

**МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ**

ФАКУЛЬТЕТ ФІНАНСІВ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ

**КАФЕДРА ФІНАНСОВИХ РИНКІВ ТА
ТЕХНОЛОГІЙ**

**ВИПУСКНА КВАЛІФІКАЦІЙНА
(ДИПЛОМНА) РОБОТА**

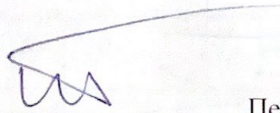
на тему: «Управління ризиками FinTech»

Здобувача вищої освіти II рівня, II курсу, групи ФМФз-22-1,
спеціальності 072 «Фінанси, банківська справа, страхування
та фондовий ринок»
освітньо-професійна програма «Фінансові технології»


(підпис)

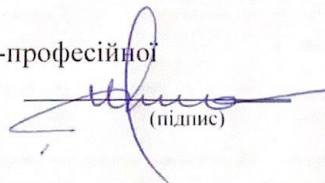
Чужа Марина Сергіївна
(прізвище, ім'я, по батькові)

Науковий керівник


(підпис)

Периарівський Олександр Васильович, к.е.н. доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

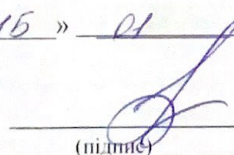
Гарант освітньо-професійної
програми


(підпис)

Корнєв Володимир Вікторович, д.е.н., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Допущено до захисту за рішенням кафедри фінансових ринків та технологій
протокол від « 15 » 01 2024 № 9

Завідувач
кафедри


(підпис)

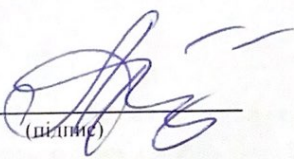
Береславська Олена Іванівна, д.е.н., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

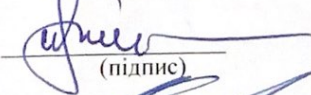
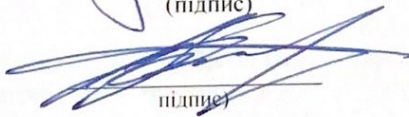
Ірпінь – 2024

Реєстрація № 7 12.01.2024 Букчоракіна В.С.
(дата) (підпис відповідальної особи)

Результати перевірки До захисту 10.01.2024 
(до захисту, на доопрацювання) (дата) (підпис)

Результат захисту 4 09.02.2024 ВЗГ
(оцінка) (дата) (підпис)

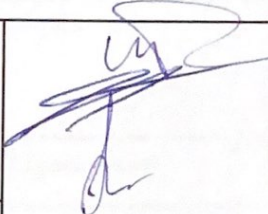
Голова комісії:  Тришостка І.О.
(підпис) (ініціали, прізвище)

Члени комісії:  Берешавська О.І.
(підпис) (ініціали, прізвище)
 Корнєв В.В.
(підпис) (ініціали, прізвище)
 Веремюк Н.Ю.
(підпис) (ініціали, прізвище)

БЛАНК ОЦІНЮВАННЯ РОБОТИ

Об'єкти контролю	Діапазон оцінки в балах	Фактична кількість балів	Примітки	Дата, П.І.П.: керівника, голови комісії членів комісії, секретаря, (підписи)
------------------	-------------------------	--------------------------	----------	--

ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ КЕРІВНИКОМ ТА РЕЦЕНЗЕНТОМ

1.Зміст випускної роботи (якість теоретичного матеріалу, його зв'язок з практичним, вміння представляти матеріал в логічній послідовності, наявність висновків та пропозицій)	від 0 до 30	22		
2.Дотримання вимог одо оформлення	від 0 до 10	8		
3.Вчасне виконання роботи на всіх етапах у встановлені кафедрою терміни	від 0 до 5	5		
4. Рецензент	від 0 до 5	5		
РАЗОМ БАЛІВ*	від 0 до 50	40		

ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ КОМІСІЄЮ ПО ЗАХИСТУ

1.Доповідь	від 0 до 10	10		
2. Роздатковий матеріал	від 0 до 5	5		
3. Знання теоретичного та практичного матеріалу, вміння відповідати на запитання	від 0 до 25	23		
5. Апробація (участь у конференціях)	від 0 до 10			
РАЗОМ БАЛІВ	від 0 до 50	38		
ЗАГАЛЬНА КІЛЬКІСТЬ БАЛІВ	від 0 до 100	78		

ПЕРЕВЕДЕННЯ ОЦІНКИ ЗА 100-БАЛЬНОЮ ШКАЛОЮ ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЕКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЕКТС	Оцінка за національною шкалою	Дата	П.І.П.: голови, членів комісії, секретаря, (підпис)
78	C	1	09.02.24	

Факультет Фінансів та цифрових технологій

Кафедра Фінансових ринків та технологій

Спеціальність 072 «Фінанси, банківська справа, страхування та фондовий ринок»

Освітня програма Фінансові технології

Затверджую

Завідувач кафедри Юлія КОВМЕНКО

«15» листопада 2022

Завдання на випускню кваліфікаційну (дипломну)

роботу здобувачу вищої освіти

Чужа Марина Сергіївна

(прізвище, ім'я, по батькові)

1. Тема випускної кваліфікаційної (дипломної) роботи «Управління ризиками в FinTech».

Затверджена наказом ректора від «15» 11.2022р. № 1208

2. Строк здачі закінченої роботи 4.12.2023

3. Мета роботи полягає в дослідженні методів управління ризиками в FinTech, а також розробка рекомендацій щодо покращення існуючих практик.

Об'єкт дослідження є процес управління ризиками в галузі FinTech.

Предмет дослідження є теоретичні та практичні аспекти управління ризиками в FinTech.

Орієнтовна база дослідження: фінансові технології в діяльності фінансових кредитних організацій та установ.

4. Вихідні дані до роботи: дані фінансової звітності та відкритих джерел.

5. Перелік графічного матеріалу: схеми, графіки, рисунки, таблиці.

6. Зміст випускної кваліфікаційної (дипломної) роботи (перелік питань з кожним розділом)

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ РИЗИКІВ В ГАЛУЗІ FINTECH

1.1 Поняття FinTech та його роль у фінансовому секторі

1.2 Основні види ризиків в галузі FinTech

РОЗДІЛ 2 АНАЛІЗ ПРАКТИКИ УПРАВЛІННЯ РИЗИКАМИ В ГАЛУЗІ FINTECH

2.1 Організація управління ризиками FinTech

2.2 Методи зниження кіберризиків в фінансовій сфері

РОЗДІЛ 3 ПРОБЛЕМИ ТА ШЛЯХИ УДОСКОНАЛЕННЯ УПРАВЛІННЯ РИЗИКАМИ FINTECH В УКРАЇНІ

7. Календарний план виконання роботи

№ п/п	Назва етапів випускної кваліфікаційної (дипломної) роботи	Строк виконання етапів роботи	
		За планом	Фактично
1	Підготовка 100% кваліфікаційної роботи та подання її на перевірку науковому керівнику	29.09.2023	29.09.2023
2	Доопрацювання роботи з урахуванням зауважень керівника та подання її а повторну перевірку керівнику	31.10.2023	31.10.2023
3	Попередній захист кваліфікаційної роботи	11-22.12.2023	20.12.2023
4	Отримання відгуку наукового керівника кваліфікаційної роботи	18-22.20.2023	21.12.2023
5	Рецензування кваліфікаційної роботи	26-29.12.2023	28.12.2023
6	Надання кваліфікаційної роботи для перевірки на плагіат	01.11.2023-04.12.2023	03.12.2023
7	Захист кваліфікаційної роботи	09.02.2024	09.02.2024

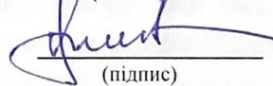
8. Дата видачі завдання «15» 11 2022

9. Науковий керівник кваліфікаційної роботи (проекту)


(підпис)

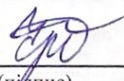
Пернарівський О. В.
(прізвище, ініціали)

10. Гарант освітньо-професійної програми


(підпис)

Корнєєв В. В.
(прізвище, ініціали)

11. Завдання до виконання отримав здобувач вищої освіти


(підпис)

Чужа М. С.
(прізвище, ініціали)

АНОТАЦІЯ

Управління ризиками FinTech

(назва випускної кваліфікаційної (дипломної) роботи)

Мета роботи полягає в дослідженні методів управління ризиками в галузі FinTech, а також розробка рекомендацій щодо покращення існуючих практик.

Завданнями роботи є:

Дослідити теоретичні аспекти управління ризиками FinTech

Проаналізувати асортимент ризиків FinTech

Проаналізувати підходи до управління ризиками в галузі Fintech

Дослідити ризики стартапів у FinTech

Виділити проблеми та визначити шляхи вдосконалення управління ризиками FinTech в Україні.

Предметом дослідження є теоретичні та практичні аспекти управління ризиками FinTech.

Об'єктом дослідження є процес управління ризиками в галузі FinTech.

Базою дослідження виступають фінансово-кредитні установи та організації.

За результатами дослідження визначені перспективи розвитку фінансових технологій в Україні та виділено основні ризики, які супроводжують цей розвиток. Оцінка ефективності управління ризиками була проведена на основі динамічного нормативу. Оцінка ця дозволила визначити, як банкінг в Україні пристосовується до викликів, пов'язаних із розвитком фінансових технологій.

Одержані результати можуть бути використані для розуміння ризиків у галузі FinTech та необхідності вдосконалення стратегій управління ними для забезпечення успішності банківських установ в сучасному фінансовому світі.

Кваліфікаційна робота містить 57 сторінок, 12 таблиць, 14 рисунків, список використаних джерел 29 найменувань, 7 додатків.

Ключові слова: УПРАВЛІННЯ РИЗИКАМИ FINTECH, ЗАГРОЗА УПРАВЛІННЯ РИЗИКАМИ FINTECH, ПОДАТКОВІ РИЗИКИ FINTECH В БАНКУ, ЗАКОНИ, РИЗИКИ FINTECH В БАНКУ .

Рік виконання кваліфікаційної роботи 2023 рік.

Рік захисту роботи 2024.

ABSTRACT

FinTech risk management

The purpose of the work is to investigate risk management methods in the FinTech industry, as well as to develop recommendations for improving existing practices.

The tasks of the work are:

- Explore theoretical aspects of FinTech risk management

- Analyze the range of FinTech risks

- Analyze approaches to risk management in the Fintech industry

- Explore the risks of startups in FinTech

- Identify problems and determine ways to improve FinTech risk management in Ukraine.

The subject of the study is the theoretical and practical aspects of FinTech risk management.

The object of the study is the risk management process in the FinTech industry.

The basis of the research is financial and credit institutions and organizations.

According to the results of the study, the prospects for the development of financial technologies in Ukraine were determined and the main risks accompanying this development were highlighted. The evaluation of the effectiveness of risk management was carried out on the basis of a dynamic norm. This assessment made it possible to determine how banking in Ukraine adapts to the challenges associated with the development of financial technologies.

The obtained results can be used to understand the risks in the FinTech industry and the need to improve their management strategies to ensure the success of banking institutions in the modern financial world.

The qualification work contains 57 pages, 12 tables, 14 figures, a list of used sources of 29 names, 7 appendices.

Keywords: FINTECH RISK MANAGEMENT, FINTECH RISK MANAGEMENT THREAT, FINTECH TAX RISKS IN THE BANK, LAWS, FINTECH RISKS IN THE BANK.

The year of performance of qualification work is 2023.

The year of job protection is 2024.

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ РИЗИКІВ В ГАЛУЗІ FINTECH.....	10
1.1 Поняття FinTech та його роль у фінансовому секторі	10
1.2 Основні види ризиків в галузі FinTech	13
РОЗДІЛ 2 АНАЛІЗ ПРАКТИКИ УПРАВЛІННЯ РИЗИКАМИ В ГАЛУЗІ FINTECH	21
2.1 Організація управління ризиками FinTech.....	21
2.2 Методи зниження кіберризиків в фінансовій сфері.	39
РОЗДІЛ 3 ПРОБЛЕМИ ТА ШЛЯХИ УДОСКОНАЛЕННЯ УПРАВЛІННЯ РИЗИКАМИ FINTECH В УКРАЇНИ	47
ВИСНОВКИ.....	60
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	62
ДОДАТКИ.....	66

ВСТУП

Управління ризиками у сфері фінансових технологій, відоме як FinTech, є надзвичайно важливим аспектом сучасного фінансового світу. Фінансові технології надають нові можливості, але також приносять нові види ризиків, що вимагають ефективного управління. Це дослідження присвячене ролі та методам управління ризиками в галузі FinTech.

Актуальність цієї теми визначається швидким розвитком фінансових технологій та зростаючою залежністю сучасного суспільства від цифрових фінансових послуг. З ростом обсягів та складності фінансових операцій виникає необхідність вдосконалення методів та підходів до управління ризиками у цій галузі.

Управління ризиками в галузі фінансових технологій, відомих як FinTech, в сучасному світі набуває особливої актуальності. Швидкі та постійні зміни в цій галузі створюють нові можливості та виклики, пов'язані з фінансовими операціями, цифровою безпекою та регулюванням. Існування та стабільність FinTech підприємств, а також захист фінансових інтересів клієнтів стають залежними від ефективного управління ризиками в цьому середовищі.

Актуальність дослідження полягає в тому, що FinTech постійно розвивається та динамічно змінюється, що призводить до збільшення рівня ризику. Зростаюча кількість фінансових технологій і продуктів робить їх уразливими перед новими загрозами, такими як кібератаки та зміни в регулюванні. Управління ризиками в FinTech стає важливою умовою для забезпечення стійкості і успіху в цій галузі.

Оптимальне управління ризиками в FinTech передбачає аналіз, ідентифікацію та врегулювання різних видів ризиків, включаючи фінансові, репутаційні, технологічні та інші. Також, враховуючи розмаїтість фінансових послуг, продуктів та платіжних рішень в цьому секторі, ефективне управління ризиками є необхідним для забезпечення довіри клієнтів та створення сприятливих умов для подальшого розвитку FinTech компаній.

Метою цього дослідження є аналіз та оцінка методів управління ризиками FinTech, а також розробка рекомендацій щодо покращення існуючих практик. Для досягнення цієї мети передбачено вирішення таких завдань:

- Дослідити теоретичні аспекти управління ризиками FinTech.
- Проаналізувати асортимент ризиків FinTech
- Проаналізувати підходи до управління ризиками в галузі Fintech.
- Дослідити ризики стартапів у FinTech
- Виділити проблеми та визначити шляхи вдосконалення управління ризиками FinTech в Україні.

Предмет дослідження - теоретичні та практичні аспекти управління ризиками FinTech.

Науковою новизною отриманих результатів є розкриття потенціалу для вдосконалення систем управління ризиками в галузі FinTech та розробка практичних рекомендацій для стейкхолдерів цієї галузі.

Методами дослідження для вирішення поставленого наукового завдання в роботі було застосовано метод системного аналізу, метод моделювання та стимуляції, аналіз та синтез, літературний та документальний аналіз.

Інформаційну базу дослідження склали праці зарубіжних авторів, бази даних, наукові журнали та статті, офіційні документи та статистика, експертні висновки та інтерв'ю, матеріали конференцій та семінарів, інтернет ресурси.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ РИЗИКІВ В ГАЛУЗІ FINTECH

1.1 Поняття FinTech та його роль у фінансовому секторі

Фінансові технології, або FinTech, представляють собою нові технології, спрямовані на вдосконалення та автоматизацію фінансових послуг та їх використання. В основному, FinTech використовується для допомоги компаніям, бізнес-власникам і споживачам у кращому управлінні фінансовими операціями, процесами та фінансовим життям, використовуючи спеціалізоване програмне забезпечення та алгоритми, які працюють на комп'ютерах та, все частіше, на смартфонах. Слово "FinTech" походить від поєднання "фінансової технології." [33]

Спочатку термін "FinTech" використовувався для опису технологій, які використовувалися в серверних системах провідних фінансових установ. Проте з часом фокус перемістився на послуги, спрямовані на споживачів, і тому визначення терміну стало більш спрямованим на споживача. В наші дні FinTech включає різні сектори і галузі, такі як освіта, роздрібний банкінг, збір коштів і некомерційні організації, а також управління інвестиціями та багато інших. [30] До FinTech також входить розробка і використання криптовалют, наприклад, Bitcoin. Хоча криптовалюти стали однією з найбільш популярних галузей в FinTech, найбільші фінансові ресурси все ще зосереджені в традиційній банківській галузі зі значними ринковими капіталізаціями в трильйони доларів.

У більш широкому сенсі термін "фінансові технології" може застосовуватися до будь-яких інновацій у способах, які люди ведуть свій бізнес, починаючи від винаходу цифрових грошей і закінчуючи бухгалтерським обліком з подвійним записом. Проте після інтернет-революції та революції мобільного інтернету/смартфонів FinTech стрімко розвивається і охоплює широкий спектр технологічних інновацій, спрямованих на особисті та комерційні фінанси. [5]

Фінансові технології (FinTech) зараз охоплюють широкий спектр фінансових операцій, включаючи грошові перекази, внесення чеків через смартфони, можливість подавати заявки на кредити, збирання коштів для стартапів і управління інвестиціями. Ці послуги доступні для споживачів без значної сторонньої допомоги. Статистика показує, що все більше споживачів використовують принаймні дві фінансові послуги FinTech, і розуміють їх як невід'ємну частину свого повсякденного життя.

Фінтех-стартапи, які набирають обертів та привертають інвестиції, часто мають одну спільну рису - вони створені, щоб конкурувати з традиційними фінансовими установами, надаючи більш гнучкі, швидкі та зручні фінансові послуги. Наприклад, компанія Affirm прагне замінити кредитні карти, пропонуючи споживачам швидкі короткострокові позики для покупок, навіть якщо у них не найкраща кредитна історія. Better Mortgage спрощує процес отримання іпотеки та пропонує цифровий шлях отримання підтвердженої позитивної відповіді всередині 24 годин від подачі заявки, обходячи традиційних іпотечних брокерів. GreenSky з'єднує позичальників, які планують ремонт житла, з банками, допомагаючи їм уникнути укорінених кредиторів та зменшити відсоткову ставку. [24]

Для споживачів без кредитної історії або з поганою кредитною історією, Tala пропонує мікрокредити у розвиваючих країнах, використовуючи дані з їхніх смартфонів для прийняття рішень про кредитоспроможність.

Кібербезпека, з огляду на зростання кіберзлочинності і децентралізоване зберігання даних, взаємопов'язані між кібербезпекою та фінансовими технологіями. Існує чотири широкі категорії користувачів фінансових технологій: 1) B2B для банків і 2) їх бізнес-клієнти, і 3) B2C для малого бізнесу і 4) споживачі. Тенденції до мобільного банкінгу, збільшення обсягу інформації, даних, більш точної аналітики і децентралізації доступу створять можливості для всіх чотирьох груп для взаємодії безпрецедентними способами. Що стосується споживачів, як і у випадку з більшістю технологій, ніж ви

молодше, тим вище ймовірність того, що ви знаєте і можете точно описати, що таке Фінтех. (Додаток В)

Справа в тому, що орієнтовані на споживача Фінтех в основному націлені на мілленіалів, враховуючи величезний розмір і зростаючий потенціал доходів (і успадкування) цього широко обговорюваного сегмента. Деякі спостерігачі за фінансовими технологіями вважають, що така увага до мілленіалам більше пов'язано з розміром цього ринку, ніж зі здатністю і інтересом представників покоління X і бейбі-бумерів до використання фінансових технологій. Швидше, Фінтех, як правило, мало що пропонує людям похилого споживачам, тому що не вирішує їхні проблеми. [31] Що стосується бізнесу, то до появи і впровадження Фінтех власник бізнесу або стартап звернувся б в банк за фінансуванням або стартовим капіталом. Якщо вони мали намір приймати платежі по кредитних картах, їм довелося б встановити відносини з кредитним провайдером і навіть встановити інфраструктуру, таку як пристрій для читання карт, підключений до провідної мережі. Тепер, з появою мобільних технологій, ці перешкоди залишилися в минулому. [5]

Отже, FinTech, представляє собою інноваційні технології, спрямовані на покращення та автоматизацію фінансових послуг та їх використання. Вони використовуються для покращення управління фінансовими операціями та процесами як для компаній, бізнес-власників, так і для споживачів. FinTech включає широкий спектр послуг, від мобільних платежів до інвестиційного управління та використання криптовалют. Ці інновації полегшують споживачам доступ до фінансових послуг, зменшують витрати та створюють конкуренцію для традиційних фінансових установ. FinTech рухається стрімко вперед, змінюючи спосіб, яким люди ведуть свій бізнес та керують своїми фінансами, і стає невід'ємною частиною сучасного фінансового світу.

1.2 Основні види ризиків в галузі FinTech

Удосконалення фінансової діяльності сільськогосподарських підприємств в сучасних умовах вимагає ретельного аналізу ризиків, які можуть впливати на їх фінансовий стан і можливості формування "ризикових резервів". Цей аналіз включає кілька ключових кроків:

1. Визначення поняття "підприємницький ризик", яке допомагає розуміти сутність і природу ризику в бізнесі.

2. Експертна оцінка чинників, які впливають на розмір ризику при ухваленні фінансових та господарських рішень. Ця оцінка охоплює різні господарські моделі та джерела формування ризику.

3. Визначення поняття "ризикове підприємство" для визначення ступеня ризику та чинників, які впливають на основні фінансові показники стійкості сільськогосподарських підприємств.

4. Оцінка можливих витрат, які може зазнати підприємство під час своєї господарської діяльності. Це включає в себе складання кошторису витрат, таких як оплата праці, закупівля паливних матеріалів, кормів, насіння та інше. Важливо враховувати можливість непередбачених витрат, які можуть виникнути випадково і не є економічно обґрунтованими.

5. Розробка стратегій для управління ризиками, включаючи плани мінімізації впливу ризику на фінансовий результат підприємства.

Узагальнюючи, аналіз підприємницького ризику передбачає розуміння природи ризику, оцінку його впливу на рішення та фінансовий стан підприємства, і розробку стратегій управління ризиками для забезпечення стабільності та прибутковості підприємства. [32]

Незаплановані витрати, які підприємство не передбачало у своєму бюджеті для виробництва продукції, можна розділити на кілька категорій, включаючи матеріальні, трудові та інші види витрат. Матеріальні витрати пов'язані з безпосереднім процесом виробництва продукції і включають в себе витрати на

сировину, матеріали та інші ресурси. Оскільки ці витрати можуть мати різні одиниці виміру, їх корисно порівнювати в грошовому виразі.

Незаплановані трудові витрати виникають внаслідок непередбачених обставин і включають в себе витрати, пов'язані з травмами, захворюваннями та іншими факторами, що впливають на працездатність працівників, а також можливі соціальні витрати.

Фінансові витрати охоплюють грошові втрати, які пов'язані з затримками у платежах, включаючи прострочену дебіторську та кредиторську заборгованість, а також зниження виручки внаслідок зменшення цін на продукцію.

Інші види витрат можуть бути пов'язані з інфляційними процесами та іншими економічними явищами.

Оцінка всіх цих видів витрат виконується протягом певного періоду (наприклад, рік, півріччя або місяць) і допомагає визначити, які витрати є основними та які є додатковими у впливі на фінансовий результат підприємства. [3]

Учасники ринку фінтех спрямовані на вдосконалення цифрових трансформацій у регульованій галузі фінансових послуг, шукаючи нові ідеї та бізнес-моделі. Розробки у цьому сегменті володіють загальними характеристиками - сумісністю, простотою та додатковою вартістю. Однак їхні відмінності дозволяють класифікувати їх за різними критеріями. Банківська діяльність, історично, є однією з ключових областей фінтех інновацій. Дослідження Карчевої І.Я. вказує на те, що існуючі типології банківських інновацій можуть не повністю відображати сучасні тенденції у банківській діяльності. [2].

Від хмарних, мобільних платіжних сервісів до інноваційних блокчейн-додатків - фінансові технології (фінтех) відіграють кілька ролей у сучасній фінансовій індустрії.

Іноватори: Фінтех-компанії використовують інноваційний двигун технологічної індустрії, щоб виводити нові послуги на ринок швидше, ніж традиційні фірми.

Порушники: Технологічні компанії, що швидко розвиваються, витісняють традиційних конкурентів, пропонуючи більш зручні та ефективні послуги або виходячи на неосвоєні ринки.

Партнери: Фінансові компанії зазвичай передають на аутсорсинг бекенд-функції фінтех-компаніям, які добре розуміються на хмарних, мобільних технологіях та технологіях машинного навчання. [35]

Ці компанії поділяють стандартні ризики, з якими стикається будь-який бізнес, від грошових потоків до кредитування. Водночас фінтех-компанії повинні враховувати унікальні ризики, зумовлені специфікою їхньої галузі. Комплаєнс зменшує ці ризики. Деякі компанії не мають вибору. Нові правила вимагатимуть дотримання вимог. Або фінансові установи, які вони обслуговують, вимагатимуть цього для підтримки власних комплаєнс-програм. Інші компанії оберуть добровільний шлях комплаєнсу.

Далекоглядні фінтех-лідери розуміють, що заспокоєння інституційних або роздрібних клієнтів за допомогою комплаєнсу створює конкурентну перевагу. Незалежно від того, звідки походить тиск щодо комплаєнсу, фінтех-компанії повинні враховувати безліч ризиків.

Чотири основні ризики у фінтеху:



Рис 1.1. Ризики FinTech [39]

Фінтех-компанії стикаються з унікальними ризиками в чотирьох основних сферах: регулювання, кібербезпека, фінанси та бізнес, а також репутація.

1. Регуляторний ризик фінтеху На відміну від своїх традиційних колег, фінтех-компанії працюють у більш фрагментованому та невизначеному регуляторному середовищі. У певному сенсі, федеральні регулятори в США не поспішали регулювати фінтех-індустрію.

Спочатку це було пов'язано з браком інституційної експертизи в нових технологіях. Вони також не бажали запроваджувати регулювання, яке могло б задушити молоду галузь. З іншого боку, федеральні регулятори агресивно переслідували фінтех-компанії. Комісія з цінних паперів і бірж особливо активно бореться з крипто-компаніями, які перетинають межу між класами активів і цінними паперами.

Деякі державні регулятори були більш проактивними. Департамент фінансових послуг Нью-Йорка запровадив правила, що охоплюють криптовалюту та криптовалютні біржі. Каліфорнійський закон про фінансовий захист споживачів поставив нових постачальників фінансових послуг під нагляд штату. Без уніфікації федерального регулювання варіації в різних штатах створюють більший ризик для компаній, що надають послуги на національному рівні. Те саме відбувається і в глобальному масштабі. Різні країни мають різні регуляторні пріоритети.

Наприклад, збереження інновацій може бути важливим у США, але захист конфіденційності споживачів має пріоритет в ЄС. Фінтех-компанії повинні орієнтуватися в цьому складному регуляторному середовищі і передбачати зміни, щоб мінімізувати свої регуляторні ризики.

2. Ризик кібербезпеки фінтех-компаній Кібербезпека - це виклик, на який має відповісти кожен бізнес. Для фінтех-індустрії кібер-ризика є більш серйозними. Зломи можуть порушити роботу інституційних клієнтів або поставити під загрозу фінанси роздрібних клієнтів. Будь-який випадок є травматичним і може покласти край існуванню молодого фінтех-компанії. Чим

ближче компанія до фінансової інфраструктури країни, тим більша загроза від підтримуваних державою сучасних постійних загроз.

Фінтех-компанії, які зберігають фінансові дані споживачів, стають мішенями для організованих кіберзлочинців. Навіть недосвідчені хакери можуть здійснювати руйнівні атаки завдяки постачальникам шкідливого програмного забезпечення як послуги. Ситуація ускладнюється тим, що швидкозростаючі фінтех-стартапи мають менше часу, досвіду та ресурсів для захисту своєї інфраструктури. Апаратні та програмні вразливості можуть з'явитися в будь-який момент. Соціальна інженерія може зламати захист простим кліком на посилання. Як розробники програмного забезпечення, фінтех-компанії особливо вразливі до ризиків, пов'язаних з третіми сторонами та ланцюжками поставок. Хмарні обчислення та постачальники X-as-a-Service дозволяють стартапам збирати операції корпоративного рівня.

Фінтех-розробники покладаються на репозиторії стороннього коду, щоб спростити та скоротити життєвий цикл проектів, що робить їхнє програмне забезпечення вразливим до атак з боку ланцюгів поставок. Ці відносини з третіми сторонами можуть створювати значні ризики. Кібербезпека фінтех-компанії переплітається з практиками безпеки її постачальників послуг. Без ретельного контролю залежність коду може відкрити вектори атак на системи фінтех-компанії - і дозволити хакерам проникнути в системи її клієнтів. Відповідність SOC 2 та іншим системам управління кіберризиками може зробити фінтех-компанії та їхніх клієнтів більш захищеними.

3. Фінансові та бізнес-ризики фінтеху Завдяки належному фінансуванню технологічні компанії на ранніх стадіях розвитку є гнучкими та толерантними до ризиків. Вони швидко виводять на ринок передові технології, переорієнтовуються на нові можливості та швидко змінюються у відповідь на попит клієнтів. [32]

Найбільша сильна сторона фінтех-компанії є водночас і значним джерелом ризиків. Операційні ризики Проблема швидкого руху полягає в тому, що ви порушуєте правила. Це може бути добре в соціальних мережах, але не

тоді, коли ви працюєте з даними кредитних карток або обробляєте банківські транзакції. Фінтех-компанії повинні балансувати між інноваціями та операційними ризиками. Технологічні ризики Водночас фінтех залежить від бізнес-моделей, що базуються на технологіях, яким притаманні певні ризики. Наприклад, алгоритми штучного інтелекту та машинного навчання можуть

Технологічні ризики Водночас фінтех залежить від бізнес-моделей, що базуються на технологіях, яким притаманні певні ризики. Наприклад, алгоритми штучного інтелекту та машинного навчання можуть посилити упередження, закладені в наборах навчальних даних. Споживчі ризики Фінтех швидко масштабується, роблячи складні фінансові послуги доступнішими для ширшого кола споживачів. Однак продаж більшій кількості людей означає продаж більш фінансово наївним людям.

Споживачі, які не розуміють фінансової послуги та її ризиків, можуть обпектися, навіть якщо фінтех-компанія не робить нічого поганого. Якщо ж щось піде не так, і це вплине на тисячі споживачів, фінтех-компанія може зіткнутися з негативною реакцією, яка може призвести до краху бізнесу. Ризики інвесторів Венчурні фонди та інші технологічні інвестори охоче роблять довгострокові ставки, фінансуючи фінтех-інновації. Ця модель добре працює доти, доки оптимізм інвесторів залишається сильним. Рецесія, геополітична невизначеність та інші фактори можуть підірвати цей оптимізм. Оскільки венчурні фірми стають більш вибагливими до своїх інвестицій, фінтех-компанії можуть втратити фінансування, необхідне їм для виживання.

4. Репутаційний ризик фінтеху Суть фінансового регулювання полягає у збереженні довіри до фінансової індустрії. Незважаючи на всі технологічні інновації, які фінтех приносить на ринок, репутація все ще має значення. Значний кіберінцидент або крах раунду фінансування зашкодить репутації фінтех-компанії. Споживачі втечуть до більш надійних конкурентів. Банки поставлять під сумнів цінність послуг компанії. Компанії, які добре керують своїм бізнесом, все одно можуть постраждати від помилок своїх конкурентів. Наприклад, крах криптовалютних бірж породжує недовіру до компаній, що

створюють блокчейн-рішення. Комплаєнс-програми, які тримають інші ризики під контролем, значно допомагають уникнути цих репутаційних ризиків [3].

Фінтех-компанії, орієнтовані на відповідність, беруть ризики під контроль. Управління ризиками є частиною будь-якого бізнесу. Фінтех-компанії працюють у більш динамічних умовах, які створюють унікальні ризики. Для фінтех-індустрії комплаєнс має важливе значення для того, щоб тримати ці ризики під контролем. Ефективний комплаєнс-контроль робить більше, ніж просто допомагає компанії дотримуватися нормативних вимог. Демонстрація комплаєнсу заспокоює бізнес і роздрібних клієнтів та надає фінтех-компаніям конкурентну перевагу.

Отже, Фінтех-компанії стикаються з унікальними ризиками, включаючи регуляторний, кібербезпековий, фінансовий та бізнес-ризик, а також репутаційний ризик. У сфері регулювання, фінтех-компанії опиняються в фрагментованому та невизначеному середовищі, де федеральні регулятори можуть не мати достатньої експертизи в нових технологіях. Кібербезпека виявляється серйозним викликом для фінтеху, оскільки кібер-ризик може призвести до порушення роботи клієнтів та загрозити фінансові активи. Завдяки гнучкості та толерантності до ризиків на ранніх стадіях розвитку, фінтех-компанії швидко впроваджують передові технології та адаптуються до змін у відповідь на попит клієнтів. Навіть при цьому, репутаційний ризик залишається важливим, оскільки довіра клієнтів та збереження довіри до фінансової індустрії взагалі є ключовими аспектами успішної діяльності фінтех-компаній.

В першому розділі були розглянуті основні поняття та теоретичні аспекти, пов'язані з FinTech. Було досліджено поняття FinTech та його роль у фінансовому секторі, а також ідентифіковані основні види ризиків, які властиві галузі FinTech. FinTech відіграє ключову роль у сучасному фінансовому секторі, надаючи інноваційні технології та послуги, які полегшують фінансові операції та змінюють спосіб, яким люди взаємодіють з фінансовими послугами. Проте разом із цим існують певні ризики, пов'язані з цією галуззю, які

потребують уваги та ефективного управління. До них відносяться ризики кібербезпеки, фінансові ризики, ризики регулювання тощо. Управління цими ризиками є важливою складовою стратегії компаній в галузі FinTech. У подальших розділах дослідження буде розглянуто конкретні аспекти управління ризиками в FinTech та розроблені ефективні методи їх запобігання та мінімізації.

РОЗДІЛ 2

АНАЛІЗ ПРАКТИКИ УПРАВЛІННЯ РИЗИКАМИ В ГАЛУЗІ FINTECH

2.1 Організація управління ризиками FinTech

В Головному управлінні ДПС у м. Києві управління за ризиками займається Управління з питань виявлення та опрацювання податкових ризиків. Управління складається з семи відділів:

1. Відділ прогнозу та аналізу
2. Відділ моніторингу операцій та ризиків
3. Відділ роботи з ризиками
4. Відділ підготовки матеріалів щодо реєстрації/відмови в реєстрації податкових накладних /розрахунків коригувань в реєстрі
5. Відділ підготовки матеріалів на відповідність/невідповідність критеріям ризиковості платників ПДВ
6. Відділ розгляду звернень з питань податкових ризиків з ПДВ
7. Відділ звітності[4]

На прикладі декількох відділ розглянемо їх основні функції та мету.

Відділ підготовки матеріалів на відповідність/невідповідність критеріям ризиковості платників ПДВ:

Мета - участь у проведенні моніторингу фінансово - господарських операцій платників на наявність податкових ризиків та в організації роботи щодо виведення платників з переліку ризикових

Таблиця 2.1

Функції відділу підготовки матеріалів на відповідність/невідповідність критеріям ризиковості платників ПДВ [Складено автором]

1	Моніторинг фінансово-господарських операцій платників податків на наявність податкових ризиків
2	Проведення аналізу інформації структурних підрозділів Головного управління ДПС у м. Києві щодо відпрацювання податкових ризиків, виявлених за результатами моніторингу фінансово-господарських операцій платників податків

3	Інформування структурних підрозділів Головного управління ДПС у м. Києві та інших користувачів інформації про виявлені податкові ризики діяльності платників податків
4	Розгляд звернень платників податків
5	Розгляд листів платників податків, які відповідають Критеріям ризиковості платника податку
6	Участь у прийнятті колегіального рішення щодо відповідності/невідповідності платника податків Критеріям ризиковості платника податку, затверджених постановою КМУ від 11.12.2019 № 1165
7	Участь у формуванні інформаційного поля про результати діяльності Головного управління ДПС у м. Києві
8	Дотримання Правил етичної поведінки в органах Державної податкової служби та вимог антикорупційного законодавства

Відділ роботи з ризиками.

Мета - моніторинг фінансово-господарських операцій платників податків з метою виявлення податкових ризиків та відпрацювання їх. (Додаток А)

Таблиця 2.2

Функції відділу роботи з ризиками [Складено автором]

1	Моніторинг фінансово - господарських операцій платників податків на наявність податкових ризиків
2	Виявлення та аналіз податкових ризиків в діяльності платників податків
3	Здійснення аналізу інформації структурних підрозділів Головного управління ДПС у м. Києві щодо відпрацювання податкових ризиків, виявлених за результатами моніторингу фінансово - господарських операцій платників податків
4	Інформування структурних підрозділів Головного управління ДПС у м. Києві та інших користувачів інформації про виявлені податкові ризики діяльності платників податків на відповідні запити
5	Участь в узагальненні результатів відпрацювання структурними підрозділами Головного управління ДПС у м. Києві платників податків – учасників схем ухилення від оподаткування, доведених ДПС
6	Участь у наданні пропозицій щодо форм автоматизації процесів моніторингу фінансово - господарських операцій платників податків з метою виявлення податкових ризиків
7	Участь у здійсненні планування діяльності Головного управління ДПС у м. Києві в частині формування та підписання плану роботи управління; підготовка звіту щодо виконання плану роботи управління
8	Дотримання Правил етичної поведінки в органах Державної податкової служби та вимог антикорупційного законодавства

Відділ підготовки матеріалів щодо реєстрації/відмови в реєстрації податкових накладних/розрахунків коригувань в Реєстрі

Мета - участь у здійсненні роботи з питань зупинення реєстрації податкових накладних/розрахунків коригувань в Єдиному реєстрі податкових накладних (далі – ЄРПН).

Таблиця 2.3

Функції відділу підготовки матеріалів щодо реєстрації/відмови в реєстрації податкових накладних/розрахунків коригувань в Реєстрі [Складено автором]

1	Розгляд повідомлень щодо подачі документів про підтвердження чи відмову в реєстрації податкових накладних/розрахунків коригувань в ЄРПН
2	Розгляд таблиць даних платників податків та пояснень, поданих до таких таблиць
3	Надання до управління правового забезпечення інформації та документів по платниках, які звернулись з адміністративним позовом до суду щодо визнання протиправним та скасування рішень, прийнятих Комісією Головного управління ДПС у м. Києві
4	Надання оцінки поясненням та копіям документів, необхідних для розгляду питання прийняття комісією регіонального рівня рішення про реєстрацію податкової накладної/розрахунку коригування в Реєстрі або відмову в такій реєстрації
5	Надання оцінки поданим таблицям даних платників податків та пояснень, поданих до таких таблиць для розгляду питання прийняття комісією регіонального рівня рішення про врахування /не врахування таблиць даних платників податків
6	Внесення пропозицій щодо необхідності змін до законодавчих, інших нормативно-правових актів
7	Дотримання Правил етичної поведінки в органах Державної податкової служби та вимог антикорупційного законодавства

Кожен з цих відділів займається своїми функціональнимим обов'язками які прописані в посадових інструкціях державаних службовців (Додаток А)

Постановою КМУ від 07.11.2023 № 1154 внесено зміни до Порядку 1165, які направлені, зокрема на збільшення кількості платників, які реєструватимуть ПН за новими показниками автоматично. Постанова № 1154 опублікована в «Урядовому кур'єрі» 09.11.2023 та набере чинності 09.12.2023 року.

Алгоритм автоматизованого моніторингу відповідності ПН/РК критеріям оцінки ступеня ризиків передбачає, що:

ПН/РК, що подаються для реєстрації в Реєстрі, спочатку перевіряються щодо відповідності ознакам безумовної реєстрації. У разі коли за результатами перевірки ПН/РК встановлено, що вони відповідають одній з ознак безумовної реєстрації, реєстрація таких ПН/РК не зупиняється в Реєстрі. [36]

Якщо ПН/РК не відповідають жодній з ознак безумовної реєстрації, далі перевіряється щодо відповідності критеріям ризиковості платника податку, показникам, за якими визначається позитивна податкова історія платника податку. (Додаток Д). Податкова накладна/розрахунок коригування, що не відповідають жодній з ознак безумовної реєстрації, перевіряються щодо відповідності відображених у них операцій критеріям ризиковості здійснення операції. (Додаток Е)

У разі коли за результатами автоматизованого моніторингу платник податку, яким складено та/або подано ПН/РК для реєстрації в Реєстрі, відповідає хоча б одному показнику, за якими визначається позитивна податкова історія – ПН реєструється в автоматичному режимі.

Постановою КМУ від 07.11.2023 № 1154 розширено перелік показників, за якими визначається позитивна податкова історія платника податку на додану вартість, зокрема:

- Платник податку протягом шести послідовних місяців придбаває та постачає одні й ті самі товари/послуги в обсягах не менше 75 % від загального обсягу операцій у цьому періоді. При цьому значення показника D більше 0,05, а значення показника $R_{\text{поточ.}}$ є меншим ніж значення $R_{\text{макс.}}$

Показник D розраховується виходячи із загальної суми сплачених платником податку та його відокремленими підрозділами сум єдиного внеску та податків і зборів, контроль за справлянням яких покладено на ДПС за останні 12 звітних (податкових) періоди.

Значення показника $R_{\text{поточ.}}$ є меншим ніж значення $R_{\text{макс.}}$, це означає, що обсяг податку на додану вартість по зареєстрованих ПН поточного місяця

не перевищує найбільшу суму податку на додану вартість по зареєстрованих ПН за останні 12 звітних (податкових) періоди. [37]

- Для платника податку, від якого у поточному місяці прийнято для реєстрації в Реєстрі ПН/РК, одночасно виконуються умови:

Щодо всіх ПН/РК, реєстрація яких зупинена у період, що не перевищує 180 днів, платником податку подані пояснення та копії документів та комісією регіонального або центрального рівня по ним прийняті рішення про реєстрацію. При цьому, щомісячний обсяг постачання, зазначений в ПН/РК за операціями останніх 6 звітних періодів, що передують поточному, перевищує 500 тис. грн.

- Позитивна податкова історія також передбачає, що платник протягом 36 послідовних звітних періодів не мав заборгованості зі сплати податків, не порушував строків подання звітності та строків реєстрації податкових накладних. При цьому, середньомісячний обсяг постачання, зазначений в ПН/РК зареєстрованих у Реєстрі, перевищує 500 тис. грн та у поточному місяці значення показника D становить більше 0,05, а значення показника $R_{\text{поточ.}}$ є меншим ніж значення $R_{\text{макс.}}$

Крім того, одну із ознак безумовної реєстрації «перенесено» в позитивну податкову історію, а саме показник щодо загальної суми податку на додану вартість, сплачену за останні 12 календарних місяців, що передують місяцю, в якому прийнято для реєстрації ПН/РК в Реєстрі.

Якщо раніше однією із ознак безумовної реєстрації було сплата платником ПДВ 1 млн грн. за останні 12 календарних місяців, то тепер цей показник змінено на 10 млн. грн, чим встановлюється запобіжник для використання ризикового податкового кредиту платниками, які при сплаті 1 млн. грн за останні 12 місяців реєструють ПН/РК за цією ознакою безумовної реєстрації. При цьому, для добросовісних платників можливість автоматичної реєстрації податкових накладних залишається, так як цей показник тепер один із показників за якими визначається позитивна податкова історія платника податку.

В Головному управлінні Державної податкової служби в м. Києві всі державні службовці будь якого рівню зобов'язані використовувати в своїй роботі, не тільки технології передбачені штатними розписом, посадовою інструкцією, тощо, а також мати на своєму мобільному пристрої технологію яка допомагає дистанційно підписувати документи. (рис 2.2)

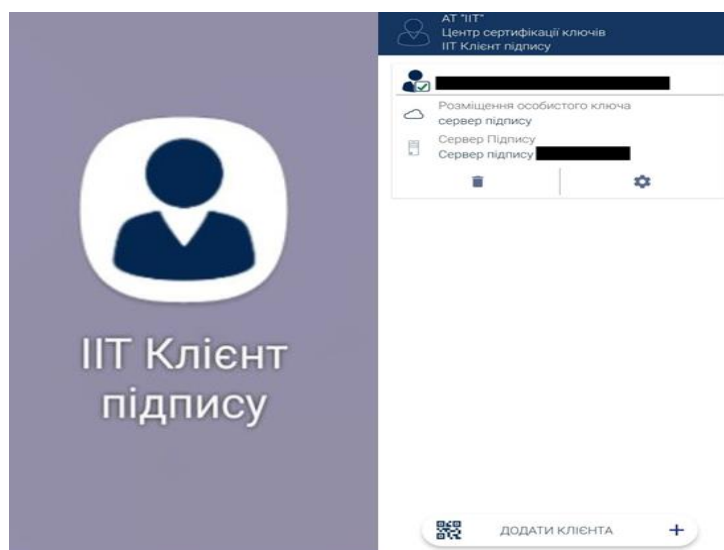


Рис 2.1. Програма цифрового підпису [Складено автором]

Отже, Головне управління Державної податкової служби в м. Києві виконує важливі функції, включаючи моніторинг та аналіз фінансово-господарських операцій платників податків для виявлення податкових ризиків. Ця діяльність спрямована на забезпечення чесності та справедливості в системі оподаткування. Участь у колегіальних рішеннях та здійснення аналізу допомагають відповідати перед законом та забезпечують прозорість оподаткування. Робота у напрямку запобігання податковим ризикам та дотримання етичних норм є невід'ємною частиною цієї діяльності.

Сучасний стан економіки України можна визнати нестабільним. Україна стикається з численними загрозами для своєї національної безпеки, серед яких особливе місце починають займати кібернетичні атаки. Зараз існує система високотехнологічних інструментів, які дозволяють здійснювати кібератаки, незалежно від рівня захищеності. Розвиток хмарних технологій і Інтернету

речей призводить до того, що традиційний підхід до кібербезпеки втрачає ефективність.

Бізнес стикається зі складними цільовими атаками від потужних хакерських об'єднань, застосуванням кіберзброї, яка може призвести до негативних наслідків для економіки. Це ставить під загрозу як окремі регіони, так і держави в цілому. Розповсюдження та постійне удосконалення механізмів кібератак підкреслюють важливість використання технологій управління ризиками в галузі кібербезпеки.

Національну безпеку слід розглядати як один із ключових аспектів національної безпеки країни. Поняття "національна безпека" може мати різні визначення в залежності від поглядів і спеціалізації фахівців. В цілому, воно характеризується як система гарантій стабільності життєдіяльності та розвитку народу та захисту його інтересів від зовнішніх та внутрішніх загроз. [5].

Кібербезпеку можна розглядати як окрему складову національної безпеки, враховуючи активний процес цифровізації суспільства. У цьому контексті важливо виділити кібербезпеку з загальної сфери інформаційної безпеки. Національна економіка стає все більш вразливою перед новими кіберзагрозами, і громадяни та бізнес-сектор часто недостатньо готові до їх виявлення і нейтралізації.

Доцільність вивчення та управління кібербезпекою як окремою складовою національної безпеки підтримується активними тенденціями переходу до онлайн-середовища, і ця тема стає все більш актуальною, особливо в контексті пандемії. Незважаючи на створення відповідних структур та законодавчих актів, існує дефіцит управлінських рішень для забезпечення кібербезпеки в фінансовому секторі та інших сферах. [8].

Поняття "кіберризик" виникло в науковому обігу та фінансовій практиці як результат усвідомлення бізнесом важливості кібербезпеки. Оглядаючи різні визначення цього поняття, можна визначити його як ризик фінансових втрат, пов'язаних з можливістю повної або часткової зупинки роботи, а також з

ймовірністю завдання шкоди, як матеріальної, так і нематеріальної, приватним особам або бізнесу. Особлива увага приділяється не лише фінансовим втратам, але і можливим наслідкам для репутації та моральним аспектам.

Цей підхід відзначає важливість розглядання кібербезпеки як більш широкого поняття, що включає в себе не лише інформаційні системи та ресурси, але і різні сфери діяльності, такі як управління ресурсами, робота з персоналом, бізнес-партнерами і клієнтами. [7].

Важливо виділити різні види кіберризиків, пов'язаних з використанням сучасних електронних технологій у фінансовому секторі. Ці ризики включають в себе можливі втрати або крадіжки інформації, а також можливість навмисних або ненавмисних розголошень конфіденційних даних.

Управління кіберризиками може бути ітеративним процесом і включати такі етапи, як ідентифікація ризиків, мінімізація цих ризиків, оцінка і моніторинг. Цей підхід дозволяє грамотно розподілити ресурси на кібербезпеку і підготувати себе до можливих атак і загроз.



Рис. 2.2. Цикл управління кіберризиками на підприємстві

На першому етапі, необхідно провести ідентифікацію ризиків та їх складових в межах конкретної сфери діяльності підприємства. Це включає в себе аналіз загроз та їх ймовірності виникнення в даній області роботи, а також визначення важливих характеристик цих загроз. Після цього проводиться аналіз впливу цих загроз і формується опис і оцінка можливих наслідків ризику, а також його значимості для діяльності підприємства. [8].

На наступному етапі, керівництво підприємства приймає конкретні рішення щодо використання комплексу інструментів управління ризиками і

заходів їх мінімізації. Ці заходи можуть бути адміністративно-правового характеру, організаційно-процедурні, або технічні. Головна мета на цьому етапі - мінімізувати ризики, зосереджуючи увагу на ключових аспектах, оскільки витрати на мінімізацію цих ризиків є важливими для підприємства.

Після впровадження заходів настає етап оцінки ризиків та їх постійного моніторингу. Важливо аналізувати ефективність заходів після їх впровадження. Успіх управління ризиками визначається тим, коли ризики зменшуються до прийняттого рівня, що був заздалегідь визначений. У контексті швидкого розвитку цифрових технологій, збір інформації про типові кіберзагрози стає важливим для ефективного використання ресурсів. При появі нових ризиків цей цикл починається знову. [9].

Важливо враховувати, що діджиталізація і впровадження ІТ та фінансових технологій стають ключовими факторами конкурентоспроможності в сучасному світі. У цьому контексті, організація управління кіберризиками має базуватися на розумінні необхідності цифрової трансформації в різних галузях діяльності в Україні.

Роль України на міжнародній платформі управління ризиками фінансових технологій (фінтех) залежить від її здатності до інновацій та розвитку цього сектору. Україна має потенціал для виробництва високоякісних фінтех-рішень завдяки своїм компетентним ІТ-спеціалістам. Креативність та інноваційний підхід українських стартапів можуть створити нові можливості у сфері управління ризиками фінтех. Залучення інвестицій та співпраця з міжнародними партнерами можуть сприяти розвитку фінтех-галузі в Україні та її впливу на міжнародній арені. Україна може стати важливим гравцем у глобальному фінтех-середовищі за умови сприяння інноваціям і високій якості продуктів. (Додаток Г)

Фінансовий сектор, зокрема, відзначається інтенсивними змінами і вимагає модернізації та впровадження фінансових технологій (фінтех). Розвиток цифрової економіки в Україні включає розширення фінансових послуг, підвищення фінансової інклюзії та впровадження інновацій в

фінансовому секторі. Важливо, що національні органи, такі як Національний банк України та інші, розробляють стратегію розвитку фінансового сектору до 2025 року, яка передбачає зміцнення стабільності, підтримку економічного розвитку та розвиток фінансових ринків. [10].

Цифрова трансформація ринку фінансових послуг в Україні також включає в себе модернізацію та використання нових технологій, що дозволяють банкам та іншим фінансовим установам надавати нові цифрові сервіси та покращувати комунікацію з клієнтами. У цьому контексті важливо забезпечити захист від кіберзлочинів та шахрайства для громадян і бізнесу, які користуються цифровими фінансовими послугами.

Насамперед, для успішної реалізації цієї стратегії у період постпандемічного відновлення національної економіки надзвичайно важливо активно працювати над мінімізацією кіберзагроз, які зростають з неймовірною швидкістю. Дослідження, проведене аналітичною компанією Canalys, підтверджує це зростання кількості успішних кібератак. За статистикою 2020 року було побито рекорд за кількістю взломів за останні 15 років [11].

Згідно з даними, збитки від кібератак у 2020 році склали понад 30 мільярдів доларів США, що більше ніж удвічі перевищує збитки попереднього року. Особливо великий вплив на це мали вимагачі віруси, які націлені на лікарні та інші заклади охорони здоров'я внаслідок пандемії. Ці атаки призвели до закриття численних компаній, і ті, хто вижив, були змушені терміново переглянути свої стратегії забезпечення кібербезпеки. Важливо зауважити, що торгові шляхи управління кіберзахистом, учинені в поспіху, можуть викликати появу нових слабких місць у системі [12].

Світовий досвід також показує, що розвиток фінтеху є цікавим як для розробників продукту-стартапів, так і для банківських установ. Вигода від цього розвитку найбільше здобувають клієнти банків та інших фінансових установ. Однією з ключових причин такого розквіту фінтеху в Україні була глобальна фінансова криза 2008 року, яка призвела до скорочення кількості діючих банків і цей тренд продовжувався впродовж 2015-2019 років. Це

збільшило навантаження на існуючі банки, з боку яких доросли доходи та попит на фінансові послуги від юридичних і фізичних осіб. Це спонукало клієнтів банків звертатися до дистанційних банківських операцій, а також змусило банки переглядати свої технології та стратегії забезпечення фінансової стійкості.



Рис. 2.3. Кількість кібератак (млн) та збитки від кібератак (млрд дол. США) за 2005–2020 рр.

Роль світової кризи, спричиненої пандемією коронавірусу, у розвитку фінтех-сектору була суперечливою. Згідно з даними Mastercard, у першому кварталі 2020 року українці стали активніше користуватися безконтактними та онлайн-платежами – збільшення на 7% та 8% відповідно. Також кількість онлайн-платежів в сфері електронної комерції зросла на 8%. Роздрібна торгівля стала більш активно використовувати цифрові канали продажу, збільшивши кількість онлайн-платежів за картками Mastercard на 12%, а покупку техніки та електроніки – на 44% [13].

Ці тенденції переходу до безготівкової економіки та цифрових послуг, безсумнівно, мали створити підґрунтя для оздоровлення фінтех-сектору та фінансового ринку України загалом. Проте вони також породжують нові

виклики у сфері управління ризиками в фінансовому секторі через зростаючу кількість кіберзагроз та маніпуляцій, які посилюються в Україні у 2020-2021 роках.

Важливо відзначити, що кінцевою метою Стратегії розвитку фінтеху в Україні до 2025 року є створення повноцінної фінтех-системи з інноваційними фінансовими сервісами та доступними цифровими послугами. Серед ключових результатів впровадження стратегії передбачається збільшення використання безготівкових платежів на 85%, розвиток інноваційних інструментів віддаленої ідентифікації та верифікації, збалансований розвиток всіх сегментів фінтеху, використання інноваційних технологій в наглядових та регуляторних процесах тощо.

У цьому контексті важливо визначити основні проблеми розвитку фінансового сектору, які становлять основу для реалізації конкретних механізмів та інструментів зазначених у стратегії пріоритетів. Дефіцит довіри клієнтів, зокрема громадян, є однією з ключових проблем банківської системи України. Ця недовіра пов'язана з економічною нестабільністю та банкрутством багатьох банків у 2015-2020 роках. Водночас цифровізація розмиває межі між банками і небанківськими фінансовими посередниками, що створює конкуренцію та вимагає більше уваги до забезпечення якості послуг.

Важливим ризиком є зростання кіберзлочинності, яка стає основною причиною фінансових втрат, особливо для банків. Кібератаки потребують швидкої реакції та ефективного кіберзахисту від фінансових установ. Такі виклики можуть затримати або сприяти розвитку фінтеху в Україні, в залежності від того, як вони будуть вирішені.

Таблиця 2.4

Топ-10 кіберризиків у 2017–2022 роках в Україні

№	Назва	Опис
1	Petya	програма-вимагач, яка шифрує дані
2	Blueborne	вразливість – у протоколі Bluetooth
3	NotPetya	програма, яка знищує дані на ПК
4	Wannacry	програма-шифрувальник, що вимагає викуп за дешифрування
5	KRACK	критична уразливість мереж Wi-Fi
6	EternalBlue	програма для одержання віддаленого доступу до системи
7	Bad rabbit	вірус-шифрувальник, розроблений для ОС сімейства Windows
8	Loki / Locky	Android-шкідливий / шифрувальник Windows
9	Reaper	вірус, спрямований на IoT-пристрої
10	Критична вразливість у доступі під root користувачем в MacOS	

Забезпечення кібербезпеки має стати стратегічним пріоритетом для підвищення стійкості фінансових систем, як на загальнодержавному, так і на рівні конкретних підприємницьких структур. Важливо комплексно розвивати заходи з кіберзахисту та сприяти формуванню цифрової грамотності.

Україна відзначається активним розвитком фінансових інститутів, що пропонують банківські послуги через мобільні додатки та Інтернет. Однак ці фінансові установи все частіше стикаються з кіберзагрозами, такими як вторгнення шкідливих програм, фішинг та шахрайські дії. Україна поки не має високоякісної системи управління інформаційною безпекою, і це становить загрозу національній безпеці, оскільки українські банки можуть стати об'єктом атак кіберзлочинців.

В 2021 році створено Бюро економічної безпеки України, яке має боротися з економічними злочинами, включаючи кіберзлочини. Координація між цим Бюро та іншими установами, такими як Міністерство внутрішніх справ, сприятиме зміцненню національної безпеки, зокрема у сфері кібербезпеки.

Нижче наведено інформацію про Україну в Національному індексі кібербезпеки за 2023 рік.

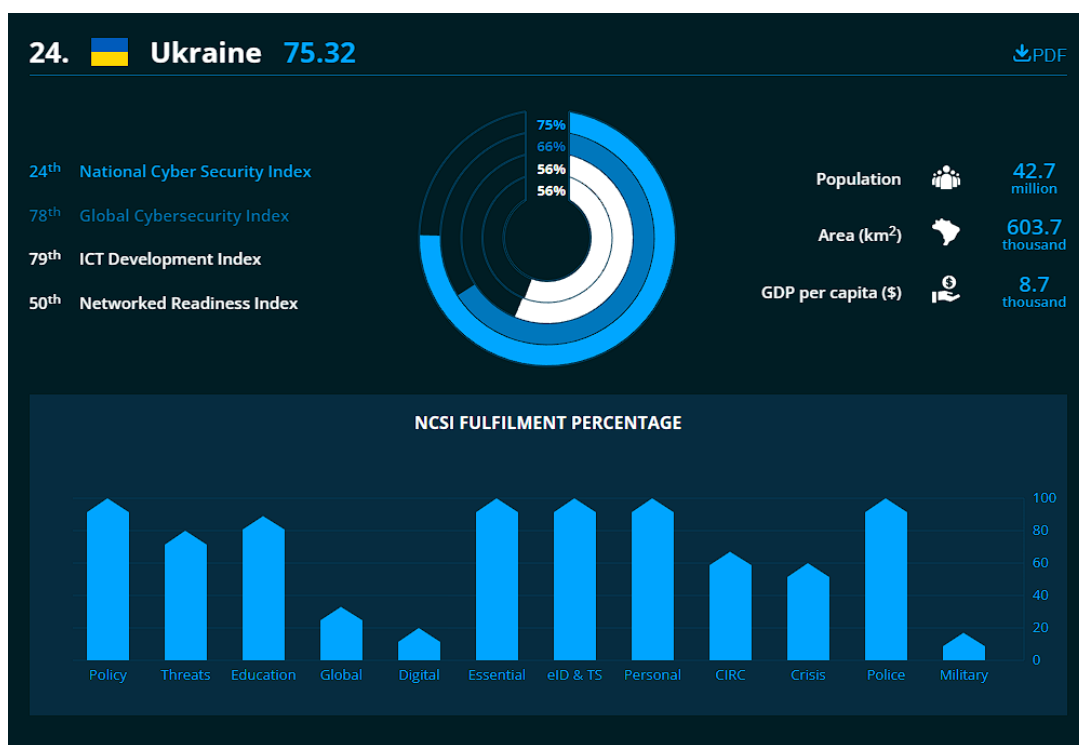


Рис 2.4 Україна у Національному індексі кібербезпеки 2023 [14]

Україні вдалося поліпшити свої позиції в галузі кібербезпеки завдяки прийняттю нових законодавчих актів. Наприклад, Постанова Національного банку України "Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України" визнає важливість інформаційної безпеки в банківському секторі та створює стандарти управління цією безпекою. Однак ці стандарти можуть бути недостатніми для ефективного захисту особистих даних клієнтів та фінансової інформації банків.

Важливою частиною інформаційної безпеки є захист інформації, яка обробляється та зберігається банками, включаючи дані клієнтів та інформацію, що стосується самого банку. Кіберзлочинці часто спрямовують свої атаки на інформацію про клієнтів (інформація front-офісів), оскільки ця інформація може бути використана для крадіжок та завдання шкоди клієнтам і репутації банку.

Зарубіжний досвід управління кіберризиками пропонує п'ять базових напрямів для запобігання кібератакам на інформацію front-офісів. Ці підходи включають:

1. Систематичну оцінку ризиків онлайн-транзакцій з огляду на чутливість інформації та інші фактори.
2. Підвищення стандартів аутентифікації для клієнтів.
3. Застосування багаторівневого підходу до перевірки даних та технологій безпеки.
4. Впровадження передових методів аутентифікації.
5. Підвищення рівня обізнаності та освіти клієнтів.

Ці стратегії також можуть бути корисними для захисту інформації front-офісів в українських фінансових установах. Важливо інтегрувати ці підходи в систему управління кіберризиками у вітчизняних фінансових установах для забезпечення більшого рівня безпеки та захисту інформації клієнтів і банків. Також важливо підкреслити необхідність підвищення цифрової грамотності та освіти клієнтів, яка може сприяти покращенню загального рівня безпеки та сприяти встановленню тривалих партнерських відносин між банками та клієнтами.

Тому, Управління кіберризиками в українському фінансовому секторі вимагає врахування цифрових технологій та загальнодержавних підходів до національної безпеки. Це включає етапи ідентифікації, мінімізації та оцінки кіберризиків, які можуть призвести до фінансових втрат та збитків у репутації. Для успішного управління ризиками важливо використовувати передові технології, а також застосовувати штучний інтелект для виявлення кіберзагроз. Залучення населення до цифрових технологій та підвищення рівня фінансової грамотності є ключовими для відновлення економіки після пандемії. Для досягнення цих цілей необхідна співпраця між державою, бізнесом та громадським сектором.

Фінансова безпека банку визначається його фінансовим станом, який повинен бути збалансованим і відповідати різноманітним фінансовим показникам. Вона також повинна забезпечувати стійкість до різних внутрішніх і зовнішніх загроз, щоб банк міг вчасно та в повному обсязі виконувати свої фінансові зобов'язання та ефективно розвиватися. [15]

Забезпечення фінансової безпеки банку вимагає ведення інформаційно-аналітичної роботи, результати якої необхідні для моніторингу та оцінки рівня фінансової безпеки. Для правильного і оперативного аналізу рівня безпеки банку та прогнозування можливих загроз, що впливають на нього, обов'язковою є функціонування системи інформаційно-аналітичного забезпечення.

Податкові ризики, зазвичай розглядані як загрозу для банку з можливими негативними наслідками, повинні піддаватися систематичному аналізу та моніторингу. Це допоможе банку приймати обґрунтовані управлінські рішення та мінімізувати податкові ризики. Покращення управління податковими ризиками також може позитивно вплинути на ринкову вартість банку, збільшивши довіру потенційних інвесторів і вкладників. [34]

Податковий ризик узагальнено може розглядатися як загроза, що виникає для суб'єкта податкових відносин і може вплинути на його фінансовий стан через можливі фінансові чи інші втрати, пов'язані з процесом оподаткування. Ці ризики можна розглядати як два основних види: зовнішні та внутрішні. (Додаток Б)

Зовнішні джерела податкових ризиків пов'язані з системою оподаткування загалом і податковою політикою країни. Ці джерела можуть включати фіскальну психологію платників, соціально-економічні та нормативно-правові чинники, зміни в податковій політиці тощо. [30]

Внутрішні джерела податкових ризиків пов'язані з функціонуванням банку як суб'єкта господарювання та його участі в податкових відносинах. Ці джерела можуть включати недоліки в плануванні, галузеві особливості та види діяльності банку. [16]

Дія цих джерел призводить до виникнення різних видів податкових ризиків для банку, які можуть бути ідентифіковані та оцінені для подальшого використання при ухваленні управлінських рішень. (рис.2.5)

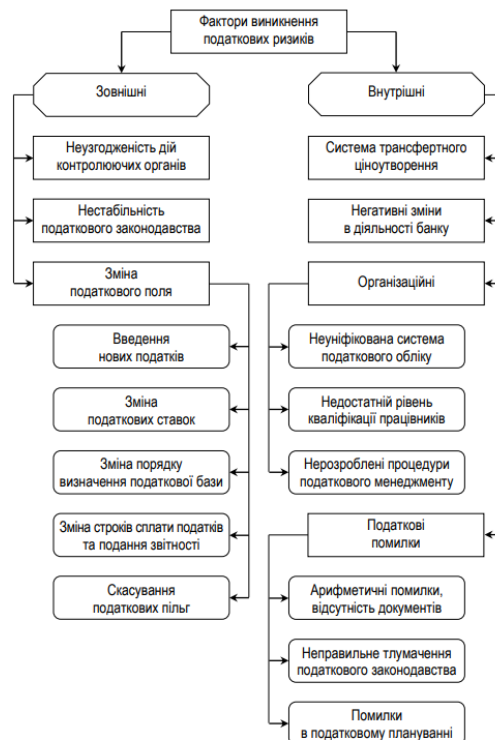


Рис. 2.5. Фактори виникнення податкових ризиків у діяльності банку[21]

Податкові ризики, що можуть виникнути в діяльності банку, з точки зору забезпечення фінансової безпеки банку можна класифікувати за такими ознаками (рис. 2.6).

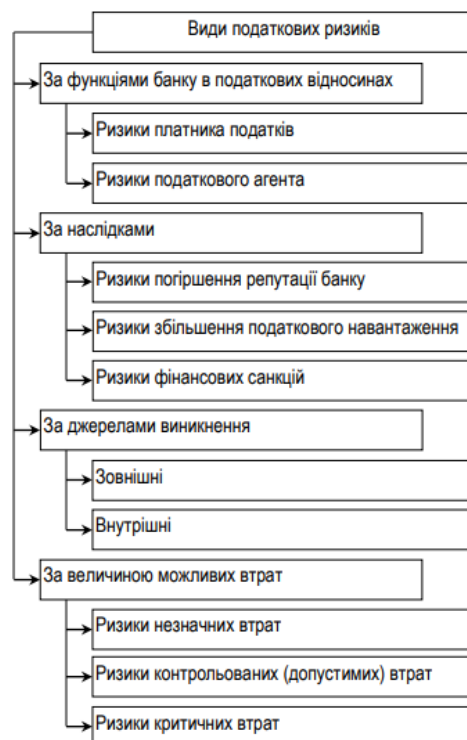


Рис. 2.6. Класифікація видів податкових ризиків з точки зору забезпечення фінансової безпеки банку. [21]

Класифікація та виділення об'єктів податкових ризиків допомагають банку ідентифікувати та аналізувати весь спектр податкових ризиків. Проте для виявлення, які ризики прийнятні, а які вимагають управління, необхідно оцінити не лише ймовірність виникнення податкових ризиків, але і можливі негативні наслідки для фінансової безпеки банку. Ці наслідки можуть включати фінансові санкції у вигляді пені, штрафів і судових витрат.

Згідно з чинним податковим і адміністративним законодавством, фінансові санкції можуть бути застосовані до банку або його керівництва. Деякі податкові порушення також можуть призвести до кримінальної відповідальності. На додаток до цього, судовий розгляд податкових справ і широке обговорення податкових конфліктів можуть негативно позначитися на репутації банку.

Для забезпечення достатнього рівня фінансової безпеки, банк повинен мати ефективну систему виявлення, відстеження та аналізу податкових ризиків. Ця система повинна бути узгоджена з загальною стратегією банку і включена до загальної системи внутрішнього контролю ризиків банку. [29]

Аналіз податкових ризиків повинен включати такі кроки:

- Розгляд податкових наслідків основних операцій банку та пов'язаних з ними податкових ризиків.
- Виявлення та оцінку ризиків, які виникають у зв'язку із функціями посередника в податкових платежах, таких як своєчасне виконання доручень платників податків щодо перерахування податків і надання інформації податковим органам.
- Визначення та оцінку ризиків, які виникають при організації податкового планування і податкового обліку, а також під час обчислення і сплати податків.
- Виявлення та оцінку ризиків, пов'язаних з виконанням банком функцій податкового агента. [17]

Система показників для аналізу податкових ризиків повинна базуватися на чинній бухгалтерській та статистичній звітності. Вона повинна включати

показники, які охоплюють всі важливі аспекти аналізу рівня податкових ризиків, і бути оптимального розміру, без зайвих дублювань та покривати всі ключові аспекти оцінки ризиків банку.

Отже, Загальна концепція податкового ризику в контексті забезпечення фінансової стійкості банку визначає ймовірність виникнення фінансових чи інших збитків через податкову діяльність банку. Важливо вчасно виявляти та оцінювати ці ризики для реалізації оперативних заходів щодо їх управління. Наведена класифікація та систематизовані фактори податкових ризиків визначають основні напрямки аналізу податкових операцій банку з метою виявлення податкових ризиків. Однак залишаються відкритими питання щодо методів вимірювання цих ризиків, що залишається предметом подальших досліджень.

2.2 Методи зниження кіберризиків у фінансовій сфері.

Фінансові технології та хмарні технології взаємопов'язані та взаємопідтримують один одного в сучасному бізнесі та фінансовому секторі. Фінансові технології (FinTech) використовують інновації в галузі програмного забезпечення та обробки даних для поліпшення фінансових послуг. Хмарні технології забезпечують доступ до великої кількості обчислювальних ресурсів та сховищ для зберігання даних через Інтернет.

Фінансові установи використовують хмарні ресурси для зберігання та обробки великого обсягу даних, що допомагає поліпшити швидкість та продуктивність їх фінансових додатків. Хмарні технології також забезпечують зручний та безпечний доступ до фінансових даних для клієнтів через різні пристрої. Фінансові технології використовують хмарні технології для забезпечення високої доступності та надійності їхніх послуг. Вони можуть використовувати хмарні інфраструктури для забезпечення резервного копіювання даних та відновлення після виникнення аварій. Хмарні технології дозволяють фінансовим установам масштабувати свої операції та

інфраструктуру залежно від потреб. Вони можуть легко розширювати свою обчислювальну потужність або зменшувати її відповідно до навантаження.

Фінансові технології також використовують хмарні технології для зберігання та обробки великих обсягів фінансових даних. Це дозволяє їм аналізувати ці дані та надавати клієнтам корисну інформацію для прийняття рішень. Хмарні технології допомагають фінансовим установам знижувати витрати на обслуговування обладнання та інфраструктури. Вони можуть ефективно використовувати спільні ресурси з іншими фінансовими установами.

Фінансові технології використовують хмарні технології для поліпшення безпеки своїх послуг. Це включає в себе захист фінансових даних клієнтів від несанкціонованого доступу та шифрування комунікацій. Завдяки хмарним технологіям, фінансові установи можуть швидко реагувати на зміни в індустрії та впроваджувати нові фінансові продукти та послуги. Це допомагає їм залишатися конкурентоспроможними на ринку.

Фінансові технології	Хмарні технології
Полегшують розробку і впровадження фінансових застосунків	Надають доступ до потужних обчислювальних ресурсів
Забезпечують швидкий та ефективний аналіз фінансових даних	Забезпечують безпеку та шифрування фінансових даних
Дозволяють оптимізувати процеси та автоматизувати операції	Гарантують надійність та бекапи даних
Розширюють глобальний доступ до фінансових послуг	Економлять час та ресурси на інфраструктурі
Сприяють розробці нових продуктів та послуг	Дозволяють спільне використання ресурсів

Рис 2.7 Переваги використання фінансових та хмарних технологій [16]

Зі збільшенням кількості міграцій в хмару, питання щодо безпеки лишається актуальним. Недавно Cloud Security Alliance (CSA), яка відома своєю роботою у сфері стандартів та рекомендацій для безпеки в галузі хмарних обчислень, виділила список загроз, які становлять серйозний ризик для організацій.

1. Витік даних: Інфраструктури в хмарі містять величезні обсяги даних, що робить їх привабливою мішенню для потенційних зловмисників. Важливість цієї загрози залежить від значущості зберіганих даних.

2. Компрометація облікових записів і обхід автентифікації: Використання слабких паролів та некоректне керування автентифікацією може призвести до витоку даних.

3. Злам інтерфейсів та API: Незахищені інтерфейси можуть стати слабкими точками у безпеці, особливо під час взаємодії з іншими сервісами.

4. Вразливість використовуваних систем: Вразливість в системах, які використовуються в хмарі, може стати серйозною проблемою, особливо в мультиарендних хмарних середовищах.

5. Викрадення облікових записів: Фішинг, шахрайство та інші види атак можуть призвести до крадіжки облікових даних та надання доступу до даних, збережених в хмарі.

6. Інсайдерські загрози: Інсайдери-зловмисники, такі як колишні працівники або підрядники, можуть завдати шкоди, отримавши доступ до хмарних ресурсів.

7. Цільові кібератаки: Зловмисники можуть націлювати атаки на конкретні організації, використовуючи хмарні ресурси для виконання шкідливих дій.

8. Постійна втрата даних: Хоча втрати даних в хмарі без можливості відновлення стали менш поширеними, вони все ще можливі через недбалість чи зловмисну діяльність.

9. Недостатня інформованість: Недостатнє розуміння можливостей хмарних технологій може призвести до проблем під час розгортання та використання хмарних рішень.

10. Зловживання хмарними сервісами: Зловмисники можуть використовувати хмарні ресурси для виконання шкідливих дій, таких як DDoS-атаки та інше.

Для забезпечення безпеки в галузі хмарних обчислень використовується різноманітні технології та управлінські заходи, призначені для захисту даних, додатків та інфраструктури, пов'язаної з хмарами. Досягнення передових рівнів

шифрування в хмарних обчисленнях сприяє підвищенню конфіденційності та приватності. Встановлення ефективного контролю доступу та використання багатофакторної автентифікації, такої як одноразові паролі, токени, смарт-карти та USB-ключі, а також застосування інструментів моніторингу та виявлення загроз сприяє підвищенню рівня безпеки в хмарних середовищах.

Шифрування грає важливу роль у захисті інформації. Шифрування не заважає зловмисникам, але робить зміст незрозумілим для потенційних перехоплювачів. У схемі шифрування, відомої як відкритий текст, інформація чи повідомлення шифруються з використанням алгоритму шифрування-шифротексту, що генерує шифр, який можна прочитати лише після розшифрування. Типово використовується псевдовипадковий ключ шифрування, що генерується алгоритмом. Незважаючи на можливість розшифрування даних без ключа, це потребує значних обчислювальних ресурсів та спеціалізованих навичок. Легко розшифрувати дані, якщо уповноважений отримувач володіє потрібним ключем, в той час як неавторизовані користувачі не можуть отримати доступ до інформації.

Існують два типи шифрування: симетричне та асиметричне. Симетричні алгоритми шифрування зазвичай вимагають менше обчислень, що робить їх більш швидкими, аніж асиметричні алгоритми. Однак симетричні алгоритми мають недолік у необхідності обміну секретними ключами між сторонами передачі даних. Оскільки ключі можуть бути піддані ризику перехоплення, їх треба регулярно змінювати та надсилати по безпечних каналах передачі даних.

Асиметричне шифрування використовує два ключі - відкритий та закритий. Відкритий ключ використовується для шифрування, тоді як закритий - для розшифрування. Зашифровану інформацію може розшифрувати лише отримувач, який має потрібний закритий ключ.



Рис. 2.8. Принцип роботи асиметричної криптосистеми [20]

Симетричне шифрування має свою проблему, якою є необхідність передачі одного і того ж ключа для шифрування та розшифрування інформації. Ця ключова інформація може бути вразливою для перехоплення третіми сторонами, оскільки будь-хто, хто знає цей секретний ключ, може розшифрувати дані. На відміну від цього, асиметричне шифрування використовує два взаємопов'язаних ключі - публічний та приватний. Публічний ключ доступний для всіх, хто бажає використовувати його для шифрування даних, тоді як приватний ключ лишається суто приватним і використовується для розшифрування інформації. Це означає, що вам не потрібно передавати приватний ключ, і публічний ключ може бути загальнодоступним. Однак асиметричне шифрування має в собі певний недолік - воно вимагає більше обчислювальних ресурсів як для шифрування, так і для розшифрування даних та потребує більше часу. [40]

Токен автентифікації, такий як апаратний токен, USB-ключ чи криптографічний токен, використовується для ідентифікації особи та забезпечення безпеки інформації. Такий токен може використовуватися як додатковий шар безпеки, покріплюючи процес автентифікації разом із паролем. Проте, важливо усвідомлювати, що втрата або крадіжка токена можуть представляти загрозу, і використання двофакторної автентифікації може сприяти зменшенню ризику.

Двофакторна автентифікація, яка є формою багатофакторної автентифікації, вимагає від користувача подання двох різних факторів для отримання доступу. Наприклад, це може бути пароль та одноразовий код, який генерується спеціальним додатком або надсилається на мобільний телефон. Цей підхід підвищує безпеку інформації, оскільки навіть якщо зловмисники дізнаються пароль, вони не матимуть доступу до іншого фактора автентифікації. Багато великих сервісів і компаній вже пропонують двофакторну автентифікацію як додатковий захист облікових записів. [32]

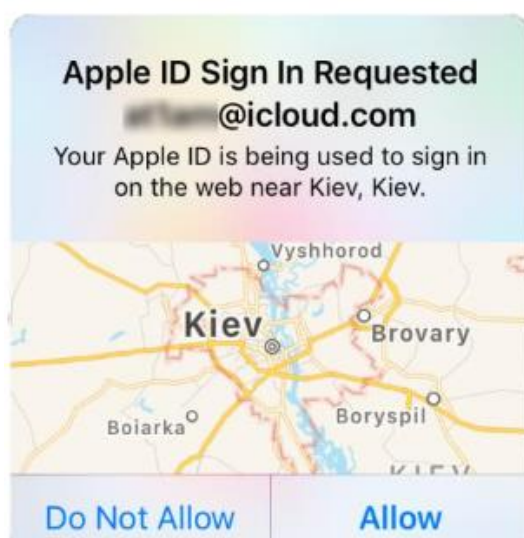


Рис. 2.9. Запит дозволу для авторизації [32]

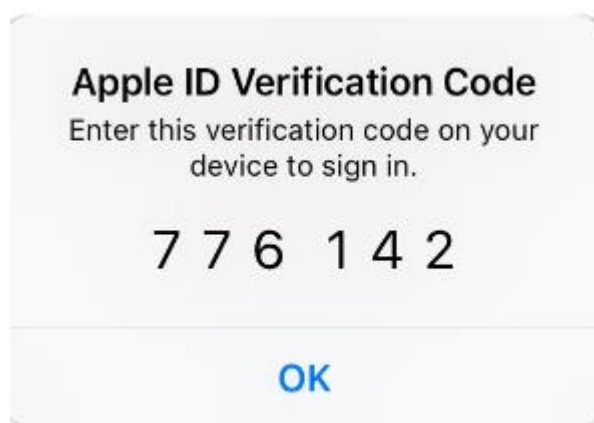


Рис. 2.10. Згенерований шестизначний код [33]

Після надання користувачем дозволу генерується унікальний шестизначний код, який обов'язково необхідно ввести для успішної авторизації. Застосування двофакторної автентифікації виявляється надзвичайно

ефективним методом підвищення рівня захисту даних у хмарному сховищі. Тобто навіть при наявності інформації щодо електронної адреси та паролю зломисник не зможе отримати доступ до збережених даних у хмарі.

Збереження даних у хмарному сховищі із можливістю створення резервних копій має велике значення, оскільки воно надає можливість відновити дані у випадку їх втрати, пошкодження чи видалення. Резервне копіювання включає у себе процес створення додаткових копій ваших даних для подальшого використання в разі потреби.

Для визначення оптимальних параметрів резервного копіювання корисно враховувати такі ключові поняття:

1. Цільова точка відновлення (RPO): Вона визначає інтервал, з якою необхідно створювати резервні копії. RPO вказує, наскільки актуальною повинна бути резервна копія в порівнянні з оригінальними даними. Наприклад, якщо RPO дорівнює годині, це означає, що резервну копію необхідно створювати щогодини.

2. Цільовий час відновлення (RTO): Це визначає час, необхідний для відновлення даних з резервної копії. RTO показує, як швидко можливо отримати доступ до даних після їх втрати або пошкодження.

Різні рівні резервного копіювання включають:

- Повне резервне копіювання (Full Backup): Воно створює повну копію всіх наявних даних. Хоча воно може бути об'ємним, воно дозволяє найточніше відновлення даних.

- Диференційне резервне копіювання (Differential Backup): Цей тип копіює тільки зміни, здійснені після останньої повної копії. Воно зазвичай має менший обсяг і спрощує процес відновлення.

- Додаткове резервне копіювання (Incremental Backup): Цей вид створює копію лише змін, які сталися після останньої копії, незалежно від того, чи було це повне або диференційне резервне копіювання. Воно є найбільш ефективним за обсягом та також сприяє прискоренню процесу відновлення.

Створення резервних копій є важливим для запобігання втраті важливих даних та забезпечення можливості їх відновлення в разі проблем. [40]

Ефективність архітектури безпеки хмарних систем визначається її можливістю правильно впроваджувати заходи забезпечення безпеки на рівні інфраструктури та даних. Управління безпекою грає ключову роль у вирішенні проблем, пов'язаних із забезпеченням безпеки. Елементи управління безпекою активуються для виявлення та вирішення можливих недоліків у системі та зменшення вразливості перед можливими атаками. Рекомендується вибирати та впроваджувати контролі захисту інформації відповідно до ризиків, оцінюючи загрози, вразливості та потенційні впливи. Проблеми безпеки хмарних систем можуть бути розглянуті у багатьох аспектах, включаючи управління ідентифікацією, фізичну безпеку, безпеку персоналу, доступність, захист додатків та приватність.

Тому, фінансові технології і хмарні технології є нероздільною частиною сучасного фінансового сектору та взаємодіють у сфері фінансових послуг. Вони відіграють критичну роль у покращенні доступності, ефективності та безпеки фінансових рішень. Фінтех-компанії активно використовують хмарні технології для розробки та розгортання інноваційних продуктів та послуг. Ця взаємодія сприяє швидкому розвитку та поширенню фінансових інновацій, а також полегшує доступ клієнтів до сучасних фінансових рішень. Оскільки фінтех і хмарні технології надають можливості для аналізу даних, безпеки та масштабування, вони спільно сприяють покращенню якості фінансових послуг і забезпеченню їх доступності для більшого кола користувачів. У цьому контексті можна вважати, що фінансові технології та хмарні технології взаємодіють тісно та взаємовигідно, сприяючи розвитку сучасного фінансового сектору.

РОЗДІЛ 3

ПРОБЛЕМИ ТА ШЛЯХИ УДОСКОНАЛЕННЯ УПРАВЛІННЯ РИЗИКАМИ FINTESН В УКРАЇНИ

У поточних умовах відбувається значна трансформація каналів банківського обслуговування з тенденцією до зростання їх цифровізації. Наприклад, банки України в останні роки активно скорочують кількість відділень – за 2015 - I півріччя 2021 рр. з 15,1 до 6,9 тис. одиниць. Ця тенденція пов'язана насамперед з автоматизацією банківських операцій та поширенням онлайн-продажів банківських продуктів, що дозволяє оптимізувати мережу, скорочувати "традиційний" банківський персонал та знижувати операційні витрати. (Додаток Є)

Протягом останніх трьох років (станом на 01.01.2021 р. відносно 01.01.2018 р.), також спостерігається поступове зменшення кількості банківських пристроїв (банкомати, ПТКСЗ та банківські термінали) – з 56,6 тис. од. до 48,8 тис. од. Проте, згідно з даними Світового банку, Україна залишається одним зі світових лідерів (23 місце в останньому за хронологією рейтингу за 2019 р.) за кількістю банкоматів на 100 тис. дорослого населення з показником 96,3, випереджаючи більшість країн-сусідів [18].

Такий процес видається природним, враховуючи недостатню розвиненість банківських послуг в Україні, включаючи кредитування та розміщення депозитів. Проте "послаблення можливостей доступу населення до банківських послуг через "вимивання" банківських відділень, особливо – з менш розвинених та менш населених громад, неминуче консервуватиме цю нерозвиненість та гальмуватиме економічний розвиток згаданих територій, що є негативним як для соціально-економічного розвитку країни, так і для самої банківської системи" [19].

Тому, попри розвиток дистанційних та цифрових технологій, за останні десять років, за даними Світового банку, кількість банківських відділень у світі збільшилася майже на 30 % – з 9,8 до 12,7 відділень на 100 тис. осіб. Показник

України є достатньо високим – приблизно 21 відділення на 100 тис. осіб. Це зокрема зумовлено тим, що за даними опитувань, в Україні понад 60 % клієнтів при виборі нового банку досі віддають перевагу установі з відділеннями, а 87 % клієнтів планують відвідувати відділення в майбутньому, оскільки для розв'язання деяких питань потребують "живого" спілкування з менеджером [20].

У нинішніх умовах банки мають як задовольняти потреби клієнтів у процесі обслуговування, так і впроваджувати інноваційні та високотехнологічні інструменти, щоб залишатися життєздатними та конкурентоспроможними.

Основні показники розвитку електронного банкінгу представлені в таблиці 3.1.

Таблиця 3.1

Залученість банків України до онлайн-банкінгу та співпраці з FinTech
[18,19]

Банк	Власна розробка інвестиційних проєктів			Власна інкубація/акселерація			Інвестиції у стартапи		
	ні	плануються	Так	ні	плануються	так	ні	плануються	так
Приватбанк			✓		✓		✓		
Укргазбанк			✓	✓			✓		
Ощадбанк		✓		✓			✓		
СенсБанк			✓	✓			✓		
Укрсиббанк	✓					✓	✓		
Райфайзен Банк			✓		✓		✓		
ОТР Bank Ukraine	✓					✓	✓		
ПУМБ			✓	✓			✓		
Credit Agricole			✓		✓		✓		

Серед найбільш технологічних банків в Україні можна виділити такі установи: АТ "Ощадбанк," АТ "Райффайзен Банк," ПАТ АБ "Укргазбанк," АТ "Сенс-Банк," АТ "ПУМБ," АТ "УКРСИББАНК," АТ "ОТР Банк". Важливо зазначити, що ці банки також співпрацюють у деяких спільних проєктах з онлайн-банкінг-компаніями, як це представлено в таблиці 6. Варто відзначити, що винятком є лише АТ КБ "ПриватБанк," який має власний потужний центр для розробки ІТ-рішень.

Таблиця 3.2

Взаємодія українських банків з FinTech-продуктами [25]

Банк	Міжнародні FinTech-продукти			Акселераційні програми	Проекти фіналістів акселерацій	Банківські FinTech продукти
	Google Pay	Apple Pay	Garmin Pay			
Ощадбанк	✓	✓	✓			Чат-бот «Онлайн-помічник» Ощад PAY, Ощад 24/7
Приватбанк	✓	✓	✓			Airpay, IPay, LigPAY, QR платежі, Приват24
Райффайзен Банк	✓			Raiffeisen Digital HUB		
ПУМБ	✓		✓			
Укрсиббанк	✓			POPCORP	UKRSIB OR Чат-боти	UKRSIB Online
ОТП Банк	✓		✓	Open Banking Lab	YouScore – bNesisCoinyPay Future Agro Finance	OTP Smart
Сенс банк	✓		✓	Sense Digital		Sense-mobile

Багато з вищезазначених банків мають свої власні інкубатори та акселератори стартапів для впровадження інноваційних продуктів та сервісів у свою практику. Основними областями співпраці між банками та онлайн-банкінг-компаніями є платіжні сервіси, автоматизація бізнес-процесів, використання великих обсягів даних (Big Data), системи штучного інтелекту та кібербезпека [20].

Лідером в українській банківській системі за надійністю та швидкістю розвитку електронного банкінгу є АТ КБ "ПриватБанк". Він вийшов за межі традиційного банкінгу та створює нову цифрову екосистему на стику фінансових послуг, роздрібної торгівлі та електронної комерції. Мобільний додаток "Приват24" використовується понад 12 мільйонами осіб, і загальна кількість роздрібних клієнтів перевищує 20 мільйонів. Важливо відзначити, що "Приват24" є найбільш функціональною онлайн-платформою, яка пропонує

більше 40 різних опцій, включаючи перекази, відкриття депозитів, ведення домашньої бухгалтерії, обмін валюти та придбання квитків. За даними Google Play, понад 5 мільйонів жителів України встановили додаток "Privat24" на свої Android-смартфони. З урахуванням того, що понад 10 мільйонів смартфонів зареєстровано в мережах українських операторів, можна зробити висновок, що "Privat24" використовує кожен другий власник Android-пристрою. Це є абсолютним рекордом серед платіжних додатків на Android серед користувачів України та Східної Європи (таблиця 3.7).

Таблиця 3.3

Перелік послуг онлайн платформи Privat24, що пропонує АТ КБ
«ПриватБанк» [18]

Назва банку	Назва системи Інтернет-банкінгу	Перелік послуг (основні можливості)
АТ КБ «ПриватБанк»	Приват24	- перегляд виписок за рахунками; - оформлення депозиту; - оформлення страхового поліса; - погашення кредиту; - купівля автобусних, залізничних та авіаквитків; - купівля квитків на спортивні змагання; - обмін валюти; - будь-які види платежів; - поповнення мобільного телефону; - переказ коштів; - замовлення додаткових платіжних карт.

Кожен день понад 500 000 користувачів АТ КБ "ПриватБанк" проводять операції за допомогою POS-терміналів, використовуючи технологію NFC. Бізнес-модель банку у сфері онлайн-банкінгу дозволяє встановлювати зворотній зв'язок з клієнтами через розумний месенджер, який дозволяє отримувати будь-які послуги та консультації банку. На сьогодні АТ КБ "ПриватБанк" пропонує 19 мобільних додатків, окрім "Privat24," призначених для різних банківських та побутових операцій.

Управління капітальними ресурсами клієнта, а також фінансове планування, що базується на довірі клієнта до банку, є ще одним перспективним сервісом АТ КБ "ПриватБанк." Спеціалісти банку зобов'язані вести моніторинг фінансового стану клієнта та розробляти пропозиції для збереження його фінансових ресурсів та їх оптимального використання. В цій

сфері банк пропонує мобільний додаток "Мої вклади," який дозволяє здійснювати всі операції з вкладами, для проведення яких раніше доводилося звертатися до відділення. За допомогою цього додатку, клієнти можуть здійснювати депозитні операції 24/7 за допомогою своїх смартфонів, планшетів або смартгодинників. Додаток також надає можливість переглядати процентні ставки та актуальні умови за вкладами банку.

АТ КБ "ПриватБанк" став ініціатором та організатором P2P кредитування на українському ринку банківських послуг, надаючи кредиторам гарантії та компетенції у пошуку позичальників, оцінюванні можливостей виникнення ризиків і стягненні боргів. З 01.03.2016 року була запущена платформа "Сервіс вигідних вкладень" для видання роздрібних кредитів [21].

За іншими дослідженнями [22], АТ КБ "ПриватБанк" посідає лише друге місце на ринку електронного банкінгу, і першим у рейтингу є Monobank – український інтернет-банкінг, який працює на ліцензії АТ "Універсал Банк" і надає свій мобільний додаток. Під час складання цього рейтингу враховували два основні принципи: попит користувачів (за даними сервісів Google Trends, Alexa, SimilarWeb за пів року) і якість та функціональність мобільного додатка (під час тестування). Додаток "моно" характеризується високою якістю, простотою, простотою реєстрації та використання, відсутністю комісій, наявністю кешбеку та нестандартними методами просування.

У онлайн системі АТ "ПУМБ" доступно 37 опцій, а в АТ "Альфа-Банк" – 35. Особливий інтерес серед користувачів викликає можливість дистанційно оплачувати комунальні послуги. Понад 70% операцій стосуються поповнення мобільних телефонів, грошових переказів та сплати комунальних послуг.

Завдяки пандемії COVID-19 цифрові банківські послуги отримали додатковий поштовх для розвитку у 2020-2021 роках. Широкі можливості дистанційних каналів стали одним із трьох основних критеріїв вибору банком клієнтами для співпраці. Це також позначилося на мобільних додатках, які стали повноцінним каналом доступу до банківських операцій та сервісів. Згідно

з дослідженням [23], було виділено десять найважливіших трендів розвитку мобільних додатків для бізнесу (див. рис. 3.1).

Онлайн-відкриття рахунку	• анкетування у додатку; • фотографування документів; • заповнення даних про бізнес інформацією із держреєстрів; • віддалену ідентифікацію; • відкриття рахунку/картки.
Віддалена ідентифікація	• відеоідентифікація; • використання електронно-цифрових підписів; • підключення до послуг обміну даними клієнта між банками.
Онбординг (процес ознайомлення)	• навчання клієнтів та знайомство їх з новим функціоналом
Віртуальні карти	• розрахунок в інтернеті та в торгових точках через NFC
Онлайн-кредитування	• перегляд суми передбаченого банком кредитного ліміту • оформлення прямо у додатку
Контроль фінансової дисципліни	• подивитися на свою компанію «очима банку» • оцінити бізнес-діяльність щодо відповідності законодавству • попередити можливі ризикові операції • уникнути блокування рахунку
Маркетплейси та нефінансові сервіси	• пропозиції від партнерів банку
Онлайн-бухгалтерія	• для підприємців та невеликих компаній, які не хочуть або не можуть наймати штатного бухгалтера
Онлайн-чати	• комунікація у зручних месенджерах (Telegram, Whatsapp) • можливості додавання файлів/фотографій рахунку
Єдиний додаток	• запуск єдиних мобільних додатків для фізичних осіб та підприємців • дозволяє підприємцям легко керувати всіма своїми рахунками/картами – і бізнесовими, та особистими – в єдиному вікні, без необхідності переходу та повторної авторизації

Рис. 3.1 – Тренди електронного банкінгу для малого та середнього бізнесу у 2020-2021 роках [23]

Основною тенденцією протягом періоду дослідження є зростання кількості електронних банківських послуг, які пропонують банки, а також збільшення користувачів цих онлайн-сервісів. Банки активно оптимізують свої бізнес-процеси, впроваджують типізацію клієнтів і стандартизують процедури для їхньої інтеграції в онлайн-сервіси. Це значно зменшило навантаження на фізичні відділення банків, оскільки стандартні операції для індивідуальних клієнтів та малих та середніх підприємств (МСБ) тепер можна виконувати в

онлайн-середовищі. Для МСБ важливими стали не лише комплекс послуг та сервісів, але також фінансові та правові консультації.

Зі збільшенням обсягів електронних банківських продуктів та послуг зростає ризик, пов'язаний з ними, зокрема операційний ризик. Збільшення користувачів електронного банкінгу також підвищує ризик кібершахрайства. Керівники банків, які брали участь в опитуванні Національного банку України, визнали кіберризик одним із найбільших джерел системного ризику. Тому банки повинні покращити системи захисту особистих даних користувачів і зміцнити засоби виявлення шахрайств. При цьому, особливу увагу слід приділити підвищенню цифрової грамотності серед вразливих груп клієнтів, зокрема серед старших громадян.

Сьогоднішні вимоги до систем фінансового контролю та управління операційними ризиками значно зросли [24].

Дослідження, проведене Національним банком України [24] і представлене в таблиці 3.4, аналізує вплив двох найбільших подій на операційний ризик: пандемії COVID-19 та кібератаки вірусом "Petya" в 2017 році. У опитуванні взяли участь 18 банків (які складають 77% активів банківської системи), що ведуть бази оперативних подій. З них лише 10 банків вважали пандемію подією, що впливає на операційний ризик. Понад третина банків не зафіксувала жодних збитків або втрат внаслідок цієї події.

Таблиця 3.4

Результати опитування про події операційного ризику (ОР) [24]

Показник	Petya	Пандемія COVID-19
Кількість банків, що відобразили подію	7	10
із них зазначили про нульові збитки	3	4
Сукупні збитки, млн грн	17.4	468.4
Середні збитки (на подію), млн грн	0.8	66.9
Медіанні збитки (на подію), млн грн	0.8	13.0

Загальні втрати банків на боротьбу з операційними ризиками, пов'язаними з COVID-19, становили 468 млн. грн. – у середньому 1,1 % від капіталу банків (рис. 3.2).

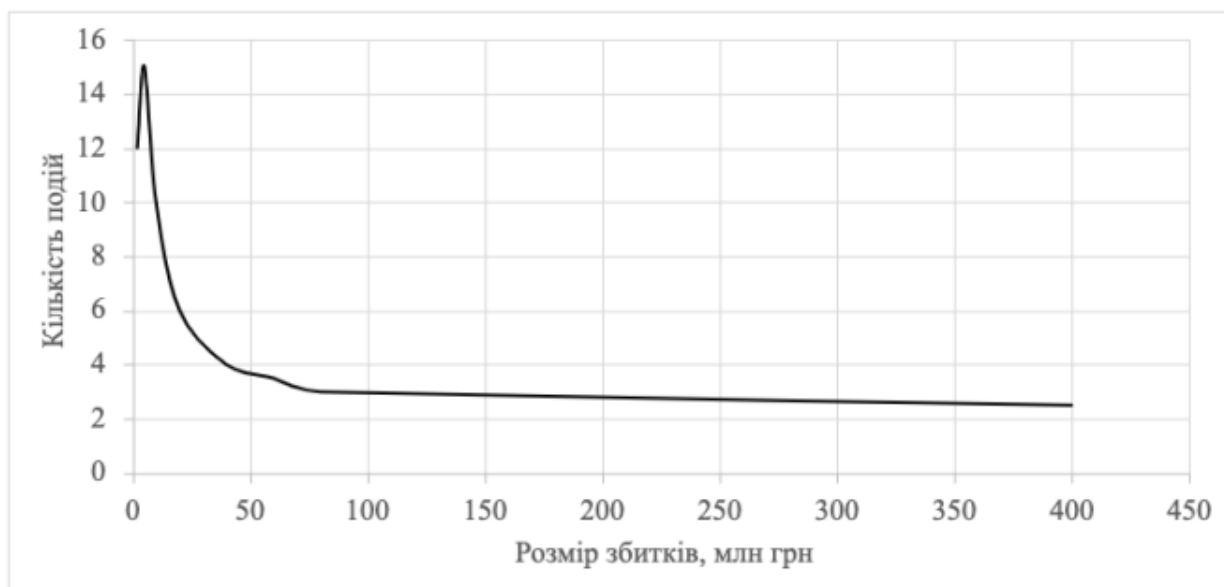


Рис. 3.2 – Розподіл збитків від подій ОР, пов’язаних з вірусом «Petya» та пандемією COVID-19 [24]

Тому, деякі фінансові установи недооцінюють операційні ризики, такі як пандемія COVID-19. Щоб захистити банки від ризиків із неплатоспроможності та банкрутства, необхідно більше капіталу. Криза COVID-19 прискорила зміни у фінансовому секторі: менше фізичних відділень, більше віддаленої роботи, більше кіберзагроз і менше готівки. Це вплине на бізнес-модель банків і їх операційні ризики. Електронний банкінг збільшує ризики для банків, і це підкреслює важливість управління цими ризиками та їх вплив на прибутковість і стабільність.

Сучасні методи оцінки ефективності управління ризиками в системі електронного банкінгу включають стрес-тестування, використання фінансових показників, статистичні аналізи, рейтингові системи і інші підходи. У даному випадку розглядається комплексний підхід до оцінки ефективності управління ризиками, який базується на динамічній нормативно-індексній моделі, розробленій з використанням методів непараметричної статистики. Ця модель дозволяє оцінити загальну ефективність системи ризик-менеджменту в електронному банкінгу і визначити бажаний рівень ризику для банків.

Спростимо процес створення такої моделі. В залежності від об'єкта дослідження, кількість етапів формування моделі може коливатися від 5 до 13.

У випадку онлайн-банкінгу розглядаються сім основних етапів формування динамічного нормативу.

В результаті аналізу динамічних відносин можна отримати два можливих варіанти:

1) Лінійний динамічний норматив, якщо всі показники можуть бути однозначно інтерпретовані і впорядковані за темпами зростання.

2) Нелінійний динамічний норматив, який формується на основі графу або матриці нормативних відносин (переваг), коли не всі порівняння між показниками мають однозначну економічну інтерпретацію.

Отже, цей підхід дозволяє створити ефективну модель для оцінки ризиків в системі електронного банкінгу, враховуючи її динаміку та особливості. [25]

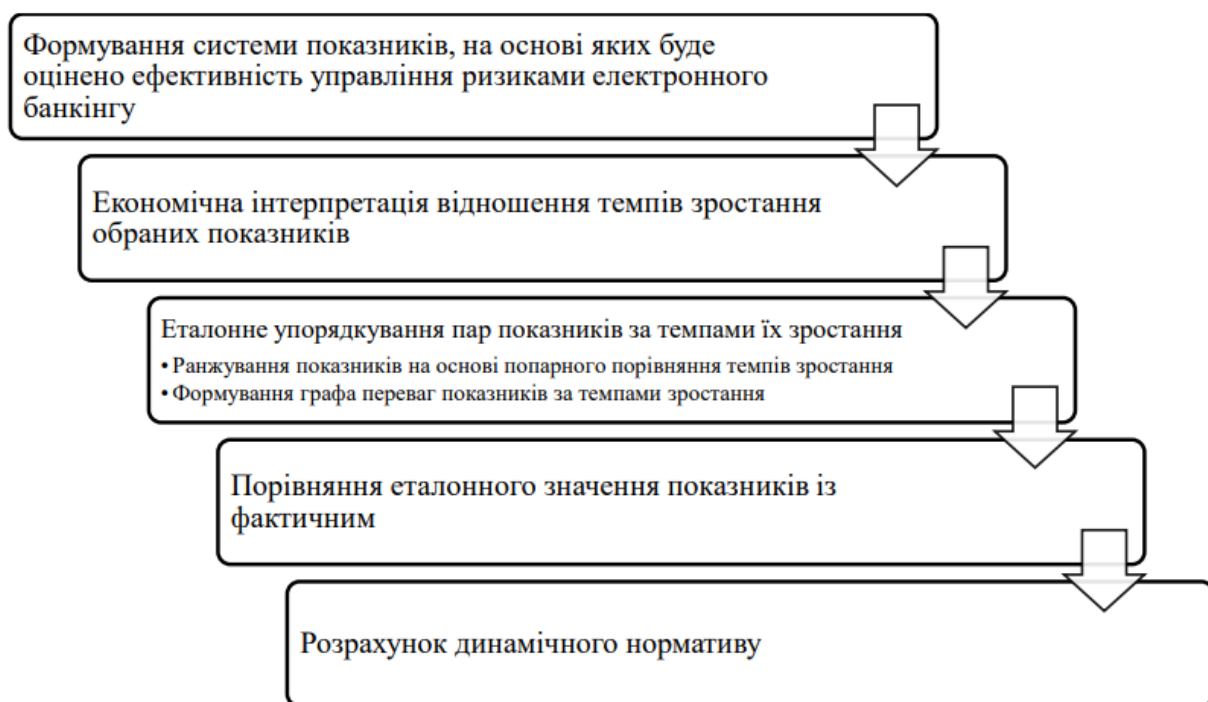


Рис. 3.3 – Процес побудови динамічного нормативу для оцінки ефективності управління ризиками електронного банкінгу [25]

Таблиця 3.5

Показники оцінки ефективності управління ризиками електронного банкінгу та нормативні співвідношення між темпами їх росту [26]

№	Показник	Алгоритм розрахунку	Нормативні зміни співвідношень	Нормативні співвідношення між темпами росту
1.	Рентабельність власного капіталу	NP/K	Збільшення	$F(NP) > F(K)$
2.	Рентабельність активів	NP/A	Збільшення	$F(NP) > F(A)$
3.	Рентабельність вкладень в ІТ-системи банку	NP/IT-E	Збільшення	$F(NP) > F(IT-E)$
4.	Мультиплікатор капіталу	A/K	Зменшення	$F(A) < F(K)$
5.	Адекватність регулятивного капіталу з врахуванням операційного ризику електронного банкінгу	RC/R	Збільшення	$F(RC) > F(R)$
6.	Коефіцієнт комісійних доходів до комісійних витрат за картками	CI/CE	Збільшення	$F(CI) > F(CE)$
7.	Частка довгострокових депозитних ресурсів у пасивах	D/P	Збільшення	$F(D) > F(P)$
8.	Питома вага обсягів кредитування через картки до кредитного портфеля	CC/CP	Збільшення	$F(CC) > F(CP)$
9.	Коефіцієнт проблемних карткових кредитів	PCC/CC	Зменшення	$F(PCC) < F(CC)$

На наступному етапі визначається система показників для розрахунку коефіцієнтів, що включені до динамічного нормативу, що дозволять оцінити ефективність ризик-менеджменту електронного банкінгу з боку банку (табл. 3.10).

Таблиця 3.6

Показники для розрахунку динамічного нормативу [25]

№	Назва	Алгоритм розрахунку	Позначення
1.	Прибуток	Прибуток після сплати податків	NP
2.	Капітал	Власний капітал банку	K
3.	Активи	Загальні активи банку	A
4.	Витрати на ІТ	Сума витрат на заробітну плату ІТ співробітників, програмне забезпечення, ІТ обладнання та операційні витрати	IT-E
5.	Регулятивний капітал	Основний та додатковий капітал за мінусом відвернення	RC
6.	Ризики	Сума активів, зважених за ризиком, відкритої валютної позиції та капіталу на покриття операційного ризику	R
7.	Комісійні доходи	Сума комісійних доходів за операціями з картками	CI
8.	Комісійні витрати	Сума комісійних витрат за операціями з картками	CE
9.	Довгострокові депозити	Сума всіх довгострокових депозитів від 1 року	D
10.	Зобов'язання	Сума всіх зобов'язань	P
11.	Карткові кредити	Сума кредитів наданих через платіжні картки	CC
12.	Кредитний портфель	Сума кредитів наданих банком	CP
13.	Проблемні карткові кредити	Сума карткових кредитів, за якими прострочений термін сплати	PCC

На основі визначених пріоритетів в темпах зростання одних коефіцієнтів відносно інших ми створимо матрицю еталонних преференцій, яка показує, які

показники мають зростати швидше або повільніше порівняно з іншими. У цій матриці кожен елемент (значення) визначається наступним чином:

1) Значення 1 в елементі матриці вказує на те, що i -й показник має зростати швидше, ніж j -й показник.

2) Значення -1 в елементі матриці вказує на те, що i -й показник має зростати повільніше, ніж j -й показник.

3) Значення 0 в елементі матриці означає, що нормативних відносин між i -м та j -м показниками не встановлено.

Така матриця допомагає визначити порядок пріоритетності між різними коефіцієнтами та показниками, що допомагає у визначенні їхнього значення та динаміки зростання.

Таблиця 3.7

Матриця еталонних преференцій для оцінки ефективності управління ризиками електронного банкінгу [27]

Показники	NP	K	A	IT-E	RC	R	CI	CE	D	P	CC	CP	PCC
NP	0	1	1	1	0	0	0	0	0	0	0	0	0
K	-1	0	1	0	0	0	0	0	0	0	0	0	0
A	-1	-1	0	0	0	0	0	0	0	0	0	0	0
IT-E	-1	0	0	0	0	0	0	0	0	0	0	0	0
RC	0	0	0	0	0	1	0	0	0	0	0	0	0
R	0	0	0	0	-1	0	0	0	0	0	0	0	0
CI	0	0	0	0	0	0	0	1	0	0	0	0	0
CE	0	0	0	0	0	0	-1	0	0	0	0	0	0
D	0	0	0	0	0	0	0	0	0	1	0	0	0
P	0	0	0	0	0	0	0	0	-1	0	0	0	0
CC	0	0	0	0	0	0	0	0	0	0	0	1	1
CP	0	0	0	0	0	0	0	0	0	0	-1	0	0
PCC	0	0	0	0	0	0	0	0	0	0	-1	0	0

Матриця преференцій відображає еталонні відносини між різними показниками, які включені до моделі для оцінки ефективності управління ризиками в системі електронного банкінгу. Для прикладу, щоб зменшити ризики, пов'язані з операціями з банківськими картками, комісійні доходи за цими операціями повинні зростати швидше, ніж комісійні витрати за ними. Тобто $F(CI) > F(CE)$. Тому відповідно до цих відносин, в матриці преференцій в рядку 7 та колонці 8 ми встановлюємо значення "1" для позначення пріоритету зростання комісійних доходів над комісійними витратами. На перетині колонки

7 та рядка 8 ми встановлюємо значення "-1", що вказує на зменшення комісійних витрат швидше, ніж комісійних доходів.

Цей процес застосовується до всіх 9 коефіцієнтів, і у випадку, якщо немає чітких нормативних відносин між темпами зростання показників, відповідним рядку та колонці матриці встановлюється значення "0". Таким чином, матриця преференцій допомагає визначити, які показники мають зростати швидше чи повільніше в порівнянні один з одним [28].

Таблиця 3.8

Динаміка втрат клієнтів monobank від кіберризиків за 2023 рік [29]

Тематика	Березень	Квітень	Травень	Червень	Липень
Социнжиніринг: під диктовку/тиском, будь-який привід	7 524 470,6	6 970 855,41	7 981 791,64	7 680 025,14	5 779 332,5
Социнжиніринг: фейкові збори (фейк - волонтери)	136 445,19	73 260,47	58 441,12	98 856,28	71 220,18
Социнжиніринг: весь	7 660 915,79	7 044 115,88	8 040 232,76	7 778 881,42	5 850 552,68
Брокери/біржа.	4 500 059,77	1 134 067,69	1 947 808,99	3 605 185,09	2 889 638,11
Фішинг	1 807 582,26	1 702 058,94	1 732 035,77	3 448 079,71	2 729 656,57
Втрата картки	288 206,43	188 335,82	207 606,62	302 498,6	221 655,39
Виманювання даних	936 999,62	1 329 396,24	1 914 510,11	2 335 318,76	1 035 317,36
Френдлі/фемілі фрод	584 126,56	258 698,23	338 419,1	454 371,29	241 143,81
Втрата карти та девайсу	120 818,42	91 093,82	34 378,07	26 268,5	190 203,92
Втрата девайсу	41 461,56	100 814,01	194 645,84	137 428,47	148 726,28
Перевипуск сім-картки шахраями (+ виманювання)	34 635,5	60 060,5	52 709,62	222 316,59	35 250, 1
	15 974 805,91 +11,35%	11 908 641,13 -25,45%	14 462 346,88 +21,44%	18 310 348,43 +26,61%	13 342 144,22
Ненадання послуги/товару	9 224 622,45	6 959 527,3	8 264 091,59	7 689 149,41	5 205 957,56
Карта передана клієнтом	0	0	1 380	0	30 000
ПІДСУМОК	9 224 622,45	6 959 527,3	8 265 471,59	7 689 149,41	5 235 957,56
ЗАГАЛЬНА СУМА	25 199 428,36	18 868 168,43	22 727 818,47	25 999 497,84	18 578 101,78

Аналізуючи дані табл. 3.8, можна виділити деякі ключові моменти та тенденції, адже втрати клієнтів від кіберризиків можуть бути ризиками банку і призвести до ризику втрати фінансової стійкості самого банку. Це ще раз підкреслює необхідність розробки ефективної системи протидії таким ризикам.

Аналіз показує, що АТ КБ «ПриватБанк» має дієвий ризик-менеджмент в галузі електронного банкінгу, що підтверджується інтегральним показником ІЕУР. Проте зниження темпів росту прибутку та збільшення кількості непрацюючих кредитів призвели до зменшення показника ефективності ризик-

менеджменту з 1,00 до 1,67 порівняно з періодом 2018-2019 років. Важливо відзначити, що зниження цього показника в 2020 році вказує на те, що в майбутньому, при відтіканні депозитів та зростанні обсягу проблемних кредитів, банк може зазнати значних фінансових втрат. У таких умовах виникає необхідність в оцінці впливу бізнес-моделі електронного банкінгу на прибутковість та фінансову стабільність банку, які в кінцевому підсумку визначатимуть життєздатність бізнес-моделі.

Отже, в третьому розділі дано докладний аналіз розвитку фінансових технологій в банкінгу України та основних ризиків, пов'язаних із цим процесом. Розглянуто етапи розвитку фінансових технологій у банкінгу та основні виклики, з якими стикаються банки в Україні в цьому контексті. Аналіз показав, що фінансові технології в Україні розвиваються досить швидко та активно. Вносять значні зміни у фінансовий сектор, спрощуючи доступ до фінансових послуг та покращуючи якість обслуговування клієнтів. Проте цей розвиток не обходиться без ризиків. Оцінка ефективності управління ризиками фінансових технологій банкінгу на основі динамічного нормативу вказує на важливість ретельного моніторингу та аналізу цих ризиків. Динамічний норматив дозволяє виявляти ризики та змінювати стратегії управління ними в реальному часі. Загалом, розвиток фінансових технологій у банкінгу України відкриває нові можливості та виклики для сектору. Ефективне управління ризиками є важливою складовою успішної інтеграції фінансових технологій у діяльність банків, та водночас відкриває можливості для покращення фінансової системи та обслуговування клієнтів.

ВИСНОВКИ

У даній кваліфікаційній роботі були розглянуті ключові аспекти управління ризиками в галузі FinTech банкінгу. Всі три розділи цієї роботи взаємодіяли, щоб представити обширну інформацію щодо ризиків, з якими стикаються банківські установи, особливо в умовах стрімкого розвитку фінансових технологій.

Основні поняття та теоретичні аспекти, було детально розглянуто поняття FinTech та його роль у фінансовому секторі. Досліджено важливість FinTech у поліпшенні та автоматизації фінансових послуг, а також його вплив на компанії та споживачів. Описано різноманітні сфери, де використовуються фінансові технології, та наведено приклади таких послуг.

Аналіз ризиків в галузі FinTech, було розглянуто різні аспекти управління ризиками. Почавши з огляду на функції та мету управління ризиками в Головному управлінні ДПС у м. Києві, надано загальний контекст управління ризиками в Україні. Далі, розглянуто ризики FinTech в банках та методи управління ними. Звернули увагу на зв'язок між фінансовими технологіями та хмарними технологіями, а також способи захисту цих технологій від кібератак. Вивчено методи та стратегії для управління ризиками, що дозволило внести пропозиції щодо ефективного управління ризиками в галузі FinTech.

Проведено аналіз розвитку фінансових технологій в банкінгу України та виділено основні ризики, які супроводжують цей розвиток. Оцінка ефективності управління ризиками була проведена на основі динамічного нормативу. Оцінка ця дозволила визначити, як банкінг в Україні пристосовується до викликів, пов'язаних із розвитком фінансових технологій.

В заключному пункті цієї кваліфікаційної роботи можна підкреслити наступне. FinTech впливає на багато сфер фінансового сектору, надаючи компаніям та споживачам нові можливості та послуги. Управління ризиками в галузі FinTech важливе для забезпечення стабільності фінансових установ і зменшення можливих загроз. Захист фінансових технологій від кібератак є

критичним завданням, і ця робота висвітлила деякі стратегії для забезпечення безпеки в цій галузі. Ефективне управління ризиками в FinTech банкінгу в Україні потребує постійного моніторингу та адаптації до змін у сфері фінансових технологій. Усі ці аспекти демонструють важливість розуміння ризиків у галузі FinTech та необхідність вдосконалення стратегій управління ними для забезпечення ефективного функціонування в сучасному фінансовому світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Алексєєв М. М. Аналіз методологічних підходів щодо застосування технологій управління ризиками у сфері кібербезпеки. *Протиборство у кібернетичному просторі*. 2022. №1(34). С. 109-114.
2. Ананьєва Ю. Вплив глобалізації на фінансову стабільність підприємств та стратегії її забезпечення. *Економіка та суспільство*. 2022. № 55. URL: <https://doi.org/10.32782/2524-0072/2023-55-14>
3. Безпалый Р.В. Фінтех-інновації: передумови становлення та сучасні тенденції. *Інвестиції: практика та досвід*. 2023. № 2. С. 44–49
4. Белінська Г.В. Ринок фінансових інновацій: сутність, особливості та передумови створення. *Наукові праці НДФІ*. 2022. № 1. С. 137–149. URL: http://nbuv.gov.ua/UJRN/Npndfi_2016_1_11
5. Боднар Є. «Агресивне податкове планування» як виклик для політики цифровізації. XI Міжнародна науково-практична конференція «Сучасні проблеми управління: трансформація публічного управління у постковідному світі». Київ, Україна, 2021. URL: <https://doi.org/10.20535/spu2021.248895>
6. Гаврилко Т.О. Fintech: зарубіжний досвід та особливості розвитку в Україні. *Науковий вісник Ужгородського національного університету. Сер. : Міжнародні економічні відносини та світове господарство*. Ужгород : Гельветика, 2023. Вип. 29. С. 17–22.
7. Гребенюк Н. О. Фінансова безпека банків: система розпізнавання загроз та усунення ризиків. *Вісник Харківського національного університету імені В. Н. Каразіна*. 2021. № 91. С. 53-64.
8. Гуменюк В.Я., Міщук Г.Ю., Олійник О.О. Управління ризиками: Навч. посіб. Рівне.: НУВГП, 2021.- 156 с.
9. Держкомстат. URL: <https://www.ukrstat.gov.ua/>
10. Домінова І.В. Оцінка ефективності ризик-менеджменту електронного банкінгу на основі нормативно-індексної моделі. *Облік і фінанси*. 2020. № 1 (87). С. 91-99.

11. Дослідження українського ринку фінансових технологій. Фінтех-2020. – 2020. – URL: <http://www.management.com.ua/tend/tend1139.htm>.
12. Забезпечення доступності ринку банківських послуг для населення територіальних громад. Я. А. Жаліло, Д. М. Гладких, Н. В. Бахур та ін. Національний інститут стратегічних досліджень. 2021. URL: <https://niss.gov.ua/sites/default/files/2021-09/bankivski-poslugy.pdf>.
13. Звіт з оверсайта інфраструктур фінансового ринку за 2020 рік, С.24 URL: https://bank.gov.ua/admin_uploads/article/Report_oversight_2020.pdf?v=4
14. Звіт про фінансову стабільність. Червень 2020 року. // Національний банк України. 2020. С. 40
15. Інновації та розбудова фінтех-ринку України – у фокусі уваги Національного банку Національний банк України. URL: <https://bank.gov.ua/news/all/inNovatsiyi-ta-rozbudovafinteh-rinku-ukrayini--u-fokusiuuvagi-natsionalnogo-banku>
16. Клієнти monobank за 15 днів жовтня надіслали «неіснуючим біржам» 6 мільйонів – Гороховський. Мінфін - все про фінанси: новини, курси валют, банки. URL: <https://minfin.com.ua/ua/2023/10/26/114931682/>.
17. Міністерство фінансів України. Міністерство Фінансів України. URL: <https://www.mof.gov.ua/uk/tax-policy>
18. Мобільні додатки банків, хто кращий в 2021? Український Спектр. – 2021. – URL: <https://uaspectr.com/2021/05/13/mobilni-dodatky-bankiv/>.
19. Орищин Т. Напрями оптимізації податкового навантаження підприємств в контексті податкового планування. *Економіка та суспільство*. 2021. № 25. URL: <https://doi.org/10.32782/2524-0072/2021-25-82>
20. Податкове законодавство. tax.gov.ua.URL: <https://tax.gov.ua/zakonodavstvo/podatkovе-zakonodavstvo/>
21. Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України : Постанова Правління НБУ від 28 жовтня 2010 року № 474. URL: <https://zakon.rada.gov.ua/laws/show/v0474500-10#Text>

22. Про національну безпеку : Закон України від 21.06.2018 № 2469-VIII (зі змінами). URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (дата звернення: 10.10.2023).
23. Пурій Г.М. Оцінка ризиковості кредитно-інвестиційної діяльності банків на фінансовому ринку України. *Науковий вісник : Фінанси, банки, інвестиції*. 2021. №1. С. 46–54.
24. Садовничий В. Клієнти на відстані. Вебсайт 50 провідних банків України – фінансовий клуб 21 липня 2020 року. URL : <https://banksrating.com.ua/analytics/kliyenti-na-vidstani/>
25. Стратегія розвитку фінансового сектору України до 2025 року. URL: https://mof.gov.ua/storage/files/Strategija_/financovogo_sectoru_ua.pdf
26. Територіальні органи ДПС у м. Києві. URL: <https://kyiv.tax.gov.ua/>.
27. Тютюн І. 37% українців не мають банківських карт. Навіщо онлайнбанкінг Україні. Бізнес. 2020. URL: <https://nv.ua/ukr/biz/experts/vidkritiy-banking-shchochekaye-nafinteh-v-ukrajini-50063500.html>.
28. Управління ризиками у підприємництві: навчальний посібник ,укладач Кармінська-Бєлоброва, Є.М. Ігнатова, М.В. – Харків: «Слово», 2014 – 169 с.
29. Управління ризиками: навчальний наочний посібник для студентів спеціальності 073 «Менеджмент» ,М. О. Кравченко, К. О. Бояринова, К. О. Копішинська ; КПІ ім. Ігоря Сікорського.– Київ : КПІ ім. Ігоря Сікорського, 2022. – 432 с.
30. Управління фінансовими ризиками в Україні, Гудзь О.Є. Економіка АПК. - 2020. - № 8. - С. 72-76.
31. Управління фінансовими ризиками: навч. посіб. С. Г. Шклярук. — Київ : ДП «Вид. дім «Персонал», 2022. — 494 с.
32. Управління фінансовими ризиками: навчальний посібник ,Вінниця: ДонНУ імені Василя Стуса, 2022. 256 с
33. Шевченко О. Розвиток фінансових технологій в умовах цифровізації економіки України. *Ефективна економіка*. 2020. URL: <http://www.economy.nayka.com.ua/?op=1&z=8053>.

34. Якубовський О.П., Пахомова Т.І., Драгомирецька Н.М. Управління ризиками та кризами (опорний конспект дистанційного курсу навчальної дисципліни): Навчальний посібник. – К.: Центр дистанційного навчання НАДУ при Президентові України, 2020. – 68 с
35. Kuznietsova N. V. Фінансовий ризик-менеджмент з урахуванням інформаційних ризиків. Реєстрація, зберігання і обробка даних. 2018. Т. 20, № 1. С. 30–39. URL: <https://doi.org/10.35681/1560-9189.2018.20.1.142900> (дата звернення: 31.10.2023).
36. NCSI : Ukraine. URL: <https://ncsi.ega.ee/country/ua/>.
37. Reshaping retail banks: Enhancing banking for the next digital age : Report. – October 18, 2023. – URL : <https://www.mckinsey.com/industries/financial-services/our-insights/reshaping-retail-banks-enhancing-banking-for-the-next-digital-age>.
38. Top fintech innovations to watch that marked in 2020. IndustryWired. URL: <https://industrywired.com/top-FinTech-innovations-to-watch-that-marked-in-2020/>.
39. What is Fintech Compliance? + Its Major Risks. URL: <https://drata.com/blog/fintech-compliance>
40. Zoom Finance 2021 Warsaw: Kantar. – 2021. –URL: https://scholar.google.com/scholar_lookup?title=Zoom+Finance+2021&author=Kantar&publication_year=2021.

ДОДАТКИ

Додаток А

ЗАТВЕРДЖУЮ
В. о. начальника
Головного управління ДПС у м. Києві
(особистий підпис)
«___» _____ року
починає діяти з _____ року

ПОСАДОВА ІНСТРУКЦІЯ ДЕРЖАВНОГО СЛУЖБОВЦЯ

категорія посади ☐ Б ☒ В

Посада _____
(заповнюється після здійснення посади, вказується всієї структурної підрозділу, до складу якої входить така посада)

Посада безпосереднього керівника	Начальник відділу
Посада керівника самостійного структурного підрозділу	Начальник управління

3. Основні посадові обов'язки

1	_____
---	-------

4. Права (крім передбачених статтею 7 Закону України «Про державну службу»)
Одержувати від структурних підрозділів Головного управління ДПС у м. Києві інформацію і матеріали, необхідні для виконання завдань і функцій, покладених на відділ.
2. Брати участь у службових нарадах, навчаннях працівників, вносити пропозиції щодо подальшого поліпшення роботи відділу.
3 Інші права, передбачені законами України, Податковим кодексом України, законодавством України про працю

5. Зовнішня службова комунікація
Центральні органи виконавчої влади та їх територіальні органи, правоохоронні органи, громадяни, юридичні та фізичні особи, фізичні особи-підприємці з питань, що належать до компетенції відділу

6. Спеціальні умови служби
Режим роботи відповідно до Регламенту Головного управління ДПС у м. Києві

Розроблено

Начальник відділу (посада особи, яка розробила посадову інструкцію)	_____ (підпис)	_____ (дата)
Начальник управління (посада керівника самостійного структурного підрозділу)	_____ (підпис)	_____ (дата)

З посадовою інструкцією ознайомлений(на)

Додаток Б



ГОЛОВНЕ УПРАВЛІННЯ
ДЕРЖАВНОЇ ПОДАТКОВОЇ СЛУЖБИ
у м. КИЄВІ

04116, м. Київ, вул. Шолуденка, 33/19

ВИТЯГ

[Redacted]

Місце проведення: приміщення Головного управління ДПС у м. Києві (каб. [Redacted])

Головував: [Redacted]

				Питання
№ п/п	Код ДП	ЄДРПОУ	Назва платника	Примітка
[Redacted]				В ході аналізу баз даних ДПС України отримано податкову інформацію, що [Redacted]

УХВАЛИЛИ:

[Redacted]

Заступник голови Комісії підпис [Redacted]

Начальник управління з питань виявлення та опрацювання податкових ризиків ГУ ДПС у м. Києві [Redacted]





Future of Fintech

MORTGAGE/ REAL ESTATE

Mortgage lending, digitization,
and financing platforms

MONEY TRANSFER/ REMITTANCES

Companies leveraging blockchain technologies for financial services

WEALTH MANAGEMENT

Investment and wealth management platforms and analytics tools

CAPITAL MARKETS

Sales & trading, analysis, and infrastructure tools for financial institutions

INSURANCE

Alternative underwriting, claims,
distribution, and/or brokerage platforms

LENDING

Peer-to-peer lending & alternative underwriting platforms

BLOCKCHAIN/ CRYPTO

Companies leveraging blockchain technologies for financial services

REGTECH

Audit, risk, and regulatory compliance software

PERSONAL FINANCE

Tools to manage bills and track personal and credit accounts

PAYMENTS/ BILLING

Payments processing, card developers,
& subscription billing software tools

THE WORLD OF FINTECH

Awareness, adoption and investment in the global fintech scene have all exploded over the past five years. This infographic explores the changing dynamics of the sector to highlight new opportunities, areas of growth and emerging challenges facing the industry

2019 HAS BEEN A YEAR OF MEGA-DEALS

Biggest announced fintech M&A deals in 2019



of global financial services institutions say they have a fintech product or service available for customers. 22 per cent say they are at pilot stage, and 40 per cent are at either research or development stage

PwC 2019

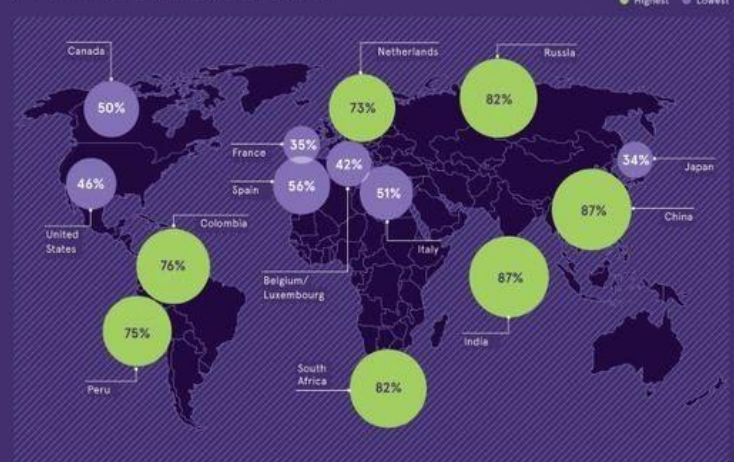
\$73.5bn

cumulative global investment in fintech companies in the first three quarters of 2019, combining venture capital, private equity and M&A

PricewaterhouseCoopers 2019

CHINA AND INDIA LEAD THE WAY IN FINTECH ADOPTION

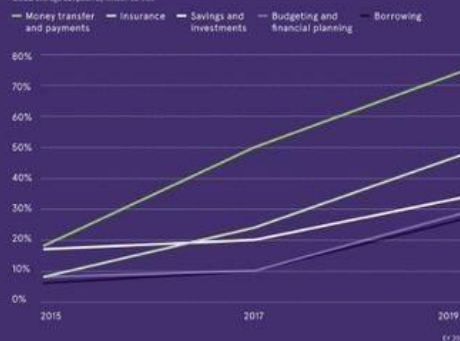
Survey of 27,000 consumers in 21 markets, percentage who had used at least one fintech service



ET 2019

MONEY TRANSFER AND PAYMENTS ARE BY FAR THE MOST USED SERVICES

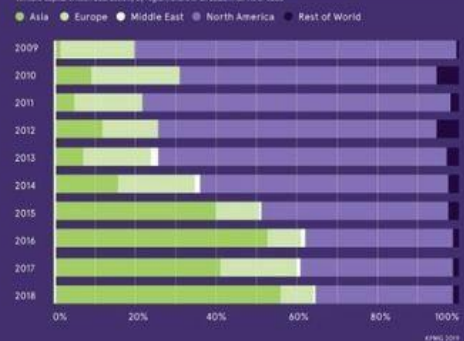
Global average adoption by fintech service



ET 2019

FINTECH STARTUPS INCREASINGLY ATTRACTING ASIAN INTEREST

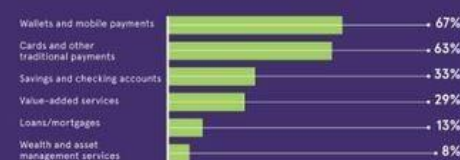
Venture capital fintech deal activity by region, share of all deals in terms of value



APWIC 2019

MOST IMPACTFUL FINTECH SERVICES

Percentage of banking executives who say the following offerings from non-traditional financial firms are having a large impact on the banking industry



Capgemini 2019

TRUST IN INCUMBENT ORGANISATIONS IS STILL HIGH

33%

of global consumers would consider a new financial organisation when considering a new service

22%

of non-adopters revealed that their decision to remain with their traditional financial provider was due to trusting it more than fintechs

ET 2019

КРИТЕРІЇ ризиковості платника податку на додану вартість

1. Платника податку на додану вартість (далі - платник податку) зареєстровано (перереєстровано) на підставі недійсних (втрачених, загублених) та підроблених документів згідно з інформацією, наявною в контролюючих органах.

2. Платника податку зареєстровано (перереєстровано) в органах державної реєстрації фізичними особами з подальшою передачею (оформленням) у володіння чи управління неіснуючим, померлим, безвісти зниклим особам згідно з інформацією, наявною в контролюючих органах.

3. Платника податку зареєстровано (перереєстровано) в органах державної реєстрації фізичними особами, що не мали наміру провадити фінансово-господарської діяльності або здійснювати повноваження, згідно з інформацією, наданою такими особами.

4. Платника податку зареєстровано (перереєстровано) та ним проваджено фінансово-господарську діяльність без відома і згоди його засновників і призначених у законному порядку керівників згідно з інформацією, наданою такими засновниками та/або керівниками.

5. Платник податку - юридична особа не має відкритих рахунків у банку/небанківського надавача платіжних послуг, крім рахунків у Казначействі (крім бюджетних установ).

{Пункт 5 в редакції Постанови КМ № 603 від 16.06.2023}

6. Платником податку не подано контролюючому органу податкової звітності з податку на додану вартість за два останніх звітних (податкових) періоди всупереч нормам [підпункту 16.1.3](#) пункту 16.1 статті 16 та [абзацу першого](#) пункту 49.2 і [пункту 49.18](#) статті 49 Податкового кодексу України (далі - Кодекс), з урахуванням вимог [підпункту 69.1](#) пункту 69 підрозділу 10 розділу XX "Перехідні положення" Кодексу.

{Пункт 6 із змінами, внесеними згідно з Постановою КМ № 1428 від 23.12.2022}

7. Платником податку на прибуток підприємств не подано контролюючому органу фінансової звітності за останній звітний період всупереч нормам [підпункту 16.1.3](#) пункту 16.1 статті 16 та [пункту 46.2](#) статті 46 Кодексу, з урахуванням вимог [підпункту 69.1](#) пункту 69 підрозділу 10 розділу XX "Перехідні положення" Кодексу.

{Пункт 7 із змінами, внесеними згідно з Постановою КМ № 1428 від 23.12.2022}

8. У контролюючих органах наявна податкова інформація, яка стала відома у процесі провадження поточної діяльності під час виконання покладених на контролюючі органи завдань і функцій, що визначає ризиковість здійснення господарської операції, зазначеної в поданих для реєстрації [податковій накладній](#)/розрахунку коригування.

Довідник кодів податкової інформації, що стала підставою для розгляду питання про відповідність платника податку критеріям ризиковості платника податку, визначається ДПС та затверджується відповідним наказом, який оприлюднюється на офіційному веб-сайті ДПС.

{Пункт 8 доповнено абзацом згідно з Постановою КМ № 1428 від 23.12.2022; в редакції Постанови КМ № 574 від 02.06.2023}

КРИТЕРІЇ ризиковості здійснення операцій

1. Обсяг постачання товару/послуги згідно з кодом УКТЗЕД/Державного класифікатора продукції та послуг/умовним кодом такого товару, зазначений у податковій накладній/розрахунку коригування до податкової накладної на збільшення суми податкових зобов'язань, яку/який подано для реєстрації в Єдиному реєстрі податкових накладних (далі - Реєстр), перевищує величину залишку, що визначається як різниця між обсягом придбання на митній території України такого/такої товару/послуги (крім обсягу придбання товарів/послуг за операціями, які звільнені від оподаткування та підлягають оподаткуванню за нульовою ставкою) та/або ввезення на митну територію України такого товару, зазначеного з 1 січня 2017 р. в отриманих податкових накладних/розрахунках коригування, зареєстрованих у Реєстрі, і митних деклараціях, збільшеного у 1,5 раза, та обсягом постачання відповідного товару/послуги, зазначеного/зазначеної в податкових накладних/розрахунках коригування, зареєстрованих з 1 січня 2017 р. у Реєстрі за відсутності такого товару/послуги згідно з кодом УКТЗЕД/Державного класифікатора продукції та послуг/умовного коду товару у врахованій таблиці даних платника податку.

(Пункт 1 із змінами, внесеними згідно з Постановою КМ № 1154 від 12.10.2022; в редакції Постанови КМ № 1428 від 23.12.2022, № 574 від 02.06.2023)

2. Відсутність (анулювання, зупинення) ліцензій, виданих органами ліцензування, які засвідчують право платника податку на виробництво, експорт, імпорт і оптову торгівлю піддашизними товарами (продукцією), визначеними підпунктами 215.3.1 і 215.3.2 пункту 215.3 статті 215 Податкового кодексу України (далі - Кодекс), стосовно товарів, зазначених платником податку в податковій накладній/розрахунку коригування, поданих для реєстрації в Реєстрі на дату їх складення.

3. Відсутність на дату складення податкової накладної/розрахунку коригування відомостей (актуального запису) в Реєстрі платників акцизного податку з реалізації пального щодо суб'єкта господарювання, який подав для реєстрації в Реєстрі податкову накладну/розрахунок коригування, у яких зазначено товар (пальне) за кодами згідно з УКТЗЕД відповідно до підпункту 215.3.4 пункту 215.3 статті 215 Кодексу.

4. Складення розрахунку коригування постачальником товарів/послуг до податкової накладної, що складена на отримувача - платника податку, якщо передбачається зміна номенклатури товару/послуги (для товарів за кодами згідно з УКТЗЕД - зміна перших чотирьох цифр кодів, а для послуг за кодами відповідно до Державного класифікатора продукції та послуг - перших двох цифр кодів, за умовними кодами такого товару - перших п'яти цифр кодів), за відсутності у врахованій таблиці даних платника податку товару/послуги згідно з кодом УКТЗЕД/Державного класифікатора продукції та послуг/умовного коду товару, на який здійснюється зміна номенклатури товару/послуги.

(Пункт 4 в редакції Постанови КМ № 574 від 02.06.2023)

5. Перевищення суми компенсації вартості товару/послуги, зазначеного/зазначеної в розрахунку коригування на зменшення суми податкових зобов'язань, поданого отримувачем такого товару/послуги для реєстрації в Реєстрі, над величиною залишку, що визначається як різниця між обсягом придбання на митній території України такого/такої товару/послуги (крім обсягу придбання товарів/послуг за операціями, які звільнені від оподаткування та підлягають оподаткуванню за нульовою ставкою) з 1 січня 2017 р., зазначеного постачальником у зареєстрованих у Реєстрі податкових накладних/розрахунках коригування, складених на отримувача такого/такої товару/послуги, та обсягу постачання з 1 січня 2017 р., зменшеного у 1,5 раза та зазначеного отримувачем у зареєстрованих у Реєстрі податкових накладних/розрахунках коригування на постачання такого/такої товару/послуги.

(Пункт 5 в редакції Постанови КМ № 1428 від 23.12.2022)

6. Подання для реєстрації в Реєстрі розрахунку коригування на зменшення податкових зобов'язань до податкової накладної, складеної та зареєстрованої постачальником товарів/послуг на неплатника податку на додану вартість, у строк, що перевищує 30 календарних днів з дня складення податкової накладної, зареєстрованої в Реєстрі без порушення граничних строків реєстрації, встановлених Кодексом, крім розрахунку коригування до податкової накладної, у якій відображені операції з постачання електричної енергії (товарна підпозиція 2716 згідно з УКТЗЕД), постачання природного газу (товарні підпозиції 2705, 2709 та 2711 11 згідно з УКТЗЕД), постачання теплової енергії (умовний код товару 00401).

(Пункт 6 в редакції Постанови КМ № 1428 від 23.12.2022)

