 2024 р.), %

Галузь	**Фінансово-страховий сегмент**	**Сфера цифрових сервісів**	**Освітні установи**	**Торговельна діяльність**	**Промисловість**	**Інші напрями**
Кіберподія, спричинена шкідливими програмами	19,4	12,0	6,5	6,4	5,3	50,4
Порушення, пов'язане з витоком або втратою персональних конфіденційних відомостей	28,3	5,0	3,1	4,9	2,0	56,7
Збої, спричинені технічними помилками під час налаштування	17,9	24,0	5,8	4,8	6,3	41,2

чи функціонування ІТ-систем						

Джерело:[30]

Фінансові організації, передусім банківські установи, у глобальному вимірі залишаються найчастішими мішенями кібератак [30]. Це пояснюється тим, що банки оперують значними грошовими ресурсами, а для кіберправопорушників існує широкий спектр способів отримання незаконної вигоди, зокрема через вимагання, несанкціоноване привласнення коштів чи здійснення шахрайських схем [51]. У відповідь на це регуляторні органи впроваджують розширені механізми нагляду та контролю у сфері кіберризиків [52].

Протидія кіберзлочинності потребує істотних фінансових вкладень з боку банківського сектору. За підрахунками спеціалістів, банківські установи інвестують у кіберзахист утричі більше, ніж організації, що не належать до фінансової сфери [55].

З огляду на те, що для ефективного подолання кіберзагроз зусиль приватних компаній може бути недостатньо (зокрема тому, що окремі суб'єкти не завжди здатні повною мірою оцінити системні наслідки кіберінцидентів), у низці випадків стає необхідним додаткове державне регулювання та участь центрального банку. Ці аспекти буде розглянуто у наступному підрозділі даного дослідження [8].

До ключових груп кіберризиків відносять:

– незаконне привласнення коштів клієнтів банківських установ,

– прямі фінансові збитки, яких зазнає сам банк,

– порушення стабільності та безперебійності функціонування фінансових сервісів,

– ймовірність виникнення системної дестабілізації всього банківського сектору у випадку кібератаки, спрямованої на провідні установи

фінансової системи.

Щоб уникнути виникнення масштабних негативних наслідків, пов'язаних із кіберризиками, центральний банк здійснює контроль за рівнем кіберстійкості всіх фінансових установ, а також завчасно інформує їх про потенційні нові види атак і рекомендовані механізми протидії.

Показник частки кіберінцидентів, що виникають через внутрішні джерела у фінансовій сфері (13 %), майже відповідає середньому рівню по всіх секторах (11 %) і є нижчим порівняно з галузями, де також обробляються значні обсяги чутливої інформації (комунальні послуги – 27 %, система охорони здоров'я – 25 %, державне управління – 18 %, транспортна сфера – 16 %). Найменша частка внутрішніх кіберінцидентів спостерігається у будівельній галузі – 12 % та у сфері роздрібної торгівлі – 11 %.

Таблиця 2.2. Специфіка процесів цифрової трансформації у банківській сфері та відповідні ризики

Специфіка цифрової трансформації у банках	Ризики, пов'язані з цифровізацією банківських сервісів
модернізація цифрових процесів охоплює не окремі операційні напрямки, а всю інфраструктуру банківської діяльності	загрози мають ширший масштаб прояву
необхідність оперативно адаптовуватися до технологічних змін та швидко інтегрувати нові рішення	потреба у безперервному оновленні й удосконаленні систем захисту з урахуванням актуальної інформації
переважання операцій у безготівковому та електронному форматі, що забезпечує дистанційне обслуговування й перехід основних	банки залишаються ключовими цілями для кіберзлочинності, що спричиняє високі потенційні фінансові збитки

продуктів у цифрове середовище	
поступове підвищення фінансової та цифрової обізнаності користувачів банківських сервісів	збільшується індивідуальний ризик для клієнта-фізичної особи, якщо він не володіє достатніми цифровими та фінансовими навичками
широке застосування новітніх технологій як засобу посилення конкурентних переваг	зростає значення довгострокових стратегічних ризиків у випадку зміщення фокусу банку на швидкий ефект від цифрових рішень
відсутність стриманого ставлення до технологічних інновацій серед значної частини працівників банку	підвищується рівень загроз, що можуть виникати всередині організації
накопичення великих масивів інформації, які потребують зберігання, аналізу й використання для оптимізації взаємодії з клієнтами	збільшується обсяг витрат на підтримку високого рівня інформаційної безпеки

Створено автором на основі джерел: [36,39,40]

Однією з тенденцій злочинної активності в сфері цифрового банкінгу. є нефінансова мотивація зловмисників. Раніше основним стимулом для більшості організованих злочинних структур був фінансовий інтерес. Нині ж спостерігається поява груп, чия діяльність спрямована на кібершпигунство у банківській сфері, включаючи збір відомостей про фінансово-політичну еліту країни, VIP-клієнтів та платежі державних підприємств.

Інша тенденція – збільшення кількості диверсійних атак. Раніше зловмисники зосереджувалися переважно на крадіжці коштів, зараз після етапу шпигунства чи викрадення даних відбуваються дії, спрямовані на руйнування

банківської інфраструктури та видалення доказів. Через це фінансові установи витрачають ресурси на відновлення систем замість розслідування інцидентів.

Третя тенденція – поширення нових методів фішингу. Банки змушені застосовувати віддалену ідентифікацію користувачів для виявлення шкідливого програмного забезпечення.

Четверта тенденція – слабка координація міжнародного співробітництва, що дозволяє злочинним угрупованням обирати для атак країни з конфліктною політичною ситуацією [51].

Загалом, фінансові установи суттєво недофінансували інформаційну безпеку, і на сьогодні вона розвивається лише на початковому рівні. Тому в секторі необхідний обмін інформацією, підвищення освітнього рівня учасників через систему обміну знаннями про кіберзагрози та загальний досвід [8].

Практично всі перевірки, що проводить НБУ, включають оцінку виконання банками нормативних вимог щодо інформаційної безпеки. На даний час не існує жодного банку, який би повністю відповідав усім встановленим стандартам [55].

Найефективніший метод протидії новим типам кібератак – організований обмін інформацією, який важливий не тільки всередині країни, а й на міжнародному рівні [30].

Щоб зменшити фінансові та репутаційні втрати, банкам потрібно впровадити комплекс заходів:

– провести аудит поточних заходів захисту та оцінити слабкі місця у власній політиці кібербезпеки;

– делегувати частину функцій кіберзахисту зовнішнім експертам для подолання розриву у кваліфікації;

– застосовувати багатофакторну аутентифікацію, що вимагає від користувача кількох облікових даних для доступу;

– систематично навчати персонал щодо ризиків та методів їх виявлення;

– інформувати клієнтів про потенційні шахрайські схеми та захист власної інформації;

– розглядати можливість укладення договорів кіберстрахування, що є невід'ємною складовою плану безпеки [8].

Кіберстрахування потребує особливої уваги через великий потенціал розвитку. Поліси таких страхових продуктів поки що не мають уніфікованих стандартів [55].

Застрахувати можна збитки від:

– технічних збоїв та програмних помилок;

– некерованих атак – фішинг, картинг, хактивізм;

– цільових атак – DDoS, промислове шпигунство, криптолокерство;

– внутрішніх атак – викрадення конфіденційних даних та комерційної інформації [56].

Договори кіберстрахування в Україні формуються на основі угоди між страховиком та страхувальником, оскільки законодавчого регулювання цієї сфери поки що немає. Спостерігається поступове зростання виплат за такими договорами, що підвищує довіру клієнтів. Наприклад, у 2021–2022 рр. виплати за ризиками, пов'язаними з вірусами-вимагачами, зросли у світі вчетверо [40].

Для отримання адекватної страхової компенсації необхідно ретельно вивчити умови договору та, за потреби, включати додаткові розширення покриття. Через специфіку кіберризиків бажано укладати окремі договори [31].

InsurTech активно розвивається, застосовуючи машинне навчання, блокчейн, аналіз великих даних, що дозволяє створювати актуальні продукти страхування кіберризиків [32].

Страхувальники повинні чітко визначати бажаний обсяг покриття договору, який зазвичай формується індивідуально відповідно до потреб клієнта та специфіки бізнесу [33]. Українські страховики пропонують можливість комбінувати основне та додаткове покриття [34].

Основне покриття включає:

– реагування на інциденти та оплату експертних послуг для припинення кібератаки;

– компенсацію втрат прибутку через збої IT-систем та крадіжку

даних;

– викупну суму для відновлення доступу до заблокованої інформації;
– судові витрати, пов’язані з позовами третіх осіб [35].

Додаткове покриття передбачає:

– витрати на розслідування та технічну/юридичну експертизу;
– антикризовий PR та відновлення репутації;
– відновлення пошкоджених даних;
– покриття штрафних санкцій від державних органів [36].

У майбутньому кіберзагрози залишаться, але хакери використовуватимуть їх більш інтенсивно. Використання AI дозволить створювати нові віруси, знаходити вразливості, генерувати фішингові ресурси [37].

Головним завданням для центрального банку та регуляторів є формування національної стратегії кібербезпеки для банківського сектору, що допоможе ефективніше протидіяти загрозам [30].

2.2. Оцінка поточного рівня цифрової трансформації банків України

Розвиток дистанційного обслуговування у банківській сфері України становить значний етап цифрової трансформації фінансового сектору. За останні роки, особливо з середини 2010-х, спостерігається стрімке зростання цього напряму, що стало можливим завдяки впровадженню сучасних технологій та покращеній доступності інтернет-з’єднання і мобільних пристроїв.

Ключові віхи еволюції, зокрема запуск перших платформ інтернет-банкінгу та поява повністю цифрових банків, значно підвищили якість обслуговування клієнтів. Вплив пандемії та воєнних подій додатково прискорив перехід користувачів до дистанційних сервісів, що дало змогу банківському сектору функціонувати навіть у кризових умовах.

Отже, дистанційне банківське обслуговування в Україні перетворюється на невід'ємну складову сучасної фінансової системи. Воно забезпечує швидкий, безпечний і зручний доступ до банківських послуг, що відповідає світовим тенденціям цифровізації та модернізації фінансової інфраструктури [7].

Щоб установа могла вважатися постачальником цифрового банкінгу, вона має забезпечувати: повний комплекс послуг, цілодобовий доступ 24/7, надання сервісів поза межами класичного обслуговування, а також уніфіковані маршрути клієнта [37].

Для дослідження обрано два державні банки: ПриватБанк та Sense Bank. Згідно з рейтингом Forbes, вони є лідерами за рівнем діджиталізації та інноваційними сервісами. Метою аналізу є визначення та порівняння специфіки дистанційного банківського обслуговування цих установ, а також оцінка переваг і недоліків [31, 25].

Порівняння спектру послуг

ПриватБанк: Банк надає можливість відкриття рахунків і депозитів онлайн, оформлення кредитних заявок через веб-ресурс і мобільний додаток, валютний обмін, SWIFT-перекази, внутрішні перекази між картками, оплату комунальних послуг. Мобільний застосунок Приват24 доступний для iOS та Android, також існує адаптивна версія сайту [25].

Особливі сервіси включають підтримку міжнародних переказів через Western Union та інші платіжні системи, власну систему кешбеку, NFC-платежі через смартфони. Для отримання кредиту необхідно мати картку «Універсальна», яку можна відкрити миттєво у вигляді віртуальної Digital-картки через Приват24 або отримати пластикову картку поштою («Нова Пошта»/поштомат) [31].

Онлайн відкриття депозитів доступне через Приват24 або веб-сайт. Всі операції за вкладами, включно з закриттям депозитів, доступні дистанційно. Для зручного управління депозитами існує окремий додаток «Мої вклади» [27].

Sense Bank: Для оформлення кредиту також необхідно отримати картку. Миттєве відкриття рахунку та випуск цифрової картки можливі через

мобільний додаток Sense SuperApp. Депозити онлайн доступні у Sense SuperApp або My Sense Bank. Мінімальна сума депозиту нижча за онлайн-послугою: 100 UAH, 20 USD, 20 EUR, тоді як у відділеннях – 1000 UAH, 200 USD, 200 EUR [28].

Онлайн-депозити для корпоративних клієнтів у обох банках дозволяють миттєве розміщення коштів, дистанційне поповнення та зняття, а також контроль залишків у реальному часі [29].

Спектр депозитних послуг у ПриватБанку та Sense Bank практично однаковий, проте на сайті Sense Bank не зазначено, чи можливо відкрити строковий депозит онлайн [30].

Таблиця 2.2 – Порівняння специфічних сервісів у ПриватБанку та Sense Bank

Особливі послуги	**ПриватБанк**	**Sense Bank**
Відкриття рахунку онлайн	Так	Так
Відкриття депозиту онлайн	Так	Так
Кредитні заявки онлайн	Так	Так
Валютний обмін онлайн	Так	Так
SWIFT-перекази	Так	Так
Перекази між картками	Так	Так
Оплата комунальних послуг	Так	Так
Мобільний додаток	iOS, Android	Sense SuperApp / My Sense Bank
Адаптивний веб-сайт	Так	Так
Міжнародні перекази (Western Union тощо)	Так	Ні
Кешбек на платежі	Так	Ні
NFC-платежі	Так	Ні
Миттєве відкриття Digital-	Так	Так

картки		
Доставка пластикової картки	Так, «Нова Пошта» / поштомат	Ні
Додаток для управління депозитами	«Мої вклади»	Ні
Мінімальна сума депозиту онлайн	100 UAH / 20 USD / 20 EUR	100 UAH / 20 USD / 20 EUR
Мінімальна сума депозиту у відділенні	1000 UAH / 200 USD / 200 EUR	1000 UAH / 200 USD / 200 EUR

[23]

Зручність експлуатації

ПриватБанк:

Інтерфейс: Додаток Приват24 належить до найбільш розвинених рішень в Україні. Він забезпечує широкий спектр функцій, проте початківцям користувачам інтерфейс може здатися надто насиченим. Мобільний додаток відзначається стабільністю роботи та високою якістю. Дизайн інтуїтивно зрозумілий, хоча іноді процес виконання базових операцій вимагає зайвих кроків.

Рисунок 2.3 – Інтерфейс мобільного додатку ПриватБанк [23]

Sense Bank:

Інтерфейс: Інтерфейс додатку менш розвинений у порівнянні з основними конкурентами. Можливі складнощі при навігації та пошуку необхідних функцій.

Мобільний додаток: Функціонує стабільно, але його зовнішній вигляд виглядає дещо застарілим. Основні операції виконуються без проблем, проте відсутні деякі сучасні функції, наприклад кешбек та інтеграція з NFC-сервісами.

Рисунок 2.4 – Інтерфейс мобільного додатку Sense Bank [23]

ПриватБанк має низку вагомих переваг, серед яких широкий спектр банківських послуг, добре опрацьований мобільний додаток і веб-платформа. Дистанційне банківське обслуговування у ПриватБанку характеризується високою зручністю та комплексністю функціоналу, а користувачі можуть взаємодіяти як із веб-версією сайту, так і через мобільний додаток. Усі основні операції доступні в онлайн-режимі: будь-які перекази, включно з міжнародними, проведення платежів, оформлення кредитів, відкриття депозитів, надання інформаційних послуг та інші. Дистанційні сервіси також доступні корпоративним клієнтам, що сприяє збільшенню обсягів коштів на рахунках. Інтерфейс додатку простий та зрозумілий, проте можливе перевантаження функцій, що іноді ускладнює користування. Такий сервіс

оптимальний для користувачів, які цінують широкий функціонал та високий рівень безпеки, однак може бути складним для новачків.

У свою чергу, дистанційне банківське обслуговування в Sense Bank також відповідає сучасним цифровим стандартам. У системі впроваджено багато інноваційних рішень, що дозволяють миттєво здійснювати різноманітні операції. Клієнти мають доступ до повного спектру онлайн-операцій: перекази, платежі, оформлення кредитів, відкриття депозитів, а також підтримку через віртуального помічника. Для корпоративних клієнтів реалізовано окремий додаток Sense Business Online, що робить сервіси максимально орієнтованими на потреби бізнесу. Інтерфейс додатку комфортний та зручний у використанні, а рекомендацією є подальше впровадження інноваційних продуктів та вдосконалення існуючих сервісів.

Конкуренція між фінтех-компаніями та традиційними банками залишається високою, тому важливо відстежувати останні тенденції та оцінювати, які рішення найкраще задовольняють фінансові потреби клієнтів. Кожен сектор має свої сильні й слабкі сторони, а ключ до успіху полягає у гармонійному поєднанні переваг обох сфер для досягнення фінансових результатів. У сучасних умовах інновації відіграють вирішальну роль у забезпеченні конкурентної переваги.

Інтуїтивно зрозумілий користувацький досвід (UX) передбачає створення цифрового фінансового сервісу, який відповідає потребам користувачів та надає прості й зручні способи виконання банківських операцій. Привабливий інтерфейс (UI) є необхідним, але недостатнім елементом: дизайн повинен орієнтуватися на користувача, враховувати його очікування та потреби, щоб взаємодія з продуктом була максимально зрозумілою.

Ефективність цифрових сервісів критично залежить від часу: чим менше кроків потрібно користувачеві для виконання операцій, тим вища ефективність. Тому важливо створювати максимально прості та зрозумілі рішення, де «менше дій — більше результату» [6,7]

2.3. Вплив цифрових сервісів на фінансову стабільність та конкурентоспроможність банків

Світовий та український ринок цифрових банківських платформ демонструють стабільне зростання, що пояснюється потребою банків оптимізувати внутрішні процеси, підвищити якість обслуговування клієнтів і забезпечити доступність сервісів у режимі 24/7. Сучасні цифрові системи дозволяють не лише автоматизувати традиційні банківські операції, а й створювати комплексні екосистеми, які включають широкий спектр фінансових та нефінансових послуг, підсилюючи конкурентоспроможність установ [25, 26].

Залежно від типу ринку платформи класифікуються на роздрібні та корпоративні, за способом розгортання — хмарні або локальні рішення, а також за географічними сегментами, що забезпечує нерівномірний, але динамічний розвиток індустрії [23, 30].

Глобальні тенденції, зокрема перехід на хмарну інфраструктуру та застосування новітніх технологій, таких як блокчейн, стимулюють банки впроваджувати сучасні цифрові рішення, що підвищує якість послуг і зменшує операційні витрати [26, 27].

В Україні цифровий банкінг розвивається під впливом високої конкуренції між фінансовими установами, які прагнуть запропонувати клієнтам максимально широкий функціонал. Традиційні банки активно оптимізують мережу відділень і переводять ключові продукти у цифрові канали: 60% установ скоротили кількість фізичних точок обслуговування, а 34% впровадили повністю цифрові процеси, що відображає значні структурні зміни в моделі обслуговування [3, 24].

Банки конкурують не лише швидкістю операцій, а й інноваційністю сервісів, яка стає ключовим фактором конкурентної переваги. Сучасний цифровий банк повинен забезпечувати повний спектр дистанційних послуг, персоніфікацію сервісів, безперервний доступ 24/7 і розширені функції, зокрема

управління особистими фінансами, прогнозну аналітику та елементи гейміфікації взаємодії з клієнтом [31, 36].

Аналіз українського ринку показує, що ПриватБанк і Sense Bank посідають провідні позиції завдяки активному впровадженню цифрових технологій. ПриватБанк пропонує широкий функціонал, включно з онлайн-відкриттям рахунків, оформленням кредитів, валютним обміном, міжнародними переказами та мобільним додатком Приват24, що підвищує його конкурентоспроможність у сегменті дистанційного обслуговування [25, 31].

У контексті цифрової конкуренції банки нарощують функціональність мобільних додатків, інтегрують нові продукти, розширюють спектр послуг і вдосконалюють користувацький інтерфейс. Важливими факторами успіху на ринку є швидкість проведення платежів, якість мобільного банкінгу, гнучкість тарифних пропозицій, інтеграція додаткових сервісів і підтримка міжнародних операцій [26, 30].

Цифровий банкінг сприяє формуванню нових джерел доходів, розширенню охоплення клієнтської бази без відкриття фізичних відділень і зменшенню витрат на обслуговування, що посилює його стратегічну роль у розвитку банків [53].

Конкуренція стимулює активну інтеграцію нових технологій, формуючи динамічний та інноваційний сегмент фінансової системи України [54].

Висновки за розділом 2

Проведений аналіз показав вплив цифрових технологій на банківську діяльність та сучасний стан цифрового банкінгу в Україні.

Цифровий банкінг нині виступає не лише інструментом модернізації окремих продуктів або каналів обслуговування, а комплексною концепцією трансформації банківської моделі. Він передбачає активне використання дистанційних технологій, автоматизацію процесів, застосування штучного інтелекту, великих даних, мобільних платформ і хмарних рішень. Це формує новий формат взаємодії між банком і клієнтом, забезпечуючи персоналізацію, швидкість та безперервність фінансових послуг.

Організаційне й правове забезпечення цифрового банкінгу в Україні розвивається поступово, із акцентом на зміцнення кіберстійкості та підвищення технологічної сумісності банківських систем. Національний банк України відіграє ключову роль у формуванні нормативних вимог до інформаційної безпеки, регулюванні дистанційної ідентифікації, управлінні кіберризиками та стандартизації електронних сервісів. Водночас нормативна база потребує подальшого удосконалення з урахуванням новітніх загроз і глобальних тенденцій.

Цифровізація змінює конкурентне середовище банківської системи: переваги мають ті установи, які швидко впроваджують інновації, модернізують цифрові канали та забезпечують високий рівень UX. Порівняльний аналіз ПриватБанку та Sense Bank показав, що конкуренція стимулює розвиток багатофункціональних мобільних додатків, екосистем послуг та автоматизованих сервісів, зміцнюючи ринкові позиції банків і встановлюючи нові стандарти якості

Світові та національні тенденції свідчать про зростання ролі штучного інтелекту, хмарної інфраструктури, відкритого банкінгу та цифрових екосистем. Україна активно адаптується до глобальних трендів, навіть за

складних умов, впроваджуючи інноваційні сервіси та посилюючи співпрацю між банками та фінтех-компаніями.

Серед ризиків цифрового банкінгу провідне місце займають кіберзагрози, шахрайство, витік даних, технічні збої та внутрішні загрози (human factor). Зростання складності кіберризиків потребує системного підходу до захисту інформації, моніторингу подій безпеки та розвитку механізмів кіберстрахування

Виявлено ключові проблеми: недостатній рівень кіберзахисту окремих банків, дефіцит кваліфікованих IT-кадрів, нерівномірна цифрова грамотність клієнтів та уповільнене оновлення нормативної бази. Для їх подолання запропоновано комплексні заходи, включно з модернізацією безпекової інфраструктури, впровадженням багатофакторних систем захисту, вдосконаленням регуляторного поля та навчанням персоналу.

Центральний банк виконує критично важливі завдання: забезпечення технологічної стійкості фінансової системи, удосконалення регуляторних вимог кібербезпеки, координацію обміну інформацією про загрози між банками, підвищення стандартів ризик-менеджменту та підтримку розвитку інноваційних цифрових рішень.

Узагальнюючи, цифрові технології створюють нову архітектуру банківського сектору, змінюючи підходи до організації роботи, безпеки, конкуренції та взаємодії з клієнтами. Ефективний розвиток цифрового банкінгу в Україні можливий за умови поєднання інновацій, належного регуляторного контролю, високого рівня інформаційної безпеки та здатності банків адаптуватися до динаміки кіберризиків. Це формує підґрунтя для підвищення стійкості, ефективності та довіри до національної банківської системи в цифрову епоху.

РОЗДІЛ 3. ПЕРСПЕКТИВИ ТА НАПРЯМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ДІЯЛЬНОСТІ БАНКІВ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

3.1. Впровадження міжнародного досвіду цифровізації банківської справи в Україні

Зростання ступеня цифровізації та посилення геополітичної напруженості підвищують ризик кібератаки з системними наслідками. Як зазначено у дослідженнях, ризик екстремальних втрат від інцидентів у кіберсфері значно зріс, що потенційно може спричинити проблеми з фінансуванням для банків і навіть поставити під загрозу їхню платоспроможність [1], [55].

Серйозний інцидент у банківській установі може підірвати довіру до неї, а в крайніх випадках призвести до обвалу на ринку та масового вилучення вкладів. Незважаючи на те, що жодного значного масового вилучення вкладів у результаті кіберінцидентів ще не відбулося, аналіз невеликих банків США показує помірний та стійкий відтік вкладів після кібератак [55], [56].

Кіберінциденти, які порушують надання критично важливих послуг, таких як платіжні мережі, можуть серйозно вплинути на економічну активність. Наприклад, атака на Центральний банк Лесото у грудні 2023 року дестабілізувала роботу національної платіжної системи країни, порушивши проведення операцій місцевими банками [8], [51].

Згідно з опитуванням МВФ та центральних банків, основи політики кібербезпеки, особливо у країнах з ринком, що формується, та країнах, що розвиваються, нерідко недосконалі. Лише близько половини опитаних країн мали національну стратегію кібербезпеки для банківського сектору або спеціальні нормативні акти, що регламентують питання кібербезпеки [1], [55].

Велика частина атак фінансується на державному рівні, що створює серйозні виклики для фінансового сектора, адже державні структури мають інші цілі та метрики роботи, ніж комерційні банки [10], [57].

Для підвищення стійкості банківського сектора органам влади слід розробити адекватну національну стратегію кібербезпеки, поряд із ефективним регулюванням та наглядовим потенціалом. Основні елементи включають:

- періодичну оцінку кіберсфери та виявлення потенційних системних ризиків, зумовлених взаємопов'язаністю та концентрацією, у тому числі зі сторони сторонніх постачальників послуг;
- заохочення «кіберзрілості» серед банків, включаючи доступ до експертних знань у галузі кібербезпеки на рівні керівництва;
- поліпшення кібергігієни банків, їх онлайн-безпеки та працездатності системи (захист від шкідливих програм та багатофакторна автентифікація), а також навчання та підвищення обізнаності персоналу [1], [52], [55].

Оскільки джерела атак нерідко розташовані за межами країни походження банку, а доходи можуть спрямовуватися через кордони, для успішного усунення кіберзагроз необхідне міжнародне співробітництво [51], [55].

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 національні органи мають мати ефективні протоколи реагування та механізми антикризового управління. МВФ активно підтримує держави-члени у зміцненні систем кібербезпеки, надаючи консультації з питань економічної політики та заходи щодо розвитку потенціалу [55], [56], [57].

У розвинених країнах центральні банки демонструють значну стурбованість кіберзагрозами для банківських установ, що відображається у вищій оцінці витрат, пов'язаних із такими атаками. Зокрема, на думку респондентів, найбільші фінансові втрати спричиняють інциденти, пов'язані з шкідливим програмним забезпеченням, включаючи як цілеспрямовані атаки на ІТ-інфраструктуру, так і ненавмисні технічні збої. У відповідь на зростання кіберризиків більшість центральних банків збільшують фінансування

інформаційних технологій: понад 60 % центробанків розвинених країн і близько 50 % установ у країнах, що розвиваються, з 2020 року підвищили бюджет на IT-інфраструктуру на 5–20 %. Крім того, приблизно чверть центробанків країн, що розвиваються, збільшила фінансування більш ніж на 20 %, що ілюструє рис. 3.1.

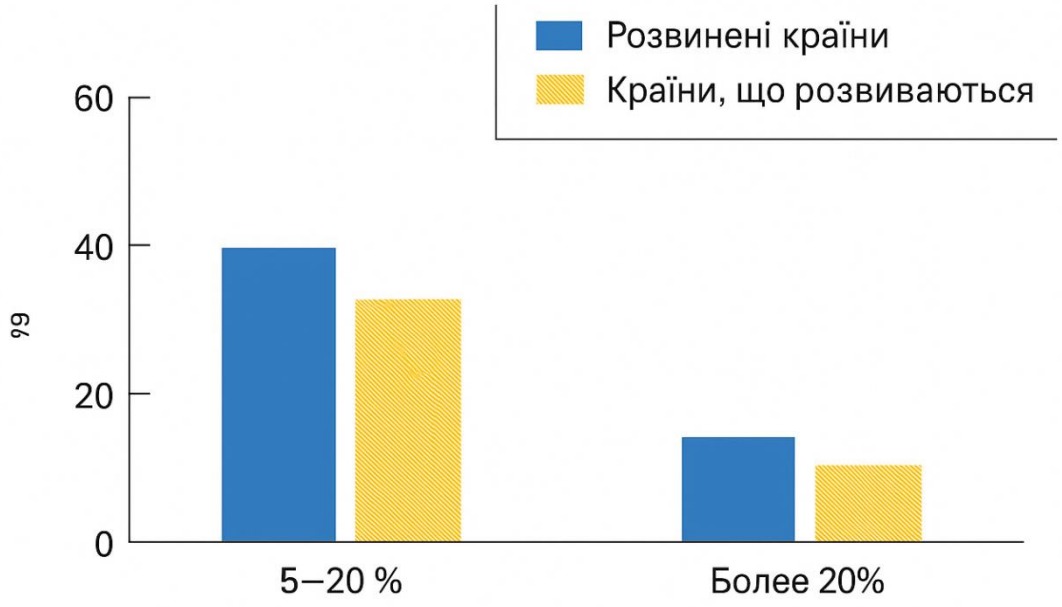

Рисунок 3.2 – Динаміка збільшення витрат центральних банків на кібербезпеку та інформаційні технології (%) станом на кінець 2024 року [1]

Для протидії зазначеним загрозам фінансові установи повинні будувати багаторівневу систему захисту, яка охоплює технології, процеси та персонал. Основні принципи кіберзахисту у фінансовому секторі можна визначити так:

– багаторівневий захист (defense-in-depth);

– постійний моніторинг і своєчасне виявлення інцидентів;

– надійна аутентифікація та контроль доступу;

– управління вразливостями та регулярне оновлення систем;

– управління інцидентами та забезпечення безперервності бізнес-процесів;

– дотримання міжнародних і національних стандартів та нормативних вимог;

– навчання персоналу та формування культури кібербезпеки.

З огляду на сучасні виклики в інформаційній безпеці, пов’язані з інтенсивною цифровізацією, Національний банк України передбачає:

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

– створення умов для безпечного впровадження цифрових та платіжних інновацій та забезпечення технологічного суверенітету;

– контроль ризиків інформаційної безпеки та операційної надійності для забезпечення безперервності надання банківських і фінансових послуг [1, 52].

Ефективна система кібербезпеки повинна не лише запобігати вторгненням, а й вчасно їх виявляти. Для цього фінансові установи створюють центри моніторингу безпеки (SOC), оснащені SIEM-системами, які збирають логи з усіх критичних систем і в режимі реального часу аналізують їх на предмет підозрілих інцидентів [55, 51]. Водночас важливо вести журнали реєстрації подій (лог-файли) на всіх вузлах і зберігати їх протягом достатнього часу. Проте, за даними опитувань, лише близько 15% українських підприємств повноцінно займаються веденням логів безпеки [32], що свідчить про наявні прогалини у виявленні кіберінцидентів.

Завдання із забезпечення інформаційної безпеки та кіберстійкості банку з метою підтримання фінансової стабільності можуть бути реалізовані шляхом:

– упровадження пропорційних регуляторних вимог щодо захисту інформації під час надання банківських послуг, роботи на фінансових ринках і здійснення переказів у платіжній системі НБУ;

– організації наглядових процедур з питань інформаційної безпеки, які включають систематичний дистанційний і контактний нагляд;

– застосування методології, що передбачає регулярне проведення кібернавчань.

Завдання щодо забезпечення операційної надійності та безперервності діяльності банків виконуються завдяки:

– формуванню пропорційних регуляторних вимог для всіх піднаглядових установ фінансового сектору;

– інтеграції питань операційної надійності у систему управління операційним ризиком.

Протидія комп'ютерним атакам при впровадженні інноваційних фінансових технологій ґрунтується на необхідності попередження та виявлення кіберзлочинів. Мета вибору цілей кіберзлочинців залежить від їх технічної підготовки, наявних інструментів та знань щодо внутрішніх процесів банку [36]. У більшості випадків ключовим чинником успіху таргетованої атаки є недостатньо захищені інформаційні системи.

Типовий сценарій таргетованої кібератаки на банківську установу включає такі етапи:

1. масова розсилка електронних листів працівникам банку, що містять шкідливе програмне забезпечення;

2. після відкриття листа відбувається інфікування комп'ютера працівника, що дає зловмиснику первинний доступ;

3. подальше дослідження локальної мережі з інфікованого вузла з метою отримання доступу до контролера домену та облікових даних адміністраторів;

4. після здобуття паролів і доступу до контролера домену атакуючий отримує можливість проникнути у внутрішню мережу банку;

5. встановлення шкідливого програмного забезпечення на банкомати для ініціювання несанкціонованої видачі готівки через віддалені команди.

Після отримання контролю над банкоматом у схему підключаються співучасники, які безпосередньо здійснюють вилучення готівки у визначений час. У більшості випадків після завершення операції шкідливе програмне забезпечення видаляється з банкоматів [36].

Окремої уваги потребує явище соціальної інженерії, яке є однією з найсерйозніших загроз кібербезпеці. Соціальна інженерія — це комплекс методів психологічного впливу, спрямованих на спонукання користувача до

дій, вигідних зловмиснику. Працівник банку як користувач інформаційної системи має певні права доступу та виконує критичні операції, тому саме він може стати найслабкішою ланкою системи захисту. Уразливість може виникати як унаслідок необережності, так і через умисні дії (наприклад, невдоволення роботою або конфлікти в колективі).

Зловмисники можуть отримати значний обсяг корисної інформації для організації таргетованої атаки зі спілкування з персоналом банку або з відкритих джерел, навіть не застосовуючи шкідливе програмне забезпечення чи складні технічні засоби.

3.2. Ключові напрямки вдосконалення цифрових рішень у банківському секторі

Для ефективного запобігання кібератакам на банківські установи фінансові організації повинні реалізовувати комплекс наступних заходів:

– впровадження апаратних, програмних та програмно-апаратних засобів захисту інформації;

– безперервний моніторинг подій безпеки;

– підвищення кваліфікації працівників, відповідальних за інформаційну безпеку;

– навчання всіх співробітників банку основам інформаційної безпеки;

– підтримка здорового корпоративного клімату, оскільки задоволений працівник рідше становить внутрішню загрозу;

– інформування та навчання клієнтів з питань фінансової та цифрової грамотності;

– розробка внутрішньої нормативної документації, що регламентує сферу інформаційної безпеки;

– ретельний підбір персоналу з урахуванням професійних, етичних та моральних якостей;

– обмін інформацією про кібератаки між банками та правоохоронними органами.

Комплексний підхід та актуальна інформація про методи та сценарії дій хакерів є ключовими для ефективної протидії кіберзагрозам.

Кібербезпека охоплює різні аспекти, серед яких:

– виявлення та усунення архітектурних уразливостей;

– захищеність мережі та веб-сайтів;

– належне зберігання конфіденційних та персональних даних;

– безпека паролів та розмежування рівнів доступу;

– дотримання співробітниками правил інформаційної безпеки;

– готовність до DDoS-атак.

У 2025 році Національний банк України запланував проведення перевірок з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг у шести банках: "Креді Агріколь Банк", "Райффайзен Банк", "Південний", "Банк Кредит Дніпро", "Комінбанк" та "Альтбанк". План перевірок сформовано на основі ризик-орієнтованого підходу, з урахуванням інформації про діяльність банків, обсяги надання фінансових послуг та специфіку їх функціонування. Це дозволить банкам вдосконалити власні можливості реагування на сучасні кіберзагрози та зміцнити кіберстійкість.

Крім того, НБУ пропонує оновлення нормативних актів щодо функціонування системи кіберзахисту та контролю за станом інформаційної безпеки в банківській системі. Зокрема, удосконалюється процес щорічного звітування банками за результатами самооцінки організації інформаційної безпеки та кіберзахисту, а також врегульовується порядок інформування НБУ про значні кіберінциденти та суттєві зміни в організації кіберзахисту. Відповідні зміни передбачені проєктом постанови Правління НБУ «Про затвердження змін до нормативно-правових актів з питань інформаційної безпеки та кіберзахисту».

Зокрема, зміни стосуються:

1. **Положення про здійснення контролю** за дотриманням банками вимог законодавства у сфері інформаційної безпеки та електронних довірчих послуг (постанова Правління НБУ № 4 від 16.01.2021) — удосконалено процедуру самооцінки та звітування, а також обов'язкове інформування НБУ про істотні зміни в організації заходів кіберзахисту;

2. **Положення про організацію кіберзахисту** в банківській системі України (постанова Правління НБУ № 178 від 12.08.2022) — запроваджено обов'язкове інформування НБУ про значні кіберінциденти.

Реалізація цих заходів сприятиме виконанню НБУ його функцій відповідно до законів України «Про основні засади забезпечення кібербезпеки» та «Про Національний банк України».

Особливу увагу слід приділяти централізованому підходу до кібербезпеки, який передбачає координацію реагування на загрози на галузевому рівні та аналіз потенційних ланцюжків подій, що можуть мати критичні наслідки.

Висновки за розділом 3

У третьому розділі досліджено ключові загрози кібербезпеці банківського сектору в умовах цифрової трансформації, проаналізовано сучасні тенденції кібератак та визначено напрями вдосконалення системи кіберзахисту.

1. Сучасний рівень цифровізації банківської діяльності та посилення геополітичних і економічних ризиків зумовлюють значне зростання системних кіберзагроз. Кіберінциденти часто супроводжуються фінансовими втратами, що впливає на ліквідність, платоспроможність та довіру до фінансових установ. Навіть локальні порушення роботи банку можуть мати ланцюгові ефекти, підвищувати ризики відтоку коштів та загрожувати фінансовій стабільності.

2. Політика кібербезпеки у багатьох країнах, зокрема тих, що розвиваються, недостатньо розвинена. Часто відсутні повноцінні стратегії та нормативні акти для банківського сектору. Зростання кількості атак з ознаками державного фінансування підкреслює потребу у міжнародному співробітництві та гармонізації стандартів кіберзахисту.

3. Банки залишаються одними з найбільш вразливих цілей через масштабність операцій, доступ до великих обсягів фінансових і персональних даних та високу залежність від цифрових систем. Переважна частина успішних атак ґрунтується на соціальній інженерії та вразливостях користувачів, що підкреслює необхідність системного навчання персоналу та вдосконалення процедур доступу і контролю.

4. Забезпечення кіберстійкості банківського сектору потребує комплексного багаторівневого підходу: побудови сучасної архітектури захисту, впровадження систем моніторингу та виявлення інцидентів (SOC/SIEM), регулярного тестування готовності до кібератак, розвитку протоколів реагування та забезпечення безперервності бізнес-процесів, з особливим акцентом на критичні сервіси, зокрема платіжні системи.

5. НБУ активізує регуляторні заходи у сфері кіберзахисту: розширює наглядові інструменти, впроваджує вимоги щодо звітності про інциденти,

удосконалює стандарти кіберстійкості та проводить планові перевірки банків. Оновлення нормативної бази спрямоване на підвищення прозорості, посилення контролю за ризиками та імплементацію сучасних методів оцінки кіберзагроз.

Узагальнюючи, кібербезпека є ключовим чинником стійкості та конкурентоспроможності банківського сектору. Ефективна система кіберзахисту потребує поєднання технологій, регуляторної підтримки, навчання персоналу та міжінституційної координації, що забезпечує стабільність фінансового ринку, безперервність критичних операцій та довіру клієнтів у середовищі зростаючих кіберризиків.

ВИСНОВКИ

На основі проведеного дослідження можна зробити низку висновків щодо розвитку дистанційного банківського обслуговування та цифрової трансформації банківського сектору в Україні. Вітчизняний сегмент дистанційних банківських технологій перебуває в активній стадії розвитку, постійно удосконалюються технології взаємодії учасників, спрямовані на зниження операційних ризиків, підвищення ефективності виконання фінансових операцій та забезпечення захисту персональних даних клієнтів у цифровій інфраструктурі. Цифрова трансформація виступає ключовим елементом загальної стратегії розвитку банківського бізнесу. Її успіх у великій мірі визначається поєднанням правильно обраних технологій, компетентності персоналу, налагоджених процесів і ефективних операцій. Саме такий підхід дозволяє банкам швидко адаптуватися до складних умов, використовувати нові можливості, задовольняти змінні потреби клієнтів, стимулювати зростання та впроваджувати інновації, часто несподіваними способами.

Для того щоб банк міг вважатися постачальником цифрового банкінгу, він повинен забезпечувати повний спектр послуг, від реєстрації клієнтів до дистанційного надання всіх фронт-офісних сервісів, забезпечувати цілодобову доступність 24/7, а також пропонувати інноваційні сервіси поза рамками традиційного банківського обслуговування. Це можуть бути інструменти гейміфікації, управління особистими фінансами, прогнозний аналіз на основі поведінки клієнтів та інші послуги, що відповідають сучасному цифровому стилю життя. Ключовим аспектом цифрового банкінгу є уніфікований клієнтський досвід, що гарантує одноманітність обслуговування у всіх каналах, персоналізовані повідомлення та доступ до інформації з єдиного джерела. Не менш важливими є інтуїтивно зрозумілий користувацький досвід (UX) та привабливий інтерфейс (UI), що забезпечують простоту і зручність у використанні цифрових фінансових сервісів. Ефективність сервісів також залежить від того, наскільки швидко клієнт може виконати операцію: чим

менше часу та дій потрібно, тим краще, адже принцип “менше означає більше” у цьому випадку безпосередньо впливає на користувацький досвід.

Мною відзначено, що розвиток дистанційного обслуговування в Україні зумовлений кількома важливими чинниками. По-перше, технологічний прогрес і впровадження безпечних та зручних методів онлайн-платежів. По-друге, зростання кількості користувачів Інтернету та мобільних пристроїв, що дозволяє банкам розширювати клієнтську базу та пропонувати ширший спектр дистанційних послуг. По-третє, прагнення банків скоротити витрати на обслуговування та підвищити ефективність роботи.

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

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

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.

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

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). UR

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

8. Кіберризики: оцінка центральних банків. URL: https://www.bis.org/ijcb.htm?m=1012.

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

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

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

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.

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.

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

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.

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.

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

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.

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

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

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.

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

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

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.

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.

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.

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

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

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

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.

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.

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.

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

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.

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

51. 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.

52. 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.

53. 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).

54. 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

55. 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

56. 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

57. 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.