Карпатський національний університет імені Василя Стефаника

Економічний факультет

Кафедра фінансів

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття першого (бакалаврського) рівня вищої освіти

на тему: **«Кібербезпека банківського сектору в умовах розвитку фінансових технологій (FinTech)»**

Виконала: студентка 4 курсу, групи ФБС-42
спеціальності 072 «Фінанси, банківська справа та страхування»
Павлюк Д.Ю.

Керівник: Кохан І.В.
кандидат економічних наук, доцент,
доцент кафедри фінансів

Рецензент: Шурпа С.Я.
кандидат економічних наук, доцент,
доцент кафедри менеджменту і маркетингу

Івано-Франківськ – 2026 р.

ЗМІСТ

ВСТУП

У сучасних умовах розвитку фінансової системи України банківський сектор функціонує під впливом масштабної цифровізації, активного впровадження фінансових технологій (FinTech) та зростання рівня глобальної технологічної конкуренції. Трансформація фінансових послуг, перехід до цифрових каналів обслуговування, поширення відкритого банкінгу та розвиток цифрових платформ формують нову архітектуру банківської діяльності.

Банківські установи відіграють системоутворюючу роль у національній економіці, забезпечуючи ефективний перерозподіл фінансових ресурсів, розвиток платіжної інфраструктури та підтримку економічної активності суб'єктів господарювання і населення. Сучасний етап розвитку банківського сектору характеризується інтеграцією інноваційних технологій, зокрема штучного інтелекту, Big Data, блокчейну, хмарних сервісів та цифрових ідентифікаційних рішень. Такі технології підвищують ефективність банківської діяльності, сприяють оптимізації бізнес-процесів і формуванню нових фінансових екосистем.

Водночас активне впровадження FinTech-інновацій супроводжується зростанням кіберризиків, що проявляються у вигляді кібератак, несанкціонованого доступу до даних, шахрайських операцій, витоку конфіденційної інформації та порушення безперервності банківських процесів. Кіберзагрози набувають системного характеру та можуть мати значний негативний вплив на фінансову стабільність банківських установ і довіру клієнтів. У цих умовах кібербезпека виступає ключовим елементом забезпечення надійності функціонування банківського сектору та його адаптації до цифрової трансформації.

Актуальність теми зумовлена необхідністю комплексного дослідження кібербезпеки банківського сектору в системі розвитку фінансових технологій, а також обґрунтування ефективних підходів до управління кіберризиками та підвищення кіберстійкості банківських установ. Особливого значення набуває

аналіз взаємозв'язку між розвитком FinTech та трансформацією підходів до забезпечення інформаційної безпеки у банківській сфері.

Метою дипломної роботи є комплексне дослідження теоретичних і практичних аспектів забезпечення кібербезпеки банківського сектору в умовах розвитку фінансових технологій, а також обґрунтування стратегічних напрямів її посилення.

Для досягнення поставленої мети у роботі визначено такі завдання:

1) розкрити економічну сутність кібербезпеки у банківській діяльності;

2) дослідити класифікацію та особливості кіберзагроз у фінансовому секторі;

3) визначити роль FinTech у трансформації підходів до забезпечення кібербезпеки банків;

4) проаналізувати динаміку та тенденції розвитку кіберзагроз у банківській системі України;

5) оцінити вплив фінансово-технологічних інновацій на рівень кіберризиків банківських установ;

6) дослідити сучасний стан систем кібербезпеки банківського сектору України;

7) обґрунтувати стратегічні напрями підвищення кіберстійкості банків у системі FinTech.

У процесі дослідження використано комплекс загальнонаукових і спеціальних методів. Методи аналізу та синтезу застосовано для узагальнення теоретичних положень щодо кібербезпеки банківського сектору; індукція та дедукція забезпечили логічну послідовність дослідження; системний підхід дозволив розглядати кібербезпеку як інтегровану складову функціонування банківської системи; порівняльний аналіз використано для оцінювання тенденцій розвитку кіберзагроз; економіко-статистичні методи застосовано для аналізу стану кібербезпеки банківських установ; метод узагальнення та моделювання використано для обґрунтування напрямів удосконалення управління кіберризиками.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ КІБЕРБЕЗПЕКИ БАНКІВСЬКОГО СЕКТОРУ В УМОВАХ FINTECH-ТРАНСФОРМАЦІЇ

1.1. Економічна сутність кібербезпеки у банківській діяльності

Банківські установи формують основу фінансової інфраструктури держави, сприяючи акумулюванню тимчасово вільних коштів, організації платіжного обігу та фінансуванню діяльності суб'єктів господарювання і домогосподарств. У цьому контексті гарантування належного рівня банківської безпеки набуває стратегічного значення, оскільки її порушення може призвести до дестабілізації фінансової системи, зниження рівня довіри з боку суспільства та виникнення кризових явищ у соціально-економічному середовищі.

Необхідність посилення безпеки банківської діяльності обумовлюється наявністю комплексу як внутрішніх, так і зовнішніх ризиків. Вагомим чинником виступає глобалізація фінансових ринків, яка, поряд із розширенням можливостей міжнародної інтеграції банківського бізнесу, одночасно підвищує рівень конкуренції та посилює залежність від зовнішньоекономічної кон'юнктури. Поглиблення цифровізації фінансового сектору супроводжується зростанням кіберризиків, пов'язаних із функціонуванням інформаційно-комунікаційної інфраструктури банків. Несанкціоноване втручання в інформаційні системи, кібератаки, шахрайські дії та витоки даних створюють суттєві загрози для збереження фінансових активів, конфіденційності клієнтської інформації та репутаційної стійкості банківських установ.

У сучасній науковій думці сформовано різноманітні підходи до трактування категорії «банківська безпека», які відображають багатовимірність цього явища. Систематизація зазначених підходів, запропонована вітчизняними науковцями дозволяє комплексно розкрити зміст цього поняття та визначити його ключові структурні характеристики (рис. 1.1):

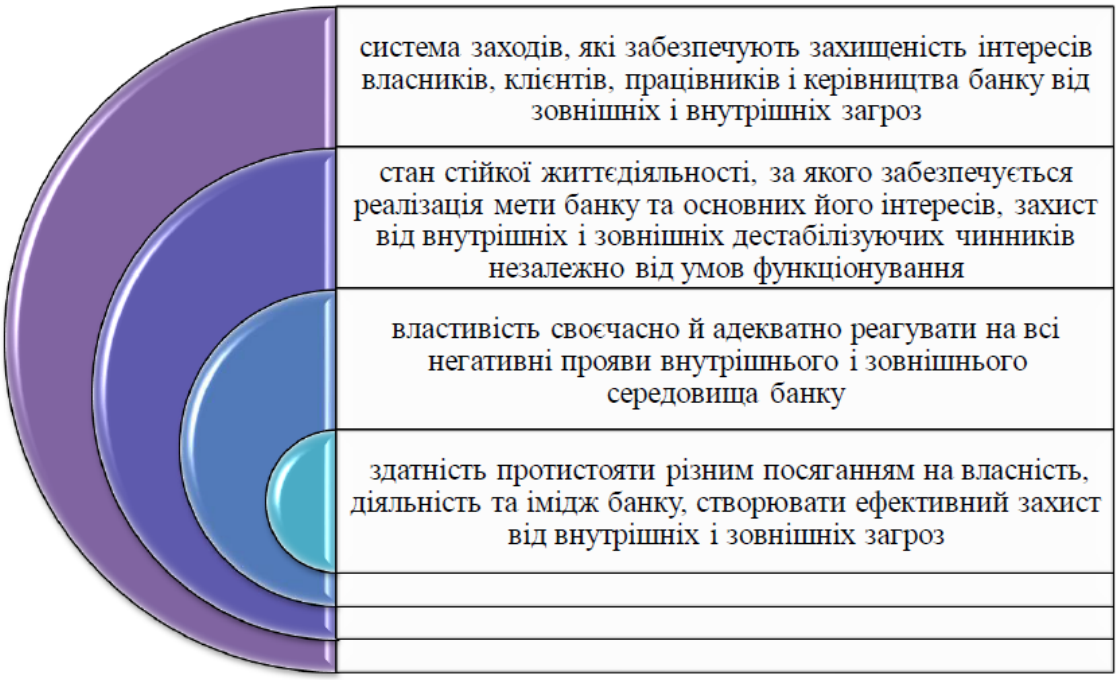

Рис. 1.1. Трактування підходів до визначення «банківської безпеки»
* систематизовано автором на основі [12; 15]

Ключовою метою забезпечення кібербезпеки банківського сектору є формування комплексної системи захисту, здатної гарантувати стійкість фінансової установи до цифрових загроз, забезпечувати безперервність її функціонування та збереження критично важливих даних. В умовах стрімкого розвитку фінансових технологій (FinTech) кібербезпека трансформується у стратегічний чинник стабільності банківської системи, оскільки будь-які порушення у сфері інформаційної безпеки можуть призвести до фінансових втрат, витоку конфіденційної інформації та підриву довіри клієнтів.

Система кібербезпеки банків повинна забезпечувати створення такого управлінського середовища, в якому кіберризики своєчасно виявляються, оцінюються та мінімізуються із застосуванням сучасних цифрових інструментів. Це передбачає інтеграцію інноваційних технологій, зокрема штучного інтелекту (AI), машинного навчання, Big Data-аналітики та автоматизованих систем моніторингу кіберінцидентів. Важливим елементом є формування культури кібергігієни та відповідального ставлення до

інформаційної безпеки серед персоналу банківських установ, що сприяє зниженню ризиків людського фактору.

Забезпечення кібербезпеки банківських установ тісно пов’язане з ефективним управлінням цифровими ризиками, що передбачає оптимізацію витрат на безпеку, впровадження інноваційних технологічних рішень та підтримання стабільного функціонування інформаційної інфраструктури. У цьому контексті система управління кіберризиками виступає ключовим елементом підвищення стійкості банків до умов невизначеності, пов’язаних із швидким розвитком FinTech та цифрових платформ.

До основних критеріїв кібербезпеки банківської установи доцільно віднести:

– рівень захищеності інформаційних ресурсів і цифрової інфраструктури;

– ефективність функціонування систем виявлення та запобігання кіберінцидентам;

– здатність протидіяти сучасним кіберзагрозам, включаючи складні цілеспрямовані атаки APT (Advanced Persistent Threat);

– рівень інтеграції інноваційних технологій у систему кіберзахисту;

– надійність організаційної структури управління кіберризиками;

– рівень підготовки персоналу у сфері інформаційної та кібербезпеки.

Об’єктами захисту в системі кібербезпеки банку виступають інформаційні ресурси, програмно-технічна інфраструктура, фінансові активи, персонал та клієнтська база. В умовах цифровізації саме інформаційні дані стають ключовим стратегічним ресурсом, а їх компрометація може мати критичні наслідки для фінансової стійкості та репутації банківської установи.

Отже, забезпечення кібербезпеки банківського сектору є складним багаторівневим процесом, що поєднує організаційні, технологічні, фінансові та правові аспекти. Його ефективність визначає не лише стабільність окремого банку, але й надійність функціонування всієї фінансової системи в умовах розвитку FinTech. На рис. 1.2 відображено ключові об’єкти кіберзахисту

банківської системи, серед яких інформаційні, фінансові, технологічні та кадрові ресурси.

Рис. 1.2. Структура об'єктів захисту в системі кібербезпеки банків

* сформовано автором на основі [15; 16]

Об'єкти забезпечення банківської безпеки доцільно розглядати крізь призму системного підходу як сукупність взаємопов'язаних елементів, що формують інтегровану архітектуру захисту фінансової установи в умовах цифрової трансформації та розвитку FinTech. У сучасній парадигмі банківської діяльності такі об'єкти виступають ключовими компонентами системи risk-based governance та забезпечення cyber resilience, що відповідає принципам сталого розвитку та ESG-орієнтованого управління.

Першу групу становлять фінансові ресурси, які включають грошові активи у національній та іноземній валютах, результати банківських операцій, фінансові інструменти, дорогоцінні метали та супровідну фінансову документацію. Захист цих ресурсів передбачає застосування сучасних інструментів фінансового моніторингу, аналітики ризиків та автоматизованих

систем контролю, зокрема на основі RegTech-рішень, що забезпечують дотримання нормативних вимог і підвищують прозорість фінансових операцій.

Другою складовою є персонал банку, включаючи керівництво, топ-менеджмент і працівників, які мають доступ до критичних інформаційних ресурсів. У контексті ESG-підходу людський капітал розглядається як стратегічний актив, а управління ним передбачає дотримання етичних стандартів, підвищення рівня цифрової грамотності та формування культури безпеки.

Третю групу формують матеріальні активи, до яких належать об’єкти інфраструктури банку. Їх захист інтегрується в загальну систему операційної безпеки та передбачає використання сучасних технологій моніторингу, автоматизації та контролю фізичного доступу. У цьому контексті важливу роль відіграють SupTech-інструменти, які дозволяють регуляторам здійснювати нагляд за станом інфраструктурної безпеки банків у режимі реального часу.

Ключове значення в умовах цифровізації має четверта група — інформація з обмеженим доступом, яка включає банківську, комерційну та іншу конфіденційну інформацію. Інформаційні активи виступають основою функціонування цифрових банківських сервісів і FinTech-платформ, тому їх захист потребує впровадження комплексних систем кібербезпеки, криптографічних методів захисту, а також використання інтелектуальних алгоритмів виявлення кіберзагроз. Зростання масштабів кібератак, зокрема APT-кампаній і витоків даних, підсилює значення інтеграції інформаційної безпеки у загальну систему управління ризиками.

Таким чином, систематизація об’єктів банківської безпеки за фінансовими, кадровими, матеріальними та інформаційними компонентами дозволяє сформувати комплексну модель захисту, що відповідає сучасним викликам цифрової економіки. Інтеграція підходів ESG, RegTech та SupTech сприяє підвищенню ефективності управління ризиками, забезпеченню прозорості діяльності банків та зміцненню їх стійкості до внутрішніх і зовнішніх загроз.

1.2. Класифікація та характеристика кіберзагроз у фінансовому секторі в умовах цифровізації

Банківський сектор характеризується підвищеним рівнем ризикогенності порівняно з іншими галузями економіки, що обумовлено специфікою його функціонування та високою залежністю від динаміки ринкового середовища, вартості активів, ліквідності й рівня довіри клієнтів. Саме тому діяльність банківських установ у більшості країн супроводжується посиленим державним регулюванням і фінансовим наглядом, метою яких є обмеження негативних наслідків реалізації ризиків та забезпечення стабільності фінансової системи.

У загальноекономічному розумінні ризик інтерпретується як імовірність виникнення небажаних або непередбачуваних подій, здатних спричинити фінансові втрати. У межах економічної теорії він розглядається як усвідомлена можливість втрати очікуваних доходів, активів або грошових ресурсів під впливом несприятливих змін зовнішнього середовища, випадкових факторів чи невизначеності.

Для банківської діяльності ризик має інтегрований характер, оскільки поєднує фінансові, кредитні, ринкові, операційні та технологічні складові. Він відображає ймовірність зниження прибутковості, втрати частини капіталу або виникнення збитків у процесі здійснення банківських операцій, що безпосередньо впливає на фінансову стійкість установи та рівень довіри клієнтів.

Сучасний етап розвитку фінансової системи визначається активним впровадженням цифрових технологій у банківську діяльність, що виступає ключовим драйвером трансформації глобального фінансового ринку. Цифровізація сприяє підвищенню ефективності операцій, пришвидшенню обробки транзакцій, розширенню доступу до фінансових послуг, скороченню витрат і оптимізації управління ресурсами. Водночас вона генерує нові види ризиків, які можуть становити суттєву загрозу стабільності як окремих банків, так і фінансової системи в цілому.

Вплив цифрової трансформації проявляється як на рівні окремих банківських установ, так і на макроекономічному рівні. Порушення роботи цифрових систем або реалізація кібератак здатні спричинити значні фінансові втрати як для банків, так і для їхніх клієнтів, а процес відновлення після таких інцидентів потребує значних ресурсів. У масштабах економіки це може призводити до відтоку капіталу, зниження інвестиційної активності, валютної нестабільності та загального погіршення фінансового стану країни.

З огляду на сучасні умови розвитку цифрової економіки, ризики цифровізації банківського сектору доцільно систематизувати за такими групами:

– технічні ризики, пов’язані з відмовами програмного забезпечення, зношеністю або несумісністю обладнання;

– операційні ризики, зумовлені помилками персоналу, недосконалістю внутрішніх процедур або недостатнім рівнем контролю;

– фінансові ризики, що виникають унаслідок шахрайських дій, несанкціонованих операцій чи кібератак;

– регуляторні ризики, пов’язані з невідповідністю діяльності банку вимогам законодавства у сфері кібербезпеки та захисту інформації;

– репутаційні ризики, що проявляються у втраті довіри клієнтів через витік конфіденційних даних або публічне розголошення кіберінцидентів;

– соціальні ризики, які відображають негативні наслідки для клієнтів, персоналу та суспільства внаслідок порушень у цифровій інфраструктурі банку.

Таким чином, кіберризики займають ключове місце в сучасній системі банківських ризиків, оскільки їх реалізація здатна ініціювати виникнення інших загроз і посилювати їхній вплив. Взаємозв’язок кіберризиків з іншими видами ризиків банківської діяльності доцільно відобразити у вигляді схеми.

Схематичне представлення місця кіберризиків у структурі банківських ризиків наведено на рис. 1.3.

Рис. 1.3. Кіберризики в архітектурі інтегрованої системи банківських ризиків

* систематизовано на основі [17; 18]

Кіберризики на сучасному етапі розвитку фінансового сектору виступають одними з найбільш критичних і динамічних загроз для банківської системи. Їх активізація безпосередньо пов’язана зі стрімким поширенням цифрових технологій, збільшенням обсягів електронних транзакцій і трансформацією фінансових послуг у цифрове середовище.

З метою протидії цифровим загрозам банківські установи впроваджують багаторівневі системи безпеки, які поєднують технічні, організаційні та програмні інструменти. Водночас навіть високотехнологічні рішення не забезпечують абсолютного захисту, оскільки кіберзлочинці безперервно модернізують інструментарій атак, активно використовуючи штучний інтелект, методи соціальної інженерії та експлуатацію вразливостей інформаційних систем.

У контексті глобалізації цифрового простору кіберзагрози у фінансовій сфері набувають транснаціонального характеру, що зумовлює необхідність координації зусиль на міжнародному рівні, включаючи обмін інформацією між банками, регуляторами та державними інституціями. Додатковим каталізатором посилення кіберризиків стала пандемія COVID-19, яка прискорила цифровізацію фінансових послуг і розширила поверхню потенційних атак через масове впровадження дистанційних сервісів.

Особливо критичними є загрози, пов’язані з порушенням цілісності фінансових даних, включаючи алгоритми обробки інформації, бази даних, електронні транзакції та цифрові записи. Подібні інциденти можуть спричинити не лише прямі фінансові втрати, але й суттєве зниження рівня довіри клієнтів, що є фундаментальним чинником стабільності банківської системи. Обмеженість технологічних рішень щодо повного запобігання таким атакам актуалізує необхідність розвитку концепції кіберстійкості (cyber resilience) у діяльності фінансових установ.

Кіберзагрози у банківському секторі характеризуються багатовимірністю та охоплюють широкий спектр ризиків — від шахрайських схем і викрадення даних до руйнування інформаційної інфраструктури та компрометації внутрішніх мереж. Їх реалізація може призвести до значних фінансових збитків, порушення платоспроможності банківських установ і дестабілізації фінансової системи в цілому.

З огляду на це доцільним є виокремлення та систематизація основних видів кіберзагроз, характерних для банківського сектору (рис. 1.4).

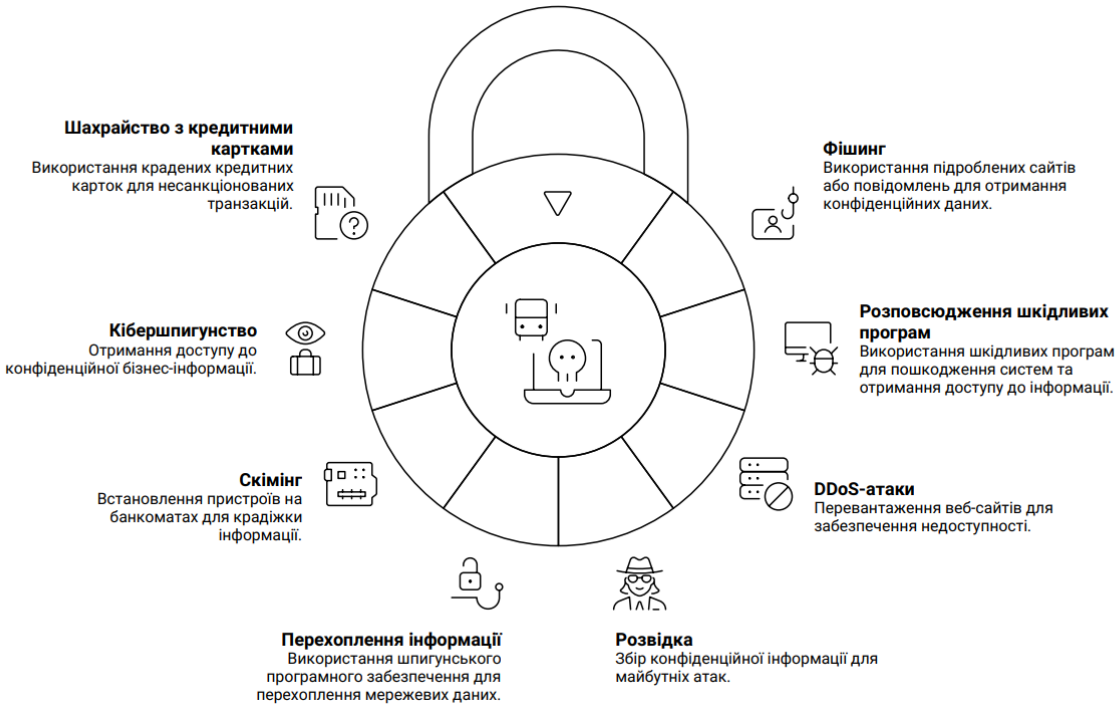

Рис. 1.4. Система кіберзагроз у банківській FinTech-екосистемі

* власна розробка автора

Сучасний ландшафт кіберзагроз у банківському секторі характеризується високою динамічністю та постійною еволюцією, що обумовлено стрімким розвитком фінансових технологій (FinTech), цифрових платформ і глобалізацією фінансових ринків. Розширення цифрової інфраструктури, зростання обсягів електронних транзакцій і впровадження інноваційних інструментів обробки даних формують нові вектори вразливостей, які активно використовуються кіберзлочинними угрупованнями. У цьому контексті кіберризики набувають статусу системоутворюючого фактору, здатного впливати на загальну фінансову стабільність банківських установ.

Незважаючи на технологічну складність більшості кіберінцидентів, значна частка загроз пов’язана з внутрішніми факторами, зокрема поведінковими ризиками персоналу, помилками користувачів і недотриманням процедур інформаційної безпеки. Це підкреслює необхідність інтеграції принципів ESG у систему управління банківською безпекою, де соціальний компонент (S) передбачає формування культури кібергігієни, відповідальності

та етичної поведінки персоналу, а управлінський компонент (G) — забезпечення прозорості, підзвітності та ефективного контролю.

Умови повномасштабної війни суттєво трансформували природу кіберзагроз, перетворивши їх на інструмент гібридного впливу на фінансову систему. Кібератаки спрямовуються як на державні інформаційні ресурси, так і на банківську інфраструктуру, включаючи платіжні системи та онлайн-сервіси. Це зумовлює необхідність впровадження систем проактивного моніторингу та реагування на загрози в режимі реального часу, що реалізується через використання інструментів SupTech на рівні регуляторів і RegTech-рішень на рівні банківських установ .

Аналіз сучасних кіберінцидентів свідчить про домінування таких типів атак, як DDoS-атаки, спрямовані на порушення доступності цифрових сервісів, та фішингові кампанії, що використовують методи соціальної інженерії для компрометації клієнтських даних. Водночас реальний масштаб кіберзагроз значно перевищує офіційні статистичні дані через латентний характер частини інцидентів і високий рівень їх оперативної нейтралізації .

Сучасні тренди цифровізації банківського сектору, включаючи розвиток дистанційного банкінгу, впровадження штучного інтелекту, використання Big Data та перехід до data-driven управління, одночасно підвищують ефективність діяльності та ускладнюють ризиковий профіль банків. У таких умовах формується нова парадигма управління ризиками, орієнтована на забезпечення cyber resilience, що передбачає здатність банків не лише протидіяти кіберзагрозам, але й швидко відновлюватися після інцидентів.

Важливим аспектом є розмежування інформаційної безпеки та кібербезпеки. Інформаційна безпека охоплює захист усіх видів інформації, включаючи фізичні та цифрові носії, тоді як кібербезпека зосереджена на захисті інформаційно-комунікаційних систем від технічних загроз. При цьому ключовими принципами залишаються конфіденційність, цілісність і доступність даних, що є базовими елементами сучасної цифрової безпеки .

Відповідно до підходів Базельського комітету з банківського нагляду, цифрова трансформація банківського сектору супроводжується зростанням стратегічних, операційних, кібер- та комплаєнс-ризиків. Стратегічні ризики пов'язані з необхідністю адаптації до технологічних змін і нових бізнес-моделей, операційні – із функціонуванням складної цифрової інфраструктури, кіберризики – із загрозами втрати даних і порушенням роботи систем, а комплаєнс-ризики – із недотриманням нормативно-правових вимог, особливо в умовах співпраці з FinTech-компаніями .

Таким чином, система кібербезпеки банківського сектору трансформується у комплексну інтегровану модель управління ризиками, що поєднує технологічні інновації, регуляторні механізми та принципи сталого розвитку. Використання підходів ESG, RegTech і SupTech дозволяє підвищити ефективність управління ризиками, забезпечити прозорість діяльності та зміцнити стійкість банківської системи до сучасних цифрових викликів.

1.3. Роль фінансових технологій (FinTech) у трансформації підходів до забезпечення банківської кібербезпеки

У сучасному фінансовому середовищі інноваційні технології у банківській сфері набувають визначального значення як ключовий драйвер підвищення конкурентоспроможності фінансових установ і трансформації їхньої взаємодії з клієнтами.

На сучасному етапі FinTech рішення охоплюють широкий спектр напрямів, серед яких провідне місце займають цифровізація фінансових процесів, впровадження нових фінансових продуктів і сервісів, модернізація систем управління ризиками, а також посилення інформаційної та кібербезпеки. Використання інноваційних рішень, зокрема штучного інтелекту, Big Data-аналітики та цифрових платформ, дозволяє підвищити якість обслуговування

клієнтів, оптимізувати бізнес-процеси та вдосконалити механізми прийняття управлінських рішень.

Таким чином, інноваційні FinTech технології виступають не лише фактором підвищення ефективності банківської діяльності, але й ключовим елементом забезпечення безпеки фінансового сектору, що визначає необхідність їх системного впровадження та подальшого розвитку (рис. 1.5).

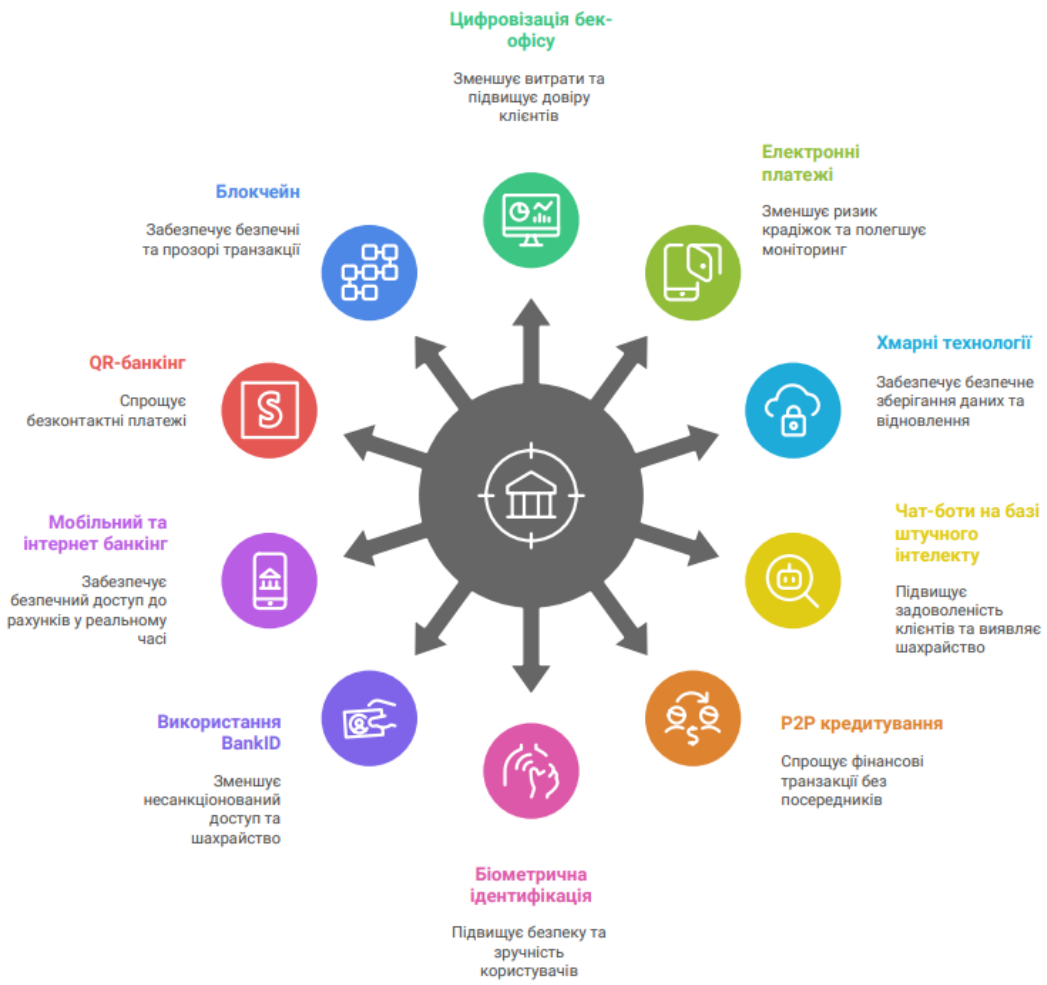

Рис. 1.5. FinTech рішення в системі захисту від кіберзагроз

* власна розробка автора

У межах сучасної цифрової трансформації фінансового сектору інноваційна активність банківських установ виступає одним із ключових детермінантів підвищення рівня кібербезпеки та загальної стійкості фінансової системи.

Серед основних напрямів цифрових інновацій, що безпосередньо впливають на рівень інформаційного захисту, доцільно виокремити автоматизацію внутрішніх (бек-офісних) процесів банківських установ. Їх цифровізація сприяє підвищенню операційної ефективності, скороченню витрат, вдосконаленню продуктового портфеля та забезпеченню дотримання регуляторних вимог .

Важливим компонентом інноваційного розвитку є розширення використання електронних платіжних інструментів, які мінімізують обіг готівки та знижують рівень фінансових правопорушень. Цифрові транзакції формують аналітичний масив даних, що дозволяє банкам здійснювати моніторинг операцій у реальному часі, виявляти підозрілі активності та оперативно реагувати на потенційні шахрайські дії .

Значну роль у забезпеченні безпеки відіграють хмарні технології, які створюють захищене середовище для зберігання та обробки банківської інформації із застосуванням сучасних криптографічних алгоритмів. Використання хмарних рішень забезпечує можливість резервного копіювання даних та їх оперативного відновлення, що є критично важливим у разі кіберінцидентів або технічних збоїв .

Інтеграція технологій штучного інтелекту та машинного навчання дозволяє суттєво підвищити рівень кіберзахисту. Алгоритми аналізу поведінки клієнтів дають змогу ідентифікувати нетипові транзакції, виявляти ознаки шахрайства та здійснювати превентивні заходи. Додатково, використання чат-ботів оптимізує комунікацію з клієнтами та підвищує ефективність обробки інформаційних запитів .

Суттєвим елементом інноваційної інфраструктури є розвиток альтернативних фінансових моделей, зокрема P2P-кредитування, яке забезпечує прямі взаємодії між учасниками фінансового ринку та оптимізує процеси розподілу ресурсів. Водночас підвищення рівня безпеки досягається через впровадження біометричних технологій ідентифікації, що ускладнюють несанкціонований доступ до даних і знижують ризики шахрайства .

Додатковим інструментом цифрової ідентифікації виступає система BankID, яка забезпечує безпечний обмін персональними даними між банками та постачальниками послуг. Паралельно розвиток мобільного та інтернет-банкінгу створює умови для цілодобового доступу до фінансових сервісів, при цьому багаторівнева аутентифікація забезпечує належний рівень захисту клієнтських рахунків .

Інноваційні платіжні рішення, зокрема QR-банкінг, спрощують процес здійснення розрахунків і підвищують їх безпеку завдяки використанню захищених каналів передачі даних. Водночас технологія блокчейн формує нову модель обробки фінансової інформації, що базується на принципах децентралізації, незмінності записів і криптографічного захисту, що суттєво знижує ризик фальсифікації даних .

Отже, інноваційна діяльність банківських установ виступає ключовим фактором підвищення рівня кібербезпеки та фінансової стійкості. Водночас процес цифрової трансформації супроводжується появою нових ризиків і викликів, що потребують комплексного підходу до управління безпекою в умовах розвитку цифрової економіки.

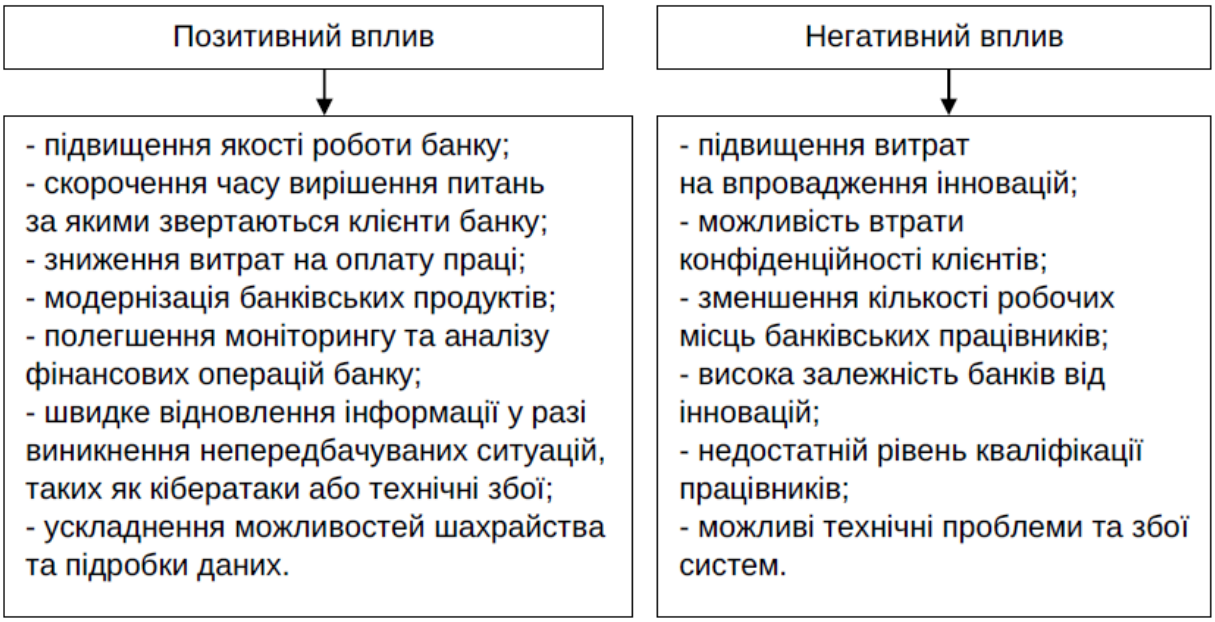

Рис. 1.6. Трансформація фінансової безпеки банків під впливом FinTech-інновацій

* систематизовано на основі [17]

Серед ключових бар’єрів, що стримують ефективне впровадження інновацій у банківському секторі, доцільно виокремити низку системних факторів. Передусім це значні інвестиційні витрати, пов’язані з розробленням і інтеграцією новітніх технологічних рішень, а також недостатня адаптованість нормативно-правового середовища до динамічного розвитку фінансових технологій. Додатковими обмеженнями виступають недостатній рівень цифрових компетенцій персоналу, нерівномірний розвиток інформаційно-комунікаційної інфраструктури в регіональному розрізі та підвищені ризики компрометації конфіденційних даних.

Водночас поширення FinTech-рішень супроводжується еволюцією схем кібер- та фінансового шахрайства, що підвищує складність забезпечення належного рівня безпеки. Окремим соціально-економічним викликом є можливе скорочення робочих місць унаслідок автоматизації банківських процесів, а також вплив макроекономічної та політичної нестабільності на інвестиційну привабливість фінансового сектору.

У цих умовах критичного значення набуває розвиток ефективної системи кібербезпеки як базового елементу захисту інформаційних активів і підтримання довіри клієнтів до цифрових банківських сервісів. Банківські установи, що оперують значними обсягами персональних і фінансових даних, виступають пріоритетними цілями для кіберзлочинців. Реалізація кібератак може призвести до несанкціонованих транзакцій, порушення функціонування платіжної інфраструктури, репутаційних втрат і суттєвих фінансових збитків.

З огляду на це, стратегічним пріоритетом для банків є формування комплексної системи кіберзахисту, яка передбачає постійне оновлення програмного забезпечення, підвищення кваліфікації персоналу у сфері інформаційних технологій, а також розроблення ефективних механізмів реагування на кіберінциденти. Лише інтеграція інноваційних технологій із надійними інструментами захисту дозволяє забезпечити стабільність функціонування банківських установ і підтримувати високий рівень довіри у цифровому фінансовому середовищі.

Важливим напрямом цифрової трансформації банківського сектору є впровадження хмарних технологій, які передбачають використання віддалених обчислювальних ресурсів для зберігання, обробки та передачі даних. Такі рішення забезпечують гнучкість банківських систем, розширюють можливості взаємодії з клієнтами, сприяють впровадженню персоналізованих сервісів і водночас підвищують рівень захисту інформаційних ресурсів.

Ключові аспекти впливу хмарних технологій на безпеку клієнтського обслуговування в банківській сфері узагальнено на рис. 1.5:

Рис. 1.5. Роль хмарних технологій FinTech у забезпеченні безпеки клієнтського обслуговування банків

* власна розробка автора

Отже, інтеграція фінансових технологій (FinTech) у банківську діяльність суттєво трансформує підходи до забезпечення кібербезпеки, переводячи їх із традиційної реактивної моделі у проактивну, ризик-орієнтовану систему управління. Незважаючи на зростання кількості цифрових загроз, впровадження інноваційних технологій формує нові можливості для побудови

ефективних механізмів моніторингу, контролю та захисту інформаційних ресурсів банків.

Застосування сучасних FinTech-рішень, зокрема штучного інтелекту, машинного навчання, Big Data-аналітики та автоматизованих систем виявлення загроз, забезпечує своєчасну ідентифікацію кіберризиків, виявлення аномальних операцій і мінімізацію потенційних втрат у режимі реального часу. Це дозволяє банківським установам не лише ефективно протидіяти кіберзлочинності, але й підвищувати рівень кіберстійкості (cyber resilience) в умовах динамічного цифрового середовища.

Водночас FinTech-технології сприяють удосконаленню архітектури кіберзахисту через впровадження багаторівневих систем аутентифікації, криптографічних методів захисту даних, хмарних рішень і цифрових ідентифікаційних платформ. Це створює передумови для підвищення надійності банківських операцій, зниження ймовірності кіберінцидентів і зміцнення довіри клієнтів до цифрових фінансових сервісів.

Таким чином, FinTech виступає не лише інструментом технологічної модернізації банківського сектору, а й ключовим драйвером трансформації системи кібербезпеки. Узагальнюючи, фінансові технології формують нову парадигму забезпечення банківської кібербезпеки, орієнтовану на проактивне управління ризиками, адаптивність до загроз і забезпечення стійкого функціонування банківської системи в умовах цифрової економіки.

РОЗДІЛ 2
ОЦІНКА СУЧАСНОГО СТАНУ КІБЕРБЕЗПЕКИ БАНКІВСЬКОЇ СИСТЕМИ УКРАЇНИ В УМОВАХ РОЗВИТКУ FINTECH (НА ПРИКЛАДІ АТ КБ «ПРИВАТБАНК»)

2.1. Динаміка та тенденції розвитку кіберзагроз у банківському секторі України

Банківська система виконує системоутворюючу функцію в економіці держави, забезпечуючи акумуляцію та перерозподіл фінансових ресурсів, підтримку підприємницької активності, фінансування інвестиційних і інноваційних проєктів, а також організацію безперебійного функціонування платіжної інфраструктури. Крім того, через механізми грошово-кредитного регулювання банки виступають важливим інструментом забезпечення макроекономічної рівноваги.

Повномасштабне вторгнення росії в Україну стало каталізатором глибоких змін у структурі кіберризиків фінансового сектору, водночас вплинувши на загальносвітовий безпековий контекст у цифровому середовищі. В умовах воєнного стану регулятор адаптував підходи до забезпечення безперервності банківської діяльності, зокрема дозволив фінансовим установам використовувати хмарні рішення. Це надало змогу банкам переносити обчислювальні потужності та дані на інфраструктуру, розміщену в юрисдикціях із підвищеним рівнем надійності, таких як США, Велика Британія, Канада та країни Європейського Союзу.

Водночас активне впровадження хмарних технологій має подвійний ефект. З одного боку, це підвищує гнучкість та стійкість банків до кризових ситуацій, а з іншого — створює нові вектори кіберзагроз. Концентрація великих обсягів фінансових і персональних даних у цифровому середовищі підвищує привабливість банків як цілей для кібератак, зокрема з боку організованих злочинних угруповань та державних акторів.

Після початку повномасштабної війни зафіксовано істотне зростання інтенсивності кібератак на об’єкти критичної інфраструктури, включаючи банківський сектор. Такі атаки здатні спричиняти не лише локальні збої, а й масштабні системні ризики для економіки країни. За інформацією Служби безпеки України, динаміка нейтралізованих кіберінцидентів демонструє стрімке зростання: від близько 800 випадків у 2020 році до понад 4500 у 2022–2023 роках, що свідчить про ескалацію кіберпротистояння.

Сучасні кіберзагрози дедалі більше зумовлюються геополітичними чинниками. Зокрема, відповідно до аналітичного звіту ENISA (2024–2025), у країнах Європейського Союзу спостерігалося різке збільшення кількості DDoS-атак, які використовувалися як інструмент кібертиску. Такі атаки значною мірою корелюють із реакцією на військові події в Україні та відображають трансформацію кіберпростору у важливу складову гібридної війни (рис. 2.1).

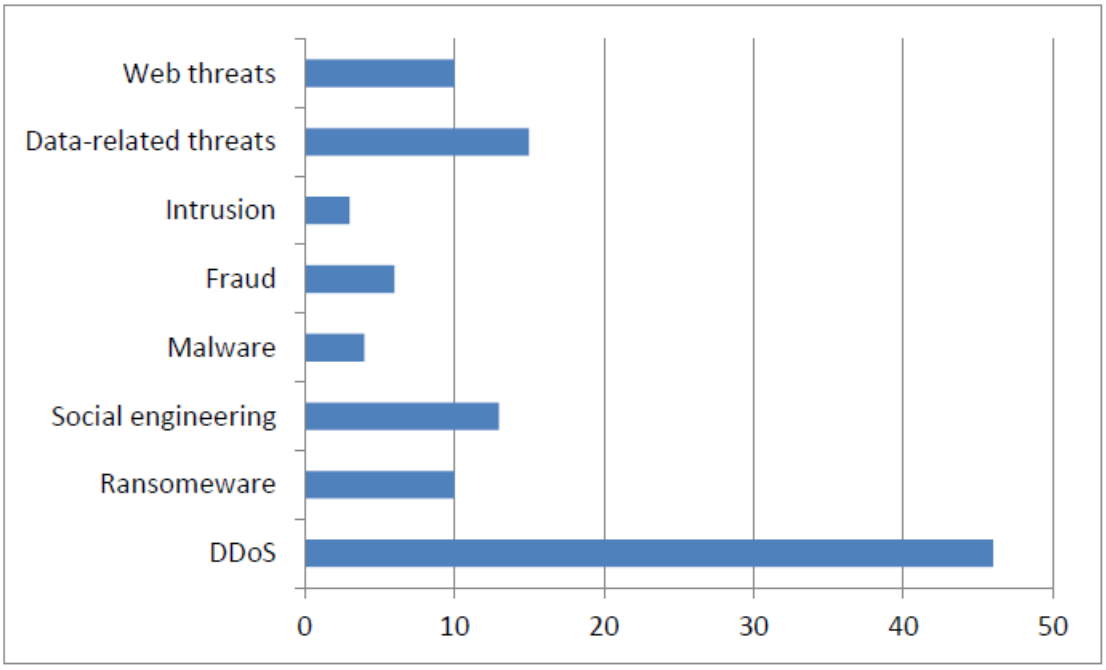

Рис. 2.1. Спектр ризиків і кіберзагроз у європейській фінансовій сфері у 2023–2024 рр..

* систематизовано на основі [15]

У контексті повномасштабної війни проти України кіберзагрози набули виразного геополітичного характеру. DDoS-атаки використовуються як

інструмент інформаційно-психологічного впливу, спрямованого на підрив довіри до фінансових інституцій і створення ефекту системної нестабільності. Це означає, що оцінка кіберризиків повинна здійснюватися не лише з позиції технічних наслідків, але й з урахуванням їх макроекономічного та соціального ефекту.

Додатково аналітична оцінка динаміки кіберінцидентів (рис. 2.2) дозволяє конкретизувати виявлені тенденції. Зокрема, у 2021 році загальна кількість зафіксованих кіберінцидентів становила 14 випадків при середній інтенсивності 2,29, тоді як у 2022 році відбулося різке зростання до 41 інциденту (+193%), що супроводжувалося підвищенням інтенсивності до 2,39. Така динаміка безпосередньо корелює з початком повномасштабної війни та активізацією кібератак на фінансову інфраструктуру.

У 2023 році спостерігається зниження кількості інцидентів до 25 випадків (–39% порівняно з 2022 роком), однак середня інтенсивність досягає максимального значення — 2,64. Це свідчить про перехід від масових атак до більш складних, таргетованих і технічно досконалих кібероперацій, що мають вищий рівень деструктивного впливу.

У 2024 році кількість інцидентів скорочується до 15, а середня інтенсивність знижується до 2,29, що може вказувати на часткову адаптацію банківської системи до нових умов кіберзагроз і підвищення ефективності заходів кіберзахисту. Водночас середнє значення за досліджуваний період становить 23,8 інциденту при середній інтенсивності 2,40, що характеризує загалом високий рівень загрозового навантаження на фінансовий сектор.

Аналітично важливим є те, що між кількістю атак і їх інтенсивністю простежується обернена залежність: зі зменшенням кількості інцидентів зростає їх складність і руйнівний потенціал. Це підтверджує тезу про якісну трансформацію кіберзагроз — від масових атак до високоточних, ресурсно забезпечених і стратегічно скоординованих кібероперацій.

Таким чином, наведена динаміка демонструє, що сучасне кіберзагрозове середовище характеризується не лише варіативністю кількісних показників, але

й посиленням їх якісних параметрів, що особливо актуалізує необхідність впровадження інтелектуальних FinTech-рішень у системи кіберзахисту банківських установ, зокрема АТ КБ «ПриватБанк».

Рис. 2.2. Тенденції змін кількісних та інтенсивнісних параметрів кібератак на банківський сектор у 2021–2024 рр.

* систематизовано на основі [17]

Водночас, за інформацією Ситуаційного центру кібербезпеки Служби безпеки України, протягом останніх двох років фінансовий сектор стабільно формує близько п’ятої частини від загальної кількості зафіксованих кіберінцидентів (приблизно 20%) (рис. 2.3). Така частка свідчить про високий рівень привабливості банківських установ для кіберзловмисників, що зумовлено концентрацією фінансових ресурсів, критично важливих даних та розвиненою цифровою інфраструктурою.

Аналітично це підтверджує, що фінансовий сектор входить до групи найбільш уразливих об’єктів критичної інфраструктури, де реалізація кіберризиків має не лише локальні, але й системні наслідки для економічної безпеки держави. Збереження стабільно високої частки інцидентів також вказує на стійку зацікавленість як кримінальних угруповань, так і державо-орієнтованих акторів у проведенні атак саме на фінансові установи.

:

Рис. 2.3. Кіберінциденти зафіксовані СЦЗК СБУ протягом 2023-2025 рр.
Джерело: систематизовано та розраховано автором на основі [35]

Деталізація структури кіберінцидентів у динаміці (рис. 2.3) дозволяє виявити низку важливих закономірностей. Зокрема, упродовж 2023 року спостерігається стійке зростання загальної кількості кіберінцидентів, що досягає пікових значень наприкінці року (понад 1700–1800 випадків щомісячно). Водночас приріст інцидентів у фінансовому секторі має більш помірний характер, однак демонструє чітку висхідну тенденцію.

У 2024 році фіксується певна стабілізація загальної кількості кіберінцидентів із незначними коливаннями, що супроводжується зростанням частки фінансового сектору до рівня близько 20–25%. Це свідчить про поступове зміщення фокусу кіберзловмисників у бік більш «цінних» цілей, до яких належать банківські установи.

На початку 2025 року спостерігається різке зниження загальної кількості кіберінцидентів, однак частка фінансового сектору залишається відносно високою, що вказує на збереження пріоритетності атак саме на фінансову інфраструктуру навіть за умов загального зменшення активності.

Аналітично важливим є те, що частка фінансового сектору не демонструє прямої залежності від загальної кількості інцидентів: навіть у періоди спаду загальної активності кіберзагроз банки залишаються ключовими об’єктами атак. Це підтверджує високу концентрацію ризиків у банківській сфері та її стратегічне значення для кіберзловмисників.

Наведені дані засвідчують не лише кількісне зростання кіберзагроз, але й їх структурну переорієнтацію на фінансовий сектор, що обумовлює необхідність посилення систем кіберзахисту, особливо у системно важливих банках, зокрема АТ КБ «ПриватБанк».

Таким чином, кіберризики у фінансовому секторі доцільно інтерпретувати як комплексну, багаторівневу загрозу, що виходить за межі окремих інцидентів і потребує системного управління. Йдеться не лише про реагування на вже реалізовані атаки, а про формування проактивної моделі кіберстійкості, орієнтованої на прогнозування, запобігання та мінімізацію наслідків кіберінцидентів. Починаючи з лютого 2022 року, в умовах повномасштабної війни, спостерігається суттєве підвищення рівня готовності банківських установ до протидії кіберзагрозам. Це є результатом накопичення практичного досвіду, вдосконалення процедур реагування, модернізації систем моніторингу та посилення кадрового потенціалу у сфері кібербезпеки. Внаслідок цього вітчизняний фінансовий сектор демонструє поступовий перехід від реактивної до адаптивно-превентивної моделі захисту.

Інституційна архітектура кібербезпеки фінансової системи України має чітко структурований характер. Ключову координаційну роль виконує Національний банк України, який одночасно виступає регулятором, суб’єктом національної системи захисту критичної інфраструктури та оператором безпеки у банківському секторі. Внутрішні підрозділи НБУ, зокрема управління захисту критичної інфраструктури, забезпечують формування політики кіберзахисту та контроль за її реалізацією. Нормативною основою цих процесів є постанова Правління НБУ №178 від 12 серпня 2022 року, яка визначає вимоги до організації кіберзахисту, критерії критичності інфраструктури та механізми взаємодії між учасниками фінансового ринку.

Важливим елементом інфраструктури кібербезпеки є платформа MISP-NBU, що функціонує на базі міжнародного рішення MISP та адаптована до національних умов. Її впровадження забезпечує стандартизований обмін індикаторами компрометації, оперативною інформацією про загрози та

рекомендаціями щодо їх нейтралізації. Інтеграція цієї платформи з діяльністю CERT-UA та іншими суб'єктами кіберзахисту формує єдиний інформаційний простір реагування, що суттєво скорочує час виявлення та локалізації інцидентів.

Координаційну функцію на рівні фінансового сектору виконує FinCERT при НБУ, який здійснює моніторинг загрозового середовища, розповсюдження попереджень та методичну підтримку банківських установ. Водночас міжвідомчу взаємодію забезпечують Департамент кіберполіції Національної поліції України та Державний центр кіберзахисту Держспецзв'язку, що відповідають за розслідування кіберзлочинів, технічне реагування та формування державної політики у сфері кібероборони.

Аналітично важливим є те, що сучасна система кіберзахисту в Україні формується за принципом мережевої взаємодії, де ефективність забезпечується не лише окремими інституціями, а їх координацією та швидкістю обміну інформацією. Така модель відповідає міжнародним підходам до побудови кіберстійкості, зокрема концепції collective cyber resilience.

У цьому контексті особливого значення набуває міжнародне співробітництво. Показовим є партнерство між Національним банком України та Міністерством фінансів США, спрямоване на посилення кіберзахисту фінансового сектору. Реалізація спільних ініціатив передбачає розвиток Центру кіберзахисту НБУ, імплементацію кращих світових практик та розширення каналів обміну інформацією про загрози. Це дозволяє інтегрувати українську фінансову систему у глобальний простір кібербезпеки та підвищити її стійкість до зовнішніх впливів.

Отже, сучасні кіберризики у фінансовому секторі України набули системного та стратегічного характеру. Їх ефективне управління можливе лише за умови поєднання технологічної модернізації, безперервного моніторингу загроз, розвитку інституційної взаємодії та поглиблення міжнародної співпраці. У цьому контексті особливої актуальності набуває впровадження інноваційних FinTech-рішень, що дозволяють підвищити адаптивність систем кіберзахисту,

що буде розглянуто на прикладі діяльності АТ КБ «ПриватБанк» у наступному підрозділі.

2.2. Аналіз впливу FinTech-інновацій на рівень кіберризиків та фінансової безпеки банків

Цифрова трансформація банківського сектору є ключовим драйвером його розвитку, забезпечуючи розширення спектра послуг, підвищення ефективності операцій та зміцнення конкурентних позицій банків. Водночас активне впровадження FinTech-рішень супроводжується зростанням складності кіберризиків, які безпосередньо впливають на рівень фінансової та інформаційної безпеки.

В умовах повномасштабної війни банківська система України функціонує під посиленим впливом загроз, що актуалізує необхідність зміцнення кіберстійкості. Фінансова безпека банків у таких умовах виступає ключовою передумовою стабільності всієї фінансової системи та довіри клієнтів. Водночас рівень захищеності банків значною мірою визначається ступенем їх цифровізації та використанням інноваційних технологій.

Інтеграція банків у цифрові екосистеми на базі мобільних додатків, API, штучного інтелекту та хмарних сервісів забезпечує підвищення доступності послуг, проте водночас розширює потенційну «поверхню атаки». Це зумовлює необхідність впровадження комплексних систем кіберзахисту та адаптації бізнес-процесів до умов цифрового середовища.

Таким чином, FinTech-інновації мають подвійний ефект: вони підвищують ефективність банківської діяльності, але одночасно ускладнюють кіберзагрозове середовище. У цьому контексті доцільним є аналіз впливу цифрової трансформації на фінансові результати банківського сектору України у 2019–2024 роках (рис. 2.4).

:

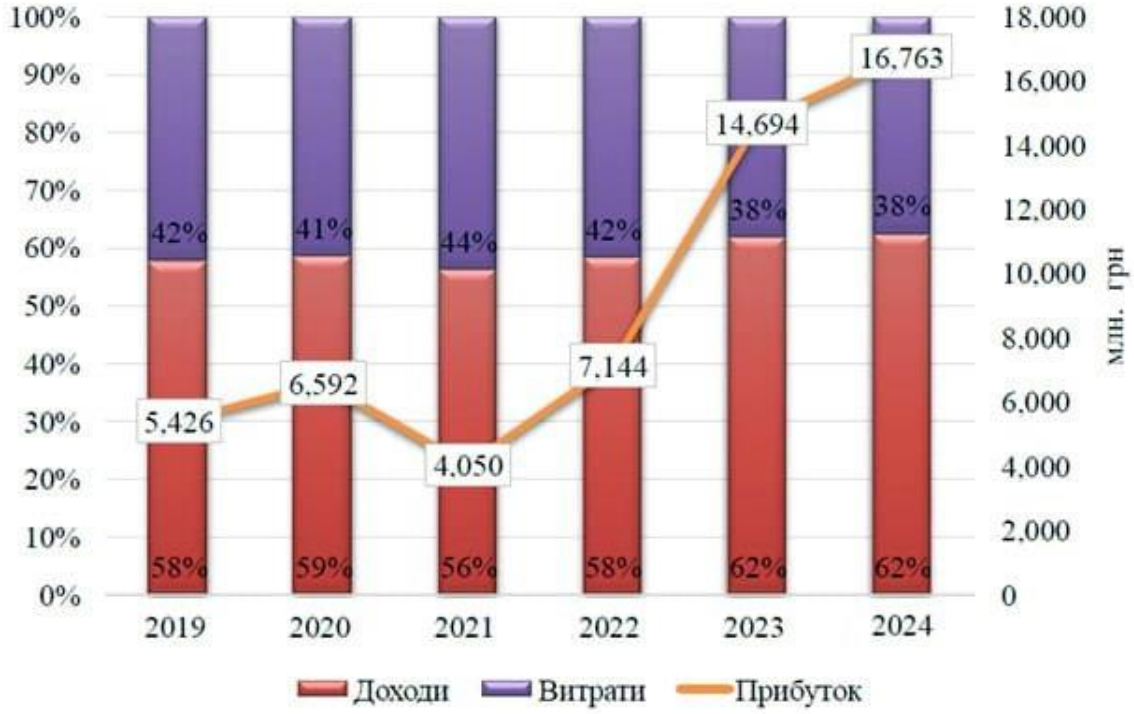

Рис. 2.4. Вплив FinTech-інновацій на фінансову результативність банківського сектору України за 2019-2024 роки

* систематизовано на основі [12]

Підвищення частки доходів, сформованих через цифрові канали обслуговування, відображає глибинну трансформацію поведінки клієнтів, які дедалі активніше надають перевагу дистанційним форматам взаємодії з банківськими установами. У цьому контексті особливо показовим є досвід АТ КБ «ПриватБанк», який завдяки масштабній цифровій екосистемі та розвитку сервісів на базі платформи Privat24 забезпечує стабільне зростання фінансових результатів і утримує лідерські позиції на ринку. Позитивна динаміка чистого прибутку банківського сектору протягом останніх років підтверджує ефективність курсу на цифровізацію, а у випадку «ПриватБанку» — ще й демонструє синергію між інноваціями, масштабом клієнтської бази та оптимізацією операційної діяльності.

Зростання прибутковості банків, зокрема «ПриватБанку», свідчить не лише про підвищення ефективності бізнес-моделей, але й про зміцнення фінансової стійкості, здатність підтримувати належний рівень ліквідності та адаптуватися до зовнішніх шоків, включаючи макроекономічні дисбаланси та воєнні ризики. Отримані фінансові результати створюють передумови для

активного реінвестування у технологічний розвиток: впровадження інноваційних цифрових рішень, модернізацію IT-інфраструктури та посилення систем кіберзахисту. Високий рівень капіталізації «ПриватБанку» забезпечує додатковий запас фінансової міцності, що є критично важливим в умовах зростання кіберзагроз і технологічних викликів (табл. 2.1):

Таблиця 2.1

Діджиталізація банків України з домінуючою роллю АТ КБ «ПриватБанк» у впровадженні FinTech рішень

FinTech	ПриватБанк	Ощадбанк	Monobank	Райффайзен Банк Аваль	ПУМБ
Канали обслуговування					
Мобільний банкінг	Дуже розвинений	Розвивається, оновлений додаток	Перший мобільний банк в Україні	Стабільний додаток з базовими функціями	Розвинений мобільний додаток
Інтернет-банкінг	Один із найбільш функціональних	З держпослугами	Повний онлайн-сервіс без відділень	Для корпоративних клієнтів	Повний спектр онлайн-послуг
Технології безпеки					
Біометрія	Використовується у додатку	Поступово впроваджується	Повністю підтримується	Часткова підтримка	Працює у мобільному додатку
Кібербезпека (2FA, шифрування)	Дуже високий рівень	Високий рівень, 2FA	2FA та біометрія	Розвинені системи безпеки	Високий рівень, 2FA
Інноваційні інструменти					
Чат-боти / AI-підтримка	AI-чат-бот у додатку	Частково впроваджено	Активно використовуються	Базова підтримка	AI для швидкої підтримки
Big Data / Аналітика	Персоналізація	Початковий етап	Високий рівень персоналізації	Корпоративна аналітика	Скоринг та покращення послуг
AI у процесингу	Виявлення шахрайства	Початковий етап	Активно використовується	Ризик-менеджмент	Боротьба з шахрайством
Доступність і інклюзія					
Цифрові кредити	Швидке оформлення у додатку	Впроваджується	Повністю цифровий процес	Для бізнесу	Швидке оформлення
Інклюзивні послуги	Програми для малозабезпечених	Державні програми	Орієнтація на масового клієнта	Для бізнесу	Підтримка малозабезпечених
Відкриті сервіси					
Краудфандинг / P2P	Обмежено	Відсутні	Відсутні	Відсутні	Відсутні
Open Banking / API	API для сторонніх сервісів	Початкові етапи	Відсутні	Для корпоративних клієнтів	API для партнерів

* запропоновано автором на основі [19; 20]

Водночас результативність цифрової трансформації визначається не лише внутрішніми ресурсами банків, але й якістю інституційного середовища.

Ключове значення мають формування гнучкої регуляторної бази для розвитку фінансових технологій, розширення цифрової інклюзії, підвищення стандартів інформаційної безпеки та підтримка створення національних технологічних рішень, що знижують залежність від глобальних IT-платформ. У цьому аспекті «ПриватБанк» виступає одним із флагманів впровадження інновацій, задаючи орієнтири для інших учасників ринку.

Сучасні фінансові технології не замінюють класичний банкінг, а трансформують його, формуючи нову модель функціонування фінансових інституцій. На прикладі «ПриватБанку» можна спостерігати перехід до комплексної цифрової екосистеми, у межах якої взаємодія «банк–клієнт» набуває безперервного, персоналізованого та технологічно інтегрованого характеру. Це забезпечує підвищення рівня клієнтоорієнтованості, операційної ефективності та безпеки.

Для порівняльного аналізу рівня цифровізації банківського сектору доцільно розглядати не лише «ПриватБанк», але й інші провідні установи, зокрема АТ «Ощадбанк», Monobank, АТ «Райффайзен Банк Аваль» та АТ «ПУМБ». Водночас саме «ПриватБанк» вирізняється найбільш комплексним підходом до впровадження фінтех-рішень, поєднуючи розвинену інфраструктуру, масштабну клієнтську базу та активне використання інструментів штучного інтелекту.

Аналіз практики застосування фінансових технологій у провідних банках України дозволяє виокремити такі узагальнення. Monobank функціонує як повністю цифровий банк, орієнтований на мобільний формат обслуговування, що забезпечує високу гнучкість і швидкість операцій. Водночас АТ КБ «ПриватБанк» є системоутворюючим лідером цифрової трансформації, який інтегрує широкий спектр інноваційних продуктів, активно використовує аналітику даних і технології штучного інтелекту, а також забезпечує високий рівень кіберзахисту. АТ «Ощадбанк» поступово модернізує свою діяльність, поєднуючи традиційні функції із впровадженням цифрових сервісів. АТ «ПУМБ» розвиває цифрові продукти з акцентом на роздрібний сегмент і МСП,

тоді як АТ «Райффайзен Банк Аваль» дотримується більш консервативної стратегії, зосереджуючись на стабільності та корпоративному обслуговуванні.

Таким чином, саме АТ КБ «ПриватБанк» разом із Monobank формують ядро цифрової трансформації банківської системи України, демонструючи найвищий рівень інтеграції фінтех-інновацій, що визначає вектор подальшого розвитку всього фінансового сектору.

За результатами проведеного аналізу встановлено, що банківські установи України демонструють послідовне прагнення до розширення спектра цифрових фінансових сервісів, що супроводжується різною швидкістю та глибиною їх впровадження. Водночас спостерігається диференціація рівнів цифрової зрілості, що зумовлює відмінності у стратегічних підходах до трансформації та технологічних пріоритетах. У цьому контексті особливу увагу привертає діяльність АТ КБ «ПриватБанк», який завдяки масштабній цифровій інфраструктурі та інноваційній політиці виступає одним із ключових орієнтирів розвитку для всього банківського сектору.

Зазначені тенденції узгоджуються із загальною динамікою поширення цифрових фінансових послуг в Україні, що проявляється у стійкому збільшенні кількості користувачів інтернет- та мобільного банкінгу. Це свідчить про поступове формування довіри населення до дистанційних каналів обслуговування та зміну моделей фінансової поведінки у бік цифровізації.

Опрацювання наведених даних дозволяє зробити висновок про наявність стійкої висхідної тенденції зростання кількості користувачів цифрових сервісів у всіх досліджуваних банках. При цьому беззаперечним лідером за масштабами охоплення клієнтської бази залишається АТ КБ «ПриватБанк», який забезпечує найвищі показники завдяки ефективному функціонуванню екосистеми «Приват24» та постійному вдосконаленню цифрових продуктів.

У межах цих трансформацій доцільним є представлення узагальненої порівняльної характеристики змін кількості користувачів цифрових банківських сервісів у провідних банках України протягом 2019–2024 рр. (табл. 2.2):

Таблиця 2.2

Динаміка користувачів інтернет- та мобільного банкінгу в українських банківських установах

Банк	2019	2020	2021	2022	2023	2024	Примітки
АТ КБ «Приватбанк»	~10 млн	~12 млн	~13 млн	~14 млн	~15 млн	~15 млн	Мобільний додаток «Приват24»
АТ «Ощадбанк»	~3 млн	~3,5 млн	~4,5 млн	~5 млн	~5,5 млн	~4,6 млн	Мобільний додаток «Мобільний Ощад»
Monobank	~1 млн	~2,9 млн	~4,5 млн	~6 млн	~7,9 млн	~10 млн	Мобільний банк без відділень
АТ «ПУМБ»	~0,8 млн	~1 млн	~1,3 млн	~1,5 млн	~1,8 млн	~2 млн	Активний розвиток цифрових сервісів
АТ «Райффайзен Банк»	~0,1 млн	~0,2 млн	~0,3 млн	~0,5 млн	~1 млн	~1,7 млн	Зростання у 2024 році

* сформовано на основі [17]

Зростання популярності дистанційного банкінгу відображає не лише технологічний прогрес, але й трансформацію споживчих уподобань, орієнтованих на швидкість, доступність і зручність фінансових операцій. У цьому процесі саме «ПриватБанк» відіграє провідну роль, формуючи нові стандарти якості обслуговування та впроваджуючи інноваційні підходи до взаємодії з клієнтами.

Крім того, важливим напрямом розвитку є забезпечення фінансової інклюзії, що передбачає розширення доступу до банківських послуг для мешканців віддалених територій та соціально вразливих категорій населення. Використання цифрових каналів дозволяє суттєво спростити доступ до фінансових операцій без фізичної присутності у відділеннях. У цьому аспекті АТ КБ «ПриватБанк» посідає провідні позиції, забезпечуючи високий рівень доступності, функціональності та безперервності цифрового обслуговування.

Узагальнені дані засвідчують стале зростання використання онлайн-банкінгу в Україні як серед населення, так і бізнесу. Кількість фізичних осіб-користувачів зросла з 44,2 млн у 2021 р. до 66,51 млн у 2024 р. (+66,5%), що відображає активне поширення цифрових фінансових сервісів. У корпоративному сегменті також спостерігається позитивна динаміка: кількість бізнес-клієнтів збільшилася з 2,3 млн до 3,01 млн (+76,4%), що свідчить про інтеграцію онлайн-банкінгу у фінансове управління підприємств. Таким чином, цифровий банкінг демонструє інтенсивний розвиток і зростання довіри користувачів до дистанційних фінансових послуг (рис. 2.5).

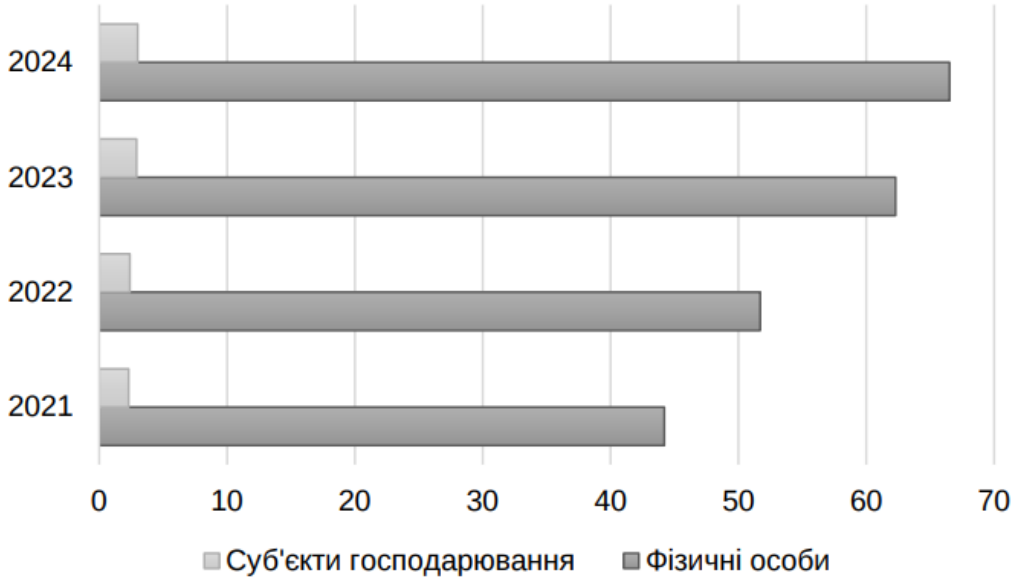

Рис. 2.5. Динаміка використання дистанційних банківських сервісів в Україні за 2021–2024 рр.

* побудовано за даними [18]

У відповідь на зростання попиту банки активізують інвестиції в IT-інфраструктуру та цифрові платформи, впроваджуючи програми лояльності, кешбек і мобільно-орієнтовані сервіси. Водночас поширюється використання біометричної автентифікації, що підвищує безпеку та зручність доступу до послуг.

За даними НБУ, обсяг безготівкових операцій зріс з 3099,1 млрд грн у 2021 р. до 4243,5 млрд грн у 2024 р., що підтверджує розширення використання фінансових технологій і зростання ролі безготівкових розрахунків (рис. 2.6).

Рис. 2.6. Динаміка безготівкових операцій за 2021–2024 рр

* побудовано за даними [21]

Дослідження структури безготівкових операцій в Україні показує, що перекази з картки на картку залишаються найбільш поширеним видом транзакцій, хоча їх обсяг дещо зменшився — з 1352 млрд грн у 2021 р. до 1318,4 млрд грн у 2024 р. Аналогічне скорочення зафіксовано й у платежах на банківські рахунки (з 721,3 млрд грн до 622 млрд грн), що пов’язано з регуляторними обмеженнями НБУ.

Натомість інші сегменти демонструють зростання, зокрема розрахунки через платіжні термінали, обсяг яких збільшився з 878,8 млрд грн до 1985 млрд грн, що свідчить про поширення безконтактних платежів і підвищення довіри до цифрових інструментів.

Паралельно змінюється структура каналів обслуговування: поряд із традиційними відділеннями зростає використання мобільних застосунків, онлайн-банкінгу та чат-ботів (рис. 2.7):

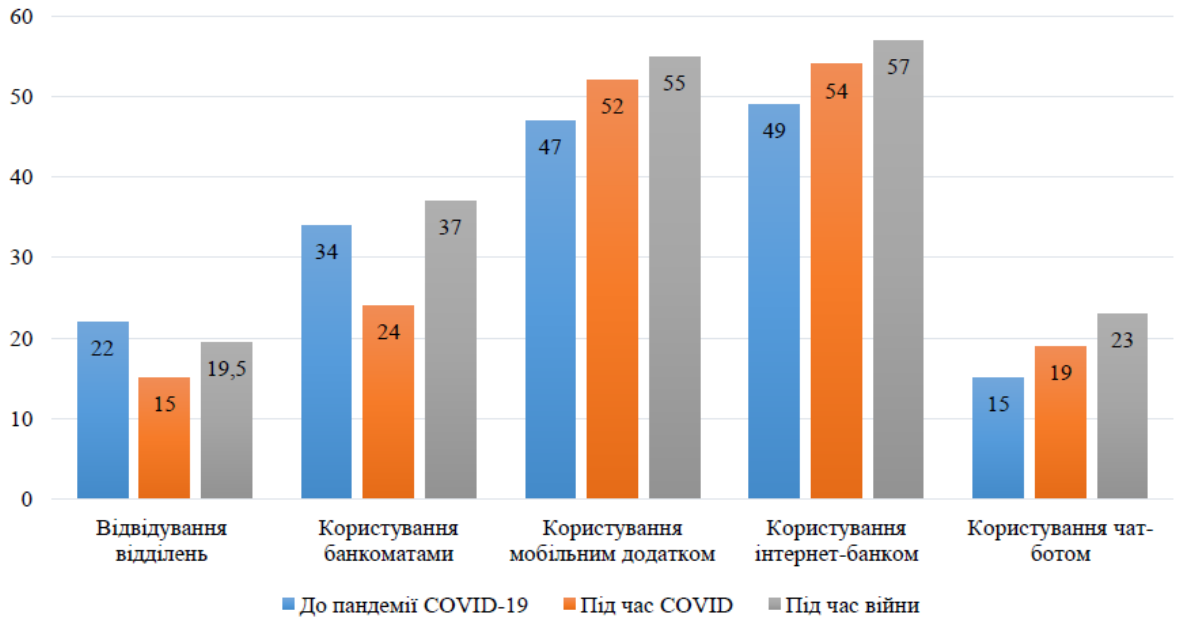

Рис. 2.7. Структура використання банківських каналів обслуговування клієнтами в Україні у 2019–2024 рр.

* побудовано за даними [16; 17]

Рівень цифровізації банків у більшості країн Європи залишається вищим, ніж в Україні, однак вітчизняний банківський сектор демонструє швидке зростання навіть в умовах війни та економічної нестабільності. Це свідчить про його здатність адаптуватися до зовнішніх викликів і формує передумови для поступового наближення до європейських стандартів якості та безпеки фінансових послуг.

Паралельно з розвитком цифрового банкінгу зростають ризики шахрайства, особливо у сфері дистанційного обслуговування. У 2024 році глобальні втрати банків від фінансових шахрайств досягли 45 млрд дол. США, тоді як інвестиції у системи антифрод-захисту становили 12,6 млрд дол. (+20% за рік). В Україні збитки перевищили 1,7 млрд грн, причому близько 80% випадків припадає на фішинг і соціальну інженерію.

Кількість фішингових ресурсів стрімко зростає: понад 11 тис. у 2024 році проти 4500 у 2023 році, при цьому близько 68% мають російське походження. Середня сума шахрайської операції становила 3065 грн (+39% до 2022 р.), а

83% інцидентів відбувалися онлайн. У більшості випадків причиною втрат є розголошення користувачами конфіденційних даних під впливом маніпуляцій.

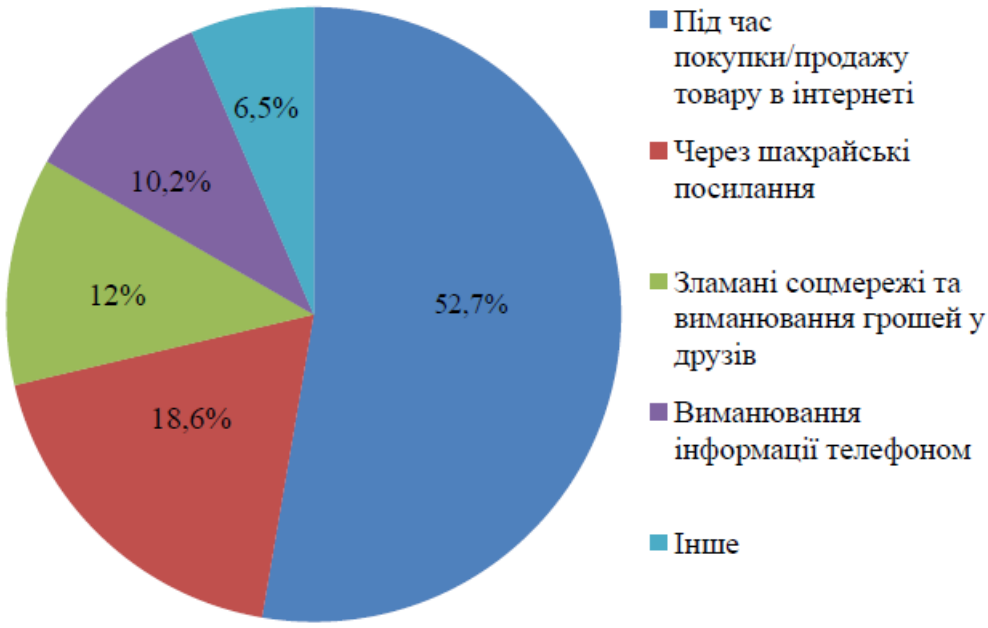

Рис. 2.8. Динаміка та структура шахрайських операцій в Україні з початку повномасштабної війни, %

* побудовано за даними [15]

У 2024 році фішинг остаточно сформувався як домінуючий інструмент кіберзлочинності в Україні: зафіксовано 4315 інцидентів, що майже на 70% перевищує показник попереднього року . Значна частина атак була спрямована на клієнтів банків і супроводжувалася використанням шкідливого програмного забезпечення та підроблених комунікацій. Водночас традиційні шахрайські практики, зокрема скімінг, поступово втрачають ефективність, що зумовлено поширенням безконтактних і токенізованих карток: їх кількість досягла відповідно 35 млн і 16,5 млн одиниць, що становить близько 60% активних платіжних інструментів . Це сприяє переорієнтації шахрайських схем у цифрове середовище.

Паралельно фіксується зростання смішинг-атак (приблизно 60 тис. випадків) та телефонного шахрайства, яке охоплює близько 38% інцидентів . При цьому спостерігається суттєве підвищення середніх сум втрат: у 2024 році вони зросли до 50–150 тис. грн проти 15–25 тис. грн у 2022 році . Вагомим

сегментом залишається шахрайство у сфері електронної комерції — понад 22 тис. звернень і близько 440 млн грн збитків, що підтверджує масштабність і диверсифікацію кіберризиків .

Водночас посилюється інституційна та технологічна протидія: у 2024 році заблоковано 44,8 тис. фішингових ресурсів і понад 2,1 тис. шахрайських телефонних номерів, а обсяг відшкодованих збитків зріс у 6,4 раза, досягнувши 44,5 млн грн . Банківські установи активно впроваджують багаторівневі системи захисту, зокрема двофакторну автентифікацію (яка дозволяє запобігти до 95% атак), біометричну ідентифікацію та алгоритми машинного навчання для виявлення підозрілої активності.

Таким чином, сучасний розвиток цифрового банкінгу супроводжується одночасним зростанням кіберризиків і підвищенням ефективності механізмів їх нейтралізації. У цьому контексті доцільним є подальший поглиблений аналіз діяльності АТ КБ «ПриватБанк», який завдяки поєднанню масштабної цифрової інфраструктури, інноваційних антифрод-рішень і активної взаємодії з регуляторами формує один із найбільш ефективних підходів до забезпечення фінансової безпеки в Україні.

У контексті дослідження впливу FinTech-інновацій на рівень кіберризиків і фінансової безпеки банківського сектору особливої ваги набуває комплексна оцінка фінансового стану окремих банківських установ. Такий підхід дозволяє не лише визначити рівень їхньої стійкості до зовнішніх викликів, але й оцінити ефективність інтеграції цифрових технологій у систему управління ризиками, виявити вразливості та сформувати напрями підвищення фінансової безпеки.

З огляду на це, доцільним є аналіз діяльності АТ КБ «ПриватБанк» як системно важливої фінансової установи, що виступає одним із лідерів цифрової трансформації банківського сектору України. Його стратегія спрямована на активне впровадження FinTech-рішень, що забезпечують розширення дистанційних каналів обслуговування, підвищення ефективності операційних процесів і одночасно формують нові кіберризики, які потребують належного управління.

Базовим інструментом дослідження фінансової стійкості банку є його баланс, який відображає структуру активів, зобов'язань і власного капіталу. Аналіз динаміки та структури активів дозволяє оцінити ефективність використання ресурсів у умовах цифровізації, визначити рівень прибутковості та здатність банку протидіяти фінансовим і кібернетичним загрозам.

Активи, як ключове джерело формування доходів, виступають індикатором того, наскільки ефективно банк адаптує свою діяльність до умов цифрової економіки та інтегрує інноваційні технології у систему забезпечення фінансової безпеки.

Таблиця 2.3

Динаміка формування активів, зобов'язань і власного капіталу АТ КБ «ПриватБанк» за 2021–2024 роки

Показник	2021	2022	2023	2024	Темп приросту, % 2022/2021	Темп приросту, % 2023/2022	Темп приросту, % 2024/2023
Активи, млн грн	401296	540596	680008	761700	34.7%	25.8%	12.1%
Зобов'язання, млн грн		482807	595162	-	-	23.3%	-
Власний капітал, млн грн	66615	57589	84846	99144	−13.5%	+47.4%	+16.9%

У межах дослідження впливу FinTech-інновацій на рівень кіберризиків і фінансової безпеки банків доцільним є аналіз трансформації фінансової структури АТ КБ «ПриватБанк» у 2021–2024 рр., що відображає результати цифровізації та зміни ризик-профілю установи.

Динаміка активів свідчить про їх суттєве зростання: з 401,3 млрд грн у 2021 р. до 761,7 млрд грн у 2024 р., при цьому темпи приросту поступово знижувалися (34,7% – 25,8% – 12,1%), що вказує на перехід від фази інтенсивного розширення до стабілізації. Одночасно відбулися структурні зміни: частка високоліквідних активів зросла (до понад 22%), тоді як питома

вага цінних паперів скоротилася (з понад 55% до близько 40%), що може інтерпретуватися як підвищення гнучкості управління ресурсами в умовах цифрової трансформації.

У структурі зобов'язань домінують кошти клієнтів (понад 90%), що підтверджує високу довіру до банку та ефективність цифрових каналів залучення ресурсів. У 2024 році депозитна база додатково зросла більш ніж на 10%, що є індикатором посилення ринкових позицій банку.

Динаміка власного капіталу характеризується відновленням після скорочення у 2022 р. (−13,5%) та подальшим зростанням у 2023–2024 рр. (+47,4% та +16,9%). Чистий прибуток у 2024 році перевищив 40 млрд грн, що сприяло зміцненню фінансової стійкості.

Таким чином, впровадження FinTech-рішень у діяльність АТ КБ «ПриватБанк» супроводжується не лише зростанням масштабів операцій, але й оптимізацією структури активів і підвищенням ліквідності, що позитивно впливає на фінансову безпеку. Водночас розширення цифрових сервісів обумовлює необхідність посилення систем кіберзахисту, що визначає подальші напрями дослідження.

З огляду на роль банків у забезпеченні макрофінансової стабільності, комплексний аналіз їх фінансового стану є важливим для оцінки стійкості в умовах цифровізації та зростання кіберризиків. Він дозволяє виявити сильні сторони, ризики та ефективність управління ресурсами.

У цьому контексті проаналізовано діяльність АТ КБ «ПриватБанк», зокрема динаміку активів, зобов'язань, грошових потоків і кредитного портфеля за 2021–2024 рр. (табл. 2.4), що дає змогу оцінити фінансову стійкість і трансформацію ризик-профілю банку під впливом FinTech-інновацій.

Грошові потоки як індикатор ліквідності свідчать про підвищення операційної ефективності та оптимізацію діяльності банку, що пов'язано з впровадженням цифрових технологій і вдосконаленням управління ризиками.

Таблиця 2.4

Аналіз динаміки руху грошових коштів АТ КБ «ПриватБанк», млн грн

Показник (млн грн)	2021	2022	2023	2024	Абсолютне відхилення 2022/2021	Абсолютне відхилення 2023/2022	Абсолютне відхилення 2024/2023
Грошові потоки до змін в опер. активах/зобов. (входи)	36910	50039	69103	84500	+13129	+19064	+15397
Чисті грошові кошти, отримані від операційної діяльності	39169	79585	92121	106500	+40416 (103,18%)	+12536 (15,75%)	+14379 (15,6%)
Чисті грошові кошти, отримані/використані в інвестиційній діяльності	(14167)	(18267)	(15405)	(16500)	−4100 (28,94%)	+2862 (−15,67%)	−1095 (-7,1%)
Чисті грошові кошти, використані у фінансовій діяльності	(20178)	(28566)	(22374)	(24000)	−8388 (41,57%)	+6192 (−21,68%)	−1626 (−7,3%)

У контексті оцінки впливу FinTech-інновацій на фінансову безпеку банків важливим є аналіз динаміки грошових потоків АТ КБ «ПриватБанк» (табл. 2.4), який відображає рівень операційної стійкості та ефективність управління ресурсами.

Операційні грошові потоки банку демонструють стійке зростання: з 36,9 млрд грн у 2021 р. до 84,5 млрд грн у 2024 р. (+129%), що свідчить про розширення клієнтських операцій і активне використання цифрових каналів обслуговування. Чистий грошовий потік від операційної діяльності зріс із 39,2 млрд грн до 106,5 млрд грн, при цьому найбільш суттєвий приріст зафіксовано у 2022 році (+103%), а в подальшому темпи стабілізувалися на рівні близько 15–16%. Це підтверджує підвищення ефективності бізнес-моделі банку та його здатність генерувати внутрішні фінансові ресурси.

Інвестиційна діяльність характеризується стабільно від'ємним сальдо (у межах −14–18 млрд грн), що є типовим для банків і відображає фінансування довгострокових проєктів та модернізацію інфраструктури.

Водночас у 2023–2024 рр. спостерігається оптимізація інвестиційної активності. Подібна динаміка простежується і у фінансовій діяльності: після зростання відтоків у 2022 році (−28,6 млрд грн) у наступні роки відбулося їх скорочення до −24 млрд грн, що свідчить про стабілізацію джерел фінансування.

Загалом результати аналізу підтверджують зміцнення фінансової стійкості ПриватБанку, підвищення операційної ефективності та вдосконалення управління грошовими потоками.

Зростання операційних надходжень у поєднанні з контрольованими відтоками формує надійну основу фінансової безпеки банку в умовах цифровізації. Це створює підґрунтя для подальшого аналізу структури кредитного портфеля та оцінки ризиків у табл. 2.5.

Таблиця 2.5

Структура клієнтського кредитного портфеля (млн грн)

Показник	2021	2022	2023	2024	Абс. відхил. 2024/2021
Кредити та дебіторська заборгованість за фінансовим лізингом (окремий портфель)	163513	167931	170042	172000	+8487
Кредити фізичним особам	61727	55103	70914	82000	+20273
Кредити юридичним особам та МСБ (сукупно, основні сектори)	17328	26462	31961	38800	+21472
Всього кредити та аванси клієнтам (брутто)	242568	250496	274917	112800	-129768

Аналіз динаміки кредитного портфеля АТ КБ «ПриватБанк» у 2021–2024 рр. свідчить про його структурну трансформацію під впливом FinTech-інновацій та необхідності мінімізації кредитних і кіберризиків. Банк реалізує

стратегію збалансованого кредитування, орієнтуючись на роздрібний сегмент і фінансування малого та середнього бізнесу.

Обсяг кредитів і лізингових операцій зріс помірно — з 163,5 млрд грн до 172 млрд грн (+5,2%), що вказує на стабільність низькоризикового сегмента. Водночас кредитування фізичних осіб продемонструвало більш динамічне зростання — з 61,7 млрд грн до 82 млрд грн (+32,8%), що є результатом активного розвитку цифрових продуктів (онлайн-кредитування, кредитні картки, «оплата частинами») та використання скорингових моделей.

Найвищі темпи приросту зафіксовано у сегменті МСБ і корпоративного кредитування — з 17,3 млрд грн до 38,8 млрд грн (+124%), що свідчить про розширення участі банку у фінансуванні реального сектору та реалізацію державних програм підтримки економіки. Водночас зниження загального обсягу кредитів у 2024 р. (до 112,8 млрд грн) може відображати очищення балансу та підвищення якості активів.

Ключовими характеристиками кредитної політики банку є диверсифікація портфеля, зростання ролі роздрібного сегмента, підтримка МСБ та використання цифрових інструментів управління ризиками. Це дозволяє підвищити якість кредитного портфеля та знизити вразливість до фінансових і кібернетичних загроз.

Оцінка фінансової безпеки банку за 2022–2024 рр. підтверджує його стійкість: попри незначне зниження рентабельності, показники ROA і ROE залишаються вище середньоринкових. Частка непрацюючих кредитів скоротилася з 15,8% до 11,6%, а високий рівень адекватності капіталу (24,2%) забезпечує достатній запас міцності для протидії ризикам.

Таким чином, впровадження FinTech-рішень у кредитну діяльність ПриватБанку сприяє підвищенню ефективності, покращенню якості активів і зміцненню фінансової безпеки, що створює основу для подальшого аналізу ключових фінансових показників (табл. 2.6).

Таблиця 2.6

Показники фінансової безпеки АТ КБ «ПриватБанк» у 2022–2024 рр.

Назва показника	Норматив	2022	2023	2024	Відхилення 2024/2022
Рентабельність активів (ROA), %	≥ 1%	2,15	2,03	1,92	-0,23
Рентабельність капіталу (ROE), %	≥ 10%	27,50	23,80	19,40	-8,10
Частка непрацюючих кредитів (NPL), %	≤ 5%	15,80	13,10	11,60	-4,20
Норматив адекватності регулятивного капіталу (Н2), %	≥ 10%	22,60	23,10	24,20	+1,60
Коефіцієнт ліквідності (LCR), %	≥ 100%	245,00	312,00	296,00	+51,00
Чистий прибуток, млрд грн	-	30,26	37,80	45,20	+14,94

Надмірно високий рівень ліквідності (LCR понад 290%) свідчить про наявність значного запасу платоспроможності, що забезпечує здатність банку виконувати короткострокові зобов’язання навіть у кризових умовах. Водночас зростання чистого прибутку з 30,26 млрд грн до 45,2 млрд грн підтверджує ефективність управління активами та результативність обраної бізнес-моделі.

Загалом рівень фінансової безпеки АТ КБ «ПриватБанк» оцінюється як високий, що дозволяє йому виконувати системоутворюючу роль у банківському секторі України та підтримувати довіру клієнтів у складних макроекономічних умовах.

Комплексна оцінка ефективності управління фінансовою безпекою передбачає аналіз ключових індикаторів ліквідності, достатності капіталу та стабільності ресурсної бази, які відображають здатність банку зберігати стійкість у коротко- та довгостроковій перспективі. У цьому контексті доцільно розглянути динаміку нормативів ліквідності АТ КБ «ПриватБанк» за 2022–2024 рр., представлену в табл. 2.7:

Таблиця 2.7

Динаміка нормативів ліквідності АТ КБ «ПриватБанк» за 2022–2024 роки

Норматив ліквідності	2022, %	2023, %	2024, %	Абсолютне відхилення (+/–), % (2023/2022; 2024/2023)	Граничне значення нормативу
Норматив короткострокової ліквідності (Н6)	71,35	70,10	73,50	–1,25; +3,40	Не менше 60 %
Коефіцієнт покриття ліквідністю (LCR) за всіма валютами	295,60	340,28	388,91	+44,68; +48,63	Понад 100 %
Норматив стабільного фінансування (NSFR)	165,84	178,72	183,15	+12,88; +4,43	Не менше 100 % (з 01.04.2023)
Рівень достатності регулятивного капіталу (Н2)	16,91	18,05	21,46	+1,14; +3,41	Не менше 10 %

*узагальнено на основі звітності АТ КБ «ПриватБанк» та даних НБУ [5; 6]

Упродовж 2021–2024 рр. АТ КБ «ПриватБанк» забезпечував стійке дотримання нормативів ліквідності, що свідчить про ефективне управління ресурсною базою в умовах зростання цифрових ризиків. Зокрема, станом на 01.01.2025 р. норматив короткострокової ліквідності (Н6) становив 73,5%, перевищуючи вимогу регулятора на 13,5 п.п., тоді як показник LCR досяг 388,9%, більш ніж утричі перевищивши мінімальний рівень. Це підтверджує наявність значного обсягу високоліквідних активів для покриття короткострокових зобов’язань. Показник стабільного фінансування (NSFR) у 2024 р. становив 183,2%, що майже вдвічі перевищує норматив і свідчить про збалансовану структуру пасивів та орієнтацію на довгострокову стійкість. Водночас рівень достатності капіталу (Н2) зріс до 21,4%, що більш ніж удвічі перевищує мінімально допустиме значення та формує значний запас фінансової міцності.

Високий рівень ліквідності забезпечується значною часткою ліквідних активів, зокрема державних облігацій, депозитних сертифікатів НБУ та коштів на коррахунках, що дозволяє банку оперативно реагувати на зміни ринкової

ситуації та потенційні відтоки ресурсів. Паралельно спостерігається зростання прибутковості: чистий прибуток у 2024 р. перевищив 40 млрд грн (+6%), що супроводжується збільшенням депозитної бази більш ніж на 10%.

Узагальнюючи, АТ КБ «ПриватБанк» демонструє високий рівень фінансової безпеки, що базується на поєднанні значної ліквідності, достатньої капіталізації та ефективного управління активами і пасивами. Така модель забезпечує стійкість банку до макроекономічних і кіберризиків, що особливо важливо в умовах активної цифровізації фінансового сектору.

Узагальнюючи результати проведеного аналізу, слід зазначити, що впровадження FinTech-інновацій у діяльність АТ КБ «ПриватБанк» має комплексний і системний вплив на рівень фінансової безпеки та кіберризиків. З одного боку, цифрова трансформація забезпечує суттєве підвищення операційної ефективності, зростання прибутковості, розширення клієнтської бази та оптимізацію структури активів і грошових потоків. З іншого — активне використання дистанційних каналів обслуговування обумовлює посилення кіберзагроз, що вимагає постійного вдосконалення механізмів захисту.

Фінансові показники банку свідчать про його високу стійкість: значний рівень ліквідності, достатності капіталу та стабільності ресурсної бази формують надійний запас фінансової міцності. Одночасно трансформація кредитного портфеля, зростання ролі роздрібного сегмента та активізація кредитування МСБ відображають адаптацію бізнес-моделі банку до умов цифрової економіки та підвищення ефективності управління ризиками.

Важливою особливістю є інтеграція інноваційних технологій у систему ризик-менеджменту, зокрема використання скорингових моделей, біометричної автентифікації, антифрод-систем та алгоритмів машинного навчання, що дозволяє мінімізувати фінансові втрати та підвищувати рівень кіберзахисту. Це забезпечує баланс між розширенням цифрових сервісів і контролем ризиків.

Таким чином, АТ КБ «ПриватБанк» виступає прикладом ефективної адаптації банківської установи до викликів цифровізації, поєднуючи інноваційний розвиток із високим рівнем фінансової безпеки.

РОЗДІЛ 3
СТРАТЕГІЧНІ НАПРЯМИ ПОСИЛЕННЯ КІБЕРБЕЗПЕКИ БАНКІВСЬКОГО СЕКТОРУ В СИСТЕМІ FINTECH

3.1. Використання штучного інтелекту, Big Data та цифрових платформ у зміцненні кіберстійкості банків

Сучасний банківський сектор функціонує в умовах інтенсивних цифрових змін, зумовлених розвитком фінансових технологій, посиленням вимог до кібербезпеки та необхідністю підвищення ефективності операційної діяльності. У цих умовах важливим чинником конкурентоспроможності банків стає впровадження інноваційних рішень, зокрема технологій штучного інтелекту, Big Data та цифрових платформ, які трансформують бізнес-моделі та підходи до управління даними і взаємодії з клієнтами.

Разом із тим цифровізація супроводжується зростанням кіберризиків, пов’язаних із обробкою значних обсягів конфіденційної інформації та розширенням онлайн-операцій. Це зумовлює необхідність формування комплексних механізмів кіберстійкості, що поєднують інтелектуальний аналіз даних, автоматизований моніторинг і адаптивне реагування на загрози. У цьому контексті штучний інтелект виступає не лише інструментом підвищення ефективності, а й ключовим елементом системи інформаційної безпеки.

Представлений на рисунку підхід відображає структурно-функціональну модель використання технологій штучного інтелекту в банківській системі за трьома основними напрямами: аналітичним, клієнтоорієнтованим та операційним. Аналітичний блок охоплює машинне навчання, прогнозну аналітику та AI-ризик-менеджмент, що забезпечують оцінку ризиків і виявлення фінансових загроз. Клієнтоорієнтований сегмент включає технології обробки природної мови, рекомендаційні системи та голосові інтерфейси, спрямовані на персоналізацію послуг. Операційний рівень представлений RPA,

комп'ютерним зором і генеративними моделями, які оптимізують внутрішні процеси та автоматизують обробку інформації.

Важливу роль відіграє інтеграційний рівень, що поєднує можливості штучного інтелекту з блокчейн-технологіями, забезпечуючи підвищення прозорості, безпеки даних і автоматизацію фінансових операцій через смарт-контракти.

Комплексне впровадження зазначених технологій формує системний ефект, що проявляється у зниженні ризиків, підвищенні ефективності, оптимізації витрат і зростанні клієнтської лояльності. Це дозволяє банкам оперативно реагувати на кіберзагрози та забезпечувати стійке функціонування в умовах цифрової економіки.

Таким чином, рис.3.1 показує інтеграцію штучного інтелекту, Big Data та цифрових платформ у систему кіберстійкості банків як ключовий чинник їх цифрової трансформації та безпеки.

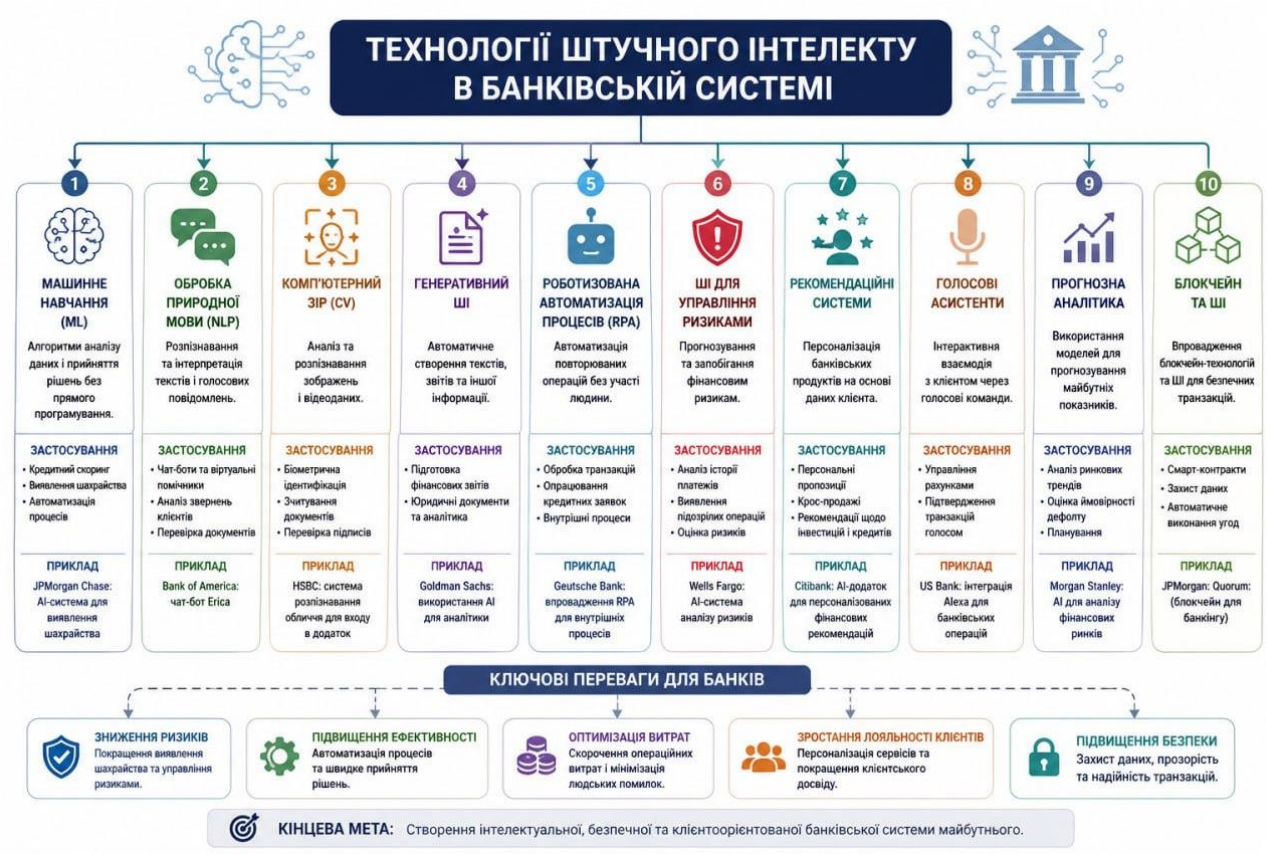

Рис. 3.1. Модель цифрової трансформації банківської кібербезпеки на основі штучного інтелекту та Big Data

* власна розробка автора

Інтеграція технологій штучного інтелекту, Big Data та цифрових платформ у банківську систему України набуває стратегічного значення в умовах цифрової трансформації фінансового сектору та посилення кіберзагроз. Як відображено на рис. 3.2, використання інтелектуальних технологій має системний характер і передбачає поєднання аналітичних, клієнтоорієнтованих та операційних рішень, що формують цілісну архітектуру забезпечення кіберстійкості банків.

Рис. 3.2. Алгоритм інтеграції технологій штучного інтелекту, Big Data та цифрових платформ у систему забезпечення кіберстійкості банків

* власна розробка

У цьому контексті процес впровадження штучного інтелекту доцільно розглядати як послідовний багаторівневий механізм, що інтегрується в загальну модель цифрової трансформації. На початковому етапі здійснюється ідентифікація ключових бізнес-потреб і визначення стратегічних орієнтирів використання AI, що узгоджується з аналітичним рівнем моделі, представленої

на рисунку. Подальший вибір технологій (ML, NLP, CV, RPA тощо) та цифрових платформ забезпечує формування технологічної бази для реалізації як клієнтоорієнтованих, так і операційних функцій банку.

Важливим елементом є формування якісного дата-середовища, що включає збір, очищення та структуризацію великих масивів даних. Саме на цьому етапі закладаються основи ефективності аналітичних інструментів і водночас забезпечується інформаційна безпека, що є критичною складовою кіберстійкості. Подальша розробка та навчання моделей штучного інтелекту дозволяє реалізувати функції прогнозної аналітики, управління ризиками та виявлення аномальної активності, що відповідає аналітичному блоку моделі.

Інтеграція AI-рішень у банківську інфраструктуру, включаючи їх впровадження через API та цифрові платформи, забезпечує автоматизацію бізнес-процесів і підвищення ефективності операційної діяльності. Це корелює з операційним рівнем рисунка, де представлені технології RPA, комп'ютерного зору та генеративного штучного інтелекту. Водночас використання технологій обробки природної мови, рекомендаційних систем і голосових інтерфейсів сприяє розвитку клієнтоорієнтованого сегмента, забезпечуючи персоналізацію банківських послуг.

Особливу роль у забезпеченні кіберстійкості відіграє інтеграційний рівень, що поєднує можливості штучного інтелекту з блокчейн-технологіями. Така синергія дозволяє підвищити прозорість фінансових операцій, забезпечити захист даних та автоматизувати виконання контрактів, що значно знижує ризики шахрайства та несанкціонованого доступу.

Завершальні етапи впровадження передбачають масштабування, постійний моніторинг та оцінку ефективності AI-рішень, що забезпечує їх адаптацію до змін зовнішнього середовища та нових кіберзагроз. У результаті формується комплексний ефект, який проявляється у зниженні ризиків, оптимізації витрат, підвищенні швидкості обробки операцій і зростанні рівня довіри клієнтів.

Таким чином, представлений алгоритм інтеграції штучного інтелекту органічно доповнює концептуальну модель, наведену на рисунку, та демонструє практичний механізм реалізації технологій AI, Big Data і цифрових платформ у системі забезпечення кіберстійкості банківських установ.

Поряд із суттєвими перевагами, що відображені на рисунку, впровадження технологій штучного інтелекту в банківській діяльності супроводжується низкою ризиків і обмежень, які потребують системного врахування. Насамперед це значні фінансові витрати на розробку, інтеграцію та підтримку AI-рішень, а також необхідність модернізації IT-інфраструктури та адаптації бізнес-процесів до умов цифрової трансформації. Додатковим фактором є витрати, пов’язані з підготовкою персоналу та формуванням нових компетенцій у сфері роботи з інтелектуальними системами.

Як випливає з рисунка, поряд із економічними та операційними викликами особливого значення набувають інформаційно-безпекові та етичні аспекти. Інтелектуальні системи можуть виступати об’єктом цілеспрямованих кіберзагроз, що створює ризики компрометації даних і порушення безперервності банківських операцій. Крім того, алгоритмічні моделі здатні демонструвати упередженість або нестабільність результатів у разі зміни вхідних даних, що негативно впливає на якість управлінських рішень. Не менш важливим є ризик порушення конфіденційності клієнтської інформації, який безпосередньо впливає на рівень довіри до банківських установ.

У зв’язку з цим ефективна інтеграція штучного інтелекту, Big Data та цифрових платформ передбачає формування комплексної системи управління ризиками. Така система має включати розробку політик захисту даних, впровадження багаторівневого тестування та валідації моделей у стандартних і стресових умовах, створення механізмів оперативного реагування на кіберінциденти, а також використання інструментів інтерпретованості та контролю якості алгоритмів. Важливим елементом є також підвищення цифрової компетентності персоналу через спеціалізовані програми навчання.

Таким чином, як демонструє рис. 3.3, досягнення максимальної ефективності від впровадження технологій штучного інтелекту можливе лише за умови збалансування їх економічних переваг із потенційними ризиками. Це дозволяє забезпечити належний рівень кіберстійкості, дотримання етичних і правових норм, а також підтримання довіри клієнтів у процесі цифрової трансформації банківського сектору.

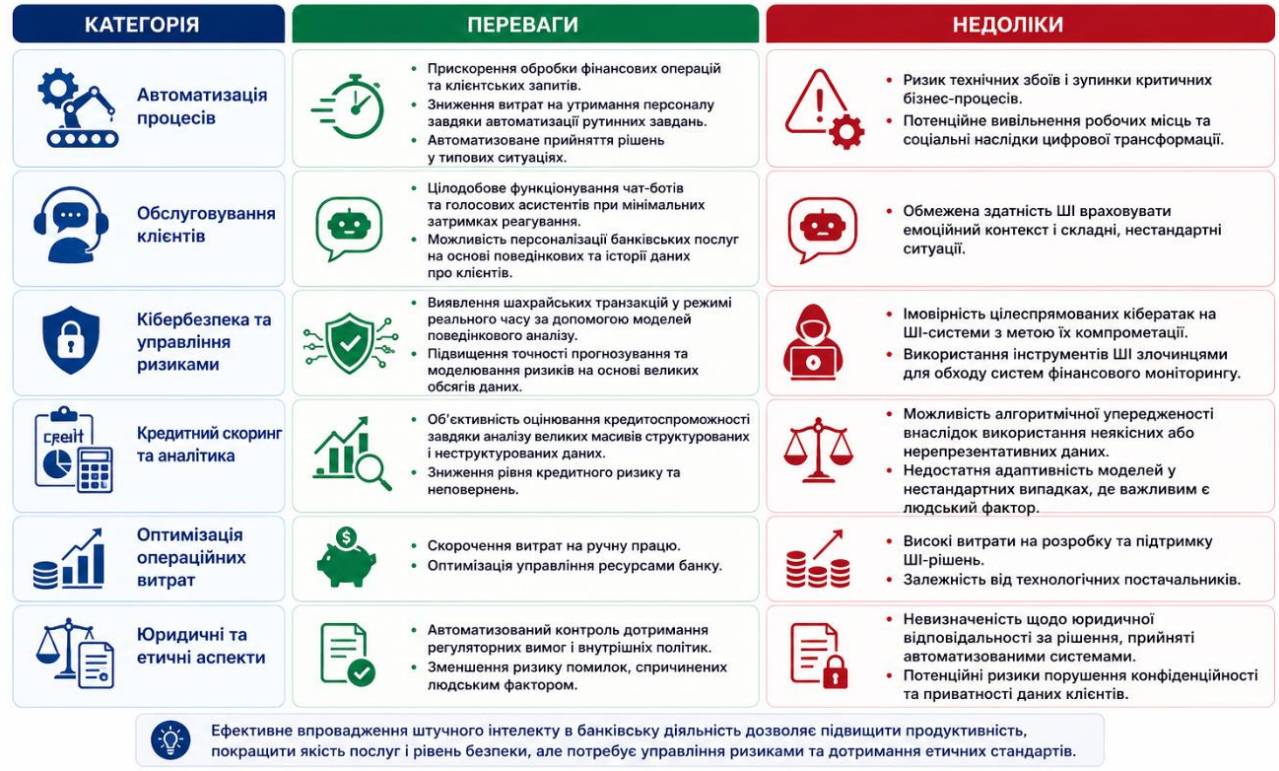

Рис.3.3. Порівняльна характеристика переваг і обмежень використання технологій штучного інтелекту в банківській діяльності

* систематизовано автором на основі [18; 19]

Отже, технології штучного інтелекту виступають одним із ключових драйверів трансформації банківського сектору, забезпечуючи підвищення ефективності операційної діяльності, посилення кіберзахисту та формування клієнтоорієнтованих фінансових сервісів. Незважаючи на наявність технологічних, регуляторних і безпекових викликів, впровадження інтелектуальних систем розглядається як стратегічний напрям розвитку банківських установ, що дозволяє підвищити їх конкурентоспроможність, оптимізувати бізнес-процеси та покращити якість обслуговування клієнтів.

В умовах сучасної України цифровізація банківської діяльності супроводжується активним впровадженням AI-рішень у ключові сфери функціонування банків, зокрема у платіжні системи, дистанційне обслуговування клієнтів, управління ризиками та забезпечення кібербезпеки. Застосування інтелектуальних чат-ботів і віртуальних асистентів дозволяє автоматизувати комунікацію з клієнтами, скоротити час реагування на запити та підвищити рівень сервісу. Водночас використання алгоритмів машинного навчання забезпечує ефективний моніторинг транзакцій у режимі реального часу, своєчасне виявлення аномальної активності та мінімізацію фінансових втрат від шахрайських операцій (рис. 3.4):

Рис. 3.4.Трансформація банківських послуг в Україні під впливом штучного інтелекту та машинного навчання

* систематизовано автором на основі [14; 15]

Аналіз представленого рис.3.4. свідчить, що застосування технологій штучного інтелекту в банківському секторі України має комплексний і багатовекторний характер, охоплюючи ключові напрями діяльності — клієнтський сервіс, кредитний скоринг, кібербезпеку та аналітику даних.

Водночас рівень імплементації інтелектуальних рішень відрізняється залежно від цифрової зрілості банківських установ та їх стратегічних пріоритетів.

Найбільш поширеним напрямом використання AI є автоматизація взаємодії з клієнтами через чат-боти та віртуальних асистентів. Це підтверджується практиками Ощадбанку, OTP Bank і ПУМБ, де інтелектуальні системи виконують функції первинної комунікації, обробки стандартних запитів і підтримки користувачів у цифрових каналах. Такий підхід дозволяє значно скоротити час обслуговування та оптимізувати навантаження на контакт-центри.

Водночас найбільш комплексну та технологічно просунуту модель використання штучного інтелекту демонструє ПриватБанк, який виступає лідером цифрової трансформації банківського сектору України. Особливістю його підходу є інтеграція AI-рішень одразу у декілька функціональних блоків: клієнтський сервіс (через екосистему Приват24), ризик-менеджмент, антифрод-системи та персоналізацію фінансових продуктів. Використання алгоритмів машинного навчання для аналізу поведінкових даних клієнтів дозволяє банку формувати індивідуалізовані пропозиції, підвищувати точність кредитного скорингу та оперативно реагувати на зміну фінансових ризиків.

Крім того, у ПриватБанк значну увагу приділено питанням кібербезпеки, де AI використовується для моніторингу транзакцій у режимі реального часу та виявлення аномальної активності. Такий підхід забезпечує формування адаптивної моделі захисту, здатної ефективно протидіяти сучасним кіберзагрозам та мінімізувати фінансові втрати від шахрайських операцій. У порівнянні з іншими банками, де AI здебільшого застосовується фрагментарно, ПриватБанк реалізує системну інтеграцію інтелектуальних технологій у всі ключові бізнес-процеси.

Важливим напрямом є також розвиток аналітичних інструментів і моделей оцінки ризиків, що простежується у практиці Monobank, де використовуються складні алгоритми (gradient boosting, нейромережі). Проте навіть у цьому сегменті ПриватБанк зберігає конкурентні переваги за рахунок

масштабності даних, розвиненої цифрової інфраструктури та інтеграції AI у повний цикл прийняття рішень.

Загалом результати оцінки підтверджують, що впровадження штучного інтелекту в банківській системі України сприяє підвищенню ефективності операцій, зміцненню кіберстійкості та покращенню якості обслуговування клієнтів. При цьому саме ПриватБанк формує еталонну модель цифрового банкінгу, в якій AI виступає не окремим інструментом, а інтегрованим елементом стратегічного розвитку та інноваційної екосистеми банку.

3.2. Формування інтегрованої системи управління кіберризиками в банківських установах

У сучасних умовах цифрової трансформації банківський сектор України виконує ключову роль у забезпеченні стабільності економіки, виступаючи важливим елементом критичної інфраструктури. Це зумовлює підвищені вимоги до надійності, безперервності функціонування та захисту від кіберзагроз.

Розвиток технологій Індустрії 4.0, зокрема штучного інтелекту, Big Data, хмарних сервісів і блокчейну, формує нові умови функціонування банків, водночас посилюючи складність і масштаб кіберризиків. У таких умовах кіберстійкість стає стратегічною складовою фінансової безпеки.

Міжнародна практика свідчить, що ефективне управління кіберризиками базується на комплексних підходах, які охоплюють ідентифікацію, попередження, виявлення та відновлення після кібератак. Важливими орієнтирами виступають стандарти NIST, ISO/IEC 27000 та рекомендації міжнародних фінансових інституцій, що забезпечують системність кіберзахисту.

Особливого значення набуває використання штучного інтелекту в управлінні кіберризиками. AI у поєднанні з Big Data дозволяє аналізувати

великі обсяги інформації в режимі реального часу, виявляти аномальні операції та прогнозувати загрози, забезпечуючи перехід до проактивної моделі кіберзахисту. Додатково застосування підходів, таких як TIBER-EU, дає змогу оцінити реальну стійкість банківських систем до кібератак.

У цьому контексті кіберстійкість доцільно визначати як здатність банку забезпечувати безперервність діяльності шляхом ефективної протидії, адаптації та відновлення після впливу кіберзагроз. Вона формується через поєднання превентивних, аналітичних і відновлювальних заходів із використанням цифрових технологій.

Представлений на рисунку підхід узагальнює концептуальні підходи до оцінки кіберстійкості, поєднуючи якісні та кількісні характеристики. Це дозволяє розглядати кіберстійкість як стратегічний параметр розвитку банку, що визначає його надійність, конкурентоспроможність і рівень довіри клієнтів.

Інтеграція штучного інтелекту, Big Data та цифрових платформ формує основу сучасної моделі управління кіберризиками, спрямованої на підвищення безпеки та адаптивності банківської діяльності (рис.3.5):

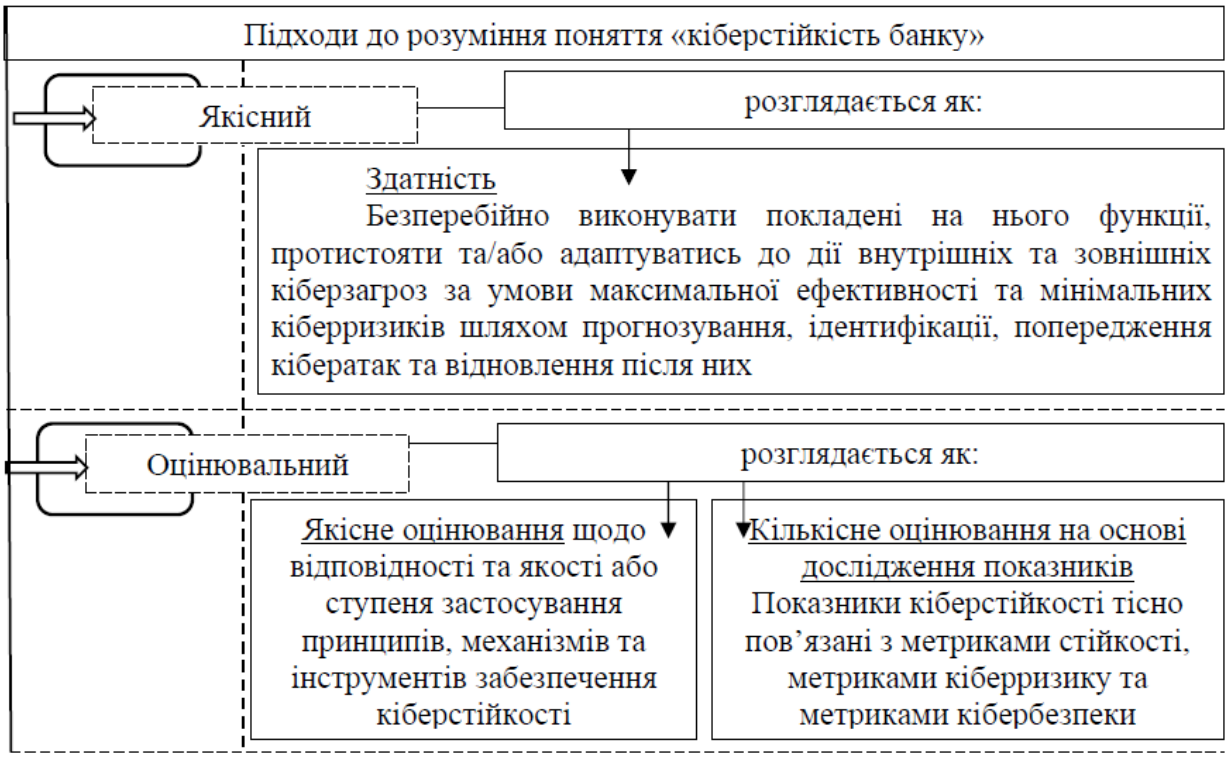

Рис. 3.5. Інтегрована оцінка підходів до формування поняття кіберстійкості банків [13]

Кіберстійкість банківських установ доцільно розглядати як багатовимірну характеристику, що поєднує якісний і кількісний підходи. Така інтеграція дозволяє комплексно оцінити здатність банку функціонувати в умовах зростання складності кіберзагроз та забезпечувати безперервність операційної діяльності.

Якісний аспект передбачає оцінювання рівня сформованості політик інформаційної безпеки, ефективності організаційних процедур та здатності банку оперативно реагувати на кіберінциденти.

В умовах поширення складних атак (DDoS, фішинг, ransomware) особливого значення набуває узгодженість процесів виявлення, локалізації та відновлення, що посилюється використанням технологій штучного інтелекту та Big Data.

Кількісний підхід базується на системі індикаторів, які відображають рівень захищеності та стійкості банку. До них належать технічні, аналітичні, управлінські, організаційні та регуляторні показники, включаючи відповідність стандартам NIST, ISO/IEC 27000, TIBER-EU та вимогам НБУ.

На основі цих критеріїв виокремлюються три рівні кіберстійкості: нормальний — із забезпеченням стабільності та контролю ризиків; низький — зі зростанням вразливості та уповільненням реагування; критичний — із порушенням функціонування та високими ризиками втрат.

Представлена на рисунку модель узагальнює ці підходи та відображає інтеграцію технічних, організаційних і регуляторних компонентів у систему управління кіберризиками. Використання AI, Big Data та цифрових платформ забезпечує безперервний цикл прогнозування, виявлення та реагування на загрози.

Таким чином, кіберстійкість виступає стратегічним параметром розвитку банку, що визначає його надійність, адаптивність і конкурентоспроможність у цифровому середовищі (рис. 3.6):

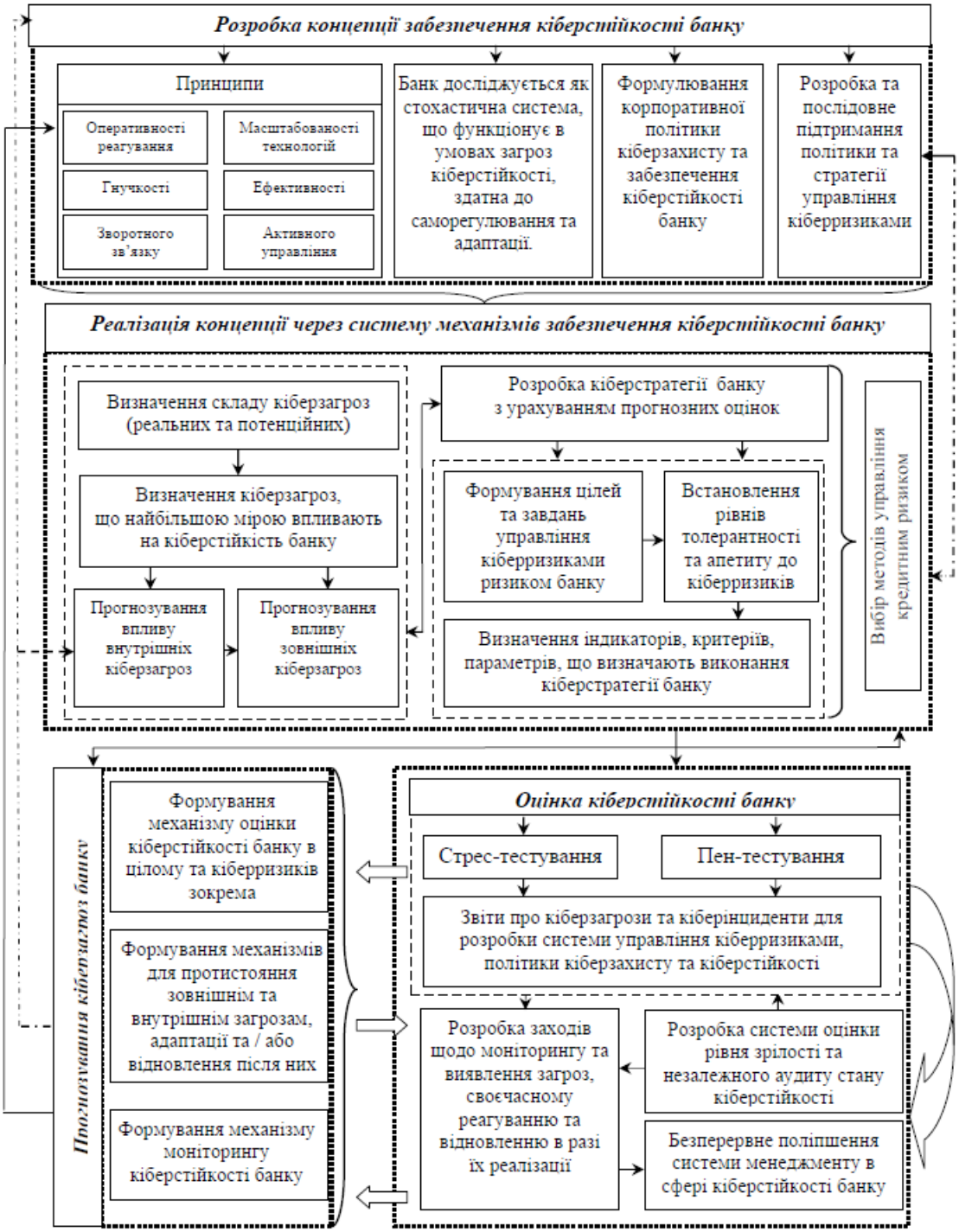

Рис. 3.6. Архітектура механізму забезпечення кіберстійкості банківської установи в системі банківської безпеки [17; 18]

Запропонований підхід до формування кіберстійкості банківської установи передбачає створення інтегрованого механізму, спрямованого на комплексне виявлення, аналіз і прогнозування кіберзагроз у цифровому середовищі. Його реалізація забезпечує узгодження інструментів попередження, адаптації та відновлення діяльності, що дозволяє не лише

реагувати на кіберінциденти, а й ідентифікувати нові ризики. Важливу роль у цьому процесі відіграють технології штучного інтелекту та Big Data, які формують основу проактивного управління кіберризиками.

Ключовим елементом системи є організаційне забезпечення, що інтегрує функції кібербезпеки, ризик-менеджменту, IT-контролю та безперервності бізнес-процесів у єдину модель. З урахуванням цього доцільним є створення Центру кіберстійкості як координуючого органу стратегічного управління, який забезпечує взаємодію підрозділів і формує процесно-орієнтовану систему реагування на кіберзагрози.

Основними функціями такого центру є інтеграція процесів кіберзахисту та управління ризиками, розроблення нормативно-методичної бази, формування баз даних кіберінцидентів, впровадження сценарних моделей реагування, координація дій підрозділів, а також розвиток інструментів прогнозування та попередження атак.

Оцінювання кіберстійкості доцільно здійснювати на основі поєднання якісного і кількісного підходів, що дозволяє визначити здатність банку забезпечувати безперервність функціонування та рівень його захищеності за технічними, організаційними й управлінськими показниками.

Розроблена модель передбачає безперервний цикл управління, який включає моніторинг, контроль, аудит, адаптацію та відновлення після кіберінцидентів. У результаті формується цілісна система кіберстійкості, що інтегрує організаційні та технологічні інструменти й забезпечує підвищення ефективності управління ризиками, мінімізацію наслідків кібератак та зміцнення конкурентоспроможності банків у цифровій економіці.

ВИСНОВКИ

У результаті проведеного дослідження сформовано комплексне та системне бачення трансформації підходів до забезпечення кіберстійкості банківських установ в умовах цифровізації фінансової системи. Визначено ключові тенденції розвитку цифрового банкінгу, обґрунтовано вплив інноваційних технологій на зміну характеру кіберзагроз та окреслено напрями вдосконалення механізмів управління кіберризиками. Це дозволило узагальнити сучасні підходи до забезпечення безпеки банківської діяльності та сформувати концептуальні засади підвищення стійкості фінансових установ до кіберзагроз.

У першому розділі встановлено, що кібербезпека банківського сектору є багатовимірною економічною категорією, яка охоплює сукупність організаційних, технічних та управлінських заходів, спрямованих на захист інформаційних ресурсів і забезпечення безперервності діяльності банківських установ. Доведено, що розвиток фінансових технологій (FinTech) суттєво трансформує характер кіберзагроз, підвищуючи їх складність, масштабність і швидкість поширення. Узагальнення наукових підходів дозволило систематизувати основні види кіберзагроз (фішинг, DDoS-атаки, шкідливе програмне забезпечення, атаки на ланцюги постачання тощо) та визначити їх вплив на фінансову стабільність банків. Обґрунтовано, що FinTech виступає одночасно як джерело нових ризиків і як інструмент їх мінімізації через впровадження інноваційних рішень у сфері кіберзахисту.

У другому розділі проведено оцінку сучасного стану кібербезпеки банківської системи України та проаналізовано вплив FinTech-інновацій на рівень кіберризиків. Встановлено, що зростання цифрових каналів обслуговування, розвиток онлайн-банкінгу та платіжної інфраструктури супроводжується збільшенням кількості кіберінцидентів та ускладненням механізмів їх реалізації. На прикладі ПриватБанк доведено, що ефективна інтеграція інтелектуальних технологій (зокрема штучного інтелекту та

аналітики великих даних) дозволяє суттєво підвищити рівень кіберзахисту, забезпечити моніторинг транзакцій у реальному часі та знизити ризики шахрайства. Водночас виявлено, що поряд із позитивними ефектами цифровізації зростають вимоги до захисту даних, управління ризиками та забезпечення кіберстійкості.

У третьому розділі обґрунтовано стратегічні напрями посилення кібербезпеки банківського сектору в умовах розвитку FinTech. Доведено, що ключову роль у формуванні сучасної моделі кіберзахисту відіграють технології штучного інтелекту, Big Data та цифрові платформи, які забезпечують перехід до проактивної моделі управління кіберризиками. Розроблено підхід до формування інтегрованої системи управління кіберризиками, що передбачає поєднання організаційних, технологічних та аналітичних компонентів. Запропоновано створення Центру кіберстійкості як координуючого органу, який забезпечує синергію між підрозділами банку та підвищує ефективність реагування на кіберзагрози.

Важливим результатом дослідження є обґрунтування необхідності використання комплексного підходу до оцінювання кіберстійкості банків, який поєднує якісні та кількісні показники. Такий підхід дозволяє не лише оцінити рівень захищеності банківських установ, а й визначити їх здатність адаптуватися до змін кіберсередовища та забезпечувати безперервність функціонування.

Узагальнюючи результати дослідження, встановлено, що ефективне забезпечення кібербезпеки банківського сектору в умовах розвитку FinTech можливе лише за умови інтеграції інноваційних технологій, удосконалення системи управління кіберризиками та посилення координації між усіма учасниками фінансового ринку. Впровадження запропонованих підходів сприятиме підвищенню рівня кіберстійкості банків, зміцненню фінансової безпеки та забезпеченню довгострокової стабільності банківської системи України в умовах цифрової економіки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1) Постанова Правління Національного банку України від 12 серпня 2022 року № 178 «Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України». URL: https://zakon.rada.gov.ua/laws/show/v0178500-22#Text (дата звернення: 26.04.2026)

3) Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII : станом на 28 черв. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 26.04.2026).

5) Про затвердження Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку: постанова Правління Національного банку України від 03.05.2023р. № v0058500-23. URL: https://zakon.rada.gov.ua/laws/show/v0058500-23#Text (дата звернення: 26.04.2026).

6) Бобришев Є.С. Вплив фінансових технологій на стабільність національної економіки. *Економіка та суспільство*. 2023. Випуск № 52. https://doi.org/10.32782/2524-0072/2023-52-96 (дата звернення: 26.04.2026).

7) Дзюблюк О., Чайковський Є. Інформаційно-ентропійна модель забезпечення фінансової стабільності банківської системи України. *Економічний аналіз.* 2025. №3. С. 146-159. URL https://dspace.wunu.edu.ua/handle/316497/55771 (дата звернення: 26.04.2026).

8) Мещеряков А. А., Сундук Т. Ф. Технологічні інновації у сфері інтернет-банкінгу: їх вплив на ефективність банківських послуг. *Здобутки економіки: перспективи та інновації.* 2024. №6. URL: https://econp.com.ua/index.php/journal/article/view/29/25 (дата звернення: 26.04.2026).

9) Владика Ю., Приступко А. Інноваційні технології в банкінгу як спосіб підвищення ефективності використання ресурсів банківської установи.

Економіка та суспільство. 2023. №56. DOI: https://doi.org/10.32782/2524-0072/2023-56-39 (дата звернення: 26.04.2026).

10) Гуцул І. Інноваційні тренди та їхній вплив на світовий фінансовий ринок. *Сталий розвиток економіки*. 2025. №1 (52). С. 366–371. DOI: https://doi.org/10.32782/2308-1988/2025-52-51 (дата звернення: 26.04.2026).

11) Овчаренко Т. Тенденції розвитку та використання штучного інтелекту у банківській сфері. *Економіка та суспільство*. 2024. №67. DOI: https://doi.org/10.32782/2524-0072/2024-67-44

12) Офіційний сайт АТ КБ"ПриватБанк". URL: www.privatbank.com.ua (дата звернення: 26.04.2026).

13) Мацьків, В. В., Щур, Р. І., Кохан, І. В. Роль штучного інтелекту у трансформації економіки та фінансової системи України в умовах післявоєнного відновлення. *Ринкова економіка: сучасна теорія і практика управління*, *23*(3(58), 2024. С. 58–77. https://doi.org/10.18524/2413-9998.2024.3(58).327139 (дата звернення: 26.04.2026).

14) Шелудько С.А. Цифровізація банківської діяльності в Україні як виклик і рушій у забезпеченні фінансової безпеки. *Проблеми сучасних трансформацій.* Серія: економіка та управління. 2025. №18. DOI: https://doi.org/10.54929/2786-5738-2025-18-08-07 (дата звернення: 26.04.2026).

15) Розмір та частка ринку цифрового банкінгу, прогнози на 2024–2032 роки URL: https://www.gminsights.com/ industry-analysis/digital-banking-market (дата звернення: 26.04.2026).

16) Офіційний сайт Світового Банку. DataBank. URL: https://databank.worldbank.org/source/global-financial-inclusion#selectedDimension_DBList (дата звернення: 26.04.2026).

17) Павлюченко Д. М. Вплив штучного інтелекту та машинного навчання на банківські послуги. Академічні візії. Випуск 32/2024. URL: https://doi.org/10.5281/zenodo.12936652 (дата звернення: 26.04.2026).

18) Кулініч Т., Стернюк О. Аналіз використання штучного інтелекту в цифровому фінансовому середовищі в Україні. Економіка та суспільство. 2024.

No. 63. URL: https://doi.org/10.32782/2524-0072/2024-63-22 (дата звернення: 26.04.2026).

19) Клименко, А. Фінтех: Цифрова трансформація в банківських та фінансових послугах. Компанія з розробки програмного забезпечення на замовлення. URL: https://maddevs.io/blog/digital-transformation-in-banking-and-financial-services (дата звернення: 26.04.2026).

20) Огляд банківського сектору та ринків капіталу до 2025 року. Deloitte. URL: https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-outlooks/banking-industry-outlook.html (дата звернення: 26.04.2026).

21) Кохан І.В., Криховецька З.М., Копчук А.Ю. Стратегічне управління цифровою трансформацією банківських установ. *Журнал «Наукові інновації та передові технології».* 2026. №2(54). С.3603-3615. (дата звернення: 29.04.2026)

22) Трусова Н. В., Чкан І. О. Кіберзахист банківської системи України в умовах цифрових трансформацій. *Науковий вісник Таврійського державного агротехнологічного університету*. 2023. Т. 1, № 47. С. 151–163. URL: https://doi.org/10.31388/2519-884x-2023-47-151-163 (дата звернення: 26.04.2026)

23) Ситник Н. С., Половчак І. Р. Цифровізація та кібербезпека у забезпеченні фінансової безпеки банків в умовах війни. *Галицький економічний вісник.* Тернопіль: ТНТУ. 2024. Том 89. № 4. С. 70–81. URL: https://elartu.tntu.edu.ua/handle/lib/46455 (дата звернення: 26.04.2026)

24) Офіційний сайт Служби безпеки України. Статистичні відомості. URL: https://ssu.gov.ua/statystychni-vidomosti-pro-robotu-iz-zapytamy (дата звернення: 26.04.2026).

25) Криклій О.А. Теорія і практика забезпечення кіберстійкості банків. *Ефективна економіка.* № 10. 2020. DOI: 10.32702/2307-2105-2020.10.50 (дата звернення: 26.04.2026).

ДОДАТКИ

Додаток А

АКЦІОНЕРНЕ ТОВАРИСТВО КОМЕРЦІЙНИЙ БАНК "ПРИВАТБАНК"
Окремий звіт про фінансовий стан станом за 31 грудня 2024 року

У мільйонах українських гривень	Прим.	31 грудня 2024	31 грудня 2023
АКТИВИ			
Грошові кошти та їх еквіваленти	6	151 768	152 282
Кредити та аванси банкам	7	86 589	134 237
Кредити та аванси клієнтам	8	112 761	92 019
Інвестиційні цінні папери в т.ч.:		375 094	271 847
- за справедливою вартістю через прибуток чи збиток	9	110 699	100 376
- за справедливою вартістю через інший сукупний дохід	9	204 240	171 471
- за амортизованою собівартістю	9	60 155	-
Поточні податкові активи	26	4	4
Інвестиційна нерухомість	10	2 005	2 340
Основні засоби	11	5 173	5 127
Нематеріальні активи за винятком гудвілу	11	1 972	1 563
Відстрочені податкові активи	26	1 629	1 952
Інвестиції в дочірні підприємства, спільні підприємства та асоційовані підприємства		30	30
Інші фінансові активи	12	13 496	9 493
Інші нефінансові активи	13	9 932	9 094
Непоточні активи або групи вибуття, класифіковані як утримувані для продажу або як утримувані для виплати власникам	14	1 008	20
Загальна сума активів		**761 461**	**680 008**
ЗОБОВ'ЯЗАННЯ			
Кошти клієнтів	15	621 596	555 525
Інші залучені кошти	16	6 199	2 630
Поточні податкові зобов'язання	26	21 553	25 790
Інші фінансові зобов'язання	17	4 072	3 038
Забезпечення у т.ч.:	18	6 013	5 438
- резерви за кредитними зобов'язаннями та контрактами фінансової гарантії		1 046	1 111
- інше забезпечення		4 967	4 327
Інші нефінансові зобов'язання	19	2 884	2 741
Загальна сума зобов'язань		**662 317**	**595 162**
ВЛАСНИЙ КАПІТАЛ			
Статутний капітал	20	206 060	206 060
Емісійний дохід		23	23
Інші резерви	9, 11	2 558	(1 741)
Результат від операцій з акціонером		12 174	12 174
Резервні та інші фонди банку	20	14 847	12 959
Накопичений дефіцит		(136 518)	(144 629)
Загальна сума власного капіталу		**99 144**	**84 846**
Загальна сума власного капіталу та зобов'язань		**761 461**	**680 008**

Затверджено до випуску та підписано 18 березня 2025 року.

Карл Мікаель Бйоркнерт
Голова Правління

Л. П. Чернишова
Заступник Голови Правління (з питань фінансів)

Л. П. Чапістрак
В. о. Головного бухгалтера

Додаток Б

АКЦІОНЕРНЕ ТОВАРИСТВО КОМЕРЦІЙНИЙ БАНК "ПРИВАТБАНК"
Окремий звіт про прибуток або збиток за рік, що закінчився 31 грудня 2024 року

У мільйонах українських гривень	Прим.	2024 рік	2023 рік
Процентні доходи в т.ч.:		77 594	66 238
- процентний дохід, обчислений із застосуванням методу ефективного відсотка	21	72 893	61 614
- інші процентні доходи	21	4 701	4 624
Процентні витрати	21	(10 706)	(6 616)
Чистий процентний дохід		**66 888**	**59 622**
Прибуток від зменшення корисності та сторнування збитку від зменшення корисності (збиток від зменшення корисності), визначені згідно з МСФЗ 9	22	(2 072)	(4 588)
Чисті процентні доходи після вирахування резерву на зменшення корисності		**64 816**	**55 034**
Комісійні доходи	23	46 602	41 589
Комісійні витрати	23	(18 834)	(17 150)
Чистий прибуток (збиток) від операцій з іноземною валютою		5 497	10 174
Чистий прибуток (збиток) від переоцінки іноземної валюти		(3 201)	(1 076)
Чистий прибуток (збиток) від операцій з борговими фінансовими інструментами, які обліковуються за справедливою вартістю через інший сукупний дохід	9	1 093	1 266
Чистий прибуток (збиток) від операцій з фінансовими інструментами за справедливою вартістю через прибуток або збиток	9	10 298	4 648
Чистий прибуток (збиток) від переоцінки об'єктів інвестиційної нерухомості		41	185
Витрати на виплати працівникам		(12 484)	(10 552)
Амортизаційні витрати	11	(2 731)	(2 175)
Інші адміністративні та операційні витрати в т.ч.:	24	(11 341)	(10 946)
- розформування (витрати на створення) резерву під юридичні ризики	18, 24	(609)	194
- адміністративні та операційні витрати	24	(10 732)	(11 140)
Інші доходи	25	1 619	2 173
Інші прибутки (збитки) - збиток від модифікації фінансових активів		(376)	(407)
Доходи (витрати), які виникають під час первісного визнання фінансових активів за процентною ставкою, вищою або нижчою, ніж ринкова		1	(1)
Прибуток (збиток), що виникає від припинення визнання фінансових активів, оцінених за амортизованою собівартістю		4	4
Прибуток до оподаткування		**81 004**	**72 766**
(Витрати на сплату податку) доходи від повернення податку	26	(40 863)	(35 001)
Прибуток за рік		**40 141**	**37 765**

Затверджено до випуску та підписано 18 березня 2025 року.

Карл Мікаель Бьоркнерт
Голова Правління

Л. П. Чернишова
Заступник Голови Правління (з питань Фінансів)

Л. П. Чапістрак
В. о. Головного бухгалтера

Додаток В

АКЦІОНЕРНЕ ТОВАРИСТВО КОМЕРЦІЙНИЙ БАНК "ПРИВАТБАНК"
Окремий звіт про сукупний дохід за рік, що закінчився 31 грудня 2024 року

У мільйонах українських гривень	Прим.	2024 рік	2023 рік
Прибуток за рік		**40 141**	**37 765**
Інший сукупний дохід			
Статті, які будуть у подальшому рекласифіковані у прибуток чи збиток:			
Фінансові інструменти що визнаються за справедливою вартістю через інший сукупний дохід:			
- Прибутки (збитки) від фінансових активів, оцінених за справедливою вартістю через інший сукупний дохід, до оподаткування	9	4 811	7 904
- Коригування перекласифікації фінансових активів, оцінених за справедливою вартістю через інший сукупний дохід, до оподаткування		(1 093)	(1 266)
- Зміни у резерві під очікувані кредитні збитки	9	1 210	6 562
- Податок на прибуток, що відноситься до фінансових активів, що оцінюються за справедливою вартістю через інший сукупний дохід у складі іншого сукупного доходу	26	(543)	215
Статті, які не будуть рекласифіковані у прибуток чи збиток:			
Будівлі та земля:			
- Інший сукупний дохід, до оподаткування, прибутки (збитки) від переоцінки	11	(21)	65
- Податок на прибуток, що відноситься до змін у дооцінці у складі іншого сукупного доходу	26	5	(30)
Загальна сума іншого сукупного доходу		**4 369**	**13 450**
Загальна сума сукупного доходу		**44 510**	**51 215**

Затверджено до випуску та підписано 18 березня 2025 року.

Карл Міхаель Бьоркнерт
Голова Правління

Л. П. Чернишова
Заступник Голови Правління (з питань фінансів)

Л. П. Чапістрак
В. о. Головного бухгалтера

АКЦІОНЕРНЕ ТОВАРИСТВО КОМЕРЦІЙНИЙ БАНК "ПРИВАТБАНК"

Окремий звіт про зміни у власному капіталі за рік, що закінчився 31 грудня 2024 року

У мільйонах українських гривень	Прим.	Статутний капітал	Емісійний дохід	Інші резерви: Резерв переоцінки будівель	Інші резерви: Резерв під прибутки та збитки за фінансовими активами, оцінених за справедливою вартістю через інший сукупний дохід	Інші резерви: Всього інші резерви	Результат від операцій з акціонером	Резервні та інші фонди банку	Накопичений дефіцит	Загальна сума власного капіталу
Власний капітал на 1 січня 2023		**206 060**	**23**	**573**	**(15 741)**	**(15 168)**	**12 174**	**11 449**	**(156 749)**	**57 789**
Прибуток за рік		-	-	-	-	-	-	-	37 765	37 765
Інший сукупний дохід		-	-	35	13 415	13 450	-	-	-	13 450
Сукупний дохід		-	-	35	13 415	**13 450**	-	-	37 765	51 215
Збільшення (зменшення) через інші зміни, власний капітал:										
- переведення (амортизація) резерву переоцінки будівель до нерозподіленого прибутку		-	-	(23)	-	(23)	-	-	23	-
Розподіл прибутку:										
- переведення до резервного фонду	20	-	-	-	-	-	-	1 510	(1 510)	-
- дивіденди, визнані як розподілені між власниками	20	-	-	-	-	-	-	-	(24 158)	(24 158)
Власний капітал на 31 грудня 2023		**206 060**	**23**	**585**	**(2 326)**	**(1 741)**	**12 174**	**12 959**	**(144 629)**	**84 846**
Власний капітал на 1 січня 2024		**206 060**	**23**	**585**	**(2 326)**	**(1 741)**	**12 174**	**12 959**	**(144 629)**	**84 846**
Прибуток за рік		-	-	-	-	-	-	-	40 141	40 141
Інший сукупний дохід		-	-	(16)	4 385	4 369	-	-	-	4 369
Сукупний дохід		-	-	(16)	4 385	**4 369**	-	-	40 141	44 510
Збільшення (зменшення) через інші зміни, власний капітал:										
- переведення (амортизація) резерву переоцінки будівель до нерозподіленого прибутку		-	-	(70)	-	(70)	-	-	70	-
Розподіл прибутку:										
- переведення до резервного фонду	20	-	-	-	-	-	-	1 888	(1 888)	-
- дивіденди, визнані як розподілені між власниками	20	-	-	-	-	-	-	-	(30 212)	(30 212)
Власний капітал на 31 грудня 2024		**206 060**	**23**	**499**	**2 059**	**2 558**	**12 174**	**14 847**	**(136 518)**	**99 144**

Затверджено до випуску та підписано 18 березня 2025 року.

Карл Мікаель Бьоркнет
Голова Правління

Л. П. Чернишова
Заступник Голови Правління (з питань фінансів)

Л. П. Чапістрак
В. о. Головного бухгалтера

Примітки, подані на сторінках 6-105 є невід'ємною частиною цієї окремої фінансової звітності.

Додаток Г

Додаток Д

АКЦІОНЕРНЕ ТОВАРИСТВО КОМЕРЦІЙНИЙ БАНК "ПРИВАТБАНК"
Окремий звіт про рух грошових коштів за рік, що закінчився 31 грудня 2024 року

У мільйонах українських гривень	Прим.	2024 рік	2023 рік
Грошові потоки від операційної діяльності			
Проценти отримані		77 394	61 373
Проценти сплачені		(10 722)	(6 212)
Комісійні доходи, що отримані		46 602	41 589
Комісійні витрати, що сплачені		(18 463)	(16 603)
Чисте (збільшення)/зменшення від операцій з іноземною валютою		5 497	10 174
Виплати працівникам		(12 169)	(10 421)
Адміністративні витрати та інші операційні виплати, що сплачені		(11 652)	(12 254)
Інші доходи		2 101	2 260
Повернення податків на прибуток (сплата)		(45 315)	(803)
Грошові потоки, отримані від операційної діяльності, до змін в операційних активах та зобов'язаннях		**33 273**	**69 103**
Зміни в операційних активах та зобов'язаннях			
Чисте (збільшення)/зменшення кредитів та авансів банкам		46 620	(29 430)
Чисте (збільшення)/зменшення кредитів та авансів клієнтам		(20 421)	(22 583)
Чисте (збільшення)/зменшення інших фінансових активів		412	(262)
Чисте (збільшення)/зменшення інших активів		(1 138)	875
Інші надходження (вибуття) грошових коштів		37	33
Чисте збільшення/(зменшення) коштів клієнтів		48 650	73 801
Чисте збільшення/(зменшення) інших нефінансових зобов'язань		(6)	(6)
Чисте збільшення/(зменшення) інших фінансових зобов'язань		797	590
Чисті грошові кошти, отримані від операційної діяльності		**108 224**	**92 121**
Грошові потоки від інвестиційної діяльності			
Надходження від продажу основних засобів		3	6
Придбання основних засобів	11	(1 529)	(1 158)
Придбання нематеріальних активів	11	(1 108)	(731)
Придбання цінних паперів в т.ч.:		(232 930)	(165 971)
- за справедливою вартістю через інший сукупний дохід		(169 652)	(165 971)
- за амортизованою собівартістю		(63 278)	-
Надходження від реалізації та погашення інвестиційних цінних паперів в т.ч.:		147 395	152 448
- за справедливою вартістю через інший сукупний дохід		147 395	152 448
Надходження від продажу інвестиційної нерухомості		-	1
Чисті грошові кошти, використані в інвестиційній діяльності		**(88 169)**	**(15 405)**
Грошові потоки від фінансової діяльності			
Виплати за орендними зобов'язаннями		(765)	(713)
Дивіденди сплачені	20	(30 212)	(24 158)
Повернення інших залучених коштів		(186)	(33)
Отримання інших залучених коштів	16	3 746	2 530
Чисті грошові кошти, використані в фінансовій діяльності	34	**(27 417)**	**(22 374)**
Вплив змін валютного курсу на грошові кошти та їх еквіваленти		7 167	3 768
Вплив очікуваних кредитних збитків на грошові кошти та їх еквіваленти		(319)	(19)
Чисте збільшення (зменшення) грошових коштів та їх еквівалентів		**(514)**	**58 091**
Грошові кошти та їх еквіваленти на початок року	6	152 282	94 191
Грошові кошти та їх еквіваленти на кінець року	6	**151 768**	**152 282**

Затверджено до випуску та підписано 18 березня 2025 року.

Карл Міхаель Бьоркнерт
Голова Правління

Л. П. Чернишова
Заступник Голови Правління (з питань фінансів)

Л. П. Чапістрак
В. о. Головного бухгалтера