МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАДИМА ГЕТЬМАНА

Факультет фінансів

Кафедра банківської справи та страхування

галузь знань	07 «Управління та адміністрування»
спеціальність	072 «Фінанси, банківська справа та страхування»
освітньо-професійна програма	«Банківський бізнес»

Форма навчання: *Денна*

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему **«Технології безпеки фінансового бізнесу»**

здобувача Бондаренка Дмитра Віталійовича _____
(Прізвище, ім'я, по батькові) *(підпис здобувача)*

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

_____ Литвиненко О.К.
(підпис) *(Прізвище, ініціали)*

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

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

Київ 2025

ЗМІСТ

ВСТУП

Актуальність теми. У сучасних умовах глобалізації, стрімкої цифровізації та ускладнення фінансових процесів питання забезпечення безпеки у сфері фінансового бізнесу набуває особливої актуальності. Цифрова трансформація фінансового сектору, з одного боку, відкриває нові можливості для зростання ефективності, зниження транзакційних витрат і покращення клієнтського досвіду, а з іншого — супроводжується зростанням ризиків, зокрема кіберзагроз, шахрайства, витоку даних, нестабільності регуляторного середовища. В умовах підвищеної конкуренції та постійних технологічних змін фінансові установи змушені впроваджувати новітні технології забезпечення безпеки, що є важливою передумовою їх стійкості, репутаційної довіри та довгострокового розвитку. Саме тому дослідження технологій безпеки фінансового бізнесу є своєчасним і затребуваним як у науковому, так і практичному контексті.

Аналіз останніх досліджень і публікацій. Питання забезпечення фінансової безпеки активно досліджуються у працях вітчизняних і зарубіжних вчених, серед яких варто відзначити А. О. Барановського, І. О. Бланка, Н. Й. Ревенчук, З. С. Варналія, П. О. Нікіфорова, К. С. Горячеву. У їхніх роботах розглядаються різні аспекти економічної та фінансової безпеки, зокрема на рівні підприємств, держави та галузей. Проте, попри наявність численних підходів до визначення поняття фінансової безпеки, у науковій літературі недостатньо уваги приділено питанням безпеки саме у сфері фінансового бізнесу в умовах цифрової економіки. Актуальність дослідження також зумовлена необхідністю комплексного осмислення загроз, ризиків та інструментів цифрової безпеки з урахуванням специфіки фінансових установ та інноваційного середовища.

Мета і завдання дослідження. Мета - проаналізувати особливості застосування сучасних технологій безпеки у фінансовому бізнесі та виявити їх роль у зниженні ризиків і підвищенні надійності функціонування фінансових установ.

Завдання дослідження:

1. З’ясувати сутність поняття безпеки у фінансовому бізнесі та охарактеризувати її значення для стабільної діяльності фінансових установ.

2. Визначити основні загрози та ризики, що виникають у сфері фінансового бізнесу, та здійснити їх загальну класифікацію.

3. Описати ключові механізми і технології, що використовуються для забезпечення безпеки у фінансовому секторі.

4. Розглянути приклади впровадження інноваційних фінансових технологій у системах безпеки банківського бізнесу.

5. Проаналізувати досвід застосування сучасних технологій безпеки у Monobank.

6. Оцінити переваги та недоліки використання цифрових технологій для підвищення фінансової безпеки в умовах цифрової економіки.

Об’єктом дослідження є процеси забезпечення безпеки у сфері фінансового бізнесу.

Предметом дослідження є сучасні технології та підходи до забезпечення безпеки, що використовуються в діяльності фінансового бізнесу.

Методи дослідження. У процесі написання дипломної роботи було використано такі загальнонаукові та спеціальні методи: аналіз і синтез — для систематизації наукових підходів до трактування фінансової безпеки; порівняльно-аналітичний метод — для зіставлення різних технологій та моделей безпеки у фінансових установах; структурно-функціональний підхід — для виокремлення ключових елементів системи фінансової безпеки; графоаналітичний метод — для візуалізації внутрішньої структури безпеки бізнесу; експертна оцінка — при аналізі практик використання фінтех-рішень у банках (зокрема, Monobank);**узагальнення** — для формулювання висновків і пропозицій щодо удосконалення системи безпеки у фінансовому бізнесі.

Теоретична, методична та практична значущість отриманих результатів. **Теоретична значущість** дослідження полягає у поглибленні змісту поняття «фінансова безпека бізнесу» з урахуванням викликів цифрової економіки, а також у розвитку існуючих наукових підходів до структурування її складових.

Методична значущість проявляється у запропонованій класифікації ризиків та загроз, моделі забезпечення безпеки фінансового бізнесу, систематизації інструментів цифрового захисту. **Практична значущість** полягає у тому, що результати дослідження можуть бути використані фінансовими установами при побудові ефективної системи управління ризиками, розробці політик кіберзахисту, а також формуванні регуляторних ініціатив на державному рівні.

Інформаційна база дослідження відображає наукові праці вітчизняних і зарубіжних дослідників у сфері фінансової та економічної безпеки; аналітичні звіти та рекомендації міжнародних організацій; матеріали з офіційних вебсайтів фінансових установ (Monobank, ПриватБанк).

Структура роботи. Робота складається зі вступу, двох розділів, висновків, списку використаних джерел та додатків.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ФІНАНСОВОГО БІЗНЕСУ

1.1 Сутність та значення безпеки у фінансовому бізнесі

У сучасних умовах нестабільного макроекономічного середовища, стрімкої цифровізації та поширення кіберзагроз питання забезпечення фінансової безпеки набуває особливої актуальності для фінансового бізнесу. Водночас у науковій та практичній площині досі не існує єдиного підходу до визначення поняття «фінансова безпека», що формує дискусійне поле для подальшого теоретичного осмислення цієї категорії.

Одні дослідники (зокрема Вудвуд В. В. і Батієвська О. В.) трактують фінансову безпеку як ефективну систему захисту підприємства від ризиків та загроз із метою досягнення його стійкого розвитку [1]. Такий підхід акцентує увагу на необхідності впровадження технологічно та організаційно ефективних заходів безпеки, які забезпечують стабільність у довгостроковій перспективі.

Водночас інші автори, як-от Рожко О. та Нестеров Є., вбачають у фінансовій безпеці передусім стан фінансової системи, за якого забезпечується фінансова рівновага та ефективна протидія зовнішнім і внутрішнім загрозам [2]. Такий підхід зміщує акцент з процесу безпеки на її результат — стабільний фінансовий стан підприємства.

Дещо іншу позицію займають Мехед А. М. та Варналій З. С., які розглядають фінансову безпеку в умовах цифрової економіки як гармонізацію інтересів підприємства та його зовнішнього середовища [3]. У цьому контексті фінансова безпека набуває стратегічного характеру і пов’язується з адаптивністю бізнесу до динамічних цифрових і регуляторних трансформацій.

Зокрема, А. О. Барановський [4] пропонує всеохопне бачення фінансової безпеки як багаторівневої системи, що включає як макроекономічні індикатори

(платіжний баланс, бюджетна стабільність, валютна система), так і здатність окремих суб'єктів фінансових відносин ефективно протистояти викликам. У такій інтерпретації фінансова безпека набуває системного характеру, вимагаючи міжсекторальної узгодженості.

Натомість Н. Й. Ревенчук [5] розглядає фінансову безпеку підприємства більш прагматично — як інструмент попередження фінансових втрат і банкрутства, що реалізується через оптимізацію використання наявних ресурсів. У подібному ключі Горячева К. С. [6] визначає фінансову безпеку як збалансований стан фінансових інструментів і послуг, який дозволяє досягати стратегічних цілей.

Фінансова безпека відіграє важливу роль у забезпеченні:

- Стабільності та стійкості фінансових установ в умовах економічної нестабільності та конкуренції.
- Захисту від фінансових шахрайств та кіберзагроз, що особливо актуально в епоху цифровізації фінансових послуг.
- Збереження довіри клієнтів та партнерів, що є критичним для успішного функціонування фінансового бізнесу.
- Забезпечення відповідності регуляторним вимогам та стандартам фінансової діяльності.

Загальна характеристика підходів до трактування сутності фінансової безпеки наведена в таблиці 1.1.

Таким чином, у сучасному дискурсі фінансова безпека розглядається як багатовимірне явище, що включає як організаційно-технічні аспекти захисту, так і економічні, інформаційні та стратегічні елементи стійкості бізнесу. Враховуючи швидку еволюцію цифрових технологій, важливо не лише забезпечити технічну захищеність фінансової інфраструктури, а й сформувати ефективну систему управління ризиками, що відповідає як регуляторним вимогам, так і очікуванням клієнтів у сфері безпеки.

Таблиця 1.1 – Порівняльна характеристика підходів до визначення фінансової безпеки

Автори	Визначення	Основні акценти
Вудвуд В. В., Батієвська О. В.	Система захисту від ризиків і загроз для забезпечення стабільного розвитку підприємства	Безпекова інфраструктура, системний підхід
Рожко О., Нестеров Є.	Стан фінансової системи з ефективною протидією загрозам і фінансовою рівновагою	Становий підхід, баланс і стійкість
Мехед А. М., Варналій З. С.	Гармонізація інтересів підприємства та зовнішнього середовища в умовах цифровізації	Стратегічний підхід, цифрова адаптивність
Барановський А. О.	Комплексна система захисту фінансових інтересів на всіх рівнях – від особистого до глобального. Охоплює стабільність функціонування фінансової, податкової, банківської та інвестиційної систем; забезпечує достатність фінансових ресурсів для виконання зобов'язань і запобігає зовнішній експансії.	Системність, макро- і мікрорівні, ресурсна забезпеченість
Ревенчук Н. Й.	Економічна безпека підприємства як інструмент мінімізації фінансових втрат і ризику банкрутства, через ефективне використання активів.	Захист від збитків, ефективність ресурсів
Горячева К. С.	Збалансований стан фінансових засобів підприємства, що дозволяє йому реалізувати фінансові завдання, бути стійким до загроз та забезпечувати сталий розвиток.	Фінансова рівновага, функціональна стійкість
Єпіфанов А. О.	Стан, що гарантує підприємству фінансову стабільність, незалежність, гнучкість у прийнятті рішень і захист інтересів власників.	Стратегічна гнучкість, незалежність
Кириченко О. А. та ін.	Ефективне управління корпоративними фінансами, що проявляється в оптимальних значеннях прибутковості, рентабельності та ринкової вартості бізнесу.	Управлінська ефективність, капіталізація
Нікіфоров П. О., Куперівська С. С.	Здатність компанії до раціонального використання ресурсів і швидкого реагування на загрози без шкоди для стабільності функціонування.	Оперативність, внутрішній контроль

Джерело: систематизовано автором [1-9]

Фінансова безпека бізнесу розглядається як безперервний процес підтримки та підвищення ключових фінансово-економічних показників підприємства, що реалізується шляхом ефективного управління фінансовими потоками та формуванням умов, необхідних для протидії зовнішнім і внутрішнім загрозам. Її основною метою є забезпечення стабільної діяльності суб'єкта господарювання та створення основ для його подальшого сталого розвитку.

До об'єктів фінансової безпеки відносять фінансово-кредитну сферу, як сукупність інструментів, механізмів і явищ, що є предметом захисної діяльності

суб'єктів. Натомість суб'єктами забезпечення фінансової безпеки виступають органи державної влади — законодавчої, виконавчої та судової гілок, а також фінансові інститути, регіональні органи управління, господарські структури базового рівня економіки та громадяни.

На думку Барановського О.І., до об'єктів фінансової безпеки слід відносити не лише фінансові ресурси й інструменти, а й систему фінансових відносин, що охоплює податкову, бюджетну, грошово-кредитну, валютну, банківську, інвестиційну, фондову, митно-тарифну сфери, а також механізми ціноутворення [4].

Забезпечення фінансово-економічної стабільності бізнесу відбувається поетапно. Початковий етап полягає у виявленні чинників, що становлять потенційну загрозу для функціонування підприємства.

Фінансова безпека підприємства формується на основі взаємодії різних компонентів, кожен із яких відіграє специфічну роль у загальній системі. Ці складові представлені на рисунку 1.1.

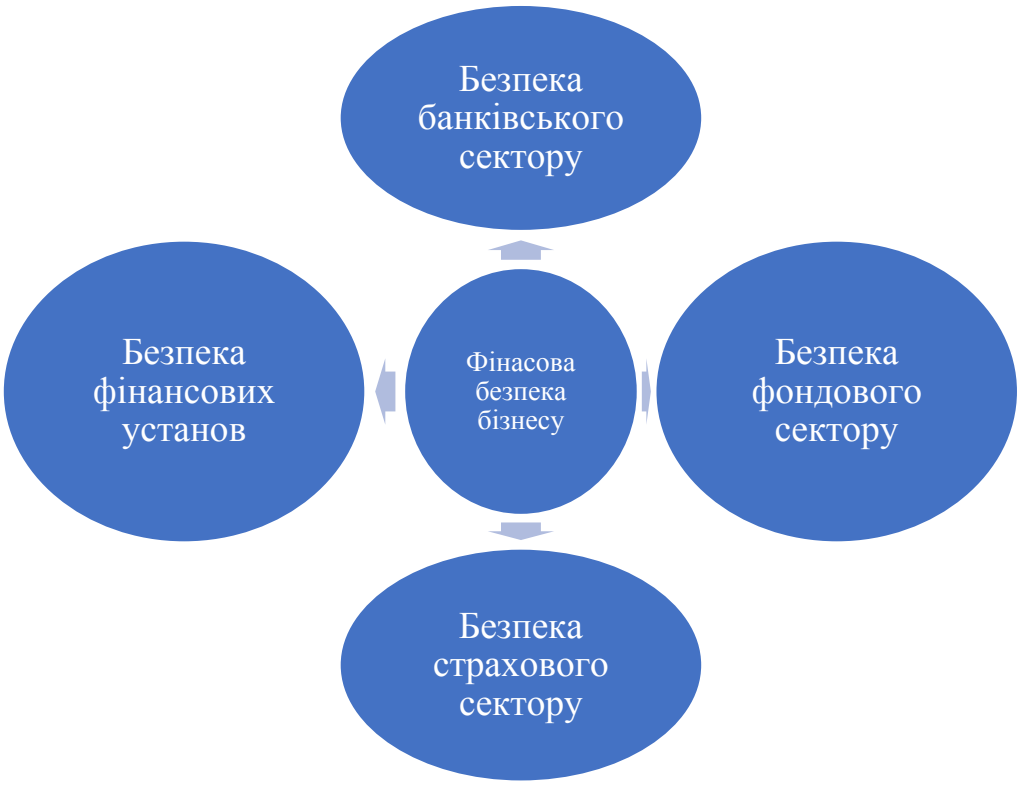

Рисунок 1.1 - Елементи структури фінансової безпеки бізнесу

Складено автором [9]

Окремим елементом є фінансова стійкість банківських установ**,** яка виступає ключовою ланкою як в межах економічної безпеки окремого бізнесу, так і національного рівня. Такий стан банку характеризується стійкістю до зовнішніх впливів, наявністю достатніх резервів та можливістю реалізовувати стратегічні цілі.

Фінансова стабільність страхових компаній — це такий рівень фінансового стану, який дозволяє забезпечити надійний захист економічних інтересів у страховому секторі та підтримку платоспроможності у межах національної фінансової системи.

У фондовому сегменті фінансова безпека виражається через забезпечення достатнього рівня ринкової капіталізації, що дозволяє гарантувати стабільність позицій інвесторів, емітентів, біржових посередників і держави [10].

Рисунок 1.2 - Фінансова безпека в економічніій безпеці бізнесу

Джерело: складено автором [10]

Формування дієвої системи фінансової безпеки підприємства виконує ключову функцію в загальній структурі економічної безпеки організації, оскільки

впливає на всі аспекти її функціонування. Фінансова безпека інтегрована у фінансовий менеджмент та реалізується через стратегічні й тактичні механізми відповідно до умов сучасного ринку.

Наукова література пропонує різні підходи до трактування поняття «фінансова безпека». Загальновизнано, що вона базується на трьох основних критеріях: стратегічному, ресурсному та функціональному.

Професор І.О. Бланк трактує фінансову безпеку як кількісно і якісно вимірюваний рівень фінансового стану суб'єкта господарювання, який забезпечує реалізацію його ключових інтересів, захищаючи від ідентифікованих ризиків, що виникають внаслідок впливу факторів внутрішнього й зовнішнього середовища. Цей рівень базується на власній фінансовій концепції підприємства і є основою його сталого розвитку [11].

На думку Нікіфорова П.О. та Кучерівської С.С., підприємство можна вважати фінансово захищеним, якщо воно ефективно управляє своїми фінансовими ресурсами, має механізми контролю, здатне оперативно реагувати на загрози, мінімізуючи їхній вплив без шкоди для загального функціонування [8].

Доктор економічних наук Єпіфанов А.О. окреслює фінансову безпеку як стан, що [9]:

1. забезпечує стабільність фінансів, ліквідність і платоспроможність у довгостроковій перспективі;
2. гарантує фінансову автономність і здатність до розширеного відтворення;
3. дозволяє протистояти загрозам, які можуть призвести до фінансових втрат, зміни структури капіталу або ліквідації підприємства;
4. передбачає гнучкість у фінансових рішеннях і захист інтересів власників.

Реверчук Н.Й. розглядає фінансову безпеку як систему захисту підприємства від можливих фінансових втрат і запобігання банкрутству, що супроводжується підвищенням ефективності використання внутрішніх ресурсів.[5]

З огляду на специфіку фінансового бізнесу, важливо акцентувати увагу не лише на безпеці окремих його суб’єктів, а й на впливі зовнішнього середовища, що формує передумови для сталого функціонування підприємницького сектору. Такий підхід має вагоме теоретико-прикладне значення, перевищуючи за аналітичною глибиною традиційний розгляд безпеки як суто внутрішньої категорії. Попри велику кількість наукових джерел, що висвітлюють аспекти економічної безпеки, часто у них не простежується нових підходів до інтерпретації макрорівневої складової проблеми.

Наприклад, О. Власюк у своїх дослідженнях розглядає безпеку підприємництва як стан захисту корпоративних ресурсів і підприємницького потенціалу, що забезпечує протидію внутрішнім і зовнішнім ризикам, а також створює базу для ефективної та стійкої діяльності бізнес-структур [12, с. 10–20]. Подібний підхід поділяє й М. Камлик, який, використовуючи процесну методологію, акцентує увагу на безпеці підприємницької активності як безперервного управлінського процесу [13, с. 9].

Поглиблений аналіз вітчизняних досліджень засвідчує, що економічна безпека окремих секторів бізнесу значною мірою інтегрована в загальнонаціональну систему безпеки, тобто має радше макроекономічну природу. Так, Н. Юрків підкреслює, що безпека реального сектору економіки, враховуючи її структурні й галузеві параметри, повністю відповідає критеріям, властивим системі національної економічної безпеки. У цьому контексті доцільним є застосування структурного підходу до аналізу стану захищеності на секторальному рівні [14, с. 22].

Аналогічну позицію займає й О. Собкевич, який, досліджуючи загрози для реального сектору економіки України, застосовує макроекономічні індикатори — рівень зношення основних виробничих фондів, динаміку інвестиційних потоків, рівень інноваційної активності, енергоспоживання, а також залежність від зовнішніх економічних чинників [15с. 139–140].

У науковій літературі [16, с. 22] також наголошується, що безпека реального сектору становить одну з головних підсистем економічної безпеки держави. Вона

фактично відображає адаптацію загальнонаціонального підходу до рівня галузевого управління, демонструючи, наскільки середовище функціонування бізнесу сприяє захисту суб'єктів від ризиків, а також реалізації їх потенціалу в системі національної економіки, зокрема щодо підтримки її конкурентоспроможності.

Попри значну кількість наукових праць у сфері економіки та фінансів, варто відзначити відсутність системного продовження досліджень щодо концептуалізації та змістового наповнення фінансової безпеки окремих секторів національної економіки. Переважна частина наукових розвідок акцентується на проблематиці фінансової безпеки окремих суб'єктів господарювання, особливо малого бізнесу, розглядаючи при цьому окремі елементи фінансового менеджменту у контексті забезпечення їх захищеності. Досліджуються також взаємозв'язки між фінансовою стабільністю держави та фінансовою безпекою бізнес-структур, а також роль фінансової політики як інструменту впливу на стан захищеності господарських суб'єктів через структурно-функціональні компоненти державної безпеки.

З огляду на зазначене, доцільно зробити два концептуальні висновки. Перший полягає у визнанні необхідності подальшого наукового вивчення механізмів, інструментів і методів державної політики у сфері управління фінансовою безпекою різних галузей і секторів економіки. Другий – у розумінні фінансової безпеки певного сектора як невід'ємної складової економічної безпеки, що, з огляду на свою вагу та функціональну значущість, набуває статусу фінансово-економічної безпеки відповідного сегмента економіки.

У цьому контексті фінансова безпека малого підприємництва розглядається як макроекономічна категорія, що належить до сфери відповідальності держави, зокрема в частині регулювання, контролю й реалізації стратегічних цілей політики безпеки. Її концептуальне обґрунтування має базуватись на положеннях, притаманних загальній парадигмі економічної й фінансової безпеки держави. Незважаючи на збереження активної наукової дискусії щодо природи та структури цього явища, більшість дослідників фінансової безпеки сходяться на думці, що її внутрішня архітектоніка охоплює три ключові елементи:

1. Економічну незалежність, яка включає володіння і контроль над ресурсами, налагоджені виробничі зв'язки, здатність до самостійного функціонування та створення конкурентної продукції, що є результатом попередніх стратегічних дій;

2. Стійкість і стабільність, які визначаються ефективністю господарської діяльності в теперішньому часі та здатністю протистояти зовнішнім і внутрішнім загрозам;

3. Потенціал до розвитку, що характеризується наявністю позитивної динаміки зростання ключових економічних показників і орієнтацією на інновації та модернізацію.

Виходячи з аналітичної логіки, можна вважати доцільним зберегти загальну архітектоніку моделі фінансової безпеки малого підприємництва, здійснивши лише часткове коригування назв складових її внутрішньої структури та конкретизацію змістового наповнення відповідних елементів (рис. 1.3).

Рисунок 1.3 - Ключові складові фінансової безпеки бізнесу

Джерело: систематизовано автором [1-10]

У цьому контексті компонент «ресурсна забезпеченість» відображає можливості доступу представників малого бізнесу до ключових фінансових ресурсів, інвестиційних потоків та капіталу. Ідеться, зокрема, про доступ до фінансових послуг, ринків капіталу та кредитних механізмів, а також про сформованість розвиненої інфраструктури фінансових послуг, наявність дієвого механізму страхування ризиків та сприятливе регуляторно-правове середовище.

Важливо підкреслити, що кожен ресурс, залучений до господарської діяльності, пов’язаний із витратами, а отже — із формуванням фінансово-економічних відносин. З цієї позиції «ресурсна забезпеченість» охоплює не лише наявність капіталу, але й ефективно функціонуючий ринок фінансових послуг, що забезпечує доступ до ресурсів. З боку державної політики — це наслідок заходів, реалізованих у минулому, результати яких проявляються сьогодні.

На рівні окремих підприємств ресурсне забезпечення, як правило, є відображенням попередньо накопичених ресурсів і стратегій фінансування.

Щодо складової «стійкість, ефективність та захищеність», її сутність полягає у здатності бізнесу функціонувати в умовах нестабільності та загроз, зберігаючи при цьому фінансову життєздатність. Це передбачає наявність адаптивної системи управління ризиками, стабільність ліквідності й платоспроможності, результативність виробничо-господарської діяльності, а також реалізацію економічних інтересів усіх стейкхолдерів. До останніх належать не лише власники бізнесу, а й персонал, партнери, інвестори, споживачі, органи державної влади й місцеві громади. Варто зауважити, що показники цієї компоненти можуть бути оцінені лише у статичному часовому зрізі, тобто характеризують поточний стан.

У свою чергу, компонент «розвиток» відображає динаміку змін, спрямованих на посилення фінансового потенціалу сектору бізнесу. Йдеться про зростання обсягів активів, інвестицій, капіталу, впровадження інновацій і технологічних рішень, що підвищують конкурентоспроможність на національному та міжнародному рівнях. Цей вимір демонструє орієнтацію на стратегічну перспективу.

Узагальнюючи, можна стверджувати, що внутрішня структура фінансової безпеки бізнесу репрезентує синтез трьох часових вимірів:

1. минуле – як рівень сформованості ресурсної бази;
2. теперішнє – як здатність протидіяти ризикам і ефективно функціонувати;
3. майбутнє – як потенціал до сталого розвитку та адаптації до змін.

Цей підхід дозволяє інтегрувати концепції фінансової безпеки на рівні держави, галузей економіки та окремих підприємств, з урахуванням новітніх технологій управління ризиками у фінансовому бізнесі.

Формування ефективної системи фінансової безпеки на рівні сектору економіки, зокрема фінансового бізнесу, вимагає інтеграції ключових характеристик безпеки, притаманних як макро-, так і мікроекономічному рівням. Водночас така система повинна виключати надмірні або надлишкові елементи, що не мають безпосереднього впливу на стійкість фінансового сектору.(Рис.1.4)

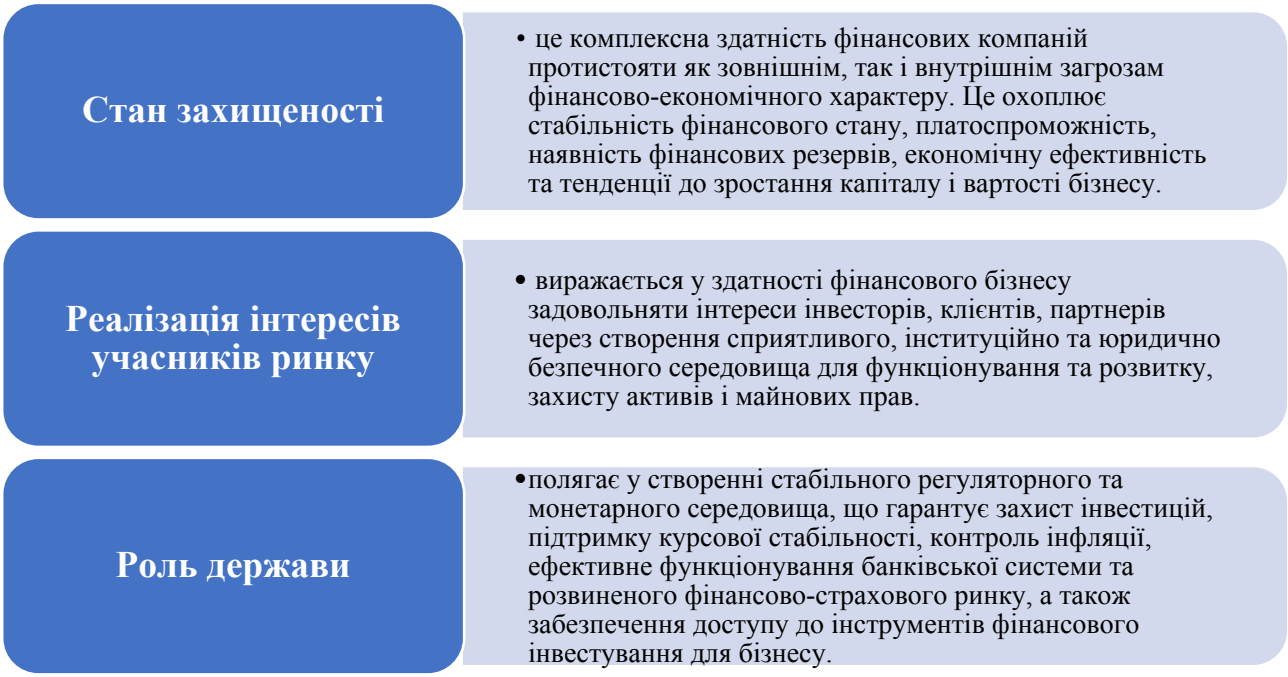

Рисунок 1.4 – Аспекти фінансової безпеки суб’єктів фінансового бізнесу

Джерело: систематизовано автором [1-16]

Спираючись на концептуальну базу аналізу безпеки економічних систем, доцільно зазначити, що в межах фінансового сектору окремі макроекономічні

складові, зокрема валютна чи бюджетна безпека, можуть бути менш релевантними в оцінці безпеки конкретного бізнесу. Натомість усі основні мікроекономічні показники доцільно згрупувати у фінансово-економічну складову**,** що відображає середній рівень прибутковості, платоспроможності, ліквідності, ділової активності та капіталізації представників фінансового бізнесу.(рис.1.5)

Рисунок 1.5- Ключові компоненти фінансової безпеки фінансового бізнесу

Джерело: систематизовано автором [13-15]

Запропонована структурна модель дозволяє не лише оцінювати поточний рівень фінансової безпеки компаній фінансового сектору, а й формувати прогностичні сценарії її змін під впливом різноманітних факторів. Саме за цими шістьма напрямами доцільно здійснювати комплексну оцінку, розробляти державні та корпоративні політики підтримки та інструменти реагування на ризики.

Розуміння внутрішньої структури фінансової безпеки бізнесу є критично важливим елементом для вибудови національної політики з підтримки стійкості фінансового сектору. Надалі увага має бути зосереджена на систематизації основних ризиків, загроз та інструментарію їх нейтралізації, що й становитиме предмет подальшого дослідження.

1.2 Загрози і ризики у сфері фінансового бізнесу

У контексті забезпечення фінансової стабільності бізнесу до дестабілізуючих чинників належать ті події або обставини, які, залежно від інтенсивності впливу, здатні суттєво порушити фінансову рівновагу підприємства, що в кінцевому підсумку знижує рівень його фінансової безпеки.

Фінансову безпеку бізнесу підривають множинні негативні фактори, які можуть призводити до порушення сталого функціонування компанії. Їх нейтралізація потребує впровадження систем превентивного реагування, які реалізуються як інструментами фінансового менеджменту, так і іншими елементами системи захисту фінансової діяльності.

Дестабілізуючі фактори виникають ще на ранніх стадіях прояву ризиків та викликів, і надалі ці елементи здатні лише посилювати один одного. Їхня природа може бути як внутрішньою, так і зовнішньою, а поява не завжди пов'язана з поточним станом фінансової безпеки компанії.

Реалізація загроз призводить до виникнення небезпек, що виражаються у глибоких трансформаціях фінансової системи бізнесу, спричинених фактичними втратами. Така ситуація демонструє прямий вплив дестабілізуючих чинників на фінансову стійкість підприємства (рис. 1.6).

Рисунок 1.6 - Структура дестабілізуючих елементів у межах фінансової безпеки бізнесу.

Джерело: систематизовано автором [16]

Серед усіх потенційних дестабілізуючих впливів найбільшу небезпеку становлять загрози, які можуть реалізуватись у разі несвоєчасної або неефективної

реакції фінансового менеджменту на зміни в середовищі. Загрози, що порушують фінансову безпеку, поділяють на реальні та потенційні**.**

Реальні загрози існують у поточний період або мають високу ймовірність реалізації в майбутньому. Їх наслідки — майже неминучі. Натомість потенційні загрози можуть активізуватися лише за певних умов, як суб'єктивного, так і об'єктивного характеру.

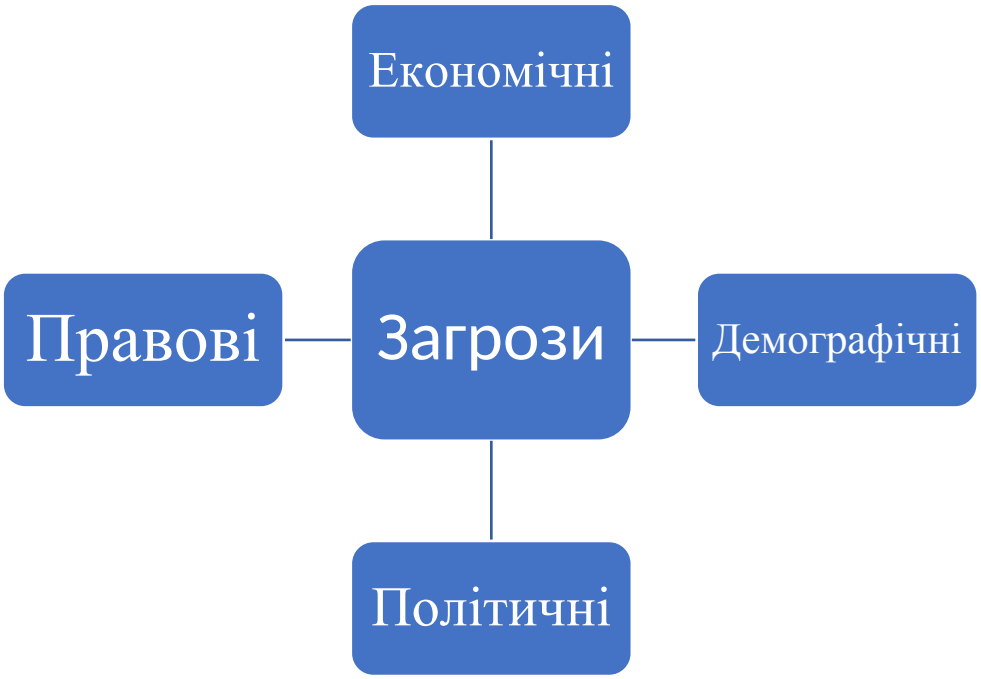

Рисунок 1.7 - Загрози як основні джерела тиску на фінансову безпеку бізнесу

Джерело: систематизовано автором [17]

Підсумовуючи, можна стверджувати, що фінансову безпеку бізнесу підривають:

- з одного боку, зовнішні загрози**,** що поєднують у собі деструктивні та дестабілізуючі чинники, (рис. 1.7).
- з іншого — наслідки внутрішніх ризиків, які прямо залежать від рішень та дій управлінського персоналу (табл.1.2)

Таким чином, рівень фінансової безпеки напряму залежить від здатності бізнесу своєчасно ідентифікувати ризики, ефективно реагувати на виклики та впроваджувати заходи щодо усунення деструктивних впливів з боку як внутрішнього, так і зовнішнього середовища.

Серед основних внутрішніх ризиків, які можуть порушити фінансову стабільність підприємства, варто виокремити системні недоліки у сфері фінансового менеджменту. Йдеться, зокрема, про помилкові управлінські рішення

— як свідомі, так і ненавмисні — що стосуються вибору фінансової стратегії, структури активів і зобов’язань, ефективності управління кредиторською та дебіторською заборгованістю, інвестиційної політики, джерел фінансування, податкової оптимізації та амортизаційних механізмів. Такі фактори мають прямий вплив на фінансову гнучкість та довгострокову життєздатність бізнесу.

Таблиця 1.2 - Ризики як основні джерела тиску на фінансову безпеку бізнесу

Категорія ризику	Опис та приклади
Кредитний ризик	Можливі втрати у разі дефолту чи прострочення платежу позичальника або контрагента. Наприклад, ризик неповернення кредиту в банку чи банкрутство емітента облігацій.
Ринковий ризик	Збитки через несприятливі зміни ринкових умов: коливання цін на цінні папери, валютні курси, процентні ставки. Наприклад, падіння курсу акцій або обвал процентних доходів на депозити.
Ліквідний ризик	Неможливість швидко отримати готівку або залучити фінансування без значних втрат. Наприклад, неплатоспроможність при масовому виведенні депозитів або відсутність покупців на ринку активів.
Операційний ризик	Втрати від збоїв у внутрішніх процесах, технічних відмов, шахрайства чи помилок персоналу. Наприклад, системний збій під час переказу коштів або шахрайські транзакції співробітників.
Регуляторний (правовий) ризик	Збитки через невиконання законодавства або зміни в регуляціях. Наприклад, штрафи за недотримання норм фінансового контролю або збільшення капітальних вимог від регулятора.
Репутаційний ризик	Втрата довіри клієнтів та інвесторів через негативні публікації чи скандали. Наприклад, публічний скандал із засиланням конфіденційних даних клієнтів.
Кіберризик	Можливі втрати від кібератак (DDoS, віруси, злом систем) і витоку інформації. Наприклад, зловмисне проникнення у банківську систему або атаку на платіжний шлюз, що зупиняє транзакції.

Джерело: систематизовано автором [18]

Зовнішні ризики охоплюють дії недобросовісних контрагентів (у т.ч. ворожих інвесторів, що набувають контроль над компанією через боргові інструменти або акції), інституційні прогалини у регулюванні фінансових ринків, слабкий захист прав інвесторів, валютно-фінансові коливання, макроекономічну нестабільність, недосконаліть фінансово-правового середовища та політично-економічні дисфункції. Такі виклики значно знижують здатність бізнесу ефективно реагувати на зовнішні впливи.

Суттєвими джерелами ризику також можуть бути:

- поведінкові чинники – дії або бездіяльність співробітників, менеджменту, державних інституцій, конкурентів, а також рішення міжнародних організацій;

- об'єктивні обставини – непередбачувані зовнішні події, науково-технологічні зрушення, коливання на фінансових ринках, форс-мажори;
- внутрішні вразливості – неефективне планування, хибні стратегічні орієнтири, слабкий кадровий потенціал, відсутність адаптивної цінової політики;
- зовнішні ринкові загрози – маніпуляції на фондовому ринку, недобросовісна конкуренція, цінові війни тощо;
- кризи непереборної сили – стихійні лиха, соціальні заворушення, військові конфлікти.

У контексті фінансової безпеки ризик трактується як ймовірність настання подій з невизначеними наслідками, які можуть позитивно або негативно позначитись на фінансово-господарській діяльності суб’єкта. Фактор ризику – це першопричина, що створює потенціал для загрозливої ситуації. Небезпека відображає можливість негативного впливу на фінансовий стан підприємства, а загроза – найбільш конкретизована форма цієї небезпеки, здатна реалізуватись у збитки або втрати.

Таким чином, ланцюг розвитку деструктивних подій виглядає як: фактор ризику → ризик → небезпека → загроза → наслідки**.**

У таблиці нижче (Табл. 1.3) відображено поступове ускладнення впливу:

Таблиця 1.3 - Співставлення ризику, загрози, небезпеки

Явище	**Компонент**	**Рівень впливу**
Виклик	Ризик (±)	Потенційна небезпека
Небезпека	–	Ймовірна шкода
Загроза	+	Реальний негативний вплив

Забезпечення фінансової безпеки підприємства передбачає впровадження системного комплексу заходів, спрямованих на збереження високої платоспроможності, оптимізацію структури оборотних коштів і капіталу, підвищення рентабельності та зростання вартості бізнесу. Досягнення цієї мети неможливе без стратегічного і оперативного управління фінансовими, матеріальними, інтелектуальними та кадровими ресурсами.

Інструментарій фінансово-економічної безпеки є складовою загальної економічної безпеки підприємства і включає методи і засоби оцінки ризиків,

системи раннього попередження, регулювання грошових потоків, диверсифікацію джерел фінансування, управління резервами тощо. Їх застосування має бути інтегрованим, своєчасним і взаємопов’язаним.

Серед найбільш значущих викликів можна назвати:

- хронічний дефіцит як внутрішніх, так і зовнішніх інвестицій;
- нестабільність фінансового законодавства;
- обмежена функціональність фондового ринку;
- високий рівень інфляції та зовнішнього боргу;
- тінізація економічної активності;
- слабкий розвиток фінансових інструментів;
- відплив капіталу за кордон.

Водночас внутрішні вразливості бізнесу посилюють зовнішні загрози. До них належать: неякісний менеджмент, слабкий маркетинг, відсутність стратегічного бачення, недостатня ліквідність, проблемна структура капіталу, дефіцит самофінансування, висока плинність персоналу та нестача кваліфікованих кадрів.

У сучасних умовах глобальних трансформацій значний дестабілізаційний вплив справляє пандемія COVID-19, яка стала каталізатором як реальних, так і потенційних фінансових загроз для бізнесу. Це ще раз підкреслює необхідність посиленої уваги до побудови ефективної системи фінансової безпеки, як базового елемента загальної стабільності компанії.

В міжнародній практиці банківського регулювання застосовуються усталені категоризації ризиків. Зокрема, Базельський комітет з Банківського нагляду (BCBS) у рамках стандартів «Базель II/III» визначив основні види ризиків банків: кредитний, ринковий та операційний, для яких встановлюються нормативи капіталу.[19] Ці три види включено до «Першого стовпа» регуляцій (мінімальні вимоги до капіталу). Водночас «Другий стовп» передбачає оцінювання і додаткових ризиків (наприклад, процентного ризику в банківському портфелі IRRBB). Європейський центральний банк підтверджує, що у першому стовпі регулювання фінансовим установам потрібно розглядати кредитні, ринкові та

операційні ризики. Американські регулятори подають більш деталізований список. Наприклад, Офіс контролера валют (OCC) виділяє дев’ять категорій ризиків у банківській діяльності: кредитний, процентний, ліквідності, ціновий, валютний, транзакційний (операційний), комплаєнс, стратегічний та репутаційний. Аналогічно, у регуляторних звітах ФРС та FDIC останніх років банки оцінюють ринкові, кредитні, операційні, а також нові сфери (наприклад, криптоактиви чи кліматичні фінанси). Таким чином, практично всі провідні фінансові системи узгоджуються щодо основних категорій ризиків, а регулюючі органи розробляють методики їх вимірювання і управління. Наприклад, Basel II/III разом із фінансовими регуляторами Великої Британії та США підкреслює необхідність врахування операційних ризиків, включно з категоріями внутрішнього й зовнішнього шахрайства. Історичні приклади (як-от спроба викрадення коштів із банківської системи) і недавні оцінки експертів (наприклад, попередження МВФ та FSB про потенційні наслідки кібератак) також демонструють, що міжнародна практика активно реагує на нові види загроз і регулярно уточнює класифікацію ризиків відповідно до глобальних тенденцій.

1.3 Механізми та технології забезпечення безпеки у фінансовому секторі

Сфера фінансового бізнесу є однією з найбільш уразливих до сучасних загроз як економічного, так і технологічного характеру. Постійні зміни в регуляторному середовищі, зростання обсягів електронних транзакцій, розвиток кіберзлочинності та глобалізація фінансових ринків формують необхідність створення ефективних механізмів забезпечення безпеки. У цьому контексті важливого значення набуває впровадження не лише нормативно-правових і організаційних засобів захисту, а й сучасних цифрових технологій.

Цифрова трансформація інфраструктури фінансової системи стала визначальним чинником підвищення її безпеки, ефективності та доступності. В умовах цифровізації саме інноваційні технології — включно з електронними

платіжними інструментами, блокчейн-платформами, інтелектуальними алгоритмами, обробкою великих обсягів даних і хмарними сервісами — формують сучасну архітектуру фінансової інфраструктури. Їхнє інтегрування сприяє не лише зручності користування послугами, а й суттєво посилює захищеність транзакцій, зменшує ймовірність шахрайства та підвищує прозорість фінансових потоків.

Зростання популярності цифрових каналів обслуговування, зокрема мобільного банкінгу, електронних гаманців і безконтактних розрахунків, сприяє витісненню готівкових операцій, що є важливим кроком до побудови більш контрольованого та безпечного фінансового середовища. Технологія розподіленого реєстру (блокчейн) забезпечує високий рівень достовірності та цілісності даних, а також унеможливлює їх фальсифікацію, що критично важливо для захисту від фінансових зловживань. Штучний інтелект та аналітика великих даних застосовуються для виявлення аномалій у поведінці користувачів, управління ризиками та оперативного реагування на потенційні загрози. Завдяки хмарним обчисленням фінансові установи можуть масштабувати цифрові сервіси з урахуванням зростання запитів, зберігаючи стабільність, продуктивність та високий рівень кіберзахисту.

Окрему увагу приділено регуляторному аспекту**,** який є фундаментом для формування безпечного цифрового середовища. Національні й міжнародні ініціативи спрямовані на забезпечення дотримання стандартів інформаційної безпеки, захисту конфіденційних даних клієнтів, протидії кіберзлочинності та впровадження принципів належного управління у сфері фінансових технологій. Це дозволяє створити гнучку й адаптивну модель фінансового бізнесу, здатну протистояти новітнім загрозам і підтримувати довіру користувачів.[20]

Міжнародна фінансова взаємодія є ключовим чинником стабільності глобальної фінансової екосистеми. Співпраця між державами включає узгодження політик у сферах монетарного регулювання, боротьби з фінансуванням тероризму, запобігання відмиванню коштів, а також координацію підходів до оподаткування та контролю капіталів. Особливе значення мають зусилля міжнародних фінансових організацій — таких як МВФ, Світовий банк, Банк міжнародних розрахунків та

інші регіональні інституції — у розробці спільних підходів до управління ризиками та забезпечення фінансової стабільності.[21]

У добу цифрових трансформацій міжнародне співробітництво все частіше охоплює питання стандартизації цифрових платіжних систем, підвищення кіберстійкості фінансових установ та просування фінтех-інновацій. Інтеграція фінансових ринків відкриває нові можливості для мобільності капіталу, але водночас вимагає консолідованих зусиль у сфері кібербезпеки, обміну інформацією про кіберзагрози та реагування на інциденти. Отже, міжнародна взаємодія є важливою передумовою формування безпечного та стійкого фінансового бізнесу в умовах глобалізованої цифрової економіки.[22]

Однією з ключових передумов сталого функціонування фінансових установ є створення ефективної внутрішньої системи управління ризиками. Це включає:

- Комплаєнс-контроль (compliance control) — діяльність, спрямована на дотримання фінансовими установами вимог законодавства, регуляторних актів та внутрішніх політик. Наявність ефективного комплаєнсу дозволяє не лише запобігати порушенням, а й знижує ризики юридичних та фінансових санкцій.
- Система управління ризиками (ERM — Enterprise Risk Management) — комплексна система ідентифікації, оцінки, моніторингу та мінімізації ризиків, зокрема фінансових, кредитних, ринкових, операційних та юридичних. Такий підхід дозволяє прогнозувати негативні події та вчасно реагувати на загрози.
- Антифрод-політики (anti-fraud policies) — впровадження внутрішніх процедур, спрямованих на виявлення та попередження шахрайських дій, що можуть бути здійснені як працівниками, так і клієнтами фінансової установи.
- Застосування міжнародних стандартів інформаційної безпеки (ISO/IEC 27001, COBIT, NIST тощо), які регламентують вимоги до захисту даних, резервного копіювання, забезпечення безпечного обміну інформацією та стійкості до зовнішніх кіберзагроз.

Технологічний прогрес дозволяє фінансовим установам суттєво підвищити рівень безпеки за рахунок впровадження низки сучасних рішень.[23] До таких технологій відносяться:

- Багатофакторна автентифікація (Multi-Factor Authentication, MFA) — механізм перевірки користувача на основі кількох чинників: пароль, біометричні дані, SMS-підтвердження тощо. Це значно ускладнює можливість несанкціонованого доступу до рахунків клієнтів.
- Технології шифрування (encryption) — використовуються для захисту конфіденційної інформації при її зберіганні та передачі, особливо в інтернет-банкінгу та мобільних додатках.
- Захист периметра IT-інфраструктури — включає використання міжмережевих екранів (firewalls), систем виявлення та запобігання вторгненням (IDS/IPS), засобів моніторингу трафіку.
- Системи виявлення шахрайства на основі штучного інтелекту (AI-powered fraud detection) — програмні комплекси, що аналізують поведінкові патерни користувачів і автоматично виявляють підозрілі транзакції в режимі реального часу.
- Використання блокчейн-технологій — особливо ефективні у сферах трансакційної безпеки, управління smart-контрактами та ідентифікації клієнтів (KYC – Know Your Customer). Блокчейн дозволяє гарантувати незмінність даних та підвищити прозорість фінансових операцій.

З метою ефективного забезпечення безпеки фінансового бізнесу в умовах цифрової трансформації економіки та зростаючих глобалізаційних викликів доцільним є виокремлення ключових пріоритетів, що визначають напрями формування стійкої фінансової архітектури:

1. Стабільність фінансової інфраструктури. Йдеться про забезпечення надійності функціонування банківських установ та небанківських фінансових організацій, зміцнення запобіжних механізмів проти фінансових дестабілізуючих процесів, зокрема кризового характеру, а також гармонізацію нормативного

середовища із загальноприйнятими міжнародними стандартами фінансового нагляду.

2. Технологічна модернізація та цифрова безпека. Упровадження інноваційних рішень – від блокчейн-платформ до цифрових активів – відіграє провідну роль у підвищенні прозорості й оперативності фінансових операцій. У той же час зростає потреба в системному кіберзахисті, здатному протистояти хакерським атакам, фінансовому шахрайству та іншим кіберзагрозам, що можуть вплинути як на окремі компанії, так і на макрофінансову стабільність.

3. Регуляторний супровід та інституційний контроль**.** Ефективна система державного та міжнародного фінансового нагляду має адаптуватися до специфіки цифрових трансакцій і віртуальних активів. Прозорі регуляторні механізми сприяють зниженню ризиків неконтрольованого обігу капіталу у віртуальному середовищі.

4. Розширення доступу до фінансових послуг. Забезпечення інклюзивності в цифровому фінансовому секторі передбачає створення умов для залучення широких верств населення та бізнесу до інноваційних фінансових інструментів, зокрема онлайн-кредитування, цифрових інвестиційних платформ та мобільних банківських сервісів.

5. Управління валютними ризиками в умовах глобалізації. Для зміцнення фінансової незалежності важливим є формування політик, спрямованих на зменшення вразливості до коливань іноземних валют, диверсифікацію валютних активів і оптимізацію зовнішньоекономічних фінансових зв’язків.

6. Реагування на системні ризики та кризові виклики. Протидія потенційним загрозам глобального масштабу вимагає застосування цифрових інструментів моніторингу та прогнозування криз, підтримки національних фінансових інститутів, а також боротьби з фінансовими махінаціями через посилення прозорості та цифрової звітності.

7. Інформаційна безпека фінансових операцій. Ключовим завданням стає захист даних клієнтів і транзакцій від витоку чи підробки, з використанням передових рішень у сфері штучного інтелекту, машинного навчання та аналітики

великих даних для виявлення аномалій та запобігання шахрайству в реальному часі.

У підсумку, формування надійної системи безпеки фінансового бізнесу в цифрову епоху неможливе без міждисциплінарного підходу, що охоплює технологічну інноваційність, ефективне регуляторне середовище та стратегічне управління ризиками на національному та транснаціональному рівнях.

Світова практика демонструє успішні приклади комплексного впровадження механізмів фінансової безпеки: Банк HSBC (Велика Британія) активно використовує біометричну ідентифікацію клієнтів (відбитки пальців, голосова біометрія) для підвищення захищеності мобільного банкінгу. JP Morgan Chase (США) впровадив аналітичну платформу на базі AI для моніторингу платежів і виявлення аномалій, що дозволяє виявляти шахрайство ще до завершення транзакцій. Європейський центральний банк у межах Директиви PSD2 зобов’язав банки впроваджувати strong customer authentication (SCA) — систему жорсткої автентифікації клієнтів, що стала каталізатором розвитку інновацій у сфері цифрової безпеки фінансових послуг.

Таким чином, ефективне забезпечення безпеки у фінансовому секторі потребує комплексного підходу, що поєднує правові, організаційні та технологічні інструменти. Впровадження передових механізмів захисту дозволяє не лише запобігати втратам, але й зміцнює довіру клієнтів, сприяє дотриманню регуляторних вимог та забезпечує стабільний розвиток фінансової системи в умовах цифровізації та глобальних викликів.

РОЗДІЛ 2
АНАЛІЗ СУЧАСНОГО СТАНУ ТА ІНСТРУМЕНТІВ БЕЗПЕКИ ФІНАНСОВОГО БІЗНЕСУ В УКРАЇНІ

2.1 Інноваційні фінансові технології в системі безпеки банківського бізнесу

У глобальному масштабі банківська система виступає ключовим драйвером у впровадженні сучасних цифрових рішень, що трансформують підходи до фінансової безпеки та операційної ефективності. Інновації у фінансовій сфері не лише покращують інфраструктуру ринку, а й сприяють підвищенню якості обслуговування, оптимізації витрат і розширенню спектра доступних послуг. Особливо важливо те, що цифровізація процесів знижує ймовірність помилок і зловживань, зміцнюючи таким чином кіберстійкість банківських установ. Світова практика свідчить, що фінансовий сектор залишається одним з найбільш динамічних у сфері впровадження цифрових інновацій, що мають безпосередній вплив на загальну безпеку фінансового середовища.

Фінансові технології виступають не лише елементом інноваційної екосистеми кожної держави, але й стають фундаментальним інструментом трансформації національних фінансових систем. Попри широку зацікавленість науковців і практиків, універсального трактування поняття «фінтех» поки не існує. Зазвичай його розглядають як сукупність цифрових рішень і сервісів, що впроваджуються у фінансову діяльність для підвищення її ефективності, адаптивності, оперативності й безпеки.

FinTech охоплює як інноваційні платформи для здійснення фінансових операцій, так і компанії чи стартапи, що спеціалізуються на розробці цифрових продуктів, орієнтованих на забезпечення безпечної та зручної взаємодії між учасниками ринку. Зокрема, інструменти, розроблені в межах фінтех-сфери,

дозволяють мінімізувати ризики шахрайства, забезпечують шифрування даних, багаторівневу автентифікацію користувачів і безперервний моніторинг транзакцій.

У цьому контексті фінансові технології стають потужним засобом підвищення стійкості банків до зовнішніх і внутрішніх загроз, зокрема кіберзлочинності. Визначення Ради з фінансової стабільності підкреслює, що FinTech — це технологічна інновація у сфері фінансових послуг, яка створює нові бізнес-моделі, сервіси, процеси або продукти з істотним впливом на функціонування ринку. З огляду на це, фінансові технології не тільки покращують обслуговування клієнтів, але й модернізують системи захисту даних та управління ризиками.

У сучасній науковій і практичній площині FinTech дедалі частіше розглядається як окремий сегмент фінансового ринку, який формує нову архітектуру фінансової безпеки завдяки застосуванню технологічних інновацій. Його розвиток є критично важливим для зміцнення довіри до фінансових інституцій, запобігання фінансовим злочинам і формування стійких механізмів реагування на загрози в цифровому середовищі.

Більшість експертів та науковців схильні розглядати фінансові технології як спеціалізовану галузь, що спрямована на впровадження інноваційних рішень з метою підвищення ефективності та безпеки фінансової діяльності. Згідно з визначенням Ради з фінансової стабільності, FinTech – це технологічне нововведення у сфері фінансових послуг, яке спричиняє появу нових бізнес-моделей, цифрових рішень, сервісів або процесів, здатних істотно змінити спосіб надання фінансових продуктів і послуг.

У такому контексті фінансові технології виступають не лише рушієм модернізації, а й критично важливим чинником трансформації системи безпеки у фінансовому секторі. У сучасній науковій літературі FinTech часто трактується як окремий сегмент фінансового ринку, що активно впливає на традиційний банкінг, стимулюючи його адаптацію до нових викликів і загроз, зокрема у сфері кіберзахисту, управління ризиками та ідентифікації клієнтів.

Інтеграція фінансових технологій у банківське середовище за останні десятиліття зумовила суттєві структурні зміни, породивши низку інноваційних напрямів діяльності. Класифікуємо ключові напрямки фінансових інновацій, які стали можливими завдяки впровадженню FinTech-рішень. Виокремлено чотири основні продуктові категорії, кожна з яких охоплює специфічні сервіси, що вимагають належного рівня безпеки при наданні:

- Фінансування (краудфандинг, кредитування, факторинг, благодійні фінансові платформи, краудінвестинг, відсоткове кредитування від приватних осіб) – ці інструменти потребують комплексних систем захисту даних та моніторингу фінансових потоків;
- Управління активами (робоадвайзери, соціальний трейдинг, індивідуальні фінансові менеджери, інвестування) – викликають потребу в підвищеній інформаційній безпеці та контролі алгоритмів прийняття рішень;
- Платежі (альтернативні платіжні інструменти, криптовалюти, блокчейн-платформи) – вимагають впровадження найсучасніших механізмів кіберзахисту та протидії шахрайству;
- Інші FinTech-напрямки (цифрове страхування, агрегатори та порівняльні сервіси, IT-інфраструктура для фінансових установ) – потребують комплексного аудиту ризиків і захисту критичної інфраструктури.

Зазначені напрямки свідчать про глибоке впровадження технологічних інновацій у класичні банківські продукти. Вони не лише розширюють можливості для клієнтів, а й висувають нові вимоги до фінансової безпеки, змушуючи фінансові інституції адаптувати свої підходи до захисту даних, ідентифікації ризиків та протидії фінансовим злочинам.

Як зазначають Процак К. В. та Коваленко Т. О., сучасна банківська система дедалі активніше інтегрує цифрові технології, що трансформують традиційні послуги у нові формати з вищим рівнем автоматизації, зручності та, водночас, підвищеними вимогами до кібербезпеки.[24]

Штучний інтелект (ШІ) дедалі активніше впроваджується у фінансову галузь як інструмент підвищення операційної ефективності, аналітики ризиків та забезпечення кібербезпеки. Його застосування дозволяє фінансовим установам не лише оптимізувати клієнтський сервіс, але й сформувати багаторівневу систему захисту від шахрайства, технічних збоїв та кіберзагроз. У цьому контексті варто виокремити кілька ключових напрямів, у яких ШІ відіграє провідну роль.

ШІ-системи забезпечують автоматичну обробку фінансових транзакцій, істотно знижуючи ризики людських помилок, прискорюючи внутрішні процеси та мінімізуючи втрати у разі технічних збоїв. Такі інструменти дають змогу не лише зекономити ресурси, а й гарантувати безперебійне функціонування ключових сервісів, що критично важливо для забезпечення стабільності банківських операцій.

Завдяки алгоритмам машинного навчання банки можуть виявляти аномальні фінансові дії — наприклад, незвичні суми переказів, транзакції до країн із високими ризиками, або дії користувачів, нехарактерні для їхньої звичайної поведінки. Також впроваджуються модулі для моніторингу дій працівників банку з метою виявлення внутрішніх загроз, таких як несанкціоновані входи в систему чи підозрілі запити у неробочий час.

ШІ значно підвищує ефективність процедур ідентифікації клієнтів (KYC) та протидії легалізації доходів (AML), автоматизуючи обробку великого масиву документів, перевірку достовірності даних, а також звірку з базами неблагонадійних осіб. Завдяки технологіям обробки природної мови (NLP), ШІ-системи можуть аналізувати текстову інформацію з документів, витягувати ключові дані та передавати їх для верифікації. Це сприяє зниженню витрат і пришвидшенню процесу onboarding без шкоди для безпеки.

Захист чутливої інформації клієнтів є одним із пріоритетів сучасного фінансового бізнесу. Для забезпечення конфіденційності та попередження витоків даних використовуються ШІ-модулі з функціями кібермоніторингу, виявлення загроз та проактивного реагування. Такі системи здатні виявляти складні атаки,

включно з фішингом і спробами вторгнення, задовго до того, як вони спричинять шкоду.

Використання віртуальних асистентів та чат-ботів на базі ШІ дозволяє банкам швидко реагувати на запити клієнтів, не відкриваючи доступу до критичних систем або чутливої інформації. Наприклад, АТ «Банк Альянс» впровадив ШІ для прискорення обробки заявок на кредит, що дозволяє ухвалювати рішення впродовж секунд без втрати контролю над ризиками. Також цифрові інструменти на основі ШІ підтримують дистанційну верифікацію документів, що особливо актуально для фінансових установ у періоди кібернестабільності.

У державних банках, таких як «ПриватБанк» і «Ощадбанк», використовуються передові рішення на базі штучного інтелекту для аналізу клієнтського профілю, життєвого циклу клієнта та транзакційної історії. Наприклад, система SIA Deloitte Latvia, впроваджена в «ПриватБанку», дозволяє точно прогнозувати фінансові потреби клієнтів та пропонувати безпечні, адаптовані кредитні продукти. При цьому пріоритет надається захисту персональних даних і мінімізації ризиків неправомірного доступу.[25]

Одним із сучасних рішень, що активно впроваджуються у фінансовій сфері для посилення клієнтського сервісу та безпеки, є чат-боти на базі штучного інтелекту. Ці цифрові помічники дозволяють установам забезпечувати цілодобову підтримку користувачів, оперативно обробляти запити й надавати вичерпні, релевантні відповіді в автоматизованому режимі. Окрім того, завдяки можливості персоналізації комунікації, такі системи не лише покращують клієнтський досвід, а й сприяють підвищенню довіри до бренду, що є критичним аспектом у забезпеченні кіберстійкості фінансового бізнесу.

Ключову роль у цьому відіграє машинне навчання — напрям штучного інтелекту, який дозволяє алгоритмам самостійно вдосконалюватися на основі історичних даних і приймати рішення з високою точністю. На відміну від традиційних програмних підходів, ML-алгоритми здатні виявляти приховані закономірності у великих обсягах фінансової інформації. Це відкриває широкі можливості для підвищення інформаційної безпеки: зокрема, технології

використовуються для виявлення нетипової поведінки користувачів, оцінки рівня кредитного ризику, аналізу транзакцій на предмет підозрілих операцій і виявлення потенційних схем шахрайства.

Інтеграція таких рішень також сприяє автоматизації рутинних процесів, дозволяючи співробітникам зосередитися на стратегічних завданнях, що потребують аналітичного мислення. Це позитивно впливає як на ефективність операційної діяльності, так і на рівень внутрішньої задоволеності персоналу.

Яскравим прикладом впровадження таких технологій є кейс Monobank, де створено спеціалізований ШІ-сервіс для аналізу ризиків, пов’язаних із діяльністю фінансових компаній. У рамках цього підходу використовуються:

– методи бустингу для точного прогнозування кредитних ризиків;
– квантільна регресія для оцінки фінансової спроможності клієнтів;
– графові моделі для виявлення зв’язків між суб’єктами, що можуть свідчити про шахрайські дії.

У Monobank застосовується близько 20 моделей машинного навчання, які опрацьовують понад 2000 параметрів — від швидкості заповнення заявки до технічних характеристик пристрою користувача (IP-адреса, тип телефона тощо). Ці інструменти не лише підвищують точність прийняття рішень, а й дозволяють ефективно управляти ризиками, зменшуючи ймовірність зловживань у фінансовому середовищі.[26]

У сучасних умовах цифровізації фінансовий бізнес усе активніше інтегрує технологію блокчейн як надійний засіб забезпечення цілісності та прозорості фінансових операцій. Завдяки децентралізованому принципу збереження даних, блокчейн формує захищені від несанкціонованого втручання реєстри транзакцій, автентичність яких підтверджується криптографічними механізмами. Це дає змогу фінансовим установам мінімізувати ризики фальсифікації, пришвидшити обробку транзакцій і зменшити витрати шляхом автоматизації процедур за допомогою смарт-контрактів.

Використання блокчейн-рішень створює низку переваг для суб’єктів фінансового ринку, серед яких:

- посилення довіри між контрагентами завдяки доступу до єдиної, незмінної інформації;
- усунення розрізненості даних через використання розподіленого реєстру, доступ до якого мають лише уповноважені сторони;
- підвищення рівня інформаційної безпеки без залучення зовнішніх посередників;
- створення прозорих, хронологічно захищених записів, що фіксують усі дії в системі;
- впровадження надійних цифрових платформ, таких як Oracle Blockchain, які забезпечують безпечне з'єднання смарт-контрактів із зовнішніми джерелами даних.

Блокчейн-оракули відіграють критичну роль у трансформації фінансових сервісів, особливо в децентралізованих сферах (DeFi, GameFi, страхування, NFT). Вони функціонують як міст між блокчейн-мережами та зовнішнім середовищем, надаючи актуальну інформацію для виконання умов контрактів. Найвідомішим провайдером цієї інфраструктури є Chainlink, хоча також активно працюють такі гравці, як Band Protocol**,** Berry Data**,** Kylin Protocol і DIA**.**

Технології Big Data дедалі більше використовуються для моніторингу операційної діяльності, виявлення аномалій та підвищення ефективності управління ризиками. Банки й фінансові компанії аналізують великі обсяги даних для формування точніших прогнозів поведінки клієнтів, ідентифікації підозрілих активностей і виявлення потенційних загроз у реальному часі. Це дозволяє оперативно реагувати на кіберзагрози, формувати персоналізовані стратегії взаємодії з клієнтами та приймати обґрунтовані управлінські рішення в умовах високої динаміки ринку.

У сучасному фінансовому бізнесі технології аналізу великих масивів даних (Big Data) відіграють важливу роль у забезпеченні надійності операцій і протидії загрозам. Зокрема, такі інструменти застосовуються для оцінки ризиків клієнтів (скоринг), виявлення шахрайських дій, а також для глибокого аналізу цільової аудиторії.

За допомогою інструментів скорингового аналізу на основі Big Data фінансові установи мають змогу формувати точні профілі клієнтів, включно з тими, хто не має кредитної історії. Такий підхід дозволяє визначити їхню фінансову надійність та передбачити можливі загрози, пов’язані з несумлінною поведінкою або шахрайськими намірами. Один із критичних аспектів – впровадження антифрод-скорингу, що дає змогу оперативно виявляти потенційно небезпечних користувачів і запобігати фінансовим зловживанням.

До переваг впровадження скорингових моделей на базі Big Data у фінансовому секторі належать:

– побудова адаптивних моделей оцінки клієнтів із використанням актуальних даних у режимі реального часу;

– висока швидкість обробки інформації для прийняття рішень;

– можливість оцінювання фінансового ризику клієнтів без історії взаємодії з банківською системою;

– розширення кредитного і фінансового скорингу;

– посилення систем протидії шахрайству шляхом автоматизованого фільтрування підозрілих операцій.

Ще один важливий аспект використання Big Data – це поглиблений аналіз цільових сегментів користувачів. Такий підхід дозволяє фінансовим установам створювати релевантні пропозиції та вдосконалювати маркетингові кампанії. Наприклад, за допомогою профілювання клієнтів можна сформувати докладний соціально-демографічний портрет користувача, визначити його фінансові інтереси, поведінкові патерни та уподобання. А технологія пошуку Look-alike аудиторій забезпечує залучення нових споживачів зі схожими характеристиками, підвищуючи ефективність рекламних дій.

Серед інших інструментів, що підтримують фінансову безпеку й операційну ефективність, варто виділити теплові карти, геоаналітику та інтелектуальну сегментацію розсилок. Вони дозволяють виявляти найбільш перспективні локації для розміщення інфраструктурних об'єктів – відділень, банкоматів чи платіжних терміналів – з урахуванням концентрації представників цільової аудиторії.

Таргетована розсилка, у свою чергу, сприяє точковому інформуванню клієнтів про актуальні фінансові продукти, спеціальні умови або зміни в обслуговуванні, виходячи з інтересів, вікових, географічних чи поведінкових характеристик користувачів.[27]

У сучасних умовах цифрової трансформації фінансовий бізнес стикається з необхідністю постійного вдосконалення засобів інформаційного захисту, підвищення технологічної гнучкості та оперативного впровадження нових продуктів. У цьому контексті все більшого поширення набуває використання хмарних технологій (cloud computing), які дозволяють не лише зменшити витрати на фізичну інфраструктуру, але й значно підвищити рівень безпеки та надійності інформаційних систем.

Застосування хмарних сервісів у фінансових установах забезпечує ефективну заміну традиційним локальним IT-інфраструктурам, які вимагають значних витрат на технічне обслуговування, оновлення програмного забезпечення та підтримку персоналу. Завдяки хмарним рішенням зберігання, обробка і передача конфіденційних клієнтських даних здійснюються в захищеному середовищі з високим рівнем резервування та автоматичної діагностики. Це дає змогу знизити операційні ризики, пов’язані з людським фактором, технічними збоями та кібератаками.

Світовий досвід демонструє стрімке зростання впровадження хмарних технологій у фінансовому секторі. Зокрема, близько 95% банківських установ у США та Європі активно використовують хмарні сервіси, а рівень інвестицій у цю сферу щороку зростає. Великі гравці ринку, серед яких PayPal і Capital One, вже перейшли на хмарну інфраструктуру, що дозволяє їм залишатися технологічно гнучкими та ефективними в умовах посиленої конкуренції з боку фінтех-стартапів. Для традиційних банків це стало сигналом необхідності перегляду підходів до забезпечення інформаційної безпеки та цифрової модернізації.

Хмарні сервіси значно полегшують масштабування проєктів і створення нових цифрових продуктів. Такі рішення дозволяють фінансовим організаціям скоротити кількість фізичних дата-центрів, оптимізувати управління даними та

впроваджувати інноваційні сервіси без суттєвого зростання витрат. Наприклад, банк Capital One скоротив кількість своїх дата-центрів з восьми до трьох, завдяки переходу на хмарну інфраструктуру, що позитивно позначилося як на вартості обслуговування, так і на рівні безпеки.

Однією з ключових переваг хмарних технологій є їхня здатність до підвищення рівня кіберстійкості. Розподілена архітектура хмарних систем забезпечує рівномірне навантаження на сервери, що сприяє безперервному функціонуванню інформаційних систем навіть у разі нештатних ситуацій. Крім того, можливість незалежного оновлення окремих модулів систем без втручання в інші компоненти інфраструктури знижує ймовірність поширення потенційних уразливостей. Застосування мультихмарних підходів також дозволяє запроваджувати додаткові рівні захисту та резервування.

На відміну від фізичних серверів, хмарні платформи не потребують значних витрат на підтримку працездатності, регулярне оновлення обладнання та розширення персоналу. Це дозволяє фінансовим компаніям зосередитися на розвитку продуктів і підвищенні якості клієнтського обслуговування. Крім того, хмарні сервіси забезпечують постійний доступ до актуального програмного забезпечення та сучасних інструментів аналітики, що зміцнює позиції компаній на ринку та знижує технологічну заборгованість.[28]

Таким чином, впровадження хмарних технологій у фінансовому секторі є не лише технологічним трендом, а й стратегічно важливим чинником підвищення кібербезпеки, гнучкості бізнес-процесів і конкурентоспроможності фінансових установ в умовах цифрової економіки.

З початком воєнної агресії проти України вітчизняні банки були змушені оперативно переорієнтуватися на використання хмарних технологій як інструмент забезпечення збереження критично важливої інформації та підтримки безперервності операційної діяльності. У відповідь на нові виклики Національний банк України розробив нормативну базу, яка регламентує використання хмарних сервісів у фінансовому секторі. Такий підхід дав змогу підтримати стійкість банківської системи в умовах надзвичайного стану.

Зокрема, відповідно до Постанови Правління НБУ № 42 від 08 березня 2022 року [29], яка набула чинності наступного дня, банкам дозволено:

- використовувати хмарні інфраструктури для обслуговування платіжних операцій, у тому числі з електронними платіжними засобами (зокрема картками), за умови розміщення серверного обладнання в юрисдикціях із високими стандартами інформаційної безпеки — таких як Європейський Союз, Велика Британія, США та Канада. Ця норма діє на період воєнного стану та ще два роки після його завершення;
- обробляти персональні дані клієнтів і здійснювати фінансові транзакції через хмарні сервіси із застосуванням як українських засобів криптографічного захисту, так і іноземних, за умови відповідності їх законодавчим вимогам країни, де фізично розміщена обчислювальна інфраструктура.

В умовах цифровізації фінансового бізнесу значну роль у підвищенні безпеки та ефективності виконання операцій відіграють смарт-контракти — програмні протоколи, що автоматично виконують умови фінансових угод у децентралізованому середовищі. Їх впровадження у банківському секторі дозволяє мінімізувати ризики людського фактору, оптимізувати витрати та забезпечити прозорість взаємодії між сторонами.

Фінансові установи активно застосовують розумні контракти у сферах кредитування, страхування та цифрових платежів. Ключовою перевагою є автоматичне виконання закодованих умов без посередників. Попри те, що смарт-контракти наразі не мають повноцінної юридичної сили, зміна їхнього змісту потребує колективного погодження нод у мережі, що унеможливлює непомітні маніпуляції.

Кожна транзакція, ініційована смарт-контрактом, фіксується в блокчейні, надаючи сторонам постійний доступ до актуального стану виконання угоди. Крім того, вбудовані механізми перевірки нод запобігають реалізації небезпечних або шахрайських сценаріїв.

До основних функцій смарт-контрактів, що мають особливе значення для фінансової безпеки, належать:

- автоматизація договірних відносин між клієнтами та установами;
- забезпечення багаторівневої авторизації платежів (наприклад, транзакція активується лише після підтвердження всіма сторонами);
- надійне збереження критично важливих даних в умовах децентралізованого середовища.

Таким чином, поєднання хмарних технологій із можливостями смарт-контрактів відкриває новий рівень захисту та адаптивності фінансового бізнесу в умовах воєнних і поствоєнних ризиків.

У сучасних умовах цифровізації фінансових послуг біометричні методи ідентифікації відіграють ключову роль у зміцненні кібербезпеки та протидії шахрайству. Банківські установи активно інтегрують біометричні рішення, зокрема розпізнавання обличчя, сканування відбитків пальців, а також інші фізіологічні параметри для підвищення точності ідентифікації клієнтів у процесі авторизації в системах інтернет-банкінгу та під час здійснення фінансових операцій. Такі інструменти мінімізують ризики несанкціонованого доступу та забезпечують стабільну взаємодію клієнтів із фінансовими платформами.

Серед новітніх напрямів особливе місце посідає голосова біометрія, яка ґрунтується на унікальних характеристиках мовлення кожної особи. Завдяки розвитку технологій штучного інтелекту, зокрема нейромережевих алгоритмів, було досягнуто значного прогресу в розробці систем голосової автентифікації, які демонструють високу швидкість і точність ідентифікації. Цей підхід не лише підвищує захист персональних даних і фінансової інформації, а й усуває потребу у традиційних паролях, знижуючи навантаження на користувачів.

За прогнозами аналітиків, глобальний ринок голосової біометрії демонструє стійке зростання: якщо у 2020 році його обсяг становив $1,1 млрд, то до 2026 року очікується збільшення до $3,9 млрд, що відповідає середньорічному темпу зростання 22,8%.[30]

Основні переваги голосової біометрії для фінансових інституцій:

1. Зниження операційних витрат. Впровадження голосової автентифікації в контакт-центрах і банках дозволяє значно скоротити витрати, пов’язані з обробкою запитів, зменшуючи кількість етапів перевірки особи.

2. Покращення клієнтського досвіду. Система дозволяє користувачам проходити авторизацію без введення паролів, PIN-кодів чи відповідей на секретні запитання, що підвищує зручність обслуговування.

3. Високий рівень достовірності. Голосовий відбиток є унікальним, подібно до відбитків пальців, що робить його надійним засобом захисту порівняно з традиційними методами.

4. Простота інтеграції. Голосові біометричні рішення не потребують складного або дорогого обладнання, що полегшує їх впровадження навіть у невеликих фінансових структурах.

Як приклад національної практики, у 2022 році ПриватБанк запровадив голосову авторизацію. До кінця вересня того ж року цією опцією скористались понад мільйон клієнтів, що свідчить про затребуваність технології серед споживачів фінансових послуг.

Технологічний прогрес сприяє формуванню нових інструментів безпеки у фінансовій галузі. У структурі цифрових інновацій особливої уваги заслуговують рішення, що підтримують функціональність ключових банківських напрямів — кредитування, депозитні операції, інвестування, а також системи платежів, клірингу та розрахунків. Окрім цього, виокремлюють окрему групу інноваційних розробок, що орієнтовані на забезпечення ефективності інфраструктури ринку та можуть застосовуватись поза межами фінансового сектору.

Зазначена класифікація відповідає підходам, які підтримує Базельський комітет з банківського нагляду. Вона охоплює три основні сегменти продуктів та комплекс послуг підтримки, які спрямовані на технологічне забезпечення безпеки, сталого розвитку та ефективної адаптації інновацій у фінансовій сфері.

Окрему нішу в сучасному фінансовому середовищі посідають необанки — цифрові банківські установи, які здійснюють обслуговування клієнтів виключно в онлайн-форматі, без розгалуженої мережі фізичних відділень. Їх поява зумовила

суттєві трансформації у структурі фінансового сектору, зокрема в частині підходів до надання послуг, конкурентної динаміки та рівня операційної ефективності. Разом із тим, поширення необанків супроводжується певними ризиками, насамперед у площині кібербезпеки та регуляторної відповідності.[31]

У науковому дискурсі окремі дослідники акцентують увагу на загрозах, які несе стрімкий розвиток цифрових банків. Йдеться не лише про потенційну втрату конкурентоспроможності традиційних фінансових установ, які не встигають адаптуватися до технологічних змін, а й про зростання вразливості до кібератак, фішингових схем і технічних збоїв. У цьому контексті діяльність необанків потребує посиленого контролю з боку регуляторів, а також впровадження сучасних систем захисту даних та безперервного моніторингу ризиків.

Попри зазначені виклики, цифрові фінансові інституції можуть виступати драйверами стійкого розвитку галузі за умови належної інтеграції в національну фінансову екосистему. Необанки здатні підвищити гнучкість і технологічний рівень банківських послуг, сприяючи зростанню фінансової інклюзії та покращенню якості обслуговування клієнтів. Відтак, ключовим завданням є пошук оптимального балансу між забезпеченням безпеки та підтримкою інновацій у межах цифрового фінансового ринку.

У сучасних умовах розвитку фінансового бізнесу особливого значення набувають технологічно вдосконалені методи оцінки кредитних ризиків, зокрема скоринг-системи. Використання математичних і статистичних моделей дозволяє фінансовим установам об’єктивно оцінювати ймовірність виконання боргових зобов’язань з боку потенційних позичальників. Такі моделі ґрунтуються на аналізі великої кількості релевантних даних, включаючи кредитну історію, соціально-демографічні характеристики, поведінкові чинники тощо.

Сучасна скоринг-інфраструктура включає низку спеціалізованих сервісів, що забезпечують збір, обробку та збереження персональних і фінансових даних користувачів. Особливого поширення набули application-скоринг (оцінка ризику на етапі подачі заявки), fraud-скоринг (виявлення шахрайських схем), behavioural-скоринг (аналіз споживчої поведінки) тощо. Застосування таких інструментів

дозволяє суттєво підвищити точність оцінки кредитоспроможності та водночас мінімізувати фінансові втрати, спричинені недобросовісними клієнтами чи фрод-активністю.

З метою забезпечення безпеки скорингових рішень, банки та фінансові компанії впроваджують багаторівневі системи захисту інформації, зокрема шифрування даних, багатофакторну автентифікацію та моніторинг аномальних транзакцій у реальному часі. Таким чином, сучасні технології оцінки кредитних ризиків відіграють ключову роль не лише в підвищенні ефективності фінансового обслуговування, а й у зміцненні загальної безпеки бізнес-процесів.

Одним із найдинамічніших напрямів цифрової трансформації у фінансовому бізнесі є розвиток платіжних технологій, орієнтованих на масового споживача та малого підприємця. Цифрові платіжні сервіси забезпечують можливість здійснення швидких і зручних фінансових операцій через мобільні застосунки, інтернет-банкінг, QR-коди, біометричні технології тощо. Їх впровадження значно підвищує доступність банківських послуг, особливо в умовах зростаючого попиту на дистанційне обслуговування.

Проте, з розширенням функціоналу цифрових сервісів зростає і спектр загроз. Фінансові установи стикаються з викликами, пов’язаними з фішингом, атакою типу «людина посередині» (MITM), компрометацією даних користувача тощо. У зв’язку з цим, забезпечення інформаційної безпеки цифрових платіжних платформ набуває критичного значення.

Серед основних технологічних рішень, що сприяють захисту платіжних даних, варто виділити використання безконтактних NFC-технологій, токенізації, біометричної автентифікації, а також інтеграцію з сертифікованими платіжними шлюзами. Поряд із традиційними банками, активну участь у розвитку цієї інфраструктури беруть фінтех-компанії, такі як Stripe, PayPal, Klarna, Adyen, а також провайдери мобільних платежів (Apple Pay, Google Pay, Alipay) і платіжні системи глобального масштабу (Visa, MasterCard, American Express).[32]

Цифрові платіжні сервіси, що стали важливою складовою частиною національної фінансової інфраструктури, потребують постійного оновлення

стандартів безпеки та законодавчої підтримки. Лише в умовах чітко регламентованого, контрольованого та технологічно захищеного середовища вони здатні ефективно сприяти розвитку фінансового бізнесу в цифрову епоху.

2.3 Технології безпеки в Monobank

Monobank застосовує комплекс сучасних заходів для захисту даних клієнтів та транзакцій. Мобільний додаток є нативним (iOS/Android) і підтримує мультіфакторну автентифікацію: вхід за PIN-кодом і за бажанням – по біометрії (Fingerprint/Touch ID, Face ID). Усі операції з платіжними картками відповідають стандарту PCI-DSS (токенізація та шифрування даних). Онлайн-платежі підтверджуються через розширений 3D-Secure без використання ненадійних SMS. Дані при передачі захищені протоколом TLS 1.2. Для укладення договорів і угод з банком використовується електронний цифровий підпис (EDS). Системи антифроду і «антихакінгу» автоматично відстежують підозрілі операції та аномалії поведінки рахунку, блокуючи шахрайські транзакції.

Протягом 2020–2024 років Monobank системно впроваджував багаторівневі технології кіберзахисту, які відповідають найкращим міжнародним практикам. Особливої уваги було приділено персоналізації систем аутентифікації через біометричні засоби, інтеграції з міжнародним стандартом PCI DSS для безпеки платіжної інфраструктури, а також застосуванню адаптивної антифрод-системи на базі алгоритмів машинного навчання. Ці заходи спрямовані на мінімізацію кіберризиків, особливо в умовах зростання кіберзагроз в період воєнного стану. Удосконалення механізмів 3D Secure та впровадження електронного цифрового підпису стали ключовими факторами забезпечення юридичної сили онлайн-операцій. (Таблиця 2.1)

Таблиця 2.1 - Технології кібербезпеки Monobank

Технологія/Інструмент	Опис	Рік впровадження / активного використання
Мультіфакторна автентифікація	PIN-код + біометрія (Face ID, Touch ID)	До 2020 (удосконалення в 2021–2023)
TLS 1.2	Шифрування трафіку додатку	З 2020
PCI DSS	Захист платіжних карткових даних	Постійна відповідність (щорічна верифікація)
3D Secure (розширений)	Підтвердження карткових платежів без SMS	З 2021
Електронний цифровий підпис (EDS)	Підписання угод без відділення	Активно з 2022
Система антифроду	Автоматичне виявлення шахрайства	Активно з 2020 (удосконалення у 2023)

Джерело: систематизовано автором [33]

Monobank зарекомендував себе як драйвер FinTech-інновацій на українському ринку, запропонувавши низку продуктів, орієнтованих на гнучкість, швидкість та повну діджиталізацію взаємодії з користувачем. Серед ключових впроваджень — сервіси «Купівля частинами» (BNPL), короткострокове мікрокредитування, валютні депозити з онлайн-керуванням, а також соціальні інструменти на кшталт «Дія.Картки». Усі продукти були реалізовані без потреби фізичного відвідування банківського відділення, що стало особливо актуальним в умовах пандемії COVID-19 та війни. Таким чином, Monobank позиціонує себе не як традиційний банк, а як фінансовий супердодаток (superapp).

Таблиця 2.2 - Основні FinTech-продукти Monobank

Продукт	Опис	Рік запуску/оновлення
Віртуальні картки	Картка без фізичного носія, доступна миттєво	До 2020
BNPL (Покупка частинами)	Безвідсоткова розстрочка у партнерських мережах	Активне розширення з 2021
“Кредит до завтра”	Мікрокредитування онлайн (до 100 тис. ₴, без паперів)	2022
Валютні депозити	Доларові/єврові вклади з достроковим розірванням	2023
«Дія.Картка»	Універсальна картка для державних виплат через "Дію"	Грудень 2024

Джерело: систематизовано автором [34]

Банк має депозити у гривні та валюті з конкурентними ставками. У 2023 р. monobank додав нові валютні депозити (6–12 міс.) з можливістю дострокового розірвання договору. Наприклад, ставки за 12-місячними доларовими вкладами з правом дострокового розірвання сягали 2,1% річних. Це допомогло залучити значні обсяги коштів — за даними на початок 2025 року вклади клієнтів monobank сягнули майже 108 млрд грн.

Офіційних вбудованих сервісів купівлі/обміну криптовалют у додатку monobank немає (через регуляторні обмеження). Клієнти можуть користуватись сторонніми обмінниками або P2P-платформами, але це поза офіційним функціоналом банку.

Динаміка клієнтської бази Monobank демонструє стале зростання впродовж досліджуваного періоду — з 3,4 млн у 2020 році до понад 9,2 млн у 2024 році. Такий приріст зумовлений зростаючим попитом на дистанційні фінансові послуги, зручність мобільного додатку та активну інтеграцію банку у цифрову економіку України. Пропорційне зростання кількості емітованих карток свідчить про ефективну стратегію утримання клієнтів та розширення спектра фінансових продуктів. Зокрема, збільшення кількості карток до майже 10 млн до початку 2024 року є свідченням високого рівня довіри до інноваційної бізнес-моделі банку.

Таблиця 2.3 - Кількість клієнтів та карток Monobank

Рік	Кількість клієнтів (млн)	Кількість емітованих карток (млн)
2020	3,4	3,5
2021	4,9	5,0
2022	6,75	7,0
2023	8,0	9,77
2024	9,2	10,0

Джерело: систематизовано автором [35-37]

У серпні 2023 Universal Bank (monobank) зайняв 2-ге місце серед усіх банків України за кількістю емітованих карток.

У квітні 2024 р. monobank анонсував масштабне оновлення дизайну застосунку (Monobank 2.0)[38]. Фокус оновлення – підтримка мультикартності: головний екран перероблено з 3D-карткою в центрі і помітно оновленими іконками, меню стало більш зручним при роботі з кількома рахунками. Кольорова гама додатку також змінилася, додано темну тему.

Додаток monobank регулярно посідає високі місця в рейтингах UX/UI. Його оцінюють у 4,9 на Google Play і App Store. На рівні війни спостерігався стрімкий ріст лояльності клієнтів: Net Promoter Score банку підскочив до 87–89% (проти 70% до початку війни), що свідчить про високу якість сервісу.[39] Сервіс підтримки користувачів («служба турботи» або «котики») наразі налічує понад 1 300 працівників по всій Україні, що також позитивно впливає на UX та оцінку клієнтів.

Сегментація клієнтів і машинне навчання дозволяють банку надсилати клієнтам таргетовані пропозиції, оновлювати кредитні ліміти чи умови кешбеку за індивідуальними моделями ризику. Також аналітика застосовується у кредитному скорингу та маркетингових розсилках. Monobank використовує традиційні для FinTech методи (ML, Big Data) для оптимізації бізнес-процесів і покращення клієнтського досвіду.

Стратегічна співпраця Monobank із цифровими ініціативами української держави (зокрема з платформою «Дія») суттєво розширила функціонал банку та сприяла його соціалізації. Ініціативи на кшталт «єПідтримки», «єВідновлення» та «Дія.Картки» стали інструментами державної фінансової політики, яка реалізується через приватного банківського оператора. Це свідчить про формування в Україні моделі публічно-приватного партнерства у сфері цифрового банкінгу, де інноваційні технології виступають посередником між громадянином і державою. Така інтеграція є ознакою зрілості цифрової екосистеми і підтверджує перспективність розвитку FinTech-сектору в умовах діджиталізації публічного управління. (Табл.2.4)

Таблиця 2.4 - Інтеграція Monobank з державними сервісами

Сервіс	Функціонал	Рік активної інтеграції
BankID через Monobank	Авторизація в «Дії» через мобільний банкінг	2021
«Дія.Картка»	Отримання всіх держвиплат на одну картку	2024
Картка «єПідтримка»	Програма підтримки під час пандемії та війни	2021–2022
Картка «єВідновлення»	Виплати на відновлення житла, інфраструктури	2023
Електронний цифровий підпис	Підписання банківських документів у додатку	2022

Джерело: систематизовано автором [34]

Клієнти можуть авторизуватися в застосунку «Дія» за допомогою monobank. Наприклад, у інструкції Diia зазначено, що, натиснувши в Дії на іконку monobank, користувач потрапляє у мобільний додаток банку для підтвердження входу (BankID). Після підтвердження монобанком застосунок «Дія» видає 4-значний код для входу. Це забезпечує швидку та безпечну ідентифікацію через держпослуги.

У грудні 2024 р. monobank презентував «Дія.Картку» – універсальну карту для отримання всіх державних виплат. На цю карту надходять соціальні виплати, компенсації та інші державні програми. Як зазначає банк, «кожна нова виплата від держави не створюватиме в гаманці +1 картку».[40] Це спрощує життя громадян, які можуть отримувати зарплату, стипендії, соцдопомогу та інші гроші від держави на єдину карту (першою на карту «Дія.Картка» надійшла компенсація за програмою «єКнига»).

Monobank випустив картки «єПідтримка» і «єВідновлення» для отримання певних державних допомог. Зокрема, «єПідтримка» призначена для державної допомоги переселенцям/різним соціальним програмам, а «єВідновлення» – для виплат по програмі відновлення України.

Банк підтримує EDS – це цифровий підпис, який клієнт може використовувати для підписання банківських угод в електронному вигляді.

Monobank – один із лідерів українського digital-банкінгу. Станом на кінець 2024–початок 2025 це другий за розміром банк у країні за обсягом депозитів (близько 108 млрд гривень) і за кількістю активних карток (9,77 млн). На початок 2025 року обсяг коштів фізичних осіб, розміщених у банках-учасниках Фонду гарантування вкладів, перевищив 1,39 трлн гривень. За інформацією Національного банку України, значна частка цих активів — понад 35% — номінована в іноземній валюті, зокрема в доларах США та євро. Така валютна структура вкладів створює додаткові виклики для забезпечення фінансової стабільності та підвищує вимоги до системи ризик-менеджменту у сфері безпеки банківського бізнесу. Перше місце утримує державний ПриватБанк. Унікальна користувацька база monobank (8–10 млн) значно перевищує всі інші «необанки» України, як-от sportbank або «А-Банк» (Astound Bank), які мають відносно невеликі аудиторії.

Monobank демонструє найвищі показники клієнтської лояльності (індекс NPS — понад 87%) серед українських банків, що є результатом якісної UX/UI-архітектури мобільного застосунку, високої швидкості обслуговування та прозорої тарифної політики. Хоча за кількістю клієнтів він поступається державному ПриватБанку, Monobank досягає порівняльного рівня ефективності, маючи суттєво меншу інфраструктуру. У порівнянні з новими FinTech-гравцями, такими як Sportbank, або міжнародними платформами (Revolut), Monobank має перевагу в локальній інтеграції з державними сервісами та адаптації до правових реалій України. (Таблиця 2.5)

Таблиця 2.5 - Порівняння Monobank з основними конкурентами за 2024 рік

Показник	Monobank	PrivatBank	Sportbank	Revolut (ЄС)
Кількість клієнтів (млн)	9,2	≈22	≈0,5	45+
NPS (індекс лояльності)	87–89%	≈70%	~65%	~80%
Кількість моб. карток	10 млн	>25 млн	<1 млн	>50 млн
Покриття	Україна	Україна	Україна	Глобальне
Рік заснування	2017	1992	2019	2015

Джерело: систематизовано автором [41-43]

ПриватБанк – головний конкурент у цифровому сегменті (додаток Privat24 має десятки мільйонів користувачів, доступних через широку мережу відділень/ банкоматів), але monobank випереджає його в показниках NPS і активності мобільного банкінгу. Sportbank (запущений 2019 р.) – перший український необанк з двома ліцензіями (Oxi Bank і один з підрозділів групи «Тігіпко»), проте його база клієнтів – кілька сотень тисяч. А-Банк (необанк від групи Astound) та інші подібні сервіси мають також порівняно скромні обсяги користувачів.

В ЄС та світі монобанк масштабом значно поступається гігантам необанкінгу. Наприклад, Revolut (Великобританія/ЄС) станом на літо 2024 року налічував близько 45 млн клієнтів по всьому світу. [43] Це дозволяє йому інвестувати мільярди доларів у розвиток. N26 (Німеччина) – ще один відомий європейський необанк – досяг 4,8 млн активних користувачів наприкінці 2024 (тобто за весь час існування). Навіть найбільш прогресивні європейські банки мають міжнародні аудиторії на порядок більші за український monobank.

Однак слід врахувати, що ці проекти працюють на значно більшій (міжнародній) вибірці населення, тоді як Monobank за період 2020–2024 закріпився як провідний український цифровий банк. Він впровадив низку інноваційних продуктів і забезпечив високий рівень безпеки. Швидке зростання кількості клієнтів, активне поповнення депозитів (до 108 млрд грн) і визнання (напр., у фінтех-рейтинг Forbes/TOP-200 FinTechs) демонструють успіх його моделі. Порівняно з іншими гравцями ринку (PrivatBank, sportbank тощо) monobank вирізняється мобільністю та інноваціями, а серед європейських необанків поступається лише за масштабом ринку (але зберігає високу якість сервісу).

2.3 Цифрові технології як чинник зміцнення фінансової безпеки в умовах цифрової економіки: переваги та недоліки

Системний розвиток інноваційної інфраструктури держави, зокрема шляхом впровадження новітніх цифрових рішень, масштабування

високотехнологічного виробництва, нарощування науково-дослідного потенціалу та активного впровадження FinTech-рішень, може стати ключовим фактором підвищення фінансової стійкості та безпеки країни. FinTech сьогодні розглядається не лише як сукупність передових технологій і нетрадиційних бізнес-моделей, а й як фундаментальний компонент цифрової трансформації у фінансовій сфері. Важливо підкреслити, що FinTech неможливий поза контекстом цифрових технологій, адже саме вони забезпечують новий рівень прозорості, контролю та надійності у фінансових відносинах, зокрема на макрорівні.

Зокрема, цифровізація фінансової сфери сприяє зменшенню ризиків у державних фінансах шляхом підвищення прозорості бюджетного процесу, що напряму впливає на рівень фінансової безпеки. Одним із ключових індикаторів тут виступає індекс відкритості бюджету, який формується на основі інтегральних показників прозорості та підзвітності публічних фінансів. Зростання бюджетної відкритості забезпечує досягнення таких результатів, як підвищення якості державних послуг, залучення громадськості до контролю за використанням бюджетних коштів, зростання підзвітності виконавчої влади та посилення ефективності державного фінансового менеджменту.

Прозорість фінансових процесів, особливо у публічному секторі, є ключовим засобом зменшення корупційних ризиків, протидії фінансовим зловживанням і скорочення тіньової економіки — тобто, чинником, що напряму впливає на загальний рівень фінансової безпеки країни. В Україні цифрові інструменти найбільш активно впроваджуються у сфері управління державними фінансами. Так, запуск цифрових платформ «Прозорий бюджет», «spending.gov.ua» та «openbudget.gov.ua» дав змогу суттєво підвищити публічну підзвітність бюджетних витрат на всіх рівнях. [46, с. 167]

Окрему роль у забезпеченні прозорості й безпеки фінансової системи відіграє банківський сектор. Національний банк України, як центральний орган грошово-кредитної політики, активно застосовує інструменти цифрової відкритості — через офіційний сайт НБУ можна оперативно отримати інформацію про стан валютного ринку, напрями монетарної політики та ключові рішення

регулятора. У межах боротьби з незаконними фінансовими операціями, зокрема з нелегальним виведенням капіталу, відмиванням грошей під виглядом іноземних інвестицій, а також з тінізацією зовнішньої торгівлі, особливе значення набуває впровадження новітніх інструментів FinReg – зокрема RegTech і SupTech**.**

RegTech (від «regulatory technology») — це технологічні рішення, що автоматизують і оптимізують процеси дотримання регуляторних вимог фінансовими установами. Це поняття стало активно використовуватись після 2017 року, коли Рада з фінансової стабільності (Financial Stability Board) почала приділяти увагу цифровим інструментам забезпечення нагляду. SupTech, у свою чергу, застосовується органами регулювання й контролю для підвищення ефективності наглядових функцій за допомогою сучасних цифрових засобів.

За визначенням Базельського комітету з банківського нагляду, SupTech – це використання технологій на стороні регулятора для поліпшення моніторингу, аналізу ризиків та загального контролю за стабільністю фінансової системи. [47]

Таким чином, сучасна парадигма забезпечення фінансової безпеки базується на тісному поєднанні цифрових інновацій, відкритості публічних фінансів та ефективних інструментів фінансового нагляду. Використання FinTech, RegTech і SupTech у комплексі формує якісно нову інфраструктуру цифрової фінансової безпеки — адаптивну, прозору й стійку до зовнішніх викликів.

Науковці, зокрема Сіренко Н., Полторак А., Атаманюк І., Волосюк Ю., Мельник О. та Фененко П., виділяють низку фінансових технологій, які, на їхню думку, виступають ключовими чинниками посилення фінансової безпеки держави та бізнесу [48]. У контексті фінансового сектору та корпоративної безпеки ці технології мають особливу значущість, адже дозволяють не лише оптимізувати операційні процеси, а й забезпечити надійний захист фінансових активів і даних. Основні з них:

1. Блокчейн-технології — забезпечують незмінність записів, високу ступінь прозорості фінансових операцій, а також створюють альтернативні моделі обліку, в яких значно знижено ризик зовнішнього втручання чи фальсифікацій. У

сфері бізнесу це дозволяє зміцнити довіру до платіжних і облікових систем, а також мінімізувати ризики шахрайства.

2. Хмарні сервіси — надають можливість швидко масштабувати інформаційні системи, знижують витрати на підтримку IT-інфраструктури та, що особливо важливо, забезпечують високий рівень резервування даних і кіберзахисту. Використання хмарних платформ дозволяє банкам та фінансовим компаніям ефективно відновлювати діяльність у разі кібератак або технічних збоїв.

3. Цифрові фінансові платформи — відкривають нові канали для надання послуг, інтеграції фінтех-стартапів та покращення клієнтського досвіду. Водночас вони формують нові виклики в аспекті захисту конфіденційної інформації, що зумовлює потребу у вбудованій безпеці на рівні архітектури таких платформ.

4. Інтернет речей (IoT) — використовується для збору великих обсягів даних з фізичних пристроїв, що дозволяє фінансовим структурам глибше аналізувати поведінку користувачів, ідентифікувати аномалії та вчасно реагувати на потенційні загрози. Наприклад, у страхуванні це відкриває доступ до даних з телематичних пристроїв, які дозволяють персоналізувати ризик-профілі клієнтів.

5. Big Data та аналітика в реальному часі — сприяють виявленню ризикованих операцій, побудові моделей прогнозування кіберзагроз, а також формуванню систем раннього попередження. Такі технології дозволяють інтегрувати поведінкову аналітику в системи управління ризиками.

6. Штучний інтелект (AI) і машинне навчання (ML) — забезпечують автоматизований аналіз великої кількості транзакцій і дозволяють виявляти нетипові дії, характерні для фінансового шахрайства. Також AI активно використовується в системах автоматичного підтвердження особистості та моніторингу на відповідність вимогам KYC/AML.

7. Відкриті API-платформи (Open Banking) — стимулюють розвиток партнерської екосистеми та водночас створюють потребу в уніфікованих протоколах кібербезпеки для захисту каналів передачі даних. Регульоване впровадження таких рішень сприяє прозорості, але потребує посилених заходів контролю з боку регуляторів і бізнесу.

У сучасному фінансовому середовищі FinTech-рішення активно впроваджуються для модернізації платіжних систем. Найпоширеніші з них включають:

- мобільні додатки для здійснення платежів;
- електронні та криптогаманці;
- безконтактні платіжні інструменти (NFC, QR-коди);
- системи цифрової ідентифікації;
- біометричні технології для підтвердження особи;
- аналітичні інструменти на основі AI для виявлення шахрайства [49].

Незважаючи на те, що концепція FinTech передбачає використання інноваційних рішень для надання фінансових послуг і оптимізації фінансових процесів, у контексті безпеки фінансового сектору такі технології можуть мати як позитивні, так і ризиковані наслідки.

Загалом впровадження FinTech-рішень у сферу безпеки фінансового бізнесу має декілька ключових позитивних наслідків:

1. Зміцнення кібербезпеки фінансових операцій. Завдяки інтеграції сучасних технологій, таких як криптографія, токенізація, багатофакторна автентифікація та поведінкове моделювання, фінансові установи отримують змогу значно знизити вразливість до внутрішніх і зовнішніх атак.

2. Підвищення доступності безпечних фінансових послуг. Цифрові технології забезпечують можливість безпечного надання фінансових послуг навіть у віддалених регіонах або в умовах обмеженої інфраструктури, знижуючи рівень фінансової виключеності.

3. Підтримка комплаєнсу та регуляторної прозорості. Завдяки блокчейну та смарт-контрактам фінансові установи можуть автоматизувати дотримання регуляторних вимог, зокрема в галузі AML/CFT. Це зменшує ризики штрафів і дозволяє оперативно реагувати на зміну законодавчих вимог.

4. Розвиток регтеху (RegTech). Інструменти FinTech підтримують розвиток технологій регуляторного нагляду, що дозволяє державним органам ефективно

здійснювати моніторинг ризиків, виявляти маніпуляції та порушення ще на ранніх етапах. У цьому контексті цифрова трансформація нагляду є передумовою формування стійкої системи фінансової безпеки.

Інтеграція фінансових технологій у структуру сучасного фінансового бізнесу створює нові можливості для підвищення його безпеки. Зокрема, ці технології здатні суттєво зміцнити механізми дотримання законодавчих вимог і зменшити ризики, пов’язані з протиправними фінансовими операціями, включно з відмиванням коштів і фінансуванням терористичної діяльності. Застосування блокчейн-платформ, які є основою криптовалют, забезпечує прозорість транзакцій та неможливість їх фальсифікації, що сприяє посиленню контролю з боку регуляторів і підвищує загальний рівень безпеки фінансових операцій.

Водночас зростання цифровізації приносить і низку викликів, які мають безпосередній вплив на безпеку фінансового бізнесу:

- Орієнтація FinTech на цифрову інфраструктуру робить її потенційною ціллю для кіберзлочинців. Уразливості в IT-системах можуть бути використані для несанкціонованого доступу до фінансових даних, крадіжки коштів або блокування фінансових сервісів. Тому впровадження комплексної системи кіберзахисту, зокрема інструментів виявлення вторгнень, шифрування даних і багатофакторної автентифікації, є критично необхідним для забезпечення стабільності бізнес-процесів.[50]
- Масове збирання й обробка персональних і фінансових даних у межах фінтех-сервісів породжує підвищені ризики порушення приватності. Недостатній рівень захисту таких даних може призвести до їх витоку, шахрайських схем і підриву довіри до компанії. Тому бізнесу слід дотримуватися принципів data protection by design, активно впроваджувати GDPR-подібні стандарти та забезпечувати прозорість у політиці обробки даних.[51]
- Попри зростання фінансової інклюзії, частина населення все ще має обмежений доступ до фінансових цифрових сервісів через відсутність необхідної інфраструктури або навичок. Така нерівність не лише загострює соціально-економічні диспропорції, а й створює додаткові ризики, оскільки фінансова

безпека є системним поняттям, що охоплює доступність, рівність і захищеність усіх учасників ринку.

Цифрові перетворення, які відбуваються в Україні протягом останніх років, значно підвищили рівень прозорості та ефективності фінансових відносин, особливо у сфері взаємодії з громадянами. Розвиток FinTech відкриває значний потенціал для зміцнення фінансової безпеки за рахунок автоматизації перевірок, надійності транзакцій і боротьби з фінансовими злочинами. Однак ці переваги потребують комплексного управління супутніми ризиками, насамперед — у кіберсфері, сфері персональних даних і цифрової доступності.[52]

Швидкі темпи інновацій вимагають гнучкої, ризик-орієнтованої нормативно-правової політики, здатної ефективно відповідати на новітні виклики. Традиційні механізми регулювання не завжди встигають адаптуватися до технологічних змін, тому важливо формувати партнерство між державними органами, фінансовим бізнесом і технологічним сектором. Така співпраця має базуватися на принципах безпечних інновацій, де пріоритетами виступають кіберстійкість, захист даних та інтересів споживачів, а також довгострокова стабільність фінансового середовища.

На основі проведеного теоретичного узагальнення, аналізу сучасного стану забезпечення фінансової безпеки в Україні та світового досвіду впровадження фінансових технологій, сформульовано низку пропозицій, які дозволять досягти поставленої мети — підвищити рівень безпеки у фінансовому бізнесі шляхом ефективного використання сучасних технологій.

1. Створення інтегрованої цифрової платформи обміну інформацією про фінансові кіберзагрози між установами

У зв’язку з високим рівнем кіберризиків у фінансовому секторі доцільно створити спеціалізовану державну платформу обміну оперативною інформацією про кіберінциденти між банками, страховими компаніями, НБУ, Держспецзв'язком, Кіберполіцією та іншими учасниками фінансового ринку. Така платформа повинна забезпечувати оперативну ідентифікацію загроз, інформування про уразливості, розповсюдження best practices і методик протидії шахрайству.

Впровадження такої системи дозволить зменшити затримки в реагуванні, знизити повторюваність атак і сприятиме підвищенню загального рівня кіберстійкості сектору.

2. Інтеграція штучного інтелекту та машинного навчання у системи моніторингу транзакцій

В умовах зростання кількості цифрових операцій важливо використовувати інтелектуальні системи для виявлення аномальної поведінки користувачів, фішингових спроб та шахрайських транзакцій. На базі технологій AI можна впровадити поведінкові профілі клієнтів, що дозволить банкам в режимі реального часу виявляти підозрілі дії (наприклад, незвичні суми, частоту платежів, локації доступу). Це знизить ймовірність фінансових втрат та зменшить навантаження на служби безпеки. Прикладом успішного застосування таких технологій є JP Morgan Chase, який виявляє шахрайство ще до завершення транзакції.

3. Поширення багатофакторної автентифікації (MFA) та біометричних засобів ідентифікації

У зв’язку з тим, що основна частина кібератак реалізується через несанкціонований доступ до акаунтів користувачів, доцільно на законодавчому рівні закріпити обов’язковість багатофакторної автентифікації у всіх цифрових фінансових сервісах, зокрема мобільному та онлайн-банкінгу. Застосування одночасно паролю, біометричних даних (відбитки пальців, Face ID), токенів та SMS-кодів дозволяє знизити ризик несанкціонованого доступу до особистої інформації користувачів на 80–90%, відповідно до досліджень McKinsey та IBM.

4. Використання блокчейн-технологій для управління безпечними транзакціями

Запровадження технологій розподіленого реєстру (DLT), зокрема блокчейну, дає змогу не лише забезпечити прозорість і незмінність транзакцій, але й спростити процедури комплаєнсу, KYC/AML і аудитів. Це особливо важливо в процесах міжбанківських розрахунків, торгівлі цінними паперами та фінансуванням зовнішньоекономічних операцій. Приклади таких рішень уже

впроваджуються у країнах ЄС, США, Сінгапурі, де блокчейн-системи застосовуються для зменшення трансакційних витрат та підвищення безпеки.

5. Розвиток національної програми цифрової фінансової грамотності персоналу

Однією з основних вразливостей у забезпеченні безпеки фінансового бізнесу є людський фактор — помилки або недбалість персоналу. З метою мінімізації таких ризиків доцільно розробити та впровадити навчальні модулі з кібербезпеки для працівників банківських і страхових установ. Навчання має охоплювати аспекти виявлення фішингу, захисту паролів, реагування на інциденти, протидії соціальній інженерії. Подібні програми рекомендовані МВФ та ENISA для усіх фінансових установ країн ЄС.

6. Формування системи цифрових індикаторів оцінки рівня фінансової безпеки

Запровадження системи оцінювання цифрової фінансової безпеки фінансових установ на основі показників, таких як рівень автоматизації процесів безпеки, відповідність міжнародним стандартам ISO/IEC 27001, частота успішних атак, ефективність інцидент-менеджменту — дозволить підвищити прозорість фінансового ринку та стимулювати інститути до інвестування в захист. Ці показники також можуть бути використані НБУ як частина комплексної оцінки надійності банків.

7. Стимулювання фінансової інклюзії з орієнтацією на безпечні фінтех-рішення для малого бізнесу

Фінансова безпека має бути доступною не лише великим банкам, а й мікро-, малим та середнім підприємствам. Держава має створити сприятливі умови для розвитку українських FinTech-стартапів, які надають безпечні платіжні, кредитні та страхові сервіси. Доцільно розробити механізми часткової компенсації витрат МСП на впровадження безпекових ІТ-рішень, створити регуляторні пісочниці (regulatory sandbox), а також популяризувати цифрову трансформацію серед підприємців.

Здійснені пропозиції мають комплексний характер і спрямовані на посилення технологічної, організаційної та інституційної стійкості фінансового бізнесу до сучасних загроз. Їх впровадження дозволить:

- знизити рівень кіберінцидентів і фінансових втрат;
- зміцнити довіру клієнтів і інвесторів до цифрових фінансових послуг;
- підвищити відповідність українського фінансового сектору міжнародним стандартам безпеки;
- стимулювати розвиток фінансових інновацій в Україні.

У сукупності це створює фундамент для стабільного, безпечного і конкурентоспроможного фінансового бізнесу в умовах цифрової трансформації економіки.

ВИСНОВКИ

У роботі здійснено комплексний теоретичний аналіз сутності, значення та структурних характеристик фінансової безпеки в контексті функціонування сучасного фінансового бізнесу. Встановлено, що фінансова безпека є багатогранним економічним явищем, яке охоплює як організаційно-технічні, так і стратегічні, інституційні та цифрові компоненти стійкості суб'єктів фінансового сектору. У підсумку сформовано уніфіковане бачення фінансової безпеки як системи захисту фінансового бізнесу від деструктивних впливів з метою забезпечення його стабільного розвитку, платоспроможності та конкурентоспроможності.

Розглянуто основні загрози та ризики**,** що впливають на фінансову безпеку. Встановлено, що їх походження може бути як внутрішнім (слабкий фінансовий менеджмент, неефективна структура капіталу, помилкові управлінські рішення), так і зовнішнім (макроекономічна нестабільність, кіберзагрози, регуляторні зміни, недобросовісна конкуренція). Узагальнено, що найвищу загрозу становлять операційні, репутаційні та кіберризики, які стрімко зростають у цифрову епоху. Узагальнено типологію дестабілізуючих чинників і описано механізм їхнього впливу на фінансову систему бізнесу**.** Такий підхід дозволяє цілісно охопити логіку розвитку деструктивних процесів та обґрунтувати необхідність їхньої превентивної нейтралізації.

Проаналізовано місце фінансової безпеки в загальній системі економічної безпеки бізнесу та наголошено на її ключовій ролі у підтриманні стабільності не лише на мікрорівні, а й у контексті макроекономічного середовища. Окреслено необхідність гармонізації внутрішніх фінансових процесів із зовнішніми інституційними умовами.

Здійснено прикладний аналіз сучасного стану систем безпеки у фінансовому бізнесі України, зокрема із акцентом на використання інноваційних фінансових технологій та цифрових інструментів у банківській сфері.

З'ясовано, що впровадження FinTech-рішень в українських банках, зокрема Monobank, сприяє підвищенню загального рівня фінансової безпеки. Використання

мобільного банкінгу, електронних гаманців, чат-ботів, а також систем багатофакторної автентифікації забезпечує зручність для користувачів і водночас підвищує захист від шахрайських операцій. Досвід Monobank засвідчує ефективність автоматизованого ризик-менеджменту, онлайн-ідентифікації клієнтів та використання біометрії для входу в систему.

Доведено, що штучний інтелект набуває особливої важливості у забезпеченні фінансової безпеки. Алгоритми машинного навчання дозволяють виявляти аномальні транзакції, ідентифікувати шахрайські схеми, аналізувати поведінку клієнтів і формувати персоналізовані моделі обслуговування. Застосування ШІ в управлінні ризиками, аналітиці транзакцій та системах KYC/AML істотно знижує вплив людського фактора та підвищує ефективність протидії кіберзагрозам.

Окрему увагу приділено блокчейн-технологіям, які забезпечують високий рівень прозорості, незмінності й достовірності фінансових операцій. Вони особливо ефективні для безпечного управління цифровими активами, смарт-контрактами та ідентифікацією клієнтів. Водночас застосування блокчейну в Україні наразі має обмежений характер через відсутність повноцінного регулювання.

Визначено, що найбільш поширеними загрозами в українському фінансовому секторі залишаються: кібератаки на платіжну інфраструктуру, фішингові кампанії, витік конфіденційних даних, внутрішнє шахрайство, а також маніпуляції на ринку фінансових послуг. На фоні зростання обсягу безготівкових операцій та цифровізації фінансових сервісів, ці загрози лише посилюються, що потребує проактивної відповіді з боку фінансових установ.

Наголошено, що ефективна система фінансової безпеки повинна поєднувати: сучасні цифрові інструменти захисту (MFA, шифрування, AI-моніторинг); організаційні заходи (внутрішні політики комплаєнсу, управління ризиками, антифрод-системи); нормативне забезпечення (відповідність міжнародним стандартам, включно з ISO/IEC 27001, PSD2, Basel III).

У ході дослідження сформульовано низку практичних пропозицій, реалізація яких дозволить підвищити рівень безпеки фінансового бізнесу в умовах цифрової трансформації. Зокрема, запропоновано створити єдину цифрову платформу обміну інформацією про кіберзагрози між фінансовими установами з метою своєчасного реагування на потенційні загрози. Обґрунтовано доцільність інтеграції систем штучного інтелекту для моніторингу транзакцій, що дозволить автоматично виявляти шахрайські дії та знижувати ризики. Рекомендовано розширити використання багатофакторної автентифікації та біометричних технологій для підвищення захисту клієнтських даних.

Окрему увагу приділено доцільності впровадження блокчейн-технологій у процеси здійснення фінансових операцій, що сприятиме прозорості та незмінності даних. Також акцентовано на важливості підвищення цифрової грамотності персоналу шляхом запровадження регулярного навчання з питань кібербезпеки. Крім того, запропоновано запровадити систему цифрових індикаторів оцінки рівня фінансової безпеки установ, що дозволить підвищити ефективність регуляторного контролю. З метою підтримки розвитку FinTech-сектору рекомендовано впровадити державні стимули для малого бізнесу у сфері фінансових технологій

Отже, на основі аналізу сучасних технологій безпеки у фінансовому бізнесі України можна зробити висновок, що цифрова трансформація не лише створює нові виклики, але й відкриває потужні можливості для побудови стійкої, безпечної та інноваційної фінансової екосистеми. Для досягнення цього необхідна тісна взаємодія між державними регуляторами, фінансовими установами, технологічними компаніями та клієнтами, а також формування культури безпеки як невід’ємної складової фінансової діяльності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вудвуд В. В., Батієвська О. В. Фінансова безпека підприємства: сутність, цілі, принципи та шляхи забезпечення. *Підприємництво і торгівля*. 2019. Вип. 25. С. 89-93. URL: http://nbuv.gov.ua/UJRN/Torg_2019_25_14

2. Рожко О., Нестеров Є. Теоретичні підходи до визначення фінансової безпеки підприємства. *Економіка та суспільство.* 2024. № 65. DOI: https://doi.org/10.32782/2524-0072/2024-65-79.

3. Мехед А. М., Варналій З. С. Фінансова безпека підприємств в умовах цифрової економіки. *Socio-Economic Relations in the Digital Society.* 2021. Т. 3, № 42. С. 55–61. DOI: https://doi.org/10.18371/2221-755x3(42)2021253524.

4. Барановський О. І. Фінансова безпека: монографія. Київ: Фенікс, 2008. 338 с.

5. Реверчук Н. Й. Управління економічною безпекою підприємницьких структур: монографія. Львів: ЛБІ НБУ, 2004. 195 с.

6. Горячова К. С. Фінансова безпека підприємства. Сутність та місце в системі економічної безпеки. *Економіст.* 2003. № 8. С. 65–67.

7. Управління фінансово-економічною безпекою : навч. посіб. / О. А. Кириченко, С. М. Лаптєв, П. Я. Пригунов, О. І. Захаров та ін. ; за ред. В. С. Сідака. Київ: Дорадо-Друк, 2010. 412 с.

8. Нікіфоров П. О., Кучерівська С. С. Сутність і значення фінансової безпеки страхової компанії. *Фінанси України*. 2006. № 5. С. 86–94.

9. Єпіфанов А. О., Пластун О. Л., Домбровський В. С. Фінансова безпека підприємств і банківських установ: монографія. Суми: ДВНЗ «УАБС НБУ», 2009. 295 с.

10. Михаліцька Н. Я. Теоретичні засади фінансової безпеки підприємства. *Науковий вісник Львівського державного університету внутрішніх справ. Серія: Економічна*. 2013. Вип. 1. С. 268–275.

11. Бланк І. А. Управління фінансовою безпекою підприємства. Київ: Ельга, Ніка-Центр, 2009. 784 с.

12. Власюк О. С. Теорія і практика економічної безпеки в системі науки про економіку: наукова доповідь. Київ: Нац. ін-т проблем міжнар. безпеки при РНБО України, 2008. 48 с.

13. Камлик М. І. Економічна безпека підприємницької діяльності: економіко-правовий аспект: навч. посіб. Київ: Атіка, 2005. 432 с.

14. Юрків Н. Я. Економічна безпека реального сектора економіки України: стратегічні пріоритети і теоретико-методологічні засади забезпечення: монографія. Львів: ПАІС, 2012. 400 с.

15. Собкевич О. В. Проблеми реального сектору економіки України у контексті економічної безпеки держави. *Глобальні та національні проблеми економіки.* 2017. Вип. 15. С. 136–141.

16. Іляш Н. І. Методологічні аспекти дослідження економічної безпеки реального сектора економіки України. *Держава та регіони.* 2013. № 4(73). С. 22–26.

17. Пасічник І. В., Курочкін С. А. Фінансова безпека банківської системи України в умовах сьогодення. *Інфраструктура ринку.* 2019. Вип. 37. С. 631–636.

18. Живко З. Б. Методологія управління економічною безпекою підприємства: монографія. Львів: Ліга-Прес, 2013. 471 с.

19. Witte N. Capital requirements in Pillar 1 or Pillar 2: does it matter for market discipline? URL: https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2988~25e3305cfa.en.pdf

20. Кульчицький І. І. Цифрова економіка та економічна безпека підприємства: стратегії управління. *Актуальні питання економічних наук*. 2024. № 6. С. 115–123.

21. Ліхоносова Г. С. Інструменти зміцнення економічної безпеки: цифровізація та усунення соціально-економічного відторгнення. *Інвестиції: практика та досвід.* 2023. № 19. – С. 16–21.

22. Ліхоносова Г. С. Фінансова безпека країни в умовах цифровізації соціально-економічних процесів. *Часопис економічних реформ.* 2023. № 2. С. 48–53.

23. Пілецька С., Мягких І. Механізм забезпечення фінансової безпеки підприємств в умовах економіки знань. *Економіка та суспільство.* 2023. Вип. 53.DOI: https://doi.org/10.32782/2524-0072/2023-53-29

24. Процак К. В., Коваленко Т. О. FinTech і комерційні банки: тенденції розвитку та особливості співпраці. *Бізнесінформ*. 2022. № 1. С. 131–137. URL: https://www.business-inform.net/export_pdf/business-inform-2022-1_0-pages-131_137.pdf

25. Як ALLIANCE BANK змінюється разом зі штучним. URL: https://bankalliance.ua/articles/yak-alliance-bank-zminyuetsya-razom-zi-shtuchnim-intelek

26. Більше грошей, безпеки та довіри клієнтів: як банки використовують штучний інтелект. URL: https://banker.ua/uk/projects/banki-shtuchnij-intelekt/

27. Big Data в банках: що це таке й у чому користь для банківського сектору. URL: https://hub.kyivstar.ua/news/big-data-v-bankah-shho-cze-take-j-u-chomu-koristi-dlya-bankivsikogo-sektoru

28. Чому банки переходять на хмарні платформи? URL: https://ua.news/ua/all-news/pochemu-banki-perehodyat-na-oblachnye-platformy

29. Про використання банками хмарних послуг в умовах воєнного стану в Україні : Постанова Правління НБУ від 08 березня 2022 року № 42 URL: https://bank.gov.ua/ua/legislation/Resolution_08032022_42

30. Голосова біометрія: що це, як працює та навіщо вона банкам? URL: https://fintechinsider.com.ua/golosova-biometriya-shho-cze-yak-praczyuye-ta-navishho-vona-bankam/

31. Приятельчук О. А. Порушення фінансових технологій: поява необанків в епоху цифрової трансформації. *Наукові записки Львівського університету бізнесу та права.* 2023. № 39. URL: https://nzlubp.org.ua/index.php/journal/article/view/993/884

32. Рисін В. В., Печенко Р. О. Роль цифрових платіжних технологій у розвитку підприємництва. *Цифрова економіка та економічна безпека.* 2022. № 3. – С. 103–108. DOI: https://doi.org/10.32782/dees.3-18

33. Безпека. URL: monobank.ua

34. Universal Bank | monobank увійшов у трійку лідерів за обсягом вкладів. URL: https://minfin.com.ua

35. Скільки клієнтів у monobank на початок 2024 року — Гороховський. URL: https://uapsm7.com

36. Monobank перевищив 10 млн емітованих карток. Liga.net. 2023. URL: https://biz.liga.net

37. Як Monobank зібрав 9 мільйонів клієнтів. Forbes Ukraine. 2024. URL: https://forbes.ua/company/monobank

38. Monobank 2.0. Огляд оновлення. Cases.media. URL: https://cases.media

39. Пристрасть і математика. Як закохати у свій бренд надовго? Кардинально протилежні поради від засновників Uklon і monobank. URL: https://forbes.ua

40. Monobank запускає «Дія.Картку» для всіх державних виплат. Shotam.info. URL: https://shotam.info

41. Національний банк України. Рейтинг банків за кількістю активних клієнтів, 2023. URL: https://bank.gov.ua

42. Офіційна презентація проєкту Sportbank, 2023. URL: https://sportbank.com.ua

43. Revolut. Official Press Kit, 2023–2024. URL: https://www.revolut.com

44. Minfin.ua. Рейтинг задоволеності банківськими послугами, 2023. URL: https://minfin.com.ua

45. Revolut. Wikipedia. URL: https://en.wikipedia.org

46. Hrytsenko L., Zakharkina L., Zakharkin O., Novikov V., Chukhno R. The impact of digital transformations on the transparency of financial-economic relations and financial security of Ukraine. *Financial and credit activity: problems of theory and practice*. 2022. No. 3 (44). P. 167–175. DOI: 10.55643/fcaptp.3.44.2022.3767.

47. Basel Committee on Banking Supervision. Instructions for Basel III monitoring. 19 October 2018. URL: https://www.bis.org/bcbs/qis/biiiimplmoninstr_oct18.pdf.

48. Sirenko N., Atamanyuk I., Volosyuk Yu. et al. Paradigm Changes that Strengthen the Financial Security of the State through FINTECH Development. The 11th IEEE

International Conference on *Dependable Systems, Services and Technologies*, DESSERT'2020, Kyiv, Ukraine, 2020. DOI: 10.1109/DESSERT50317.2020.9125026.

49. Худолій Ю., Свистун Л. Сучасні тенденції FINTECH та їх вплив на безпеку банківських установ. *Економіка і регіон.* 2021. № 3 (82). С. 115–123. DOI: 10.26906/EiR.2021.3(82).237.

50. Zadvornykh S. Fintech and financial security – perspectives and dangers. *Proceedings of III International Scientific and Practical Conference.* Osaka, Japan, 2019. P. 392–401.

51. Musabegovic I., Özer M., Djukovic S., Jovanovic S. Influence of financial technology (fintech) on financial industry. *Economics of Agriculture.* 2019. Year 66, No. 4. – P. 1003–1021. DOI: 10.5937/ekoPolj1904003M.

52. Єфремова К. Технології цифрової економіки та фінансова безпека. *Право та інновації.* 2024. № 2 (42). С. 7–11. DOI: https://doi.org/10.37772/2518-1718-2023-2(42)-1.